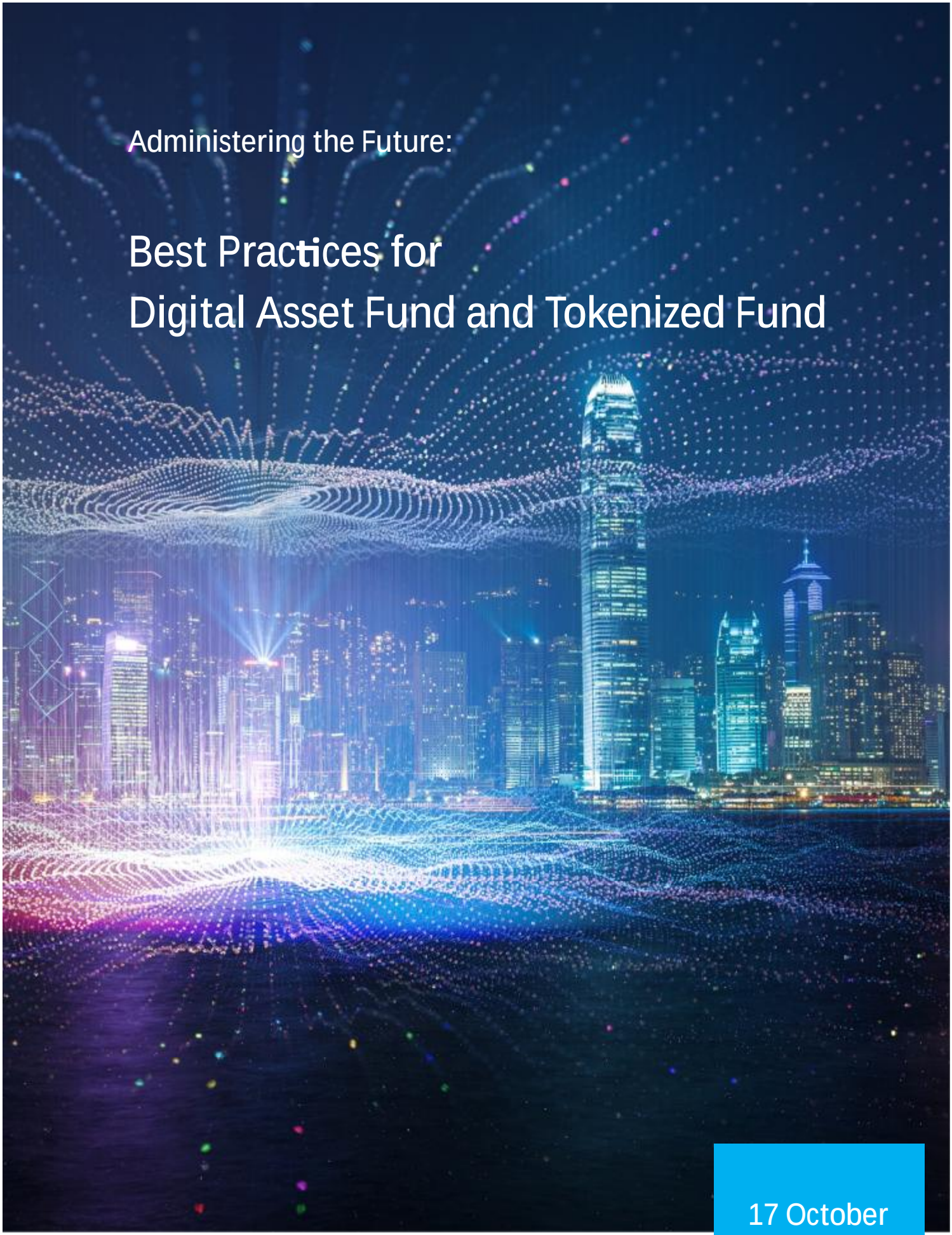


Administering the Future:

Best Practices for Digital Asset Fund and Tokenized Fund

The Association of Fund Administrators of Hong Kong and the Greater Bay Area

17 October 2025

Contents

1. Introduction 2

2. Key Terminologies 3

3. The Evolving Regulatory Landscape of Hong Kong's Digital Asset Market 4

4. Administering the Future:
   Best Practices for Digital Asset Fund (DA fund) and Tokenized Fund (TK fund) 6

5. Framework Approach 7

6. Basic Concept of DA/TK Funds 8

   6.1 .Clarifying the Difference: Tokenized Funds ≠ Digital Assets Fund 8

   6.2. The Role of Wallets and Wallet Structures 10

   6.3. Summary of Key Risk Management Implications for Fund Administrators 12

7. Case Studies and the Associated Fund Administration Best Practices 14

   7.1. TK Fund Case Studies and Best Practices 14

   7.2. DA Funds Case Studies and Best Practices 20

Appendix – Sample Due Diligence Frameworks: Industry Best Practices 26

   Appendix 1 – Enhanced Due Diligence on VATP/DA Custodians 27

   Appendix 2 – Enhanced Due Diligence Framework for Self-Hosted Wallets 31

About the Editors 32

Acknowledgements 33

Disclaimer 34

1. Introduction

Hong Kong is solidifying its position as a globally trusted digital asset hub, championed by a progressive and clear regulatory environment. As fund managers and their essential partners —fund administrators— seek to capture opportunities presented by this dynamic asset class, new digital asset-focused capabilities need to be developed to service evolving operational requirements and manage the corresponding set of risks.

For fund administrators, these new capabilities arise from a need for fund administrators to engage both with new transactional infrastructure (like blockchains, smart contracts and wallets) and new market participants (like Virtual Asset Trading Platforms (VATPs), digital custodians, and tokenization agents).

To meet these critical needs, The Association of Fund Administrators of Hong Kong and the Greater Bay Area has developed this best-practice framework for both public and private digital asset funds and tokenized funds, entitled "Administering the Future: Best Practices for Digital Asset Fund and Tokenized Fund"

This initiative is designed to strengthen the technical knowledge of fund administrators, empowering them to more actively engage with fund managers of digital asset funds and tokenized funds, in order to fortify investor protection, ensure operational integrity, and maintain stringent AML/CFT compliance. This, in turn, reinforces Hong Kong's leadership in the global digital assets market. Collaborative engagement with stakeholders—particularly the regulators, financial industry participants, service providers, and technology providers—will be pivotal in evolving this guidance into actionable standards.

2. Key Terminologies

Throughout this report, certain terms are defined and used to group related concepts, helping to streamline the content for readability and comprehension. This approach is intended to keep the focus on key messages and guiding principles, without overwhelming the reader with granular specifics.

- The term "Fund Administrator" (or "FA") and "Transfer Agent" (or "TA") refers to an single entity or combination of entities whose primary role is to provide services to fund managers encompassing the traditional functions of calculating the Net Asset Value (NAV), producing financial reports, and performing transfer agency duties, including investor KYC and maintaining the official fund share register.
- The term "Digital Assets" (or "DA") is used throughout this report to broadly refer to virtual assets (e.g. as defined under Section 53ZRA of the AMLO and generally includes "cryptocurrencies"), stablecoins. Any specific sub-category of Digital Asset intended for emphasis in the paper will be clearly identified.
- The term "Digital Asset fund" (or "DA fund") refers to a fund that invests directly in digital assets such as cryptocurrencies (e.g., Bitcoin, Ethereum) — which are created, recorded, and transacted on distributed ledger technology. The fund's strategy is focused on the performance of these underlying digital assets, and its ownership structure (i.e. the share register) may be maintained using traditional, off-chain methods.
- The term "Tokenized fund" (or "TK fund") refers to a fund in which the traditional share register is represented fully or partially as digital tokens on a distributed ledger. This means investor ownership is recorded on-chain, using smart contracts to automate key processes such as subscriptions (minting new tokens), redemptions (burning tokens), and transfers (reassigning tokens). The fund's underlying investments, however, are not necessarily digital assets and may include traditional securities like money market securities, stocks and bonds. The defining characteristic is the tokenization of the fund's shares / share register, which enables operational efficiencies, enhanced transparency, and new distribution models.
- The term "On-chain" refers broadly to a category of new technologies underpinning Digital Assets, like distributed ledger technologies (including blockchains), smart contracts, tokens and wallets. The term "O**ff**-chain" refers broadly to a category of technologies underpinning the traditional financial market infrastructure.
- The term "Smart Contract" is a self-executing software protocol that automates the terms of an agreement between parties. It is deployed on a distributed ledger or blockchain, where the code automatically executes predefined actions—such as minting, burning, or transferring tokens—when specific conditions are met. Unlike traditional contracts, smart contracts can be configured to operate without intermediaries, enabling transparent, tamper-resistant, and automated enforcement of contractual logic.

3. The Evolving Regulatory Landscape of Hong Kong's Digital Asset Market

Hong Kong has constructed one of the world's most comprehensive and sophisticated regulatory frameworks for digital assets, positioning itself as a leading global hub that balances innovation with robust investor protection. The current environment is not static; it is characterized by a dynamic and purposeful evolution, driven by a clear government strategy and proactive regulators. This trajectory can be understood through three interconnected layers: the established foundational regime, the forward-looking strategic roadmap, and the proposed legislative expansions to close regulatory gaps.

