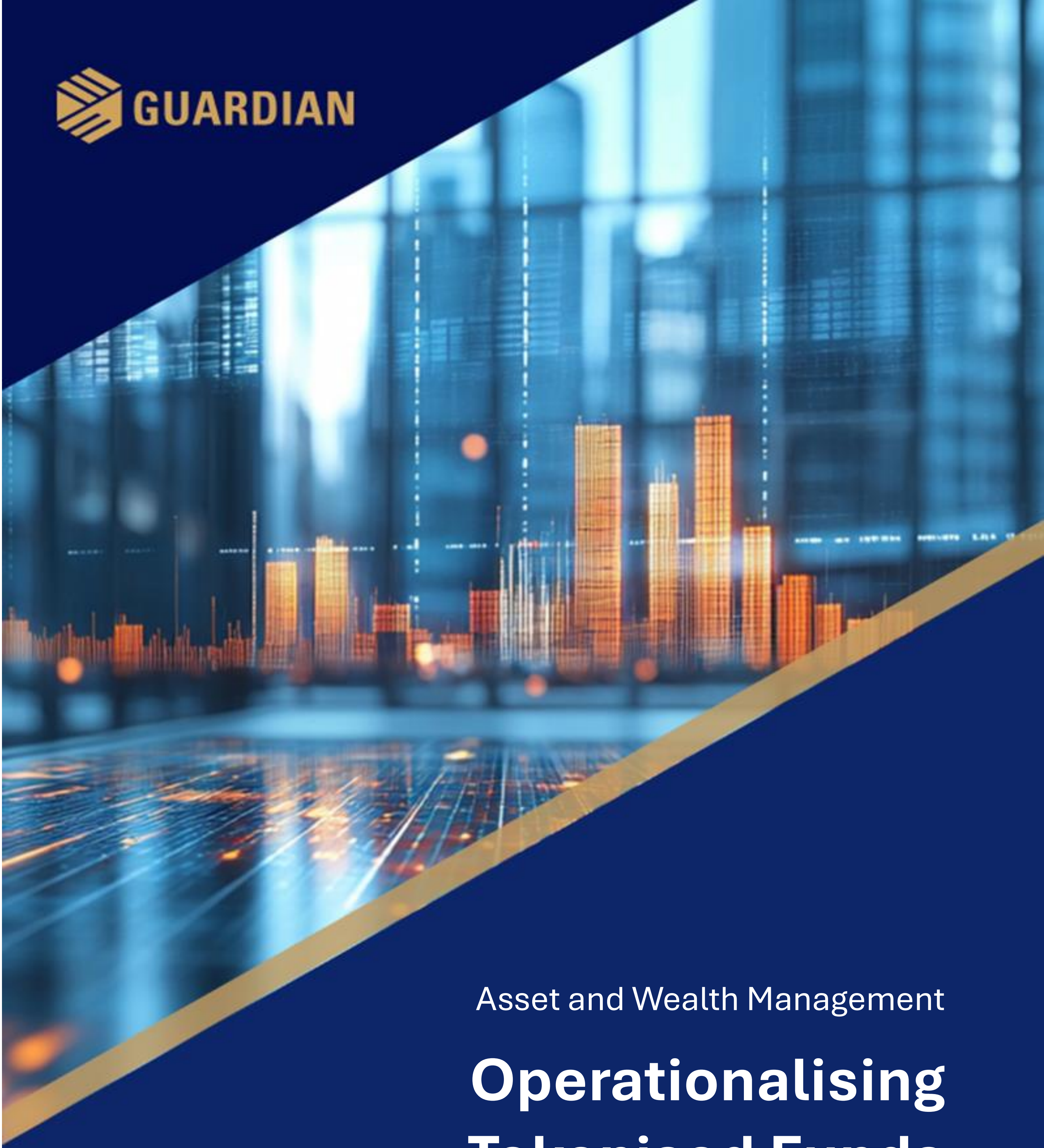
GUARDIAN



Asset and Wealth Management

Operationalising Tokenised Funds

November 2025

Disclaimer

This report and its contents are made available on an “as-is” basis without warranties of any kind. The content in this report does not constitute regulatory, financial, legal or any other professional advice and should not be acted on as such. None of its authors and contributors shall be liable for any damage or loss of any kind howsoever caused as a result from the use of the information contained or referenced in this report.

This report does not seek to address policy objectives or recommend any specific solution or product. Whilst the content strives to provide more clarity on the subject matter, the authors of this report make no representation or guarantees on the performance or adequacy of the solutions or models. The examples used in the report are only for illustration purposes.

Document Version

Version	Date	Author	Rationale
1.0	November 2025	Guardian Asset & Wealth Management Industry Group	First publication

Acknowledgement

This is a joint report developed by the Guardian Asset and Wealth Management Industry Group. The report was led by Deutsche Bank and Phillip Securities.

The report received additional contributions from organisations listed alphabetically:

- Baker McKenzie
- Citi
- Drew & Napier
- Fidelity International
- Franklin Templeton
- Interop Labs
- Monetary Authority of Singapore (MAS)
- Memento Blockchain
- Schroders
- Swift
- The Financial Conduct Authority (UK FCA)
- United Overseas Bank Limited (UOB)

Contents

1. Executive Summary

Tokenisation is moving from pilots to production in asset and wealth management with tokenised money market funds (tMMFs) as a leading product globally. Using tMMFs as a key reference, this report acts as a playbook for launching and scaling tokenised funds—grounded in legal reality, designed for interoperability and scale, and proven through pilots and live use cases—so that industry participants can operate with confidence, regulators can supervise with clarity, and innovators can build responsibly.

This comprehensive report covers major considerations relating to tokenised funds, including:

- **Legal Structure**— We start the report with views on the legal structures and the regulatory considerations for tokenised funds. This section explains what the token legally is, who owns what, and which investor rights apply across jurisdictions. This section provides clear legal considerations for a tokenised fund (ownership, registers, disclosures, investor protection).

- **Legal views of Interoperability and settlement finality** — This section focuses on the legal considerations for cross-chain distribution, bridged tokens (Lock-&-Mint vs Burn-&-Mint), and cross-chain settlement finality (the moment when a transfer is irrevocable and unconditional, which is critical for risk, tax, and insolvency analysis). It illustrates how tokens move between networks, when risk truly passes on from one entity to another, and the complexity of legal and tax considerations in cross-chain and cross-jurisdiction interoperability.

- **Use cases, technology & operations** — The next section dives into several practical use cases from Guardian's Asset & Wealth Management industry group, mapping out the entire lifecycle of tokenised funds. From multi-chain primary issuance to secondary trading with payment-versus-payment (PvP) with stablecoins, real-time payment-versus-delivery-versus-payment (PvDvP) foreign exchange swaps across networks and post-trade lifecycle orchestration. It also features a public-permissioned architecture with post-trade lifecycle servicing designed to accelerate adoption by asset and wealth managers. The use cases showcase a broad spectrum of real-world possibilities for tokenised financial services across both private and public chains, providing a reference for those planning to take the first steps in tokenisation.

- **Road to scalability and adoption** — Finally, the report identifies **important enablers** (onboarding & KYC, network effects, operational risk controls, market structure & liquidity, technical standards) and user experience as key milestones to ensure scalable adoption.

2. Legal Structure and Regulatory Considerations

The foundation of any tokenised fund lies in its legal structure. Before the benefits of blockchain technology — such as programmability, automation, and real-time settlement — can be realised, asset managers must ensure that the legal framework underpinning the fund is robust, compliant, and fit for purpose. This chapter examines the principal models for integrating tokenisation into investment funds, analyses their legal and regulatory implications, and discusses the operational consequences for managers and investors.

A key consideration in tokenisation is the question of how ownership is represented and transferred. Traditional investment funds rely on off-chain fund share registers maintained by administrators, which serve as the authoritative record of ownership. Tokenisation introduces the possibility of maintaining these registers on a blockchain, either as a mirror, a parallel record, or as the sole authoritative source. The choice of model has far-reaching implications for investor rights, regulatory compliance, and operational risk.

2.1 Different Models of Tokenisation

In the Guardian Funds Framework, three general archetypes of tokenised fund share register forms were discussed.

- Model 1: Mirror the authoritative fund shareholder register.
- Model 2: Partial on-chain authoritative fund shareholder register.
- Model 3: Full on-chain authoritative fund shareholder register.

In this section, there are four models of tokenisation and these would fall within the three general archetypes of tokenised fund share register forms.

- "Digital Mirror", which would fall within Model 1.
- "Digital Twin (Distributor)" and "Digital Twin (Feeder Fund)", which would fall within Model 2.
- "Digital Native", which would fall within Model 3.

The models of tokenisation can range from being lightly adopted in the fund to the form where tokenisation is completely integrated into the fund. **Table 1** summarises the features of the four different models.

	Level of Tokenisation	**Purpose of Tokenised Register**	**Tokenisation Carried Out By**	**Type of Register Used**
Digital Mirror	Low	Internal purposes only and non-authoritative record of investors' holdings	Fund / Fund manager	Traditional form register and blockchain register
Digital Twin (Distributor)	Medium	Authoritative record of holdings by distributor, on behalf of investors	Distributor	Traditional form register and blockchain register
Digital Twin (Feeder Fund)	Medium	Authoritative record of investors' holdings in feeder fund	Fund / Fund Manager	Traditional form register and blockchain register
Digital Native	High	Authoritative record of investors' holdings in digital native fund	Fund / Fund Manager	Only blockchain register

Table 1: Four models of tokenised funds

<u>Digital Mirror</u>

The ownership of units in a Digital Mirror fund is represented on the register of members maintained in a traditional form usually by the fund administrator of the Digital Mirror fund. However, a "mirror" of the traditional register is created and maintained on a blockchain or distributed ledger, solely for internal purposes of the fund. The on-chain register of a Digital Mirror fund does not authoritatively represent the ownership of the Digital Mirror fund; such authority still rests with the traditional register maintained off-chain.

<u>Digital Twin</u>

The Digital Twin model applies in scenarios where (1) a traditional fund already exists that investors want exposure to, and (2) tokenisation can provide an alternative access route to this fund for investors.

Tokenisation can either be carried out by a distributor or a fund manager.

- **Digital Twin (Distributor),** where tokenisation is carried out by a distributor of the interests in the traditional fund. The register of members in the investment fund is maintained in its traditional form. However, licensed distributors, acting as nominees on behalf of investors, utilise a register maintained on a blockchain or distributed ledger to record the holdings of the investors for whom they act as nominee. The distributors / nominees are named as the holder of the units in the fund register, and the identities of the ultimate owner of the units are disclosed only in the on-chain register maintained by the distributors / nominees. Tokens representing the ownership of the investors in the fund as recorded in the blockchain or distributed ledger maintained by the distributor will be issued to such investors.

- **Digital Twin (Feeder Fund),** where tokenisation is carried out by a fund manager, who could be the manager of a traditional fund which has attracted investors' interests or another manager seeking to assist their clients to gain exposure to traditional funds. This model involves a master-feeder structure. In order for investors to gain exposure to a traditional fund and utilise tokenisation in the process, a fund manager would set up a tokenised feeder fund that would invest into such a traditional fund. The register of members of the master fund is maintained in the traditional form off-chain; whereas the register of members for the feeder fund is maintained on a blockchain or distributed ledger. Investors will be given tokens representing their ownership in the feeder fund. Such tokenised feeder fund may even be established in a separate and subjected to different regulations from the master traditional fund.

<u>Digital Native</u>

Digital Native funds are funds that maintain their register of members on-chain. Subscription, redemption and transfer of units in the fund are all carried out automatically on-chain by smart contracts. The tokenised register of a Digital Native funds by itself authoritatively represents the ownership of the fund and investors will be issued tokens representing their ownership in the fund.

The choice of models discussed above would depend on the manager's readiness, investor appetite for digital solutions and legal clarity. Legal and beneficial ownership structures vary accordingly, affecting investors' rights and recourse.

- Managers could adopt a Digital Mirror fund format if they are still exploring the features of tokenisation and do not yet want to integrate tokenisation into the fund.

- Digital Twin (Distributor) or Digital Twin (Feeder Fund) are alternatives for either distributors or fund managers who do not wish to change their existing funds or create entirely new digital native funds, but still wish to avail their customers to some benefits of tokenisation through distributors or by way of setting up a feeder fund.

- A Digital Native model is for managers who are ready to adopt tokenisation and are confident that their target investors are also similarly willing to invest in tokenised funds.

2.2 Legal and Beneficial Ownership of Fund Units

This section seeks to discuss the legal characterisation of the ownership held by investors of the fund that invests into the underlying portfolio assets (the "Primary Funds"), in the various forms stated above in Singapore.

Direct Ownership

Investors holding the tokens of Primary Funds structured as Digital Mirror funds or Digital Native funds may have both legal and beneficial ownership of the Primary Funds.

Indirect Ownership

Investors may likely hold indirect ownership in Primary Funds where the fund structure uses a Digital Twin form.

- In a Digital Twin (Feeder Fund) model, the feeder fund may hold the legal and beneficial ownership of the Primary Fund and investors may hold the legal and beneficial ownership of the feeder fund.

- In a Digital Twin (Distribution) model, the distributor / nominee may hold the legal ownership of the Primary Fund and investors may hold the beneficial ownership of the Primary Fund, if the subscription agreement entered into by the distributor / nominee and the investors envisages this.

Because of the indirect ownership held by investors in a Digital Twin model, investors would likely not be able to exercise any rights against the Primary Fund by themselves.

In the case of a Digital Twin (Feeder Fund) model, investors would only be able to exercise rights under the fund documents of the feeder fund, and that would generally be against either the feeder fund itself (where it is structured as a private company or variable capital company), the general partner (where the feeder fund is structured as a limited partnership), or the trustee (where the feeder fund is structured as a unit trust). In the case of a Digital Twin (Distribution) model, investors would generally only be able to exercise rights against the distributor / nominee under the subscription agreement. It is possible that the distributor / nominee may exercise the rights it has as a holder of the legal ownership of the Primary Fund for the benefit of the investors.

2.3 Regulations Applicable to Offerings of Fund Tokens

The offering requirements of tokenised funds would differ across different jurisdictions. Financial institutions should seek their own legal advice to ensure that the offering is conducted in a manner that meets the relevant requirements of each jurisdiction. **Figure 1** provides an illustration of the applicable regulations (non-exhaustive) in Singapore.

The Monetary Authority of Singapore (MAS)'s Guide to Digital Token Offering makes it clear that in the case of a digital token, the MAS will examine the structure and characteristics of, including the rights attached to, a digital token in determining if the digital token is a type of capital markets products under the Securities and Futures Act 2001 ("SFA"). This may involve, among others, looking at the underlying asset which the digital token seeks to represent, and if such underlying asset is a capital market product, the offering of the digital token will be subjected to the SFA.

A tokenised fund unit would generally represent a unit in a collective investment scheme ("CIS") and thus there is regulatory certainty that offerings of and dealings in tokenised fund units should follow the usual requirements applicable to CIS under the SFA. This includes the requirement for managers to obtain a capital market services license for fund management and distributors to obtain a capital market services license for dealing in capital market products for the managing of and dealing in tokenised funds respectively, unless where exempted. The requirement to provide a registered prospectus to investors except where exempted under the SFA would also apply for the offering of tokenised fund units.

Permissibility of Maintaining a Blockchain-based Register for a Limited Partnership and Variable Capital Company ("VCC")

Section 6 of the Electronic Transactions Act 2010 ("ETA") provides for legal recognition of electronic records, by declaring that information is not to be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic record. As such, there is some certainty that a register of members of a fund maintained on a blockchain would likely have legal effect, validity and enforceability like a traditional register of members of a fund.

Notwithstanding the foregoing, regulation 12(3) of the Limited Partnership Regulations, and section 66(9) the Variable Companies Act 2018 (the "VCC Act") indicate, respectively, that a register of the partners and members of the VCC must be kept at the principal place of business of the limited partnership and the registered office of the VCC and open for inspection by among others, the partners of the limited partnership and the members of the VCC. There is some uncertainty about whether the maintenance of the registers aforementioned on a blockchain would satisfy the requirements stated, although an argument can be made that a blockchain register can be accessed for inspection in the principal place of business of the limited partnership and registered office of the VCC as long as the technical infrastructure (e.g. the availability of internet connection) in the aforementioned places supports such access.

Requirement of an Instrument of Transfer for Transfer of VCC Shares

In relation to VCCs, section 40(3) of the VCC Act states that a VCC must not register a transfer of shares or debentures unless a proper instrument of transfer has been delivered to the VCC. In view of recent developments of blockchain and tokenisation activities, there is currently no express regulatory guidance on whether an instrument of transfer can take the form of an instruction on a blockchain for the transfer of units provided by the fund or investors. Singapore regulations provide guidance on the recognition of digital records and the requirements for maintaining official registers. In tandem with technological developments, further guidance regarding the use of blockchain for official registers and the legal finality of token transfers will be helpful to provide certainty to the industry. Managers must ensure full regulatory compliance, including licensing, prospectus requirements, and robust investor disclosures concerning the operational and technological risks of tokenisation.

Figure 1: An illustration of the applicable regulations in Singapore

2.4 Investor Protection and Operational Risk

Sufficient relevant disclosures are at the core of investor protection. In relation to tokenised funds, a key aspect of the sufficiency of disclosure relates to providing clear and comprehensive disclosures about the risks of tokenisation and blockchain, including operational risks related thereto. These may include risks relating to:

- Unpredictability of distributed ledgers such as relating to its performance and development
- Potential inability to amend transactions caused by theft or fraud
- Potential manipulation of ledger
- Loss of private keys

These disclosures could be disclosed in the offering documents of the funds (e.g. prospectus or private placement memorandum), distribution agreements or the terms and conditions acknowledged by customers prior to their subscription of the tokenised fund units.

Tokenised funds, especially in the case of Digital Native funds, rely significantly on the operational resilience and the security of the blockchain. Prior to offering tokenised fund units, managers and distributors should engage with relevant experts and service providers to carry out beta testing and penetration tests to identify and remediate all identified high risk findings prior to the offering of the tokenised fund units. Managers should also carry out constant monitoring of the blockchain, especially in the case of open-ended funds, to ensure that subscription, redemptions and transfers (if permitted) can be carried out smoothly. All digital token custodians engaged by the fund should have their security systems thoroughly checked to prevent and counter cyberattacks.

2.5 Interoperability and Settlement Finality for Cross-Chain Token Transfers

In the rapidly evolving landscape of tokenised funds, the ability for tokens and assets to move seamlessly across different blockchain networks has emerged as both a technological necessity and a legal challenge. As asset managers and financial institutions seek to distribute fund tokens across multiple chains, the legal nature of these cross-chain transactions becomes increasingly complex that spills over to key tenets like ownership and settlement finality.

In summary,

- the legal structuring of interoperability in tokenised funds is a multifaceted issue that requires careful consideration of both technological and legal factors. Bridging models must be evaluated not only for their operational efficiency but also for their legal robustness, tax implications, and regulatory compliance.
- Settlement finality must be clearly defined and contractually enforced to mitigate risk. As the industry moves toward greater interoperability and multi-chain distribution, ongoing dialogue between technologists, legal experts, and regulators will be essential to ensure that innovation is matched by legal certainty and investor protection.

2.5.1 Bridging Considerations

To facilitate cross-chain token and asset transfers, bridges are implemented across networks. As outlined in the *Interlinking Networks Technical Whitepaper* (MAS, November 2023), two bridging models dominate current practice: the “Lock and Mint” model and the “Burn and Mint” model.

- In the “Lock and Mint” model, the original token is locked on the source chain within a smart contract, before a new “wrapped” token is minted on the destination chain to represent the locked asset. To reverse the process, the wrapped token is burned on the destination chain, which then unlocks the original token on the source chain.
- In contrast, the “Burn and Mint” model involves burning the original token on the source chain and minting a new token on the destination chain, effectively destroying and recreating the asset in the process.

While these mechanisms are technologically sophisticated, they introduce significant legal uncertainties. One of the most pressing questions is whether the newly minted token on the destination chain constitutes a new property asset in legal terms, or merely a representation or continuation of the original asset. This distinction is not merely academic; it has direct implications for tax treatment, regulatory classification, and the enforceability of property rights. For example, if bridging is characterised as an asset transfer, it may trigger capital gains tax or other tax liabilities for the transferor. Where it is viewed as asset creation and destruction with no gains being derived by the transferor, different regulatory and contractual frameworks may apply. At present, the legal nature of bridged tokens remains an open question.

In practice, regardless of whether a token is locked or burnt on a source chain, and subsequently minted on a destination chain, the entire transaction concerns the same underlying asset as the subject matter. The economic reality is that the nature of a token that is bridged from a source chain to a destination chain would functionally be the same on both sides. However, from a technical perspective, tokens are being destroyed and minted, which suggests that there is no "transfer" of asset *per se*.

There are several considerations flowing from the uncertain legal nature of bridged tokens:

- **Tax:** The tax treatment of a bridged token would depend on whether token bridging is characterised as an asset transfer, as opposed to asset creation and destruction. If characterised as a transfer, there could potentially be tax implications on the transferor, such as capital gains tax.
- **Settlement finality**: While conventional rules of title transfer (such as the *nemo dat* rule[1]) could apply to token bridging, it remains unclear if the title is deemed to have passed from one party to another in a transaction, such that the receiving party could start asserting property rights.
    - **Regulatory:** The question of whether token bridging would be classified as a peer-to-peer asset transfer, as opposed to a redemption or buyback followed by a reissuance of an asset, has regulatory implications — especially since different rules govern each scenario.
    - **Contract:** Where uncertainty remains over the legal nature of bridged tokens, parties can consider resolving existing gaps through contractual provisions.

2.5.2 Settlement Finality Considerations

The uncertainties regarding settlement finality in token arrangements is not a new issue as highlighted in various Bank for International Settlements ("BIS") reports:

- "Settlement finality is the legally defined moment at which the transfer of an asset or financial instrument, or the discharge of an obligation, is irrevocable and

[1] The *nemo dat* rule is that the transferor of goods cannot pass a better title than he himself possesses, which means that a buyer of goods cannot acquire ownership if the seller is not the owner and does not have authority to sell them, even if the buyer is acting in good faith.

unconditional and not susceptible to being unwound following the bankruptcy or insolvency of a participant (CPMI (2017)). Depending on the technology and other design choices, operational transfer and final settlement may not coincide in token arrangements, which may lead to settlement risk[2]."[3]

- "In traditional systems, settlement finality is a clear and well-defined point in time, backed by a strong legal basis. For DLT arrangements, settlement finality may not be as clear. In arrangements that rely on a consensus algorithm to effect settlement finality, there may not necessarily be a single point of settlement finality. Further, the applicable legal framework may not expressly support finality in such cases."[4]

Consideration: Is there a clear and well-defined point in time when the transfer is irrevocable and unconditional?

From a technical perspective, even if the point in time is taken to be when the token is minted on the destination chain (regardless of whether lock and mint or burn and mint is used), this will depend on the blockchains involved.

Using **Figure 2** below as an example:

- Layer 2 zero-knowledge rollups tie their finality and security mechanisms to those of the underlying Layer 1, Ethereum. In the case of ZKsync, it provides for an execution delay of three hours to allow sufficient time for emergency interventions by its Security Council.

- For Ethereum, finality is typically achieved after two epochs, which translates to approximately 13 minutes under normal network conditions, when sufficient duration has passed to allow for sufficient block confirmations to prevent reversals.

- For proof-of-work blockchains there may not be any single, immediate moment, but rather a state of probabilistic finality which is achieved after a transaction has been included in a block and subsequent blocks continue to be added on top of it, making it increasingly difficult and uneconomical to reverse. For Bitcoin, a common standard for high-value transactions is six confirmations, which equates to approximately one hour, as this is the point where the economic cost of a 51% attack to reverse the transaction becomes prohibitively high for a rational actor.

[2] For instance, if an operational transfer on the ledger and legal finality do not coincide, the state of a transaction on the ledger could be retroactively reversed e.g. through legal actions. This could lead to settlement risk.

[3] https://www.bis.org/cpmi/publ/d225.pdf

[4] https://www.bis.org/cpmi/publ/d157.pdf

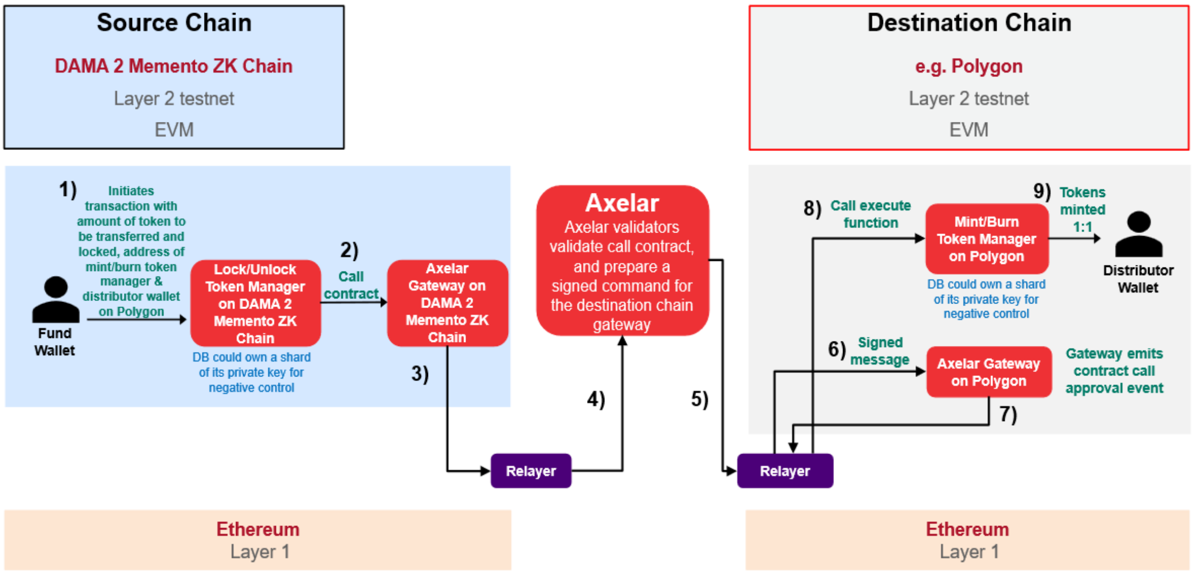

Source Chain
DAMA 2 Memento ZK Chain
Layer 2 testnet
EVM
Destination Chain
e.g. Polygon
Layer 2 testnet
EVM
1)
Initiates transaction with amount of token to be transferred and locked, address of mint/burn token manager & distributor wallet on Polygon
Fund Wallet
Lock/Unlock Token Manager on DAMA 2 Memento ZK Chain
DB could own a shard of its private key for negative control
2)
Call contract
Axelar Gateway on DAMA 2 Memento ZK Chain
3)
Axelar
Axelar validators validate call contract, and prepare a signed command for the destination chain gateway
4)
5)
Relayer
Relayer
8)
Call execute function
Mint/Burn Token Manager on Polygon
DB could own a shard of its private key for negative control
9)
Tokens minted 1:1
Distributor Wallet
6)
Signed message
Axelar Gateway on Polygon
Gateway emits contract call approval event
7)
Ethereum
Layer 1
Ethereum
Layer 1

Figure 2: Multiple Possible Points of Finality in a Cross-Chain Transaction

Even if technically there is a single, immediate moment which can be identified, there is nothing stopping two parties from agreeing to a different point in time when title to the token transfers between themselves in their contract, or pursuant to a rulebook as indicated in Figure 2 above, or even only when payment has been received by the seller (using a retention of title clause).

Agreeing on a different point in time is essentially deciding when risk passes — akin to different Incoterms in a trade transaction. For example, the Fund above could argue that its obligations under the underlying sale contract should be fulfilled once the token is burned in its wallet on the source chain, since it has no contractual relationship with the destination chain, and the distributor is in a better position to handle any issues arising from problems with the destination chain. Viewed from this perspective, it should be the distributor who bears such risks.

However, a third party purchaser on a different blockchain would probably only be able to inspect the Layer 1 chain, and would normally take it at face value that the distributor was the owner of the token if it was minted on the destination chain, delivered to the distributor's wallet (at point 9 in Figure 2), and the transfer was recorded on the Layer 1 chain. The third-party purchaser would not normally be aware of for example any retention of title provisions in the underlying sales contract, and if this transaction involved goods, the third-party purchaser would be able to take good title from the buyer in possession (for example, under the Sale of Goods Act 1979). Nonetheless, since it is unlikely that a token would be considered 'goods', the *nemo dat* rule would apply to allow the original owner's title to prevail.

To preserve the overall integrity of the market, the recording of the transfer on the Layer 1 chain should also be treated as the legal point in time where title to the token transfers, and is treated as irrevocable and unconditional. This aligns with the technical position, as changes may in some cases still be made to the Layer 2 blockchain.

Nevertheless, this would not address the insolvency risks discussed in the next section.

Consideration: Is there a clear and well-defined point in time when the transfer is irrevocable and unconditional, AND is not susceptible to unwinding following the bankruptcy or insolvency of a participant?

In the payment space, legislation like the Singapore Payment and Settlement Systems (Finality and Netting) Act 2002 provide the legal basis. This Act applies to certain designated systems (like the Continuous Linked Settlement ("CLS"), Fast and Secure Transfers ("FAST") and MAS Electronic Payment System ("MEPS")) clearly provide that transactions under the rules of the designated system are final and irrevocable, and "must not be reversed, repaid or set aside and no order is to be made by any court for the rectification or stay of the transfer, netting or settlement".[5]

For transfers of securities in Singapore, CDP Settlement Rule 7 provides that (a) money settlement with a Settlement Participant is final when money is debited from or credited to the cash account maintained by CDP on its books for the Settlement Participant for the purposes of settlement; and (b) securities settlement with a Settlement Participant is final when securities are either credited to, or debited from, the Settlement Participant's securities account[6]. This is reinforced by Section 81SR of the Securities and Futures Act 2001 which overrides the application of the provisions in bankruptcy and company liquidation law for book-entry securities and provides that no order may be made for the rectification of the Depository Register.

For transfers of tokens, no such legislation currently applies in Singapore. Unlike the CDP which acts as the central counterparty for all transactions involving book-entry securities and is able to bind all participants to a common set of rules, there may not be an equivalent central counterparty or common rulebook in a cross-chain transaction.

2.5.3 Cross-Chain Legal Considerations

From both legal and technical perspectives, a cross-chain transaction is fragmented into separate contracts concluded respectively on the source chain and destination chain. The existence of multiple points of potential finality in a cross-chain transaction gives rise to considerable risks, with two key issues being

- the absence of any single contract that binds all parties in a transaction, and
- the lack of easy recourse in the event of any mistake in contract.

[5] Section 7, Payment and Settlement Systems (Finality and Netting) Act 2002.

[6] Central Depository (Pte) Limited (CDP)'s PMI Disclosure Brochure (Dec 2023).

For instance, an investor on the destination chain, who is expecting to receive a token, may find it difficult to enforce their rights against an asset manager who had issued the token on the source chain. To explain, the asset manager takes on a similar role to that of a stablecoin issuer who sets the terms on which the token can be redeemed. These terms may only bind parties on the source chain. On the other hand, an investor on the destination chain may only be bound by the terms set by the destination chain, which the asset manager is not a party to.

In an event a mistake occurs in a transaction — for instance, where a token is not delivered to the intended recipient, but to a different party on the same destination chain — the intended recipient (i.e. the investor) may not be able to rely on and enforce the terms they are bound by on the destination chain against the asset manager, where such terms conflict with the asset manager's terms. For example, the end investor may wish to dispute the point of finality as contractually agreed between the asset manager and the intermediary (i.e. the bridge) but may find it difficult to do so as they are not privy to that contract.

Further, where such mistake arises, the immediate concern would be whether the transaction can be reversed. Setting aside the potential difficulties of reversing a transaction from a technical standpoint, the legal questions that arise are whether the contract provides for the circumstances under which and to what extent a transaction can be reversed. While Singapore law provides that a contract is voidable if it is found to be entered into on the back of a unilateral mistake, such mistake is necessarily determined having regard to the state of mind of a programmer at the time of writing the software which enabled the mistake.

Notwithstanding the above, funds structured as a VCC could benefit from statutory provisions that provide for rectification of the register in the event of a mistake, either by the Registrar or the courts. However, funds with other types of structures that do not benefit from equivalent statutory regimes would have to rely on contract to resolve any issues arising out of mistake.

2.5.4 Cross-Border Offering Considerations

The cross-border offering of tokenised funds and the settlement of such transactions raise unique legal and regulatory challenges, as these products may be subject to multiple regimes depending on their structure and the jurisdictions involved. This would necessitate navigating the differing stages of legal and regulatory development across countries in respect of these issues.

A case study is included in **Annex A**, outlining how the UK law would likely apply to the distribution and operation of tokenised funds offered to UK investors from abroad, including key compliance, marketing, and investor protection considerations relevant to cross-border activity.

3. Settlement Assets

3.1 Impact of Settlement Assets on the Adoption of Tokenised Funds

Settlement assets include tokenised bank liabilities and well-regulated stablecoins. They allow for atomic settlement and on chain delivery-versus-payment (DvP), eliminating the need for multiple actions and assets leaving the chain. This DvP model reduces settlement risk and reliance on off-chain fiat systems. Using settlement assets alongside digital assets brings the industry closer to realising the full potential of instantaneous settlement, reduced transaction costs, streamlined compliance, and enhanced revenue for investors in the longer run through the pursuit of a more cost-efficient model. Over time, as different forms of settlement assets and tokenised funds become more widespread, they will unlock new revenue streams for financial institutions. These include the use of tokenised assets as collateral in lending, enabled by enhanced liquidity, active secondary market trading, and faster settlement processes.

There is a symbiotic relationship between adoption of settlement assets and tokenised funds. As more settlement assets move on-chain, more tokenised vehicles are being launched to provide more on-chain investment options. Traditional financial institutions may also be drawn to launching tokenised investment vehicles to access new investor pools within the digital asset ecosystem. This growing interest, coupled with the rise of regulated initiatives, signals a maturing landscape for digital assets.

3.2 Stablecoins, Tokenised Deposits and wCBDCs

Well-regulated stablecoins are increasingly being used as a settlement asset for tokenised assets, including tMMFs. The year 2025 has been pivotal for stablecoins, with growing regulatory clarity such as the passing of the GENIUS Act in the US which serves a catalyst for broader adoption. Stablecoins are increasingly adopted for cross-border payments, especially in emerging markets with volatile currencies, large unbanked populations, and high costs associated with cross-border payments. The interoperability, wide acceptance, and availability of stablecoins across multiple networks add to their appeal for cross-border use cases.

However, financial institutions and investors should consider the risks associated with stablecoins, such as de-pegging due to market volatility of the backing asset's value and. Not all stablecoins are created equal; those with provable reserves, independent audits, and full backing by cash and cash equivalents are more likely to be widely adopted as settlement assets. Many jurisdictions, including the United States, European Union, Singapore, and Hong Kong, are developing or have established regulations specific to stablecoins or cryptoassets. For instance, MAS has introduced a framework for stablecoins, requiring issuers to meet standards for value stability, reserve management, and redemption policies, especially for Single-Currency Pegged Stablecoins (SCS) exceeding a certain value. Clear regulatory policies are essential for the adoption of stablecoins as settlement assets, as they provide the necessary trust for institutional investors and allow integration into regulated financial markets infrastructure. Implementing international standards, such as the recommendations made by FSB and BIS, is also important to prevent regulatory arbitrage.

Multiple commercial banks are exploring, researching, and issuing tokenised deposits as an alternative to stablecoins or CBDCs. Tokenised deposits are digital representations of traditional bank deposits that are recorded on a blockchain, issued and managed within regulated banking environments. They may offer faster and more efficient transaction settlement compared to traditional payment rails, reduced counterparty and settlement risk, and enhanced security and transparency under a supervisory framework.

Another form of settlement asset is Wholesale Central Bank Digital Currencies (wCBDCs), which is issued by a central bank for use by commercial banks and other authorised financial institutions in interbank payments and securities settlements. A 2024 survey by BIS indicated that wCBDCs were the most widely used settlement asset for tokenised financial assets, followed by non-tokenised deposits and tokenised deposits. The intended use of wCBDCs for handling large-value transactions and as a settlement asset between banks, central banks, and other financial institutions makes them a viable settlement currency for tMMFs using a distributor model. They are expected to serve a role similar to central bank reserves in the current system and offer functionalities such as programmability and composability.

Regardless of the forms of settlement asset used for tokenised funds, financial institutions need to innovate and provide essential infrastructure to support client demand. This includes secure digital custody, seamless on and off-ramp support, digital wallets for sending and receiving digital assets and/or settlement assets, and compliant processes for KYC and AML requirements.

3.3 Considerations for using Stablecoins as a Form of Settlement

Managers may be contemplating subscriptions and redemptions of fund units, or distributions by way of stablecoins. Stablecoin settlement introduces additional regulatory considerations. **Figure 3** provides an illustration.

> Under Q23 of the FAQs on the Payment Services Act ("PS Act") dated 19 April 2024, the MAS had stated that stablecoins may meet the definition of a "digital payment token" ("DPT") under the PS Act. MAS takes a technology-neutral stance and will examine the characteristics of the stablecoin to determine the appropriate regulatory treatment. In addition, based on their characteristics today, USDC and USDT are examples which are considered DPTs.

> Dealing in DPTs is a licensable activity under the PS Act. However, notwithstanding the foregoing, paragraph 2(i) of the First Schedule to the PS Act provides an exemption from licensing under the PS Act where any provision of payment services by a person licensed or exempted from licensing under the SFA is solely incidental to or necessary solely for that person to carry on business in such licensed or exempted activity under the SFA. On the basis that settlement in stablecoin is only incidental to a manager's and distributor's carrying on business in fund management and dealing in capital market products respectively, it is unlikely that managers and distributors involved in funds that accept settlement in stablecoin would be subjected to licensing requirements under the PS Act for dealing in DPTs.

Figure 3: An illustration of the regulatory considerations for using stablecoins

Managers must also address risks such as de-pegging and adopt necessary anti-money laundering / countering the financing of terrorism ("AML/CFT") policies and procedures with, among others, sufficient and well-documented due diligence carried on stablecoin issuers and stringent wallet whitelisting among the other industry good practices.

- Firstly, managers should note the risk of de-pegging. Managers contemplating stablecoin settlement should utilise stablecoins issued by reputable stablecoin issuers with clear and sufficient reserve-backing to reduce the chances of de-pegging and potential losses suffered due to holding of stablecoins. It is prudent for managers to convert stablecoins into fiat following settlement, in order to reduce the risk of devaluation of the fund's assets and to manage liquidity risks.
- Secondly, to address money-laundering / terrorism financing risks, managers should ensure that all wallets used for subscription, redemptions and distributions by way of stablecoins by investors undergo a whitelisting process, including verification of ownership of the wallet. Managers may consider partnering with licensed DPT custodians to be more assured that the wallets used by investors of the funds are subjected to strict compliance requirements.

There are other broader considerations which are not covered in this report, such as multi-jurisdictional issuance, custodial arrangements and consumer protection.

4. Operationalising Tokenised Funds

With the legal structure and regulatory considerations of tokenised funds covered in Chapter 2, and settlement assets covered in Chapter 3, this chapter moves on to demonstrates how interoperability and settlement can be operationalised for tokenised funds, through different implementations by leading institutions in Singapore.

- Multi-chain distribution in the primary market (Franklin Templeton)

- Secondary market trading and stablecoin settlement (Phillip Securities)
- Interoperability and digital FX (Fidelity and Citi)
- Enabling TradFi-DeFi payment linkage (Swift)
- Integrated operating platform and model (Deutsche Bank)

4.1 Multi-Chain Distribution in the Primary Market (Franklin Templeton)

Franklin Templeton (FT) has been building the Benji Technology platform since 2017, a proprietary blockchain-integrated stack designed to facilitate trading, management, and administration of token-based investments. In 2021, FT launched their first tMMF in the US, under a mutual fund structure governed by the Investment Company Act of 1940. In 2025, FT launched additional tMMFs via a Luxemburg UCITS Fund, a British Virgin Islands Private fund and a Singapore Variable Capital Company fund structure.