The Established Foundation: A Principle-Based, Risk-Focused Regime

The cornerstone of Hong Kong SFC's approach is the "same business, same risks, same rules" principle. This philosophy asserts that if a digital asset falls under the definition of a "security" or "futures contract" under the Securities and Futures Ordinance (SFO), existing capital markets rules apply. This brought DA fund managers and their distributors under the SFC's purview early on.

A pivotal moment was the introduction of the mandatory licensing regime for Virtual Asset Trading Platforms (VATPs) under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO). This regime, which came into full force in June 2023, requires all centralized platforms operating in or targeting Hong Kong investors to be licensed by the SFC.

The Strategic Vision: The SFC's "A-S-P-I-Re" Roadmap

Recognizing that regulation must evolve with the market, the SFC unveiled its "A-S-P-I-Re" Regulatory Roadmap in February 2025. This strategic blueprint outlines five pillars designed to future-proof Hong Kong's virtual asset ecosystem, addressing gaps and new challenges such as liquidity fragmentation and regulatory arbitrage.

- Access (A): This pillar aims to streamline market entry and attract global liquidity. Initiatives include establishing clear licensing frameworks for OTC trading services and dedicated digital asset custodians (separate from VATPs), and creating pathways to attract major global platforms and institutional liquidity providers to deepen market liquidity.
- Safeguards (S): This pillar facilitates a secure and competitive virtual asset ecosystem by harmonizing compliance with global standards through a flexible, outcome-driven approach. It ensures robust investor protection while enabling sustainable market growth by prioritizing core regulatory objectives and allowing operational flexibility. The framework adopts risk-proportionate oversight tailored to participant risk profiles and promotes regulatory clarity aligned with TradFi standards. This includes examining adaptable custody technology and insurance solutions. Additionally, it enhances clarity regarding investor onboarding processes and product classification.
- Products (P): This pillar aims to responsibly expand product offerings based on investor sophistication. It involves exploring frameworks to allow professional investors access to new token listings and derivative products, and considering regulated staking, lending, and borrowing services, all underpinned by TradFi-caliber risk management safeguards.
- Infrastructure (I): This pillar focuses on modernizing regulatory oversight through technology. The roadmap commits to deploying advanced surveillance and blockchain analytics tools for market-wide monitoring and enhancing cross-agency and international cooperation to detect and combat illicit activities.
- Relationships (Re): Emphasizing education and engagement, this pillar aims to empower investors through clear communication and tackle the influence of "finfluencers." It also focuses on cultivating a talent network to support the sustainable growth of the industry.

The ASPIRe roadmap is not a replacement for existing rules but a strategic evolution, signalling the SFC's intent to make the regulatory environment more nuanced, competitive, and attractive for global business while steadfastly upholding its core mandates.

Closing the Gaps: Proposed Regulation for Dealers and Custodians

While the mandatory licensing regime for Virtual Asset Trading Platforms (VATPs) established a well-regulated core for trading activities, significant segments of the ecosystem, particularly over-the-counter (OTC) trading and dedicated custody services, remained outside the formal regulatory perimeter. To address this gap and complete the construction of a holistic digital asset ecosystem, the Financial Services and the Treasury Bureau (FSTB) and the Securities and Futures Commission (SFC) launched a joint consultation on 27 June 2025 to introduce dedicated regulatory regimes for virtual asset dealing and custodian service providers.

This initiative directly extends Hong Kong's strategic efforts to foster a secure, robust, and globally competitive virtual asset environment, as guided by the Government's latest policy statement on digital asset development. Crucially, the proposals are designed to drive tangible progress under the SFC's ASPIRe roadmap, specifically enhancing "Access" by attracting qualified participants to the city, broadening investor choice, and further integrating Hong Kong's virtual asset liquidity with global markets.

The consultation outlines a framework that will empower the SFC to license, supervise, and enforce regulations for these two critical types of service providers

- Regulating Digital Asset Dealing Services (OTC): The consultation proposes a mandatory licensing regime for all entities engaged in the business of dealing virtual assets. This will bring OTC desks, which offer investors a critical and widely used channel for virtual assets conversion including fiat-to-virtual, virtual-to-fiat and virtual-to-virtual exchanges services, under formal regulatory oversight. The objectives are to mitigate AML/CFT risks, prevent fraud, and ensure these operators adhere to standards consistent with those expected of VATPs, thereby creating a level playing field and safeguarding retail investors at a key entry point to the ecosystem.
- Regulating Digital Asset Custodians: Acknowledging asset safekeeping as a distinct and critical function, the consultation proposes a dedicated licensing regime for custodians. This move directly addresses one of the largest perceived risks in the ecosystem by aiming to enforce stringent standards on asset segregation, cybersecurity, and governance. The regime is designed to ensure that whether custody is provided by a standalone service provider or as part of another service, it meets the robust standards necessary to protect client assets.