4.1.1 Value Proposition and Market Fit

MMFs, particularly US government MMFs, are a mainstay of the current financial ecosystem. These funds provide a "safe haven" for investors looking to preserve cash in times of market uncertainty, allow corporate treasurers and portfolio managers to optimise cash management strategies, offer yield-bearing options for brokerage clients looking to fund settlement accounts, and provide competitive returns that typically exceed most savings and checking accounts.

Yet, for all their benefits, today's MMFs exist within an account-based ecosystem and are subject to the limitations inherent in today's financial market infrastructure. Shareholder records are only updated after daily trading has concluded; yield eligibility is determined once daily based on start-of-day snapshots of shareholders; yield is accumulated and only paid out monthly; redemptions of MMF shares take a minimum of 24 hours and must be routed through intermediaries.

Tokenising MMFs, by utilising digital wallets to manage investments, and administering shareholder records on-chain can help address many of these issues. Tokenising MMFs unlock greater utility and new use cases that can potentially enhance the existing financial services system.

4.1.2 Legal Structure

tMMF products from the Benji Technology platform are approved in the US, Luxembourg, British Virgin Islands and Singapore.

Some tokenised securities may only serve as a back-up record of ownership, functioning merely as digital receipts where actual ownership is conveyed via traditional fund shares and recorded on mainframe-based systems. In some cases, the tokenised security may not even provide any native rights to holders, and changes in ownership are not formally recorded until the off-chain ledger is updated.

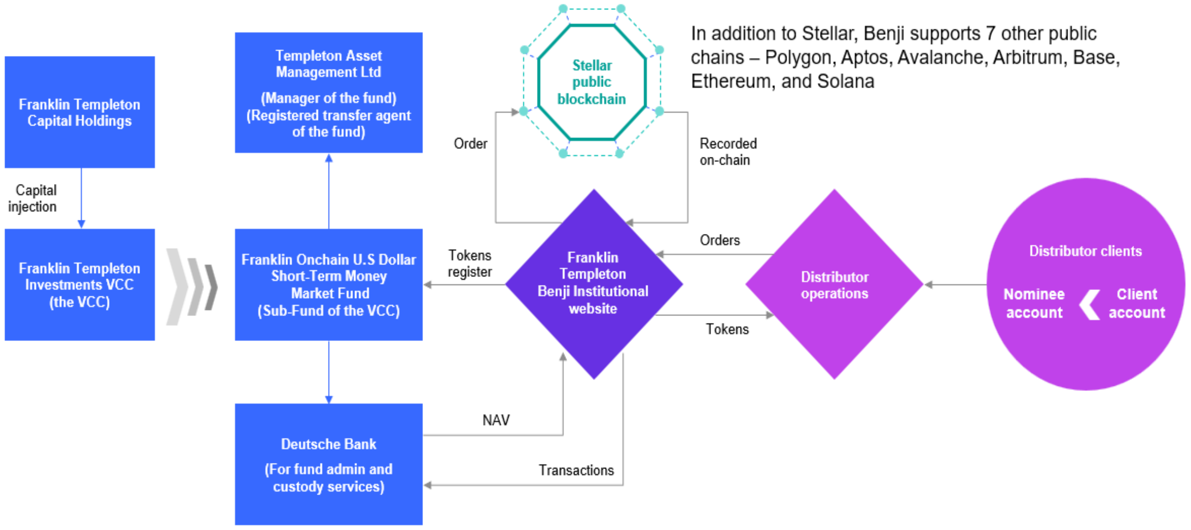
In contrast FT's tMMF share registers are kept on public blockchains and exist as the only authoritative share registers, The Benji Tokens (as part of the Tokenised Register) act as *prima facie* evidence of the shares. Taking Singapore as an example, the lawful holder of the sgBENJI Token would, by operation of law and the VCC's constitution, also be the owner of the corresponding share. Under normal operating conditions, upon an investor successfully subscribing for shares in a VCC and being issued a share, there will be a simultaneous minting and issuance of the Benji Token correlating to that share, both of which would be held by the investor.

4.1.3 Product Design

For sgBENJI, the funds structure is set out below.

- **Fund Umbrella:** Franklin Templeton Investments VCC
- **Tokenised Sub Fund:** Franklin OnChain U.S. Dollar Short Term MMF
- **Fund Manager:** Templeton Asset Management Ltd
- **Digital Transfer Agent:** Templeton Asset Management Ltd (utilising the Benji Technology Platform)
- **Custodian:** DB International Trust (Singapore) Limited
- **Fund Administrator:** Deutsche Bank AG, Singapore Branch
- **Public Blockchain:** Stellar (default). Eight other public blockchains are also supported.

Figure 4 provides a high-level understanding of the subscription and redemption flows.


Franklin Templeton Capital Holdings
Capital injection
Franklin Templeton Investments VCC (the VCC)
Templeton Asset Management Ltd
(Manager of the fund)
(Registered transfer agent of the fund)
Franklin Onchain U.S Dollar Short-Term Money Market Fund
(Sub-Fund of the VCC)
Deutsche Bank
(For fund admin and custody services)
Stellar public blockchain
Order
Recorded on-chain
Tokens register
Franklin Templeton Benji Institutional website
Orders
Tokens
NAV
Transactions
Distributor operations
Distributor clients
Nominee account
Client account

In addition to Stellar, Benji supports 7 other public chains – Polygon, Aptos, Avalanche, Arbitrum, Base, Ethereum, and Solana

Figure 4: Overview of subscription and redemption flows for sgBENJI tMMF

While not all features are currently available for the sgBENJI tMMF, the technology advancements available through the Benji Technology Platform have allowed FT to build never-before-available features and functionality into product design, offering significant enhancements and new forms of utility on-chain, including:

- A solution to allow KYC compliant, permissioned wallet-to-wallet transfers on supported blockchain networks, as well as functionality to allow the purchase or redemption of tokenised securities using stablecoins
- Instantly record changes in tokenised security ownership, rather than waiting to update the shareholder ledger on the next business day. Wallet-to-wallet transfers of tokenised securities can happen 24 hours a day, 7 days a week, 365 days a year
- Intraday yield payments: dividends calculated real-time, if a tokenised asset is transferred throughout the day
- Yield that can be distributed to shareholders each calendar day, including weekends and holidays
- Claw-back or replacement of tokenised securities moved illicitly or lost.
- Self-custody of tokenised investments, so that users can manage their own hot or cold wallets

4.1.4 Technology, Infrastructure, Smart Contracts

Below are key technology considerations when FT implemented the various tMMFs:

- **Cyber Security**. FT's security architecture includes the capability to identify, detect, prevent, and respond to information security events. There are robust security controls including but not limited to firewalls, logical access control, network intrusion detection/prevention systems, data loss prevention, destination filtering, web filtering, antivirus, antimalware, encrypted communication, device encryption, backup, disaster recovery, and centralised, round-the-clock security monitoring. Service providers processing FT's data would also require the same level of security that FT maintains internally.

- **Authentication**. FT employs a defence in depth approach to security which includes layered technical, administrative/process, and physical security controls for safeguarding information assets. For example, authenticated instructions can only be sent via authorised users via the Benji Institutional website. Security standards also include parameters for password strength, complexity, expiry, and encryption.
- **Tokenisation**. FT tokenises the share registry of the Fund (i.e. minting, burning, and all actions related to the tokens) via their proprietary BENJI Technology Platform. While shareholder transaction records are kept on the public blockchain, shareholder's personal identifiable information records are kept on internal systems. These two records are then seamlessly joined in their internally developed "BENJI" blockchain-enabled Transfer Agent platform.
- **Token Standards**. The token standard used by BENJI is ERC20 for relevant EVM chains (Ethereum, Arbitrum, Avalanche, Base, and Polygon). Stellar Asset Contract (SAC) is used for Stellar, which is compatible with the widely adopted SEP-41 token interface, similar to the ERC-20 standard. The Aptos blockchain primarily uses the Fungible Asset (FA) standard for fungible tokens. The primary token standard on the Solana blockchain is Solana Program Library (SPL).

4.1.5 Compliance, Risk and Governance

Below are key compliance, risk and governance considerations when FT implemented the various tMMFs:

Compliance

- **AML/KYC**. All traditional AML/KYC policies and procedures are maintained. All current responsibilities are followed and adhered to.
- **On-Chain Controls**. On-chain monitoring will be utilised to enhance oversight of blockchain-based transactions. This will include tracking, analysing, and reporting on on-chain activities to ensure compliance, detect anomalies, and mitigate risks.
- **Audit Trail**. All token activities are immutably recorded on a public blockchain, while sensitive client data remains safeguarded off-chain in traditional database.

- **Control over ownership via whitelisted wallets only**. Benji tokens are restricted to whitelisted wallets only to hold or transact without conversion/redemption. Although token activity occurs on public blockchains, the ability to purchase, redeem, or hold the token is restricted to wallets assigned during the KYC process. This preserves AML/CFT traceability and control over ownership.

Risk Management

- **Custodial Assurance**. DB International Trust (Singapore) Limited performs the role of custodian for the underlying TMMF assets.
- **Operational Risk Mitigation.** Non-public information is housed in an internal database system that is seamlessly "joined" with the blockchain by the platform. All Fund and shareholder records in the blockchain-integrated system are under full and complete control. FT maintains the ability to correct any errors in share recordation, including any errors in the blockchain.

Governance

- **Internal Oversight**. Complete integration with existing compliance, operations and risk teams processes and policies, ensuring robust oversight and monitoring of tMMFs.
- **Regulatory Engagement.** sgBENJI is fully approved and registered as an Authorised Scheme under section 286 of the Securities and Futures Act 2001.
- **Customer Protection**. The tokenised registry is the only record of share ownership, meaning a direct relationship between token and share ownership.

4.1.6 Operational

Below are key operational considerations when FT implemented the various tMMFs:

- **Global Support**. BENJI Technology Platform is supported by global service centres housing inhouse Digital Transfer Agent service representatives.
- **Business Continuity**. FT operates triplicate nodes on supported blockchains, creating significant technical redundancy. This means that blockchain operations could be maintained even when all other nodes fail. In an extreme scenario of a network failure, FT maintains complete, up-to-date on-chain records that could be migrated to other supported blockchain or traditional data stores. The use of multiple networks, each holding a full cop of the register compounds this redundancy and delivers enhanced security and business continuity. While the likelihood of a public blockchain going down may be significantly less than an traditional database or off-chain IT network, blockchain uptime forms a key part of FT's suitability assessments.

4.2 Secondary Market Trading and Stablecoin Settlement (Phillip Securities)

Working alongside partners such as Alta Exchange and Hamilton Lane, Phillip Securities has contributed to the tokenisation and listing of private credit funds and MMFs on regulated digital asset exchanges. This has enabled accredited and institutional investors to access, trade, and settle fund units using blockchain infrastructure, with instant settlement supported by stablecoins.

The firm's market making desk and in-house tokenisation engine facilitates secondary market liquidity and compliance with regulatory standards, while its operational experience in managing tokenised alternative assets has helped the firm transition from traditional to digital fund structures.

4.2.1 Value Proposition and Market Fit

The primary consideration behind selecting MMFs was their suitability for market making. The ability to efficiently price the underlying assets and the inherent stability of MMFs are critical factors in achieving narrow bid-ask spreads, typically defined as less than 10 basis points.

Due to their low volatility and highly predictable net asset value, MMFs enable market makers to provide continuous, 24/7 pricing with minimal bid-ask spreads. The well-anchored fair value of MMFs reduces the need for extensive price discovery, supporting efficient and transparent trading. Additionally, the predictable liquidity resulting from regular redemption and subscription processes offers market makers a reliable price anchor, further enhancing the stability and attractiveness of MMFs as a foundation for tokenisation and secondary market activities.

Other considerations included having an existing MMF, and having the necessary licenses and capabilities such as a market making desk and an in-house tokenisation engine.

4.2.2 Legal Structure

In order to establish the tokenised product and its associated processes, Phillip Securities (PSPL) worked with Drew & Napier on the following legal structure:

- End client indicates their interests to subscribe to tMMF (underlying asset is Phillip Capital Management's (PCM) MMF). PSPL enters the order to subscribe to PCM MMF (after payment). PCM MMF will only reflect PSPL in the fund registry (which is the current MMF arrangement).

- PSPL holds the underlying MMF in trust for the end client. The client ownership information is reflected in the unit trust nominee database in PSPL's unit trust system.
- PSPL tokenises the MMF, creating tMMF tokens (1:1 match with the underlying unit trust held in custody) on the appropriate blockchain network. PSPL transfers the tMMF tokens to the end client's wallet.
- The blockchain ledger and the traditional unit trust database is in-sync at all times.
- Essentially, the tMMF tokens reflects the omnibus level ownership, with the tokens have a direct 1:1 relationship with the custodised underlying MMF units.

4.2.3 Product Design

As many components of the end-to-end lifecycle of asset tokenisation fall within Phillip Capital's capabilities, this lowered the barrier to tokenise the MMF. The following functions are involved in this tokenisation project:

- **Asset Origination**: PCM provided an existing MMF as the underlying assets for tokenisation.
- **Tokenisation Engine**: PSPL, with prior experience with the tokenisation of alternative assets, was familiar with the technology needed to scale fast and to implement compliance standards on-chain.
- **Operations**: PSPL's operations team had prior experience in managing tokenised alternative assets. This lowered the learning curve on operational procedures and workflows.
- **Compliance**: PSPL's compliance team supported reviews of legal opinions, agreements, and provided valuable inputs to enable the offering of tokenised assets to their distribution network.
- **Liquidity Provision (Market Making)**: PSPL's market making team supported liquidity of the token and the on/off-ramping (where necessary) of stablecoins in the subscription and redemption of the tMMF. More detail of this process is in the section below.

<u>tMMF Subscription Process</u>

Figure 5 provides an overview of the end-to-end tMMF subscription process (redemption is in reverse). Please note that for secondary trading (without subscription and redemption), the process is purely between the market maker and the exchanges.

In the subscription process, the market maker takes on the on/off-ramping role to allow the acceptance of stablecoins or digital currencies, exchanging them for fiat currencies so that the traditional fund operations can remain fiat based.

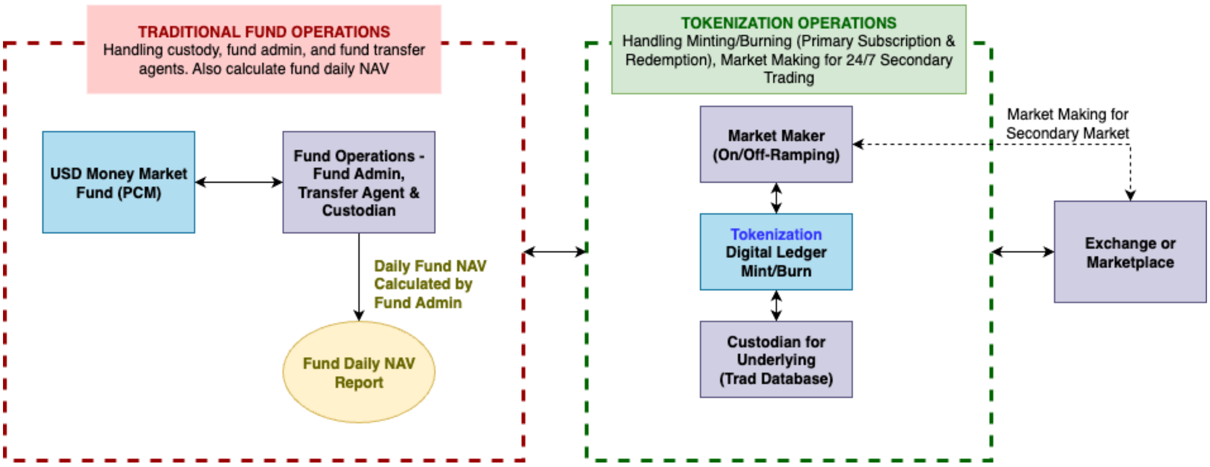

TRADITIONAL FUND OPERATIONS
Handling custody, fund admin, and fund transfer agents. Also calculate fund daily NAV
USD Money Market Fund (PCM)
Fund Operations - Fund Admin, Transfer Agent & Custodian
Daily Fund NAV Calculated by Fund Admin
Fund Daily NAV Report
TOKENIZATION OPERATIONS
Handling Minting/Burning (Primary Subscription & Redemption), Market Making for 24/7 Secondary Trading
Market Maker (On/Off-Ramping)
Tokenization Digital Ledger Mint/Burn
Custodian for Underlying (Trad Database)
Market Making for Secondary Market
Exchange or Marketplace

Figure 5: Overview of Subscription Process for PCM tMMF

4.2.4 Technology, Infrastructure, Smart Contracts

The Symphony Platform was built in-house for different stakeholders to manage the lifecycle events of tokenised products. It can support the following lifecycle management functions:

- Issue Token
    - Smart contract deployment of the target asset onto either EVM-compatible chain or XRPL (Ripple Ledger)
    - Define token features - include compliance and regulatory requirements
    - Link token to RWA – allowing ease of reconciliation at any time
    - Mint (Primary Subscription) and Burn (Primary Redemption) of asset token
    - Enforce jurisdiction-based or investor-type restriction
- User Registry
    - AML/KYC of client – include key regulatory or compliance information (such as country of residence, accredited investor status)
    - Whitelist wallet addresses of clients that are allowed to transact
- Handle Asset Servicing
    - Input of daily pricing written directly onto the smart contract

- Secondary Trading and Market Making
    - Connect to approved exchanges
    - Input orders
    - Monitor transactions (i.e. transfer)
- Access Management
- Audit and Reporting

Referencing the composable token standards proposed in the Guardian Funds Framework (**Figure 6**), the design of the smart contract took into consideration the Compliance Layer (implemented via smart contract standards such as ERC-3643).

The ERC-3643 standard was used to ensure that tokens can only be transacted amongst approved (KYC completed) parties. This model is also known as "**Private Token, Public Network**" or "**Permissioned Asset on Permissionless Rails**" model.

The Guardian Funds Framework proposed this model for the following benefits:

- **Transparency**. All transactions are visible on a public ledger (even though internal info can be encrypted). Public network is decentralised and with no single party having control over transactions.
- **Composability**. The permissioned asset can interact with other DeFi or public smart contracts in the future.
- **Network Security**. Public chains usually have larger validator sets, making them less likely to be attacked successfully.
- **Interoperability**. This makes the asset integration with existing wallets, custodians and exchanges much easier.

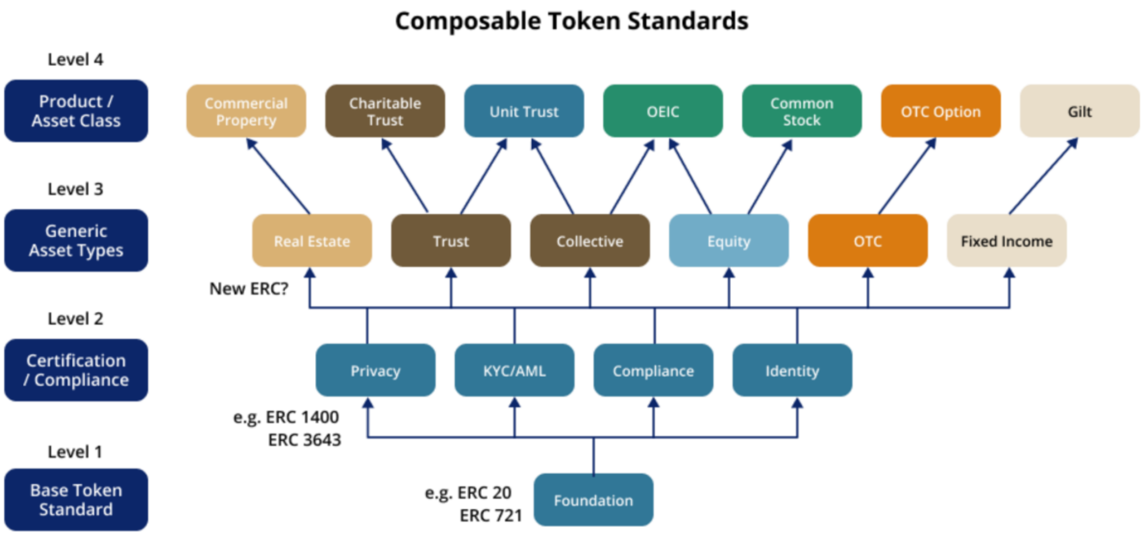
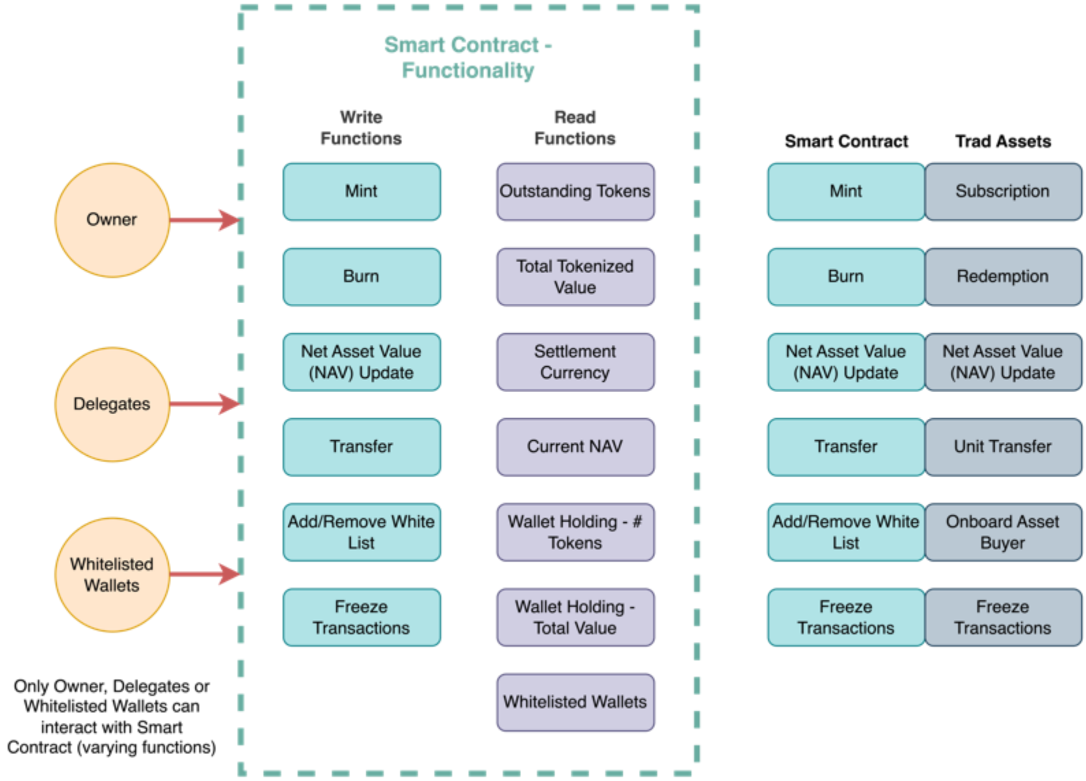


Figure 6: Abstraction Levels of the Guardian Composable Token Taxonomy (GCTT)

The **smart contract** used in this project contains the following functionalities – which can be mapped to traditional asset operations (function centric) in **Figure 7** below.


Smart Contract - Functionality
Write Functions
Read Functions
Owner
Delegates
Whitelisted Wallets
Mint
Burn
Net Asset Value (NAV) Update
Transfer
Add/Remove White List
Freeze Transactions
Outstanding Tokens
Total Tokenized Value
Settlement Currency
Current NAV
Wallet Holding - # Tokens
Wallet Holding - Total Value
Whitelisted Wallets
Only Owner, Delegates or Whitelisted Wallets can interact with Smart Contract (varying functions)

Smart Contract	Trad Assets
Mint	Subscription
Burn	Redemption
Net Asset Value (NAV) Update	Net Asset Value (NAV) Update
Transfer	Unit Transfer
Add/Remove White List	Onboard Asset Buyer
Freeze Transactions	Freeze Transactions

Figure 7: Mapping of Smart Contract Functionalities Against Traditional Asset Operations

Figure 8 below illustrates the implementation of ERC-3643 and ERC-20 Smart Contract Suites – showing how the smart contracts interact with current off-chain compliance processes for AML/KYC.

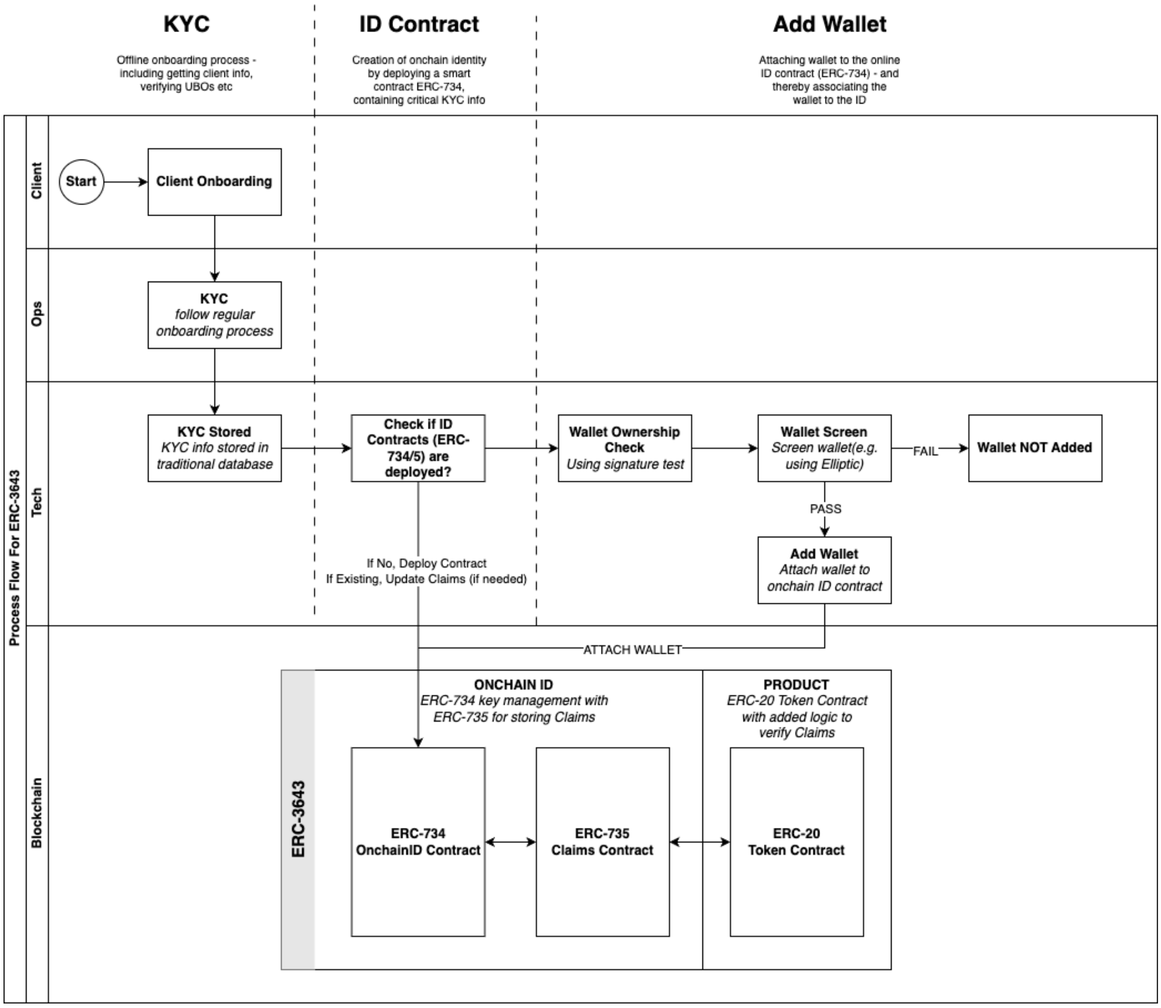

KYC
Offline onboarding process - including getting client info, verifying UBOs etc
ID Contract
Creation of onchain identity by deploying a smart contract ERC-734, containing critical KYC info
Add Wallet
Attaching wallet to the online ID contract (ERC-734) - and thereby associating the wallet to the ID
Process Flow For ERC-3643
Client
Ops
Tech
Blockchain
Start
Client Onboarding
KYC follow regular onboarding process
KYC Stored KYC info stored in traditional database
Check if ID Contracts (ERC-734/5) are deployed?
If No, Deploy Contract
If Existing, Update Claims (if needed)
Wallet Ownership Check Using signature test
Wallet Screen Screen wallet(e.g. using Elliptic)
FAIL
Wallet NOT Added
PASS
Add Wallet Attach wallet to onchain ID contract
ATTACH WALLET
ERC-3643
ONCHAIN ID
ERC-734 key management with ERC-735 for storing Claims
PRODUCT
ERC-20 Token Contract with added logic to verify Claims
ERC-734 OnchainID Contract
ERC-735 Claims Contract
ERC-20 Token Contract

Figure 8: ERC-3643 Process Flow for PCM tMMF

4.2.5 Compliance, Risk and Governance

Tokenisation of MMFs introduces new operating models. Governance must remain robust to protect investors, ensure regulatory alignment, and preserve trust in the financial system. The framework below integrates traditional financial safeguards with on-chain transparency.

Compliance

- **KYC/AML Integration**. All wallet addresses are verified and whitelisted post-KYC/AML checks, ensuring that tMMF tokens can only be transacted between verified parties.
- **On-Chain Controls**. Smart contracts enforce compliance rules (ERC-3643), such as transfer restrictions, investor type eligibility, and jurisdictional constraints.
- **Audit Trail**. All token transfers are immutably recorded on a public blockchain, while sensitive client data remains safeguarded off-chain in traditional database.

Risk Management

- **Custodial Assurance**. Each tMMF token is 1:1 backed by MMF units held in Phillip custody, ensuring no risk of fractional reserves.
- **Operational Risk Mitigation**. Ring-fenced roles ensure fund managers only handle fiat flows, while stablecoin conversions are managed by market makers with segregated processes.
- **Liquidity Risk**. Predictable MMF subscription/redemption cycles serve as a price anchor, while market makers ensure continuous liquidity for secondary trades.

Governance

- **Clear Accountability**. Responsibilities are divided between PCM (fund origination), PSPL (compliance, custody & market making), and PSPL's Digital Assets Team (platform, tokenisation & smart contracts).
- **Internal Oversight**. Compliance, Risk, and Operations teams review legal structures, monitor secondary market trading, and oversee AML/KYC adherence.
- **Regulatory Engagement**. Ongoing dialogue with MAS ensures alignment with evolving frameworks and adoption of industry best practices.
- **Customer Protection**. Investors retain full rights to the underlying MMF through the nominee arrangement, with tokenisation serving as an additional representation layer rather than a substitution.

The above approach combines the **rigour of traditional unit trust frameworks** with the **transparency and programmability of blockchain**, ensuring that risks are contained and compliance obligations are met.

4.2.6 Operational

The design of the processes for tMMF has a few goals:

- **Ringfenced Risk** of participating entity within Phillip Capital. For example, the fund manager will only deal with fiat currency even if the end tokens can be traded or subscribed in stablecoins (which will be managed by market makers with the exchange).
- **Operational Efficiency** for fund managers. The processes will ensure that current fund operations do not have to change to accommodate tokenisation needs.
- **Scalability** by enabling both external and internal distributions.
- Ensure **Customer Protection** at the token level and underlying asset level.
- **Pass-through Structure** which will have no re-issuance of regulatory documents – thus saving time and effort.

4.3 Interoperability and Digital FX (Fidelity and Citi)

As part of Project Guardian, Fidelity International and Citibank jointly developed a proof-of-concept that integrates a tMMF with an embedded digital FX swap, enabling real-time, on-chain settlement of multi-asset transactions. This POC aims to streamline treasury operations, enhance liquidity, and reduce FX risk for institutional investors.

4.3.1 Value Proposition and Market Fit

As tokenisation in various capital markets use-cases continue to evolve and materialise, there could be a potential future where various forms of digital assets, including tMMFs, of different currency denominations are being traded and settled in real-time across multiple DLT platforms. In this scenario, FX markets would therefore play a critical role in ensuring timely liquidity for investors looking to convert their domestic currency into the currency(ies) that with which they intend to purchase the relevant digital assets with. Seamless FX conversion would also allow investors to quickly and efficiently access digital assets across global markets, while potentially supporting wider objectives such as portfolio diversification and risk management.

Usage of DLT technology in both FX settlement and cross-network orchestration can potentially synchronise the exchange of multiple currencies and assets across different multiple networks, which could enable new multi-asset use cases that settle in delivery-versus-payment-versus-payment (DvPvP)manner seamlessly and efficiently.

tMMFs are expected to be the fastest (among digital assets) to reach meaningful adoption, estimated to grow to USD 400 bn by 2030[7]. The U.S. has the largest number of issuers of MMFs globally, as well as the deepest and most liquid capital markets with over USD 6.1 Tr AUM[8]. Non-USD investors who wish to gain exposure without FX risk would generally have to book and manually reconcile FX hedging separately. This would typically create friction and could potentially result in funding timing mismatches where the FX settlement is slow (e.g., T+1) or delayed, leading to potential FX funding risks. In addition, a delay in settlement would also impact a party's ability for real-time, precise liquidity management.

The developed technical solution involves a simulated tMMF (Digital MMF) and digital FX swap. The use case is targeted at investors who wish to earn yield on a tMMF denominated in a foreign currency, while simultaneously being hedged against currency risk via a digital FX swap on a real-time basis, therefore potentially allowing for a wider distribution of tMMF. This use case aims to focus on interoperability as well as to highlight the unique programmable PvDvD aspects, as part of a holistic playbook to realise the end-to-end benefits of tokenisation.

[7] *From ripples to waves: The transformational power of tokenising assets, Mckinsey, June 2024*

[8] *Who borrows from money market funds?, BIS Quarterly Review, Dec 2023*

The pilot demonstrated that synchronised settlement of tMMF shares against an FX swap is technically feasible and can reduce settlement frictions. Importantly, to realise the broader benefits of close to real-time settlement and automation, a digitally native token model, where the token itself is the legal share, appears essential. This design enables close to real-time settlement, and post-trade workflows to run fully on-chain, while allowing sensitive investor data to remain permissioned.

Beyond the settlement layer, questions remain on the market liquidity required for commercial viability. A resilient secondary market for tMMFs would need well-defined roles for custodians, transfer agents, and liquidity providers, alongside investor-protection mechanisms such as rule-based transfer restrictions.

Since the POC in 2024, Fidelity International and Citi has been exploring different use cases where tMMFs could deliver incremental value. Potential areas include institutional treasury management (for example, same-day subscriptions and after-hours settlement), collateral mobility (recognition of tMMFs in secured lending, repo, or margining), and distribution efficiency. These avenues remain exploratory, but they illustrate how asset managers and banks, by combining tokenised assets with regulated digital cash rails, could gradually build towards commercially viable models that align with policy progression and market readiness.

4.3.2 Legal Structure

In an envisioned commercial setting, the following non-exhaustive legal and regulatory issues should be considered:

On the DvP Transaction of tMMF against Settlement Assets

- Digital Twin or Digital Native
  - Digital Twin: A lighter-touch approach where tokens represent the fund without conferring the fund registry. It could offer lower implementation costs and fewer regulatory hurdles but would likely deliver only modest efficiency gains, as most operational processes remain unchanged.
  - Digital Native: A fully on-chain model enabling end-to-end digital fund management. It promises greater efficiency and scalability but would introduce technological, and legal and regulatory complexity.
- Investor suitability/eligibility to hold the tMMF and settlement asset
- Fund jurisdiction: The domicile of the fund remains central to its regulatory treatment if multiple jurisdictions adopt divergent approaches.

- Legal status of DLT as form of record keeping: The recognition and treatment of DLT, as a legally valid form of record-keeping for the maintenance of fund registers and investor records, vary across jurisdictions.

<u>On the PvP Transaction of Settlement Assets of Different Currencies</u>

- Need for certainty as to the legal and regulatory status and treatment of settlement assets, e.g. tokenised bank liabilities, stablecoins, central bank digital currencies, etc
- Investor eligibility to hold settlement assets
    - For example, where tokenised bank liabilities are used, both an investor and the liquidity provider would likely have to be customers of the same bank that issues the tokenised bank liabilities; be identified by their digital wallets; and be eligible to hold such tokenised bank liabilities.
- Capital control(s) of the base currency, if applicable
- Having a sufficiently robust contractual framework that regulates the trades, the relationship between the platform and participants, and as between the participants (e.g. onboarding / access agreements executed between the platform and participants, platform rulebooks that set out the terms governing trades, etc.). This would include terms on the governing law, jurisdiction, dispute resolution mechanisms, etc.
- Having regard to any 'automatic' or 'immutable' aspects of DLTs and smart contracts, provisioning for management, fallbacks, 'manual intervention', remedies, including the ability to make amendments/corrections in respect of trades where there are errors, disputes, requirements by law or regulation, etc. (whether on-chain or off-chain)

4.3.3 Product Design

The technical solution looks at interoperability across two separate DLT networks – (a) for settlement assets (DLT Network 1); and (b) for tMMFs (DLT Network 2). Where an investor confirms the terms of its transaction for the purchase or sale of the MMF's tokens, the process for the Digital FX swap (consisting of a FX spot and a FX forward) and the Digital MMF are as follows (**Figure 9**):

- **Digital FX Spot:** A FX spot PvP will be entered into between the investor and Citi as the Market Maker and orchestrated on DLT Network 1, via a PvP smart contract. Once instructions from the investor and Citi in respect of the relevant currency pair are synchronised and the requisite checks (such as anti-money laundering checks which would be conducted off-chain) are confirmed by a smart contract, the settlement instructions will be sent to debit or credit their respective fiat accounts. Alternatively, if settlement asset (such as central bank digital currencies or regulated tokenised bank liabilities) may be used (subject to the applicable laws of the relevant jurisdiction(s)), then PvP could potentially be achieved via the exchange of (for example) digital SGD from the investor with (for example) digital USD[9] from Citi on a conditional, "all-or-nothing" basis (see diagram below).

- **Digital FX Forward:** Once the FX spot has been executed, a simultaneous FX forward smart contract will be programmed to realise a PvP in the opposite direction at a specific future time or future event. For example, this smart contract could be linked to an external Oracle for the specific future time trigger, or to trigger whenever the tokens of the tMMF are redeemed.
- **Digital MMF:** tMMF DvP will be executed, via the simultaneous transfer of payment from the Investor, against the receipt of tokens of the tMMF by the Investor from the Transfer Agent (TA).

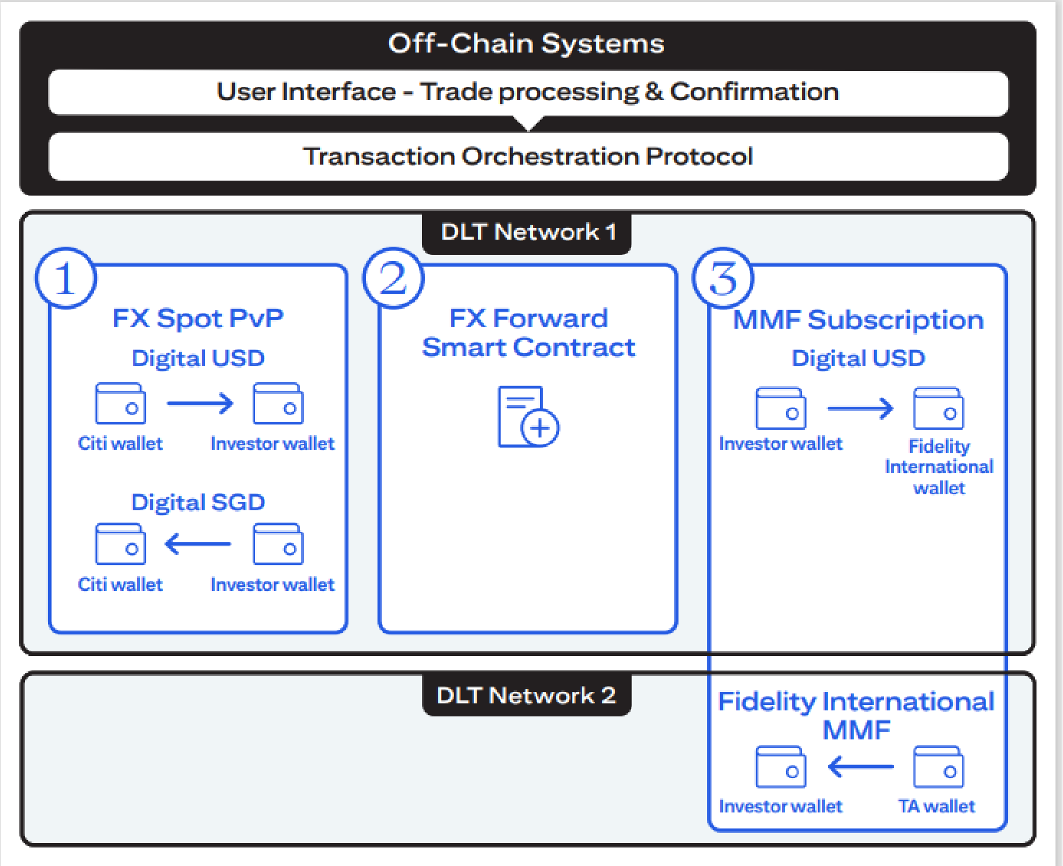


Figure 9: Digital FX Swap and tMMF Process

[9] *Digital SGD, Digital USD and tMMF are each wholly simulated, conceptual test tokens or solutions, and are not prototype or commercial products or solutions. The legal and regulatory categorisation and/or treatment of each of the digital USD, digital SGD and/or tMMF is subject to legal and regulatory analysis and assessment under applicable regulatory regime(s).They and any related proposed solutions are subject to Citi's and/or Fidelity International's respective internal and/or regulatory approvals, and are subject to change, modification, withdrawal, or termination, at Citi's and/or Fidelity International's absolute discretion at any time.*

4.3.4 Technology, Infrastructure, Smart Contracts

The interoperability solution sought to enable direct, secure cross-chain settlement. When a settlement is due on another blockchain, the smart contracts trigger a request. A dedicated messaging server picks up this request, signs it, and transmits it via a protected link directly to a corresponding server on the target chain. This receiving server then delivers the request to the destination's interop smart contract. The contract verifies the signature and transaction ID, executes the settlement, and sends a confirmation.

This approach bypasses complex, resource-intensive networks and heavy processing, relying instead on straightforward, highly secure, point-to-point communication.

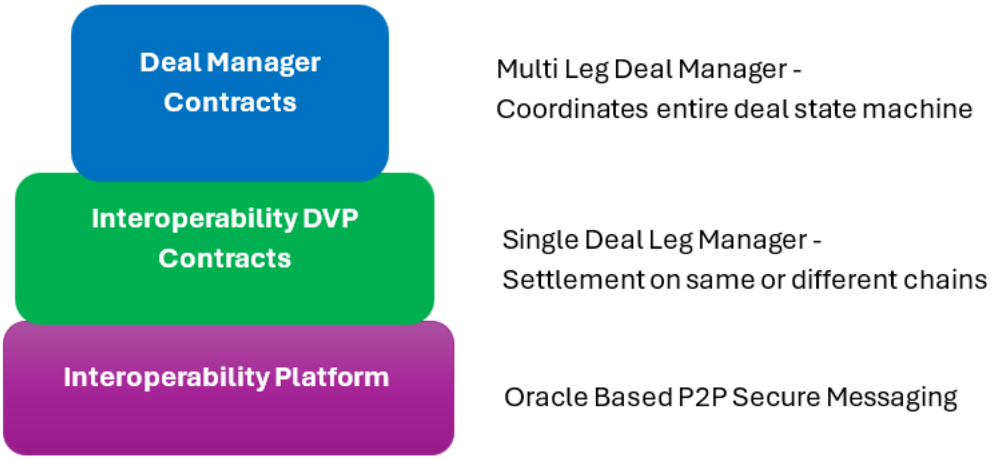

Deal Manager Contracts
Multi Leg Deal Manager - Coordinates entire deal state machine
Interoperability DVP Contracts
Single Deal Leg Manager - Settlement on same or different chains
Interoperability Platform
Oracle Based P2P Secure Messaging

Figure 10: Multi-layered Approach for Cross-Chain DvP/PvP

In this multi-layered approach (**Figure 10**), each layer is independent from the others and provides essential functionality:

- **Interoperability layer.** Coordinates on and off chain message passing. It is built for point-to-point connectivity, as opposed to relying on an external network to provide the smallest possible attack surface while transmitting messages between chains. It is secured using mTLS, and the messages are signed and assigned a nonce so on the receiving chain smart contract can verify the sender and that the message was only sent once.
- **Single Deal Leg Manager.** A DvP/PvP contract that handles instructions covering both asset/payment locations – either on the same chain as the DVP contract itself, or one or both assets on remote chains when interoperability is needed. In our use case the payment was on the same chain while the MMF fund was on a remote chain.
- **Deal Manager Layer.** Handles multi-leg deals made up of several DVP contracts. It ensures the deal state machine is executed or rolled back in case of exceptions.

In this use case, it coordinated 4 separate DVP contracts: The Swap near leg, the fund investment, the fund redemption, and the Swap far leg.

4.3.5 Compliance, Risk and Governance

Key design considerations for the solution includes the following:

- **Whitelisting.** Whitelisting of all tokens (tMMF, settlement asset) ensures that all transactions only occur between verified and eligible parties
- **Interoperability Smart Contract.** Ensures that both the DvP and PvP transaction occur on an all or nothing basis in a sequential manner, as described in the Technology section. Prior to settlement, ensure that there is sufficient balance across all Wallets for the transaction to settle.
- **Token standards.** Token standards underpin interoperability and compliance in tokenised financial markets. The **ERC-3643** standard has been designed with compliance in mind, offering features such as embedded identity management and transfer restrictions to support regulatory requirements. However, **ERC-20** remains the most widely adopted standard due to its long-standing use and integration across decentralised finance (DeFi) ecosystems. The choice of token standard therefore involves a trade-off between regulatory functionality and ecosystem readiness. Understanding adoption trajectories and integration challenges is critical to enabling widespread, compliant deployment.

4.3.6 Operational

In an envisioned commercial setting, the following non-exhaustive legal and regulatory issues can be considered.

<u>On the DvP Transaction of tMMF against Settlement Asset</u>

- Market Liquidity and Settlement dynamics: The POC demonstrates that DvP settlement between tMMFs and settlement asset can occur in real-time, with 24/7 availability and near-instantaneous transfer finality. However, challenges emerge when aligning continuous, real-time settlement with legacy fund structures
  - Most MMFs calculate net asset value (NAV) once daily, creating a disconnect between real-time mint/burn capabilities (settling in seconds) and valuation processes. Transactions after the daily cut-off are executed at the next NAV, limiting intraday price discovery.
  - The secondary market for tMMFs could, in theory, operate continuously, but its design should aim to consider reconciling real-time trading with the constraints of daily NAV updates in the primary market.

  - Developing regulated frameworks for tMMFs' liquidity provision, price discovery, and market infrastructure would be essential to unlocking scalable, institutional adoption of regulated tMMFs.

On the PvP Transaction of Settlement Asset of Different Currencies

- Whether there is an executable FX price and trade confirmation process at the time of transaction, e.g., 24x7, bank holidays, RTGS closes
- Whether the FX liquidity provider have sufficient liquidity in digital form, e.g., tokenised bank liabilities or stablecoins, at the time of transaction.

4.4 Bridging Traditional and Digital Finance (Swift)

As digital assets and settlement assets such as stablecoins, tokenised bank liabilities, and CBDCs continue to gain traction, financial institutions face both expanded capabilities and increased complexity due to ecosystem fragmentation. Without interoperability and agreed community standards, these innovations risk forming isolated "digital islands" disconnected from established financial infrastructure. With tokenisation set to become a multi-trillion-dollar market globally by 2030 [10.15], bridging the gap between traditional and digital finance becomes a critical priority.

Swift is evolving its infrastructure to facilitate seamless transactions across both conventional and emerging asset types, including stablecoins, tokenised securities, and CBDCs by leveraging its existing global connections. This evolution builds on Swift's foundation of existing messaging standards, robust security frameworks, and established identity and access management protocols.

4.4.1 Value Proposition and Market Fit

As part of this evolution, Swift has developed a digital assets orchestrator that facilitates access and mitigates settlement risk by addressing 4 key use cases as shown in **Table 2**.

Use Case	Description	Assets
DvP	Synchronised exchange of tokenised assets and settlement assets across two blockchains	Fixed income instruments (digital bonds) Carbon credit CBDC Fiat

[10] Standard Chartered / Synpulse, Real-world asset tokenisation: A game changer for global trade, July 2024

[15] McKinsey estimates tokenization will be less than $2 trillion by 2030, June 2024

PvP	Synchronised exchange of two forms of settlement assets: digital against fiat across one blockchain and the correspondent banking chain; and digital against digital across two blockchains	Stablecoins Fiat money CBDC
Fiat cash settlement of on-chain transaction	Orchestrated settlement of the fiat cash leg of an on-chain tokenised asset transaction	Fiat money
Corporate actions events on tokenised assets	Orchestrated income events (coupon and full redemption) on a digital bond against fiat and settlement asset	Fixed income instruments Stablecoins Fiat

Table 2: Overview of Swift Use Cases in Digital Asset Orchestration

Across all 4 use cases, industry stakeholders contributed to the design and validation of the workflow and target architecture. Leveraging secure global messaging protocols and API-based integration, the digital assets orchestrator functions as a single gateway to multiple settlement systems within the traditional financial ecosystem, while extending interoperability into digital asset platforms.

Beyond platform interconnectivity, the orchestrator also mitigates risks associated with asynchronous settlement – particularly in delivery-versus-delivery (DvD) scenarios where transaction legs are processed across distinct systems. By executing workflows aligned with pre-defined industry (ISO) standards, the orchestrator enables synchronised settlement and provides end-to-end lifecycle visibility to all transacting parties.

4.4.2 Product Design

Post-trade secondary market settlement remains a major hurdle in digital asset adoption, requiring real-time, cross-platform interoperability, standards and extended reach.

Swift has served as a Trusted Interoperability Provider (TIP) in a number of industry trials in recent years, including the ECB's 2024 tests[11] – alongside 64 participants comprising central banks, financial market participants and DLT operators – that used DLT for wholesale settlement in central bank money.

[11] Dec 2024, 'Eurosystem completes tests using DLT for central bank money settlement'

The TIP also acts as a technical delegated agent, empowered by market participants to perform specific actions on their behalf, in strict alignment with market guidelines. These delegated actions may include:

- Triggering the payment initiation on the cash settlement ledger based on a bank mandate provided over the Swift network
- Orchestrating the delivery of the asset conditional to payment execution based on verified mandates from delivering and receiving agents
- Sending corporate action notifications and executing some of the corporate action events such as coupon payments and full redemption

Each activity is performed under proper delegation mandates provided by market participants and the asset registry owner. This allows the TIP to shield participants from having to implement dedicated solutions or interfaces for each tokenised asset they want to settle.

As trusted actor, the TIP ensures consistent, secure, and efficient execution across fragmented systems, reinforcing trust and operational integrity in a digital-first financial ecosystem.

To test this approach, Swift's has been conducting digital asset trials designed to enable interoperability across the full post-trade lifecycle of a bond, including DvP, interest payments, and redemptions using fiat currency, stablecoins or CBDC. While the trial centers around a bond lifecycle, the workflow and market practice are applicable to security tokens, like tMMFs or Carbon Credits.

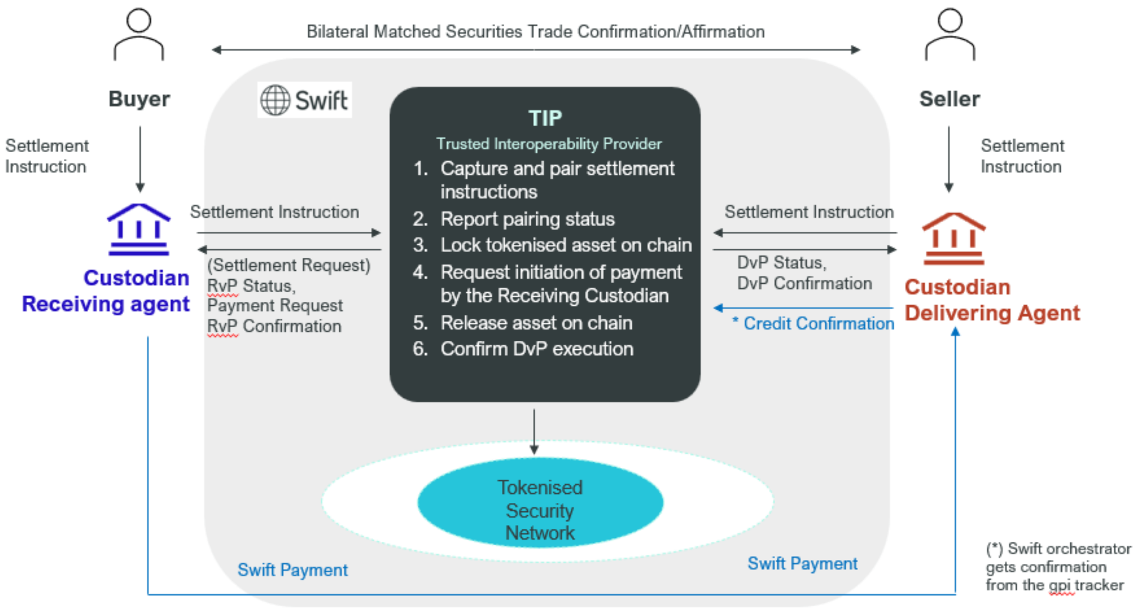

Bilateral Matched Securities Trade Confirmation/Affirmation
Buyer
Seller
Swift
TIP
Trusted Interoperability Provider
1. Capture and pair settlement instructions
2. Report pairing status
3. Lock tokenised asset on chain
4. Request initiation of payment by the Receiving Custodian
5. Release asset on chain
6. Confirm DvP execution
Settlement Instruction
Settlement Instruction
Settlement Instruction
Settlement Instruction
Custodian Receiving agent
Custodian Delivering Agent
(Settlement Request) RvP Status, Payment Request RvP Confirmation
DvP Status, DvP Confirmation
* Credit Confirmation
Tokenised Security Network
Swift Payment
Swift Payment
(*) Swift orchestrator gets confirmation from the gpi tracker

Figure 11: On-chain DvP Securities Settlement with Fiat

Referring to **Figure 11**, the post-trade DvP workflow begins with the submission of settlement instructions by the respective custodians (delivering and receiving agents) on behalf of the seller and buyer. The Delivering agent sends a MT543 (delivering instruction) to the TIP, acting as agent of the Registry owner. Upon receipt, the TIP issues a MT578 (Settlement Allegement) to the Receiving agent, prompting the submission of the corresponding MT541 (receiving instruction).

Once both instructions are received, the TIP validates and pairs them using the Unique Transaction Identifier (UTI) and other key trade details. If successfully matched, the TIP notifies both custodians of the match status via MT548 (Settlement Instruction Status).

The TIP then proceeds to lock the relevant quantity of the digital security (MMF) instrument on the digital settlement execution ledger, ensuring the asset cannot be transferred prematurely. Following this, the TIP initiates a payment activation request (pain.013) to the Receiving agent (or Paying agent if specified), requesting the movement of funds for settlement.

The Receiving agent (or Paying agent) executes the payment by sending a pacs.009 (Financial Institution Credit Transfer) to the Delivering agent, referencing the UETR (Unique End-to-End Transaction Reference) for tracking. Upon receipt of the confirmation of payment, the TIP instructs the digital ledger to unlock and release the previously locked securities to the Receiving agent.

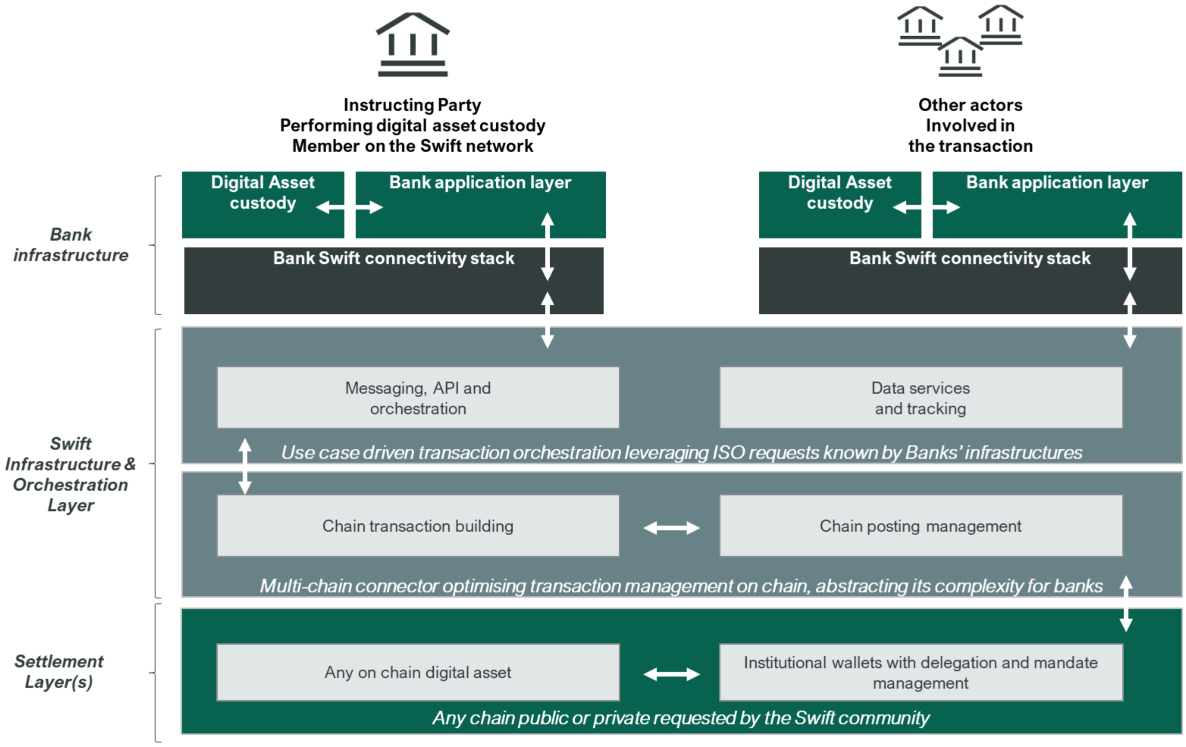
Finally, the TIP sends settlement confirmations: MT547 (Deliver Against Payment Confirmation) to the Delivering agent and MT545(Receive Against Payment Confirmation) to the Receiving agent, indicating successful completion of the DvP process. Copies of these confirmations may also be sent to the Registry owner for record-keeping.

4.4.3 Technology, Infrastructure, Smart Contracts

Supporting this workflow, Swift relies on 3 main layers as shown in **Figure 12**.

- The bank infrastructure is used to perform:
    - Signing of the blockchain related instructions
    - Creating and processing Swift messages (MT54X) required to initiate the settlement instructions.
- The Swift infrastructure is used to:
    - Capture the instructions from banks and convert them into an orchestrated settlement execution flow
    - Validate the mandates received from various parties that authorise the movement, using signed messages or blockchain transactions

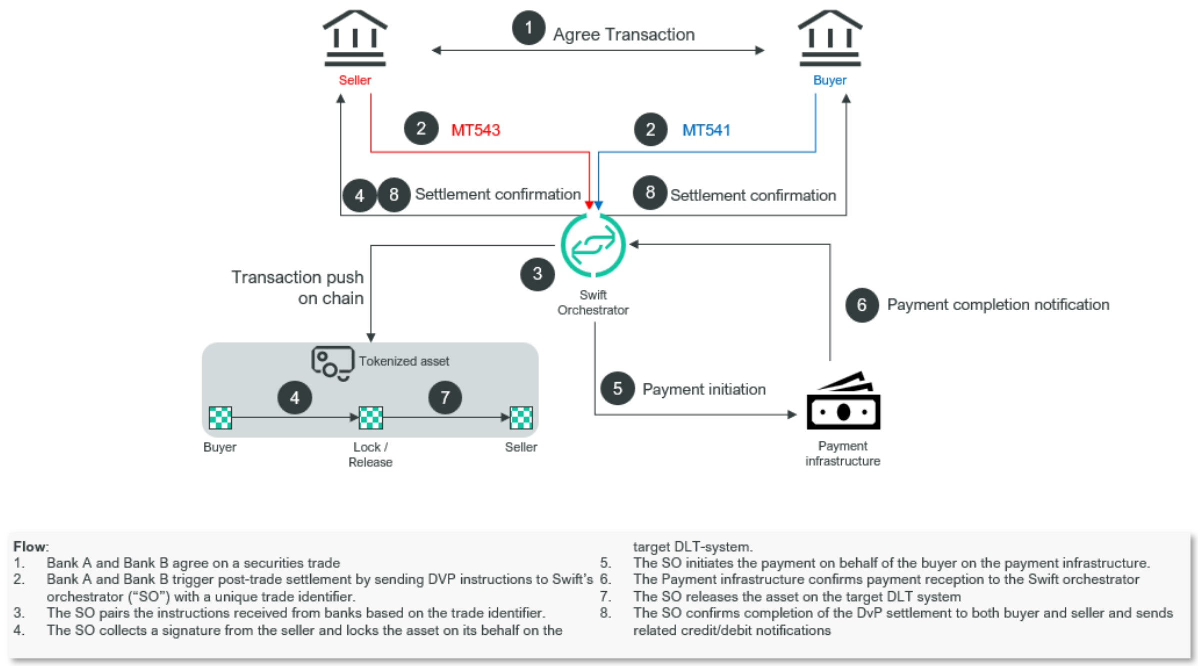
    - Prepare transactions for each settlement system:
        - The asset ledger building required transactions to execute a lock and release orchestration
        - The cash ledger, building the required transactions (digital) or messages (fiat)
    - Execute the requested actions in a structured manner to ensure synchronised DvP settlement across all ledgers.
- The settlement layers are equipped with:
    - Delegation rights granted at token and settlement system level by market participants to Swift as a TIP
    - Smart contracts and other connectivity mechanisms to enable instructions on the ledgers on behalf of market participants
    - Event notifications from assets or ledgers to monitor progress and status of instructed actions



Instructing Party
Performing digital asset custody
Member on the Swift network
Other actors
Involved in
the transaction
Bank infrastructure
Digital Asset custody
Bank application layer
Bank Swift connectivity stack
Digital Asset custody
Bank application layer
Bank Swift connectivity stack
Swift Infrastructure & Orchestration Layer
Messaging, API and orchestration
Data services and tracking
Use case driven transaction orchestration leveraging ISO requests known by Banks' infrastructures
Chain transaction building
Chain posting management
Multi-chain connector optimising transaction management on chain, abstracting its complexity for banks
Settlement Layer(s)
Any on chain digital asset
Institutional wallets with delegation and mandate management
Any chain public or private requested by the Swift community

Figure 12: Three-layered Architecture

With this set-up, the transaction flow that can be deployed across different types of cash legs (fiat or digital, commercial or central bank money) has been successfully performed, as shown in **Figure 13**.



Flow:

1. Bank A and Bank B agree on a securities trade
2. Bank A and Bank B trigger post-trade settlement by sending DVP instructions to Swift's orchestrator ("SO") with a unique trade identifier.
3. The SO pairs the instructions received from banks based on the trade identifier.
4. The SO collects a signature from the seller and locks the asset on its behalf on the target DLT-system.
5. The SO initiates the payment on behalf of the buyer on the payment infrastructure.
6. The Payment infrastructure confirms payment reception to the Swift orchestrator
7. The SO releases the asset on the target DLT system
8. The SO confirms completion of the DvP settlement to both buyer and seller and sends related credit/debit notifications

Figure 13: Transaction Flow

4.4.4 Compliance, Risks and Governance

Swift is dismantling barriers between fragmented digital ecosystems by enabling seamless interoperability across digital assets and currencies. Leveraging its established infrastructure, Swift serves as a single gateway that connects institutions across diverse platforms, technologies, and regulatory environments. This allows them to adopt digital assets while maintaining the reliability of traditional systems and upholding compliance and governance within existing financial frameworks.

By leveraging existing market practices and standards alongside the Swift network and identity framework, institutions achieve backward compatibility with compliance processes and applications. This enables financial institutions' screening engines to access all necessary transaction details, including the identities of participating institutions, within the instruction payload as required by the travel rule.

4.4.5 Operational

To ensure the orchestrated DvP workflow runs reliably across tokenised assets and fiat cash rails, three operating pre-requisites must be in place and actively governed.

- **Ecosystem Participation.** Every participant involved in the settlement flow (e.g., buyer/seller custodians, paying/receiving agents, and the registry owner's agent operating the orchestration/TIP function) must be connected to Swift and able to exchange ISO 20022/15022 messages and/or Swift-exposed APIs. This ensures a common identity, security, and routing fabric and allows institutions to leverage

Swift's existing community reach as a "single window" into multiple settlement systems.

- **Standards Adoption.** All flows running over Swift rely on standardised requests. For securities, participants are using ISO15022 related standards such as MT54x. For payments, participants are using ISO20022 request types such as pacs, pain and camt. All exchanges can be done as APIs or messages. Tracking service relying on UETR is integrated in the solution for end-to-end traceability. The solution builds as much as possible upon existing market practices – adjusted for DLT systems - to maximise STP and reduce integration efforts.
- **Orchestration and Atomicity.** The orchestrator/TIP will only release locked securities after confirmation that funds have been transferred. Delays or missing confirmations stall the process and increase settlement risk.

These new functions should bring benefits across four key areas:

- Interoperability across digital assets and currencies
- Accelerating digital transformation in payments and securities
- Enhancing risk management and compliance
- Driving ecosystem collaboration and innovation

4.5 Integrated Operating Platform and Model (Deutsche Bank DAMA 2 MVP)

4.5.1 Value Proposition and Market Fit

Project DAMA 2 Minimum Viable Product (MVP) is a **Blockchain-as-a-Service platform** designed to support asset and wealth managers in their adoption of regulated tokenised finance.

It offers an integrated suite of tokenisation services with a focus on **multi-chain distribution and post-trade asset and investor operations**, such as custody, investor records and cross-chain aggregation of on-chain records, to streamline the transition to digital finance.

The platform is specifically designed to mitigate challenges associated with vendor fragmentation, manage the risks and costs of initial implementation, address uncertainties inherent in emerging technologies, and accelerate deployment timelines.

Its Blockchain-as-a-Service model minimises the need for in-house blockchain infrastructure, with **hub-and-spoke interoperability** enabling seamless distribution across 80+ chains, reducing liquidity fragmentation and vendor sprawl.

By embedding regulatory controls, digital identity, and composable compliance into the workflow, DAMA 2 **aligns with institutional governance and operational resilience requirements**, positioning itself as a scalable, compliance-ready platform for tokenised assets. The MVP also serves to highlight considerations like legal and settlement finality factors in cross-blockchain transactions to facilitate holistic uses.

DAMA 2's future iterations would include artificial intelligence-assisted construction, deployment and review of smart contracts, for example, Nebula from Third Web for deployment and AI Audit Agent from Netherminds – to further increase the user friendliness and confidence in deploying complex token contracts. The use of a high throughput Layer 2 also lends itself to future possibilities to support agentic AI payments that are high volume and low in (fractional) value.

4.5.2 Product Design

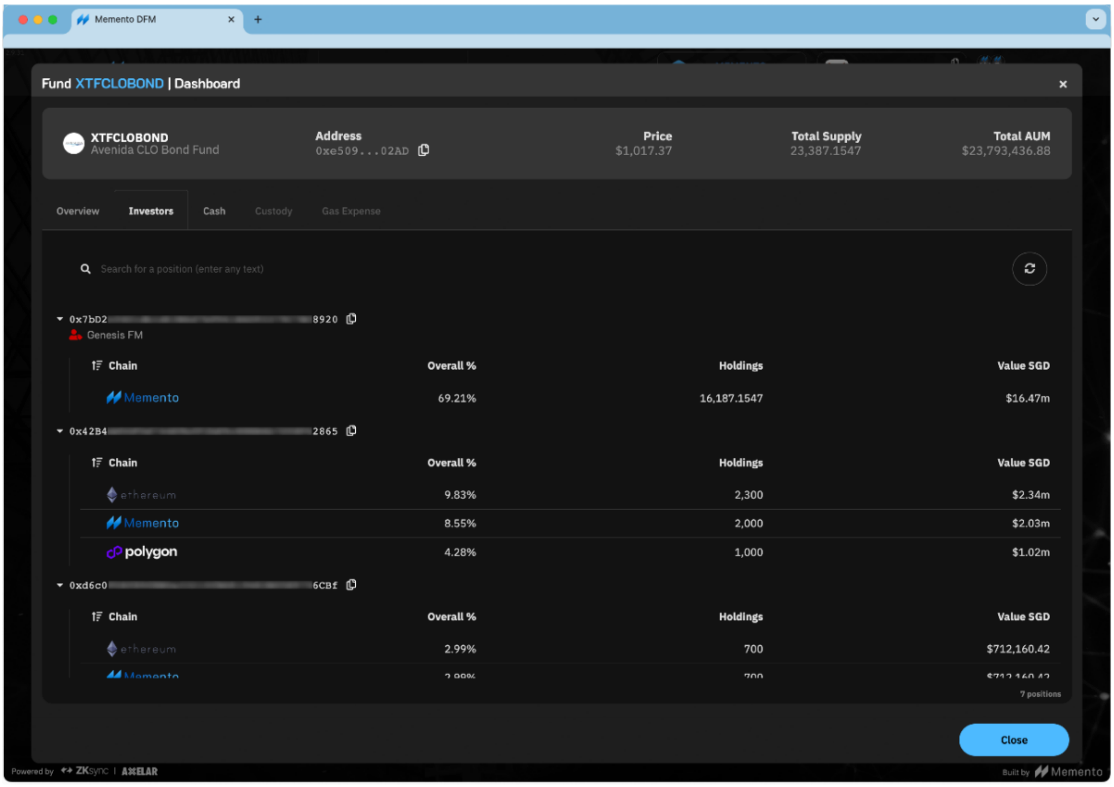
DAMA 2's MVP has incorporated participating asset and wealth managers inputs, and is launched at the Singapore FinTech Festival 2025 using a vanilla tMMF that is:

1. Issued on Memento ZK Chain – a permissioned zero-knowledge L2 for scalability and privacy,
2. Funds tokens are distributed 1:Many (1:M) from the L2 to 3 selected public EVM and non-EVM L1 networks to demonstrate interoperability,
3. With built-in, plug-and-play asset servicing microservices to manage end-to-end fund lifecycles across chains – on-chain subscription, redemption, income distribution, with consolidated asset servicing books of records; and
4. Subscribed using a mimicked stablecoin.

<u>On-Chain Transfer Agency and Investor Recordkeeping</u>

- In the MVP, the investor register is maintained on-chain, with the TA-investor recording function encoded as a smart-contract controller that (a) enforces transfer restrictions; (b) synchronises corporate-action state (subscriptions, redemptions, distributions); and (c) services data exports to custody and fund-admin systems
- An aggregator service will pull all transaction and investor records across the different chains and wallet addresses (**Figure 14**) into off-chain functionalities for issuers/distributors overview. Recent SEC Division of Trading & Markets FAQs

confirm a registered transfer agent may use a blockchain ledger as the official Master Securityholder File[12,13,14], subject to existing obligations.



Fund XTFCLOBOND | Dashboard

XTFCLOBOND	Address	Price	Total Supply	Total AUM
Avenida CLO Bond Fund	0xe509...02AD	$1,017.37	23,387.1547	$23,793,436.88

0x7bD2[redacted]8920
Genesis FM

Chain	Overall %	Holdings	Value SGD
Memento	69.21%	16,187.1547	$16.47m

0x42B4[redacted]2865

Chain	Overall %	Holdings	Value SGD
ethereum	9.83%	2,300	$2.34m
Memento	8.55%	2,000	$2.03m
polygon	4.28%	1,000	$1.02m

0xd6c0[redacted]6CBf

Chain	Overall %	Holdings	Value SGD
ethereum	2.99%	700	$712,160.42
Memento	2.99%	700	$712,160.42

7 positions

Figure 14: DAMA 2 Aggregated Investor Recordkeeping

4.5.3 Legal Structure

Legal Finality and Recordkeeping

- The proofs of transaction records on Memento ZK Chain L2, on the L1s that the tokens are distributed to and on Axelar interoperability bridges are evidence of transaction finality and audit trails, to aid legal enforceability and to meet regulatory requirements.
- The permissioned Layer 2 allows for selective disclosure and privacy, which can help meet data protection and confidentiality requirements.
- Legal agreements and operational service level arrangements would clearly define the roles, responsibilities, and liabilities of the Layer 2 Sequencer and other participants to satisfy regulatory scrutiny.

[12] SEC Division of Trading and Markets FAQs, *"The FAQs address a registered transfer agent's use of distributed ledger technology as its official Master Securityholder File or a component thereof."*

[13] Dechert LLP, "The FAQs confirm that a transfer agent may use distributed ledger technology as its official 'master securityholder file.'"

[14] Simpson Thacher & Bartlett LLP "The FAQs indicate that transfer agents may use blockchain as the official Master Securityholder File, provided records remain secure, accurate, and accessible to the SEC."

- Chapter 2.5 of the report on settlement considerations is relevant to this structure.

4.5.4 Technology, Infrastructure, Smart Contracts

DAMA 2 employs a public-permissioned, multi-layer architecture that combines Ethereum's security with a Memento ZK Chain zero-knowledge Layer 2 for scalability and privacy, and a Layer 3 app store for plug-and-play asset servicing (**Figure 15**).

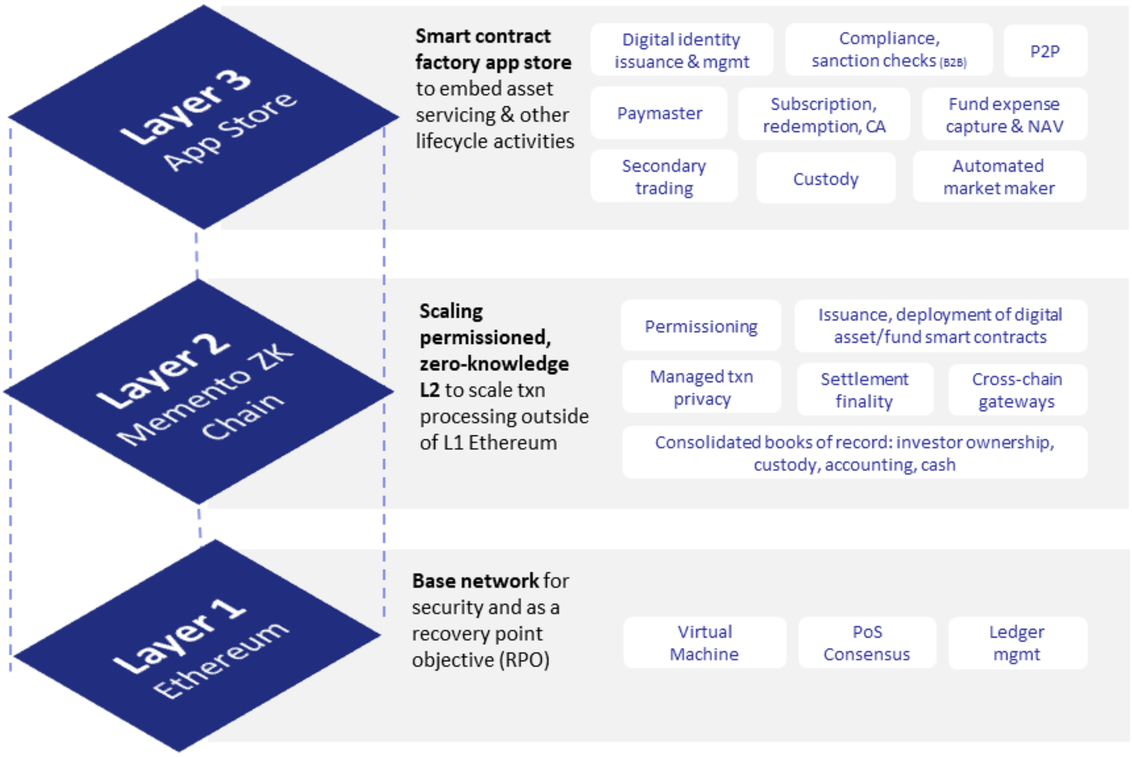

Layer 3
App Store
Smart contract factory app store to embed asset servicing & other lifecycle activities
Digital identity issuance & mgmt
Compliance, sanction checks (B2B)
P2P
Paymaster
Subscription, redemption, CA
Fund expense capture & NAV
Secondary trading
Custody
Automated market maker
Layer 2
Memento ZK Chain
Scaling permissioned, zero-knowledge L2 to scale txn processing outside of L1 Ethereum
Permissioning
Issuance, deployment of digital asset/fund smart contracts
Managed txn privacy
Settlement finality
Cross-chain gateways
Consolidated books of record: investor ownership, custody, accounting, cash
Layer 1
Ethereum
Base network for security and as a recovery point objective (RPO)
Virtual Machine
PoS Consensus
Ledger mgmt

Figure 15: DAMA 2 Layer 1-2-3 Tech Stack

A Public Permissionless Ethereum as Layer 1

- By anchoring its Layer 2 on Ethereum Layer 1, DAMA 2 leverages a base blockchain with a strong track record of security and decentralisation. Ethereum's consensus mechanism (Proof-of-Stake) makes it economically prohibitive for attackers to reorganise the chain or execute a 51% attack, which is critical for legal certainty, on-chain record integrity and investor protection.

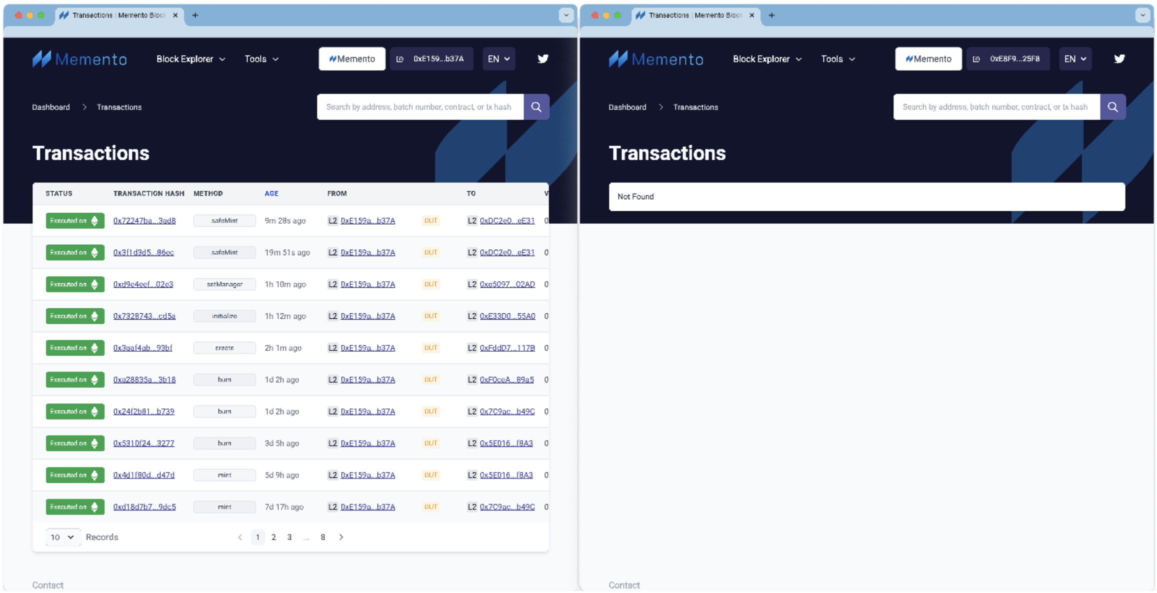
- This anchoring provides a robust technical foundation for legal validity and finality of transactions, which is essential for clear, immutable records of ownership and transfer. In DAMA 2's case, Ethereum acts as a continuity Recovery Point Objective (RPO) where trusted states of transaction integrity on Layer 2 are cryptographically written as proofs on Ethereum.

Routing ZK Proof Commitment to Pre-identified Layer 1 Validators via Private RPC

- To anchor onto Ethereum while ensuring Layer 1 gas fees are not being paid to sanctioned actors, DAMA 2 employs a private Remote Procedure Call (RPC) model to submit ZK proofs directly to trusted L1 relays or block builders, consistent with the work reported in the report ‘From Wallet to Chain’ with Nethermind.

A Permissioned Zero-Knowledge Proof High Throughput Chain

- The capabilities layer is represented by **Memento ZK Layer 2, a permissioned zero-knowledge proof high throughout chain**. This is built on the ZKsync Prividium operating in permissioned Validium mode. This means that execution and state are private; batches are verified on Ethereum using validity proofs while participants’ access is enforced at the application layer. This achieves low-latency confirmation in milliseconds for time-sensitive on-chain fund actions, selective disclosure for audit/regulators, and a deterministic cybersecurity envelope anchored to Ethereum.
- The permissioned Layer 2 is managed by a single, trusted entity (the Sequencer). This setup allows for materially faster transaction processing and privacy, although it introduces a central point of control, governance and due diligence. This centralisation is both a benefit and a risk:
  - **Benefit:** The dual-layer approach (public Layer 1 + permissioned Layer 2) mitigates systemic risks such as consensus attacks, chain reorganisations, and data integrity breaches.
  - **Risks:** It may raise concerns about resilience and single points of failure. The Sequencer will need to satisfy risks controls, transparent governance and insider risks, operational risk controls, and contingency planning.
- **Managed transaction privacy:** Logically separate Layer 2 transaction visibility between each user through dedicated RPC endpoints (**Figure 16**). Where required, regulators can be granted an overview of all transactions for full oversight.


Transactions | Memento Block
Memento
Block Explorer
Tools
Memento
0xE159...b37A
EN
Dashboard
Transactions
Search by address, batch number, contract, or tx hash
Transactions | Memento Block
Memento
Block Explorer
Tools
Memento
0xE8F9...25F8
EN
Dashboard
Transactions
Search by address, batch number, contract, or tx hash
Contact
Contact

Transactions

STATUS	TRANSACTION HASH	METHOD	AGE	FROM		TO	V
Executed on	0x72247ba...3ad8	safeMint	9m 28s ago	L2 0xE159a...b37A	OUT	L2 0xDC2e0...eE31	0
Executed on	0x3f1d3d5...86ec	safeMint	19m 51s ago	L2 0xE159a...b37A	OUT	L2 0xDC2e0...eE31	0
Executed on	0xd9e4eef...02e3	setManager	1h 10m ago	L2 0xE159a...b37A	OUT	L2 0xe5097...02AD	0
Executed on	0x7328743...cd5a	initialize	1h 12m ago	L2 0xE159a...b37A	OUT	L2 0xE33D0...55A0	0
Executed on	0x3aaf4ab...93bf	create	2h 1m ago	L2 0xE159a...b37A	OUT	L2 0xFddD7...117B	0
Executed on	0xa28835a...3b18	burn	1d 2h ago	L2 0xE159a...b37A	OUT	L2 0xF0ceA...89a5	0
Executed on	0x24f2b81...b739	burn	1d 2h ago	L2 0xE159a...b37A	OUT	L2 0x7C9ac...b49C	0
Executed on	0x5310f24...3277	burn	3d 5h ago	L2 0xE159a...b37A	OUT	L2 0x5E016...f8A3	0
Executed on	0x4d1f80d...d47d	mint	5d 9h ago	L2 0xE159a...b37A	OUT	L2 0x5E016...f8A3	0
Executed on	0xd18d7b7...9dc5	mint	7d 17h ago	L2 0xE159a...b37A	OUT	L2 0x7C9ac...b49C	0

10 Records ‹ 1 2 3 ... 8 ›

Transactions

Not Found

Figure 16: L2 Managed Privacy – Comparison of Transaction View between Different Wallets

Open Architecture Wallet Structure

- Participants can integrate their own (pre-approved) wallets or wallet providers to the DAMA 2 architecture. This recognises asset and wealth manager's choice of providers for this service. There is also a default competitive wallet services that users can opt for.

1:M Interoperability Bridge

- **Powered by Axelar**, the interoperability bridge links Layer 2 to over 80 EVM and non-EVM public Layer 1 and Layer 2 blockchains. Its capabilities include flexibility for customised work to link to private chains to minimise liquidity venue fragmentation.

- Additionally, ZKsync provides a native Layer 2 bridge from Memento ZK Chain to other implementation of ZKsync's Layer 2 technologies to act as a 2nd bridge between all ZKsync chains.

- **Interoperability and distribution.** For multichain distribution of fund shares, the MVP standardises on Axelar Interchain Token Service (ITS). ITS manages canonical supply across connected chains, creating token instances with native-like fungibility and a single EVM address per EVM destination chain, under a public validator set and audited contracts.

- This eliminates bespoke bridges for each network hop and supports distribution automation via the ITS Portal. Where distribution targets non-EVM chains, Axelar's message layer abstracts heterogeneity while preserving compliance hooks initiated on DAMA 2. The canonical aggregated register of token ownership remains on DAMA 2; remote instances are pulled and auto-reconciled against the authoritative supply to ensure no under-over mint of tokens.

Paymaster Functionality

- This allows users and treasuries to manage gas fees in fiat money, removing the need to handle cryptocurrencies and the associated regulatory and governance considerations.

Virtual Layer 3 (L3)

This functions as the financial service application and user interface tier, hosting a curated smart-contract "app store" that users can select for fund lifecycle services—subscriptions, redemptions, compliance checks, and corporate actions. This modular marketplace functionality seeks to accelerate time to market while enabling asset managers to compose regulated workflows.

4.5.5 Compliance, Risk and Governance

DAMA 2 architecture supports integration with compliance functions (e.g., AML, sanctions screening) at both the protocol and application layers, which is increasingly expected by regulators for tokenised financial products.

Compliance 'Common Utility.' Reusable and updatable smart contracts implement jurisdictional sanctions/blacklists and counterparty constraints at an industry level that fund contracts can check before transactions and state changes (mint, transfer, redeem). This increases compliance efficiency, concentrates audit trails, and enables rapid rule updates across products and chains – minimising incremental costs of adoption.

Table 3 below further describes how DAMA 2 achieves equivalent regulatory objectives through different technological approaches.

REGULATORY CONCERN	DAMA 2 TECHNICAL SOLUTION	FUNCTIONAL OUTCOMES
Transaction reversal through consensus "51%" attacks	• Battle-tested Ethereum as L1 cryptographic settlement layer and as an **RPO**. • Uses a L2 blockchain that contains transaction records with a centralised sequencer as its expert steward. **Forced inclusions via L1 into L2 are controlled by an access list.**	• Minimise the possibility of consensus attacks by relying on Ethereum. Attacks on Ethereum are a theoretical possibility today, with an estimated $20 billion needed to disrupt finality (more to change transactions), excluding significant financial penalties.
Systemic risks due to obstruction of settlement finality	• The point of **settlement finality** on L2 is **defined legally** and takes precedence, e.g., on transfers.	• Settlement finality achieved via legal agreements, technology choice and billions in economic guarantees (L1).

Market abuse, e.g., MEV Frontrunning	• **No public mempools in L2**, preventing Maximum Extractable Value (MEV) attacks. • **Directed Order Flow** allows asset managers to interact with private mempools, whitelisted buildrs, relayers & proposers on L1 for frontrunning protection.	• MEV attacks cannot occur on L2 as it uses a trusted, centralised sequencer. • Directed order flow on L1 ensures transactions are only visible & processed by whitelisted actors
Transaction privacy	• L2 transactions are validated by a trusted, centralised single sequencer. • **Prividium** – specialised RPC endpoints enable logical separation of transactions visible to each user, while retaining the ability for "super users" like regulators to view all transactions. • **Zero-knowledge proof** for a batch of transactions submitted to L1 without revealing details of each txn. • **Confidential data** such as personally identifiable information (PII) are **stored off-chain**, with on-chain tokens bearing pointers to the off-chain information.	• Privacy of L2 transactions is preserved through customised user entry points (RPC), access controls and logical separation of data visible to each user, and shielded from L1 validators using cryptographic techniques.
Validator technology risk management	• L2 is operated and secured by a trusted, centralised single sequencer and would satisfy this requirement. • Direct interactions with L1 can be routed via **Directed Order Flow** to whitelisted builders, relayers, proposers. • Axelar's best-in-class validator security includes **quadratic voting** and **periodic validator key rotations**.	• Cybersecurity risk management achieved via either identification/due diligence or large pool size of validators to ensure robustness.
Zero-day vulnerability defenses	• L2 is operated by a trusted, centralised single sequencer and would manage its speed of response via **agreed SLA** and best practice standards. • L1 Ethereum is built to foster **validator diversity**: there is no single validator software. • Axelar connectivity delivers layered risk management: **hub-and-spoke mitigation, custom Verifier sets, open-source code, permissionless validator set.**	• L2 speed of fix driven by SLA and best practices. • Decentralised and diverse validator sets avoid single points of failure and prioritises liveness.
Gas payments to undesirable validators	• L2 uses a trusted, centralised sequencer. • L1 gas payments are traceable. Through **directed order flows**, gas can be paid only to known validators. • Axelar connectivity can be secured by a defined set of **permissioned Verifiers**—with underlying governance and verification proofs secured by a decentralised set of 75 validators.	• Sanctions compliance and Counter-Terrorist Financing (CTF) achieved via technological means.

Table 3: DAMA 2 Technical Solution and Regulatory Functional Outcomes

4.5.6 Operational

In the unlikely event of an attack on Ethereum as Layer 1, DAMA's Layer 2 Memento ZK Chain would continue the following as normal:

- Transactions continue with immediate transfers between transaction participants and/or smart contracts.
- Technical settlement finality (no transaction reversal) is safeguarded by the single trusted sequencer
- Sequencer can run multiple nodes to ensure continuous availability and prevent single point of failure.
- Legal terms and conditions add further administrative safeguards against unauthorized reversals, like traditional industry post-trade settlement agreements.
- Off-chain data is not impacted by the Layer 1 attack and is not at risk of being breached

The key impacts to Layer 2 are as follows:

- Proofs (as RPOs) are not written from Layer 2 to Layer 1 until Ethereum recovers and reverts the malicious blocks (after which the Memento ZK Chain can realign with the honest chain).
- Should Ethereum be irreversibly corrupted, the ZKsync Stack could be configured to use a different EVM-compatible Layer 1 chain to continue publishing verifiable state changes.
- Axelar is built on a hub-and-spoke network topology that allows compromised blockchain connections to be quickly isolated until normal blockchain operation has been restored, limiting cross-chain contagion of security breaches.

5. Analysing the Opportunities and Risks

The preceding chapters have illustrated how the future of tokenised asset management is being shaped through innovative use cases.

Each example has highlighted different facets of digital asset settlement, from primary issuance and multi-chain distribution to secondary market trading, programmable FX swaps, interoperability and post-trade lifecycle orchestration. Building on these practical experiences, it becomes clear that the design of DvP platforms—whether public, private, hybrid, or isolated—fundamentally influences both the opportunities and risks faced by market participants.

The following illustrative Opportunities-Risks Matrix and discussions aims to contribute to users' awareness of the trade-offs.

5.1 Risk-Opportunity Trade-offs in DvP Smart Contract Models

Figure 17 provides a matrix that frames the landscape of on-chain finance in terms of risk and opportunity associated with DvP models across different smart-contract platforms. On-chain settlement asset enables atomic settlement and DvP, eliminating the need for multiple actions or assets to move off-chain. The strongest opportunities lie in systems that combine the robustness, 24/7 uptime, and global scale of public networks with the control of private or whitelisted networks, integrated via a non-custodial connectivity layer.

In such models, compliance can be pushed to the endpoints, enabling products that span jurisdictions while reducing settlement and counterparty risk. By removing custodial intermediaries at the connectivity layer, these architectures mitigate insolvency or mishandling of funds, while supporting global DvP at scale.

In the context of DvP, opportunities extend to financial "super apps" that connect tokenisation, trading, and yield with payments and banking.

High Risk, High Opportunity Connected, public DvP platforms. Global liquidity and innovation, but with significant exposure to regulatory, technical, and settlement risks	**Low Risk, High Opportunity** Hybrid DvP platforms. Private-public configurations with non-custodial connectivity, supporting programmable compliance and global scale
High Risk, Low Opportunity	**Low Risk, Low Opportunity**

Isolated, public DvP platforms. Atomic settlement possible, with limited adoption, fragmented liquidity, and high exposure to technical and market risks	Isolated, private DvP platforms. Controlled settlement environment, but minimal scale, liquidity, or cross-market utility

Figure 17: Risk-Opportunity Matrix

Opportunities

- 24/7 global atomic settlement of tokenised assets via DvP
- Reduced settlement risk and transaction costs through on-chain settlement asset as settlement currency
- Programmable compliance embedded in DvP workflows across markets
- Composability between payments, trading, and collateral management through DvP infrastructure
- Faster time to market for new financial products that rely on instantaneous settlement

Risks

- Unclear on-chain settlement finality rules across multiple jurisdictions can create uncertainties over investor rights
- Liquidity fragmentation between blockchain networks limiting atomic settlement at scale
- Technology failures, including in the Cloud infrastructure stack, disrupting DvP processes and finality
- Cybersecurity breaches targeting settlement logic in smart contracts

5.2 Open Architecture Custody / Wallet Architecture

As tokenised finance continues to evolve, asset managers and institutional investors are increasingly faced with a critical decision: how to manage digital asset custody in a way that balances user control, operational efficiency, and regulatory compliance. From self-custody wallets to appointed custodians and default wallet solutions, each approach offers distinct advantages—and exposes users to different risks.

Understanding these trade-offs is essential for building resilient, scalable, and user-friendly digital asset strategies.

Self-Custody Wallets

Self-custody wallets, also known as non-custodial wallets, place full control of digital assets in the hands of the user. This model is particularly attractive to asset managers seeking to capitalise on the speed and flexibility of decentralised finance (DeFi). By connecting directly to decentralised networks through dedicated RPC proxies, users can access tokenised markets, execute trades, and manage yield strategies without relying on intermediaries. Role-based access controls and decentralised validation mechanisms ensure that transactions are secure and compliant, while Paymaster services can sponsor gas fees to streamline user experience.

The benefits of self-custody are clear: faster go-to-market, 24/7 uptime, and global scalability. More importantly, self-custody preserves asset segregation by design—no intermediary ever holds principal, reducing exposure to counterparty risk. Regulatory analyses, such as those from Interop Labs and Rozovsky & Cohen[15,16], highlight how non-custodial systems can embed compliance logic at the protocol level, enabling KYC, AML, and sanctions enforcement without compromising user control[17,18].

However, self-custody is not without its challenges. The top three risks include:

- **Key Management Risk**: Users are solely responsible for safeguarding their private keys. Loss or compromise of these keys can result in irreversible asset loss.
- **Operational Complexity**: Managing self-custody wallets requires technical proficiency, including understanding transaction signing, network fees, and wallet security practices.
- **Limited Recourse**: In the event of errors or fraud, users have limited avenues for recovery, as there is no intermediary to provide restitution or dispute resolution.

Appointed Custodians: Institutional Oversight and Operational Support

For institutions with their digital-ready regulated custodians, these custodians can plug into platforms such as DAMA 2 to manage the users' private keys, provide insurance coverage, and offer integrated services such as compliance reporting, auditing, and settlement support. This model aligns with the user's existing regulatory frameworks, operational continuity and fiduciary oversight.

[15] Interop Labs. (2024). Programmable Interoperability: The Key to Standardisation in Regulating Tokenised Assets. Elevandi Knowledge Hub, Point Zero Forum 2024.

[16] Rozovsky, J., & Cohen, L. R. (2024). The New Regulatory Paradigm: How Decentralised Systems Will Improve Financial Oversight. Axelar Network.

[17] Interop Labs. (2025). Response to the SEC Crypto Task Force RFI. U.S. Securities and Exchange Commission.

[18] Rodrigue, J-P. (2020). The Geography of Transport Systems: Point-to-Point versus Hub-and-Spoke Networks. Hofstra University.

Appointed custodians mitigate several risks associated with self-custody, but they introduce their own set of considerations:

- **Counterparty Risk**: Entrusting assets to a third party introduce exposure to the custodian's financial health and operational integrity.
- **Latency and Friction**: Intermediated processes can introduce delays in transaction execution and settlement, potentially limiting responsiveness in fast-moving markets.
- **Cost and Complexity**: Custodial services often come with significant fees and contractual obligations, which may not be suitable for all asset managers or use cases.

Platform Default Wallet

Platform wallets offer a plug-and-play experience that appeals to users seeking simplicity. These wallets abstract away the complexities of key management and transaction signing, enabling quick onboarding and seamless integration with platform services. For new entrants or low-risk use cases, default wallets can serve as a practical entry point into tokenised finance.

Yet, this convenience comes with trade-offs:

- **Custodial Dependence**: Default wallets are usually custodial, meaning the platform holds the private keys. This centralisation can expose users to platform-specific risks, including hacks or insolvency.
- **Limited Portability**: Assets may be locked within the platform's ecosystem, reducing flexibility and interoperability with external networks or services.
- **Opaque Governance**: Users may have limited visibility into how their assets are managed or how compliance policies are enforced, which can be problematic in regulated environments. Hence, platform operator's transparency and governance standards are of utmost importance

5.3 Choosing the Right Model – Context Matters

Ultimately, the choice between self-custody, appointed custodians, and default wallets depends on the user's risk tolerance, technical capability, regulatory obligations, and operational needs. Self-custody offers unmatched control and transparency but demands technical discipline. Appointed custodians provide institutional-grade safeguards at the cost of agility. Default wallets offer ease of use but may limit autonomy and introduce platform risk.

For asset managers navigating tokenised finance, a hybrid approach may offer the best of all worlds—leveraging self-custody for high-frequency trading, custodians for long-term holdings, and default wallets for onboarding and experimentation. As the ecosystem matures, the ability to flexibly switch between custody models—without compromising security or compliance—will be a defining feature of successful digital asset strategies. Risks analysis and management with the right expertise and team continues to be an important facilitative factor of such competitive flexibility.

6. The Road to Scalability and Adoption

Digital assets face significant challenges on the path toward scalable adoption in financial markets. While scalability is an innate feature of blockchains, its application to regulated capital market products raises considerations around regulatory compliance, operational requirements and interoperability.

The section below will focus on the immediate milestones that need to be addressed for digital asset implementations to become more digitally native and scalable.

Building Network Effects for Onboarding and KYC

Mainstream adoption of digital assets necessitates efficient participant onboarding and compliance with regulatory obligations such as Know-Your-Customer (KYC), Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), and sanctions regimes. While this section is not meant to dive specifically into these requirements, efforts around on-chain identification can be grouped into the following:

- **Allow-listing.** Existing implementations predominantly rely on *whitelisting wallet addresses* individually. This method leverages existing onboarding KYC models while requesting for the client's wallet address that is added into the allowlist.

- **Digital identity.** There is limited commercial deployment of *verifiable credentials* – digital attestations of identity or compliance status that can be proven without revealing the underlying data. This model introduces a distribution of trust amongst participating members in screening and onboarding other participants. An effective governance model is required to integrate verifiable credentials into the onboarding process, assigning responsibility for credential issuance, validation, revocation, and dispute resolution among stakeholders.

Integrating to Existing Operational Requirements

Fund managers today are taking steps to explore moving parts of the fund lifecycle on-chain for operational efficiency as seen in the case study section above, but a full digitally native ecosystem is still on the horizon. Tokenised funds today still require on/off-chain coordination across functions which may still be traditional such as custody, transfer agency and fund administration, and across jurisdictions depending on the domicile of the fund.

As we move towards a digital native ecosystem, digital asset platforms must ensure that token issuance, investor record maintenance, subscriptions, redemptions, and corporate actions can be performed efficiently, while bringing additional value exceeding that of existing established industry processes and regulatory obligations.

Addressing the Delta in Operational Risks

The transition from traditional systems to digital asset infrastructures introduces a new layer of operational risks that differ substantially from those in conventional financial environments. Smart contracts facilitate majority of the activity on blockchains, and naturally this includes the reliance on smart contract code for core functions especially in public environments where it is published and transparent. More broadly, this extends to the complexities of digital custody and key management, and new forms of settlement risks linked to blockchain consensus mechanisms.

- **Smart contract risks.** Upgradeability introduces both flexibility and risk—robust governance and controls are necessary to ensure only authorised parties can make upgrades. Asset issuance and burning (redemption) processes must include strict access controls and audit trails.
- **Digital custody risks.** Secure wallet and key management practices are critical, encompassing access controls, multi-signature wallets, and use of MPC (multi-party computation) technologies.
- **Business continuity planning (BCP).** Disaster recovery protocols must be established to handle potential infrastructure or network failures, including but not limited to avoiding single points of failure, setting clear RTO/RPO, maintaining redundant, independently operated components, and regularly validating backups and failover.
- **Settlement risks.** In the use of public blockchains, probabilistic settlement can be a challenge given that settlement is only final when consensus and finality is reached, before immutability happens.

Interoperability Across Digital Assets

Commercial adoption of tokenised finance increasingly revolves around multi-chain distribution, enabling issuers to reach diverse liquidity pools across interoperable networks.

Cross-chain asset servicing supports seamless lifecycle management of tokenised instruments, while tokenised collateral use-cases—such as margining, repo, and structured finance—unlock capital efficiency. Additionally, digital assets across networks facilitate instant settlement and programmable payments, bridging traditional and decentralised ecosystems. Underpinning these innovations are robust technical standards, for example cross-chain communication protocols combined with oracle APIs that ensure reliable data exchange.

Data formats like ISO 20022 and the Common Domain Model (CDM) standardise messaging for interoperability and API specifications. Such technical standardisation allows varying smart contract interaction to custody and settlement, and to enable modular integration. Ongoing work by the FIX community as well as leading Web3 firms like Netherminds on integrating FIX standards into smart contracts would add a global trading standard as a universal financial messaging layer to bridge TradFi, DeFi, and tokenized markets across asset classes — equities, bonds, derivatives, loans, funds and even structured products. Standardisation remains an important piece of work for blockchain to reach the equivalent of the "SMTP[19]" interoperability moment in email.

Security and compliance are reinforced through privacy-preserving cryptographic protocols such as zero-knowledge proofs, which validate conditions without disclosing sensitive values. While quantum computing looms in the horizon, blockchain's encryption and multi-signature schemes should be able to delay early attacks to offer a level of partial resistance as a start. Its cryptographic upgradability to be post-quantum computing resistant is its real defence, although potentially more of a community-technical challenge – hard forks, consensus changes, key migrations, etc – that needs to already be considered in parallel with the regulated financial services growth and use of blockchains.

Finally, smart contract standards—ERC and EVM-compatible frameworks—provide the foundational logic for composability and cross-network operability.

Ease of Adoption and User Experience

Over recent years, much effort has focused on areas such as throughput, key management, consensus, interoperability, and programmability. While technical innovation remains essential, wider and sustainable integration requires an equal focus on usability and user experience.

- **Onboarding and User Experience:** Clear, intuitive sign-up, identity, and key/recovery flows that non-experts can complete; interfaces and abstractions that hide protocol complexity while preserving required controls.
- **Integration Cost:** Standardised APIs/SDKs, reference architectures, and compatibility with existing enterprise stacks and data models.
- **Security and Compliance by Design:** Controls for custody, segregation of duties, data protection, and regulatory reporting embedded into workflows.
- **Interoperability and Portability:** Reliable movement of assets/messages across networks and vendors

[19] SMTP established the universal language for emails between different domains and servers.

7. Conclusion

The journey from tokenisation pilots to production-ready solutions represents a pivotal moment in the evolution of asset and wealth management. This report has demonstrated that the foundational elements for successful tokenisation – robust legal frameworks and structures, proven technology solutions, and clear operational models – are no longer theoretical constructs but practical realities being implemented by leading institutions globally.

The legal structures examined in this report provide institutional participants several important considerations such as ownership models, regulatory compliance, investor protection and operational risks. The legal considerations surrounding interoperability, particularly the complexities of cross-chain distribution and settlement finality, underscore the importance of establishing clear jurisdictional frameworks before scaling operations.

The report included implementations by Franklin Templeton, Phillip Securities, Fidelity, Citi, Swift, and Deutsche Bank, which demonstrated that tokenised funds are not merely conceptual but operational realities delivering tangible benefits. These implementations demonstrated enhanced efficiency, reduced settlement risk, and new revenue opportunities whilst maintaining the rigorous standards that institutional investors demand. The diversity of approaches also proved that tokenisation can be adapted to various business models and regulatory environments.

Furthermore, the relationship between settlement assets and tokenised funds creates a powerful network effect that accelerates adoption. As more assets move on-chain, the value proposition for tokenised vehicles strengthens, attracting traditional financial institutions to launch digital offerings and access new investor pools. This ecosystem effect accelerates the maturation of the entire digital asset landscape.

The scalability enablers identified – streamlined onboarding, robust risk controls, technical standards, and enhanced user experience – represent achievable milestones rather than distant aspirations. Early movers who address these elements systematically will establish competitive advantages that compound through network effects.

The infrastructure is operational. The legal frameworks are established. The business case is proven. The question facing market participants is no longer whether tokenisation will transform asset and wealth management, but how quickly they can adapt to capture its benefits.

8. References

3. Tokenisation in the context of money and other aspects: concepts and implications for central banks, BIS, CPMI, October 2024. https://www.bis.org/cpmi/publ/d225.pdf

4. Distributed ledger technology in payment, clearing and settlement: An analytical framework, BIS, CPMI, February 2017. https://www.bis.org/cpmi/publ/d157.pdf

5. Section 7, Payment and Settlement Systems (Finality and Netting) Act 2002.

6. Central Depository (Pte) Limited (CDP)'s PMI Disclosure Brochure (Dec 2023) at https://api2.sgx.com/sites/default/files/2023-12/628136%20SGX%20PMI%20Disclosure%20Brochure%20CDP%20MT6.pdf.

10. From ripples to waves: The transformational power of tokenising assets, McKinsey, June 2024.

11. Who borrows from money market funds?, BIS Quarterly Review, Dec 2023.

13. Standard Chartered / Synpulse, Real-world asset tokenisation: A game changer for global trade, July 2024.

14. Dec 2024, 'Eurosystem completes tests using DLT for central bank money settlement'

15. McKinsey estimates tokenization will be less than $2 trillion by 2030, June 2024.

18. Interop Labs. (2024). Programmable Interoperability: The Key to Standardisation in Regulating Tokenised Assets. Elevandi Knowledge Hub, Point Zero Forum 2024.

19. Rozovsky, J., & Cohen, L. R. (2024). The New Regulatory Paradigm: How Decentralised Systems Will Improve Financial Oversight. Axelar Network.

20. Interop Labs. (2025). Response to the SEC Crypto Task Force RFI. U.S. Securities and Exchange Commission.

21.Rodrigue, J-P. (2020). The Geography of Transport Systems: Point-to-Point versus Hub-and-Spoke Networks. Hofstra University.

Annex A: Case Study on Cross-Border Offering Considerations in the UK

A. Regulatory Classification and Jurisdictional Compliance

The UK's regulatory framework for licensing of cryptoasset providers is currently undergoing major change, as new legislation has been proposed which, once enacted, will overhaul the current regime.

Under the current UK framework, a tokenised fund unit is likely to be regulated in a manner similar to traditional funds and securities, meaning that all related regulatory implications – including those concerning authorisation, distribution, marketing, and investor protection – will apply.

Overview of the current regime

The principal legislation governing cryptoassets is the Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 ("**MLRs**"). The MLRs require cryptoasset exchange providers and custodian wallet providers to register with the Financial Conduct Authority ("**FCA**") for anti-money laundering ("**AML**") purposes. Depending on the nature of the token and the activities involved, AML registration may be required even if a firm is already authorised by the FCA under other licensing regimes.

Outside of the MLRs, cryptoassets fall within scope of regulated products only where they have the characteristics of another specified or regulated instrument, but such cryptoassets will be regulated as that instrument. For example, cryptoassets that are securities (i.e. security tokens) will generally be regulated under the Financial Services and Markets Act 2000 ("**FSMA**") as a specified investment listed under the FSMA (Regulated Activities) Order 2001 ("**RAO**"). Depending on the relevant settlement mechanisms, other regulatory frameworks may also be applicable (e.g. for payment services).

A fund token could be considered a unit in a CIS or a share (if structured as shares in a closed-ended company) – both of which are specified investments regulated under the RAO. It is also possible for tokenised funds to be characterised as alternative investment funds ("**AIF**"). Undertaking specified regulated activities in respect of such tokens may therefore require FSMA authorisation.

In respect of distribution and marketing activities (further discussed below), fund tokens could fall within scope of certain marketing restrictions and requirements applicable to specified investments and AIFs. If the fund tokens are characterised as a transferable security, the offeror would also need to consider prospectus requirements and exemptions.

We note that a future regime is proposed for the regulation of cryptoassets in the UK, including the regulation of stablecoins as a distinct asset. HM Treasury has consulted on near-final legislation to create new regulated activities, to be incorporated into the FSMA framework via amendments to the RAO. These activities will include, for example, dealing in qualifying cryptoassets, arranging deals, operating trading platforms, safeguarding, and staking. Subject to finalisation and further regulatory guidance, under this framework, fund tokens are like to be treated as a "specified investment cryptoasset" – this is a new type of regulated asset though it will likely be regulated in much the same way as a traditional fund unit/investment.

When considering cross-border offerings, it is therefore essential to assess the appropriate regulatory classification of the tokenised fund/fund unit, and ensure that all necessary licences or authorisations are obtained (or that appropriate exemptions apply), in every country where the fund is marketed or made available.

B. Cross-Border Distribution of Tokens

For overseas funds, there are several key considerations that would impact on the ability to distribute or market fund tokens with different classes of investors in the UK. The position will also need to be reassessed once the UK's future cryptoasset regime is fully developed.

FSMA authorisation

If the tokenised fund or fund units are treated as specified investments (e.g. CIS units), there are certain FSMA regulated activities that are likely to be triggered in respect of e.g. managing the fund, or (when distributing fund tokens in the UK) dealing in or carrying out arranging / advisory activities in respect of fund tokens.

Firms carrying on fund activities or offerors of fund tokens based outside of the UK could seek to rely on certain licensing exclusions for "overseas persons" (subject to an assessment of UK nexus). Importantly, this typically only applies where (a) the overseas person deals with or through a UK-authorised firm or (b) in the case of reverse solicitation or the person otherwise complies with the UK financial promotions regime (see below).

Unless the fund is itself authorised or recognised as some form of regulated fund that can be marketed to retail investors, compliance with the UK financial promotions regime may entail reliance on certain exemptions that are likely to limit the target investor base to institutional investors or large corporates, and it would be challenging to offer fund tokens widely to a retail investor base.

Similarly, if an FCA-regulated intermediary is used to market fund interests in the UK, the intermediary will be required to comply with certain restrictions from promoting unregulated funds in the UK – the effect of which is that investment firms generally may not be able to market such fund tokens unless it is to persons who are categorised for such purposes as professional clients or eligible counterparties (i.e. not retail investors).

UK financial promotion regime

As noted above, any marketing to UK investors (including from overseas) must be conducted by an authorised firm, unless the communication is approved by an authorised firm with the relevant permissions, or an exemption under the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 ("**FPO**") applies. Unauthorised firms offering interests in overseas funds commonly restrict marketing to large corporates and institutional clients to rely on FPO exemptions, with appropriate disclaimers. The parameters of exemptions that could potentially be used in respect of retail investors and natural individuals are relatively narrow and require detailed assessment.

AIF marketing

As noted above, a tokenised fund could also be characterised as an AIF. For non-UK AIFs, the marketing restrictions pursuant to the Alternative Investment Fund Managers Regulations 2013 (the "**UK AIFMRs**") mean that fund units (i.e. fund tokens) in such tokenised funds may generally only be marketed via the National Private Place Regime ("**UK NPPR**"), which requires a filing to be made to the FCA.

AIFs registered under the NPPR can only be marketed to professional investors (i.e. certain authorised firms, large undertakings, institutional investors, as well as retail clients that "opt up" to be treated as professional clients subject to certain criteria). In addition, AIF managers will need to comply with requirements under the UK AIFMRs, which includes certain investor disclosure requirements, as well as ongoing notification and reporting obligations.

Retail distribution

Most investment funds that can be marketed to retail investors in the UK are UK UCITS (undertakings for the collective investment in transferable securities), which are investment funds authorised under the UK onshore version of the UCITS Directive (2009/65/EC). It is a relatively onerous process to obtain authorisation as a UK UCITS.

For overseas funds,[20] the Overseas Funds Regime ("**OFR**") is a new gateway to allow certain non-UK investment funds to be promoted in the UK, including to retail clients. If a fund applies for and is given 'recognised scheme' status under the OFR, it can be promoted in the same way as a UK authorised CIS. As an initial step, the HM Treasury will

[20] There are other routes through which overseas funds can be promoted to retail investors in the UK, though these are relatively complex or onerous and will need to be assessed in detail. For example, an overseas fund can also apply under section 272 of FSMA for recognised status – unless such fund is eligible for the OFR.

need to make equivalence determinations for a particular country – i.e. that another country's regime for investment funds is equivalent to the UK regime – after which an investment fund domiciled in that country may apply to the FCA for recognition. The OFR comprises two separate equivalence regimes for retail investment funds and MMFs – however, we note that no equivalence decision has been made in the UK relating to MMFs yet.

Prospectus requirements

A prospectus is generally required when transferable securities (which could in principle include e.g. fund tokens of tokenised funds structured as a closed end CIS) are offered to the UK public or admitted to trading on a UK regulated market. There are certain prospectus exemptions that depend on the nature of the investor (e.g. where offers are made only to "qualified investors", a class of non-retail investors), as well as other investors that depend on the number of offerees, minimum investment per investor, etc.

C. Multi-listing for Multi-Chain/Cross-Chain Distribution

In the UK, fund tokens could in principle be listed on digital-native exchanges/platforms and traditional stock exchanges, provided that each participating entity (whether e.g. the relevant exchange, issuer or service provider) holds the required authorisations and/or registrations.

There is clearly growing interest in fund tokenisation, with market participants and infrastructure providers exploring the potential for multi-listing of tokenised fund units across different venues and blockchain networks. In September 2025, the London Stock Exchange Group launched a blockchain-based platform for private funds and facilitated its first transaction.

However, the practical implementation of multi-listing for tokenised funds remains at a nascent stage and key issues like settlement finality in particular will need to be carefully considered.

In the UK, the Digital Securities Sandbox ("**DSS**") – launched by the Bank of England and the FCA – provides a regulated live environment for financial market infrastructures to test how emerging technologies can be used for notary, maintenance, and settlement of financial securities, either independently or alongside the operation of a trading venue. For example, the DSS enables the issuance, trading, and settlement of digital securities on distributed, programmable ledgers, subject to ongoing regulation by both the FCA and the Bank of England. It should be noted that the DSS provides a temporary exemption to the cryptoassets framework in the MLRs, so that engaging in DSS activity does not in itself make a firm a cryptoasset exchange provider or a custodian wallet provider under the MLRs.

If settlement of tokenised fund units occurs within the DSS, Digital Securities Depositories (“**DSDs**”) are not currently required to be designated under the Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (“**SFRs**”), though this may change under a future permanent regime. The current SFRs framework is designed to provide legal certainty for the finality of settlement in designated payment and securities settlement systems, by setting out the circumstances in which a transfer or settlement is deemed final within a designated system and cannot be unwound or reversed, which has key implications in the event of insolvency, among other considerations. Without SFR designation, DSDs will need to fall back on the contractual provisions or platform rulebook that determine when a transaction is final. In this regard, insolvency proceedings could potentially unwind transactions in a DSD’s system, regardless of any contractual or rulebook provisions to the contrary.

Participants of a DSD should therefore take this into account when choosing to engage with a DSD. A DSD will be expected to inform users if it is not a designated system and must disclose the rules governing finality. Contractual arrangements will need to specify how finality works in these circumstances, particularly where there is a discrepancy in settlement confirmation between layers.

Where settlement for tokenised funds takes place within the DSS, Delivery versus Payment (DVP) settlement must be permitted, and contractual arrangements must establish the point of finality. DSDs will also be subject to risk management, reconciliation, conflict of interest management, governance, and client protection obligations.

D. Anti-Money Laundering (AML) / Know Your Customer (KYC), Financial Crime and Data Privacy Requirements

UK-authorised fund managers, distributors and other service providers in relation to tokenised funds will need to meet the full spectrum of regulatory obligations under the MLRs and other FCA rules and requirements, including customer due diligence (CDD) and KYC, ongoing monitoring, and suspicious activity reporting, as well as the Travel Rule as it applies to in-scope cryptoassets.

In terms of generally applicable requirements (that are relevant also to entities that are not licensed by the UK financial regulators), key UK financial crime-related legislation include the Criminal Finances Act 2017, which among other things sets out corporate offences of failure to prevent facilitation of tax evasion and the Proceeds of Crime Act 2002 ("**POCA**"), the Terrorism Act 2000 and Sanctions and Anti-Money Laundering Act 2018 which can have broader extraterritorial application, as well as various sanctions regimes under the UK framework. In particular, POCA sets out certain primary money laundering offences (relating to concealing, aiding and abetting the retention/use/control of, and handling proceeds of crime), and also criminalises the failure to report and tipping off when discovering suspicious payments.

Where transactions with UK nexus (for example, because a UK client is involved) trigger substantive suspicions of criminal activity, a firm will need to consider and take advice on whether the relevant UK financial crime legislation may be engaged (noting that this is likely to be a fact-specific case-by-case analysis, in particular with the complexities surrounding territoriality in the context of blockchain-based transactions).

Firms should in particular ensure that there are appropriate on-chain controls – e.g. smart contracts to enforce compliance rules (transfer restrictions, investor type eligibility, jurisdictional constraints) and on-chain monitoring to enhance oversight of blockchain-based transactions (tracking, anomaly detection), as well as appropriate audit trails and record-keeping. KYC processes should capture and verify the identity of beneficial owners, not just intermediaries or nominees. Where third-party service providers (e.g., custodians, distributors) are involved, firms should ensure that these parties also meet equivalent AML/KYC standards.

Fund managers, offerors, and distributors must also ensure that their activities comply with applicable data privacy laws and that personal data is handled appropriately. In the UK, the primary legislation governing this area is the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

E. Tax Reporting Obligations

Taxpayers need to keep records of transactions involving cryptoassets, in order to be able to complete their tax returns and in case required for any future audit. The records that should be retained include:

- the type of cryptoasset
- date of the transaction
- if they were bought or sold
- number of units involved
- value of the transaction in pound sterling (as at the date of the transaction)
- cumulative total of the investment units held
- bank statements and wallet addresses, in case these are needed for an enquiry or review.

In terms of reporting, it should be noted that the UK is implementing the OECD Crypto-Asset Reporting Framework (CARF) with effect from 1 January 2026. This will require UK cryptoasset service providers to collect customer and transaction information and report the same to HMRC. Crypto asset service providers in the UK will need to collect information about:

- all individual users, including their name, date of birth, home address, country of residence, their National Insurance number or Unique Taxpayer Reference (for UK residents) or their tax identification number (TIN) and the country where it was issued (for non-UK residents);
- all entity users (companies, partnerships, trusts and charities), including legal business name, main business address, their company registration number (for UK companies) or their TIN and the country where it was issued (for non-UK companies) and for some entities information about their controlling person; and
- cryptoasset transactions (for users in the UK and other CARF jurisdictions), including the value, type of cryptoasset, type of transaction and number of units.

The CARF will implement automatic exchange of information, with HMRC sharing information with other tax authorities (in jurisdictions which have implemented the CARF) when UK cryptoasset service providers serve overseas users (and vice versa). The CARF comes into force in the UK on 1 January 2026, and the first reporting deadline will be 31 May 2027 for the 2026 reporting period. Penalties will apply for non-compliance.

Copyright © Monetary Authority of Singapore All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanised, photocopying, recording or otherwise, without the prior written permission of the copyright owner.