By establishing clear rules for dealers and custodians, these proposals directly operationalize the "Access" and "Safeguards" pillars of the ASPIRe roadmap. They aim to create a fully encompassing regulatory perimeter where all key activities—trading, dealing, and custody—are subject to proportionate oversight, thereby significantly enhancing the integrity and resilience of the entire digital asset value chain in Hong Kong.

4. Administering the Future: Best Practices for Digital Asset Fund (DA fund) and Tokenized Fund (TK fund)

Fund managers have emerged as early adopters of digital assets, driving the growth of a new category of funds with digital asset exposure at various stages of the fund lifecycle.

As DA/TK funds expand into new use cases, managers' needs around fund operations and compliance are evolving. Driven by the need to interact with new on-chain infrastructure like distributed ledger technologies, blockchains, smart contracts, and wallets, as well as new financial instruments like virtual assets and stablecoins, fund managers are, amongst other things, faced with a need to evolve their risk management and compliance processes to include a digital asset context.

Like with traditional funds, managers of DA/TK funds are increasingly looking to third-party administrators for critical operational support. Fund administrators are thus becoming increasingly essential players in the DA/TK ecosystem, managing key lifecycle aspects of investment schemes. As their role expands to include day-to-day risk oversight, a structured industry dialogue is needed to establish clear best practices and capability standards.

In Hong Kong's dynamic digital asset market, administrators can expand their support and services to the industry in scenarios that extend well beyond traditional fund administration activities (e.g. NAV calculation, transfer agency duties, etc). Technological innovation to move fund lifecycle activities on-chain and ongoing regulatory developments demand a fit-for-purpose approach to operational risk management. This document, Administering the Future: Best Practices for Digital Asset Fund and Tokenized Fund, offers practical guidance to help administrators strengthen investor protection, ensure operational integrity, and align with Hong Kong's regulatory ambitions as articulated in the SFC's "A-S-P-I-Re" roadmap.

Our analysis is structured on the core principles and responsibilities associated with fund administration, in particulate from a transfer agency (i.e., investor level) perspective, which is generally more applicable to TK funds; and a fund accounting and compliance (i.e., investment level) perspective, which is generally more applicable to DA funds, and centered around five key pillars of fund administration capabilities raised by the industry as critical to successfully service DA/TK Funds:

- *Due diligence: Enhanced due diligence on digital service providers*
- *AML/KYC: Investor KYC, transaction monitoring (KYT) and compliance reporting*
- *NAV: Net asset value calculation and accounting, in respect of transactions and holdings reporting, price reference and variance validation*
- *Transfer Agency: Transfer agency operations including token mint/burn process*
- *Reconciliation: Operational efficiency, in particulate robust on-chain and off-chain reconciliations*

By adopting this framework, fund administrators do not merely comply with regulations; they become pivotal enablers of trust and stability in Hong Kong's digital asset market. These best practices provide the operational foundation necessary to support the innovative products outlined in the SFC's "Products" pillar, from TK funds to DA funds. In doing so, fund administrators play an indispensable role in reinforcing Hong Kong's leadership as a secure and mature global digital asset hub.

5. Framework Approach

The best practice paper was developed through a structured and collaborative approach. Interviews were conducted with market experts to gather insights and practical suggestions.

The overall direction and framework were then guided by a dedicated committee group from the AFA Association, ensuring alignment with industry standards. Additionally, market experts were invited to serve as advisors, providing specialized guidance and validation throughout the development process.

This multi-stakeholder approach ensured the paper was both authoritative and reflective of real-world expertise.

This paper is structured into two key parts to provide a comprehensive analysis of DA/TK funds, their operational nuances, and best practices for fund administrators and service providers.

- Part 1 (Section 6) – Basic Concept of DA/TK Funds: This section explores the fundamental concepts of DA/TK funds, distinguishing between tokenized funds (TK fund) — where a fund's shareholder register is represented partially or fully using on-chain infrastructure — and funds investing in digital assets (DA fund) — where the fund allocates capital to digital assets, or other assets created and managed on-chain. It clarifies key principles that set the foundation for subsequent commentary and introduces newly essential concepts like wallets, smart contracts, and tokens. Furthermore, it explains how these on-chain elements interact with traditional fund administration concepts across different types of DA/TK funds.

  The introduction of on-chain infrastructure enables a wider set of interactions between traditional ecosystem participants—such as custodians, fund managers, fund administrators, and transfer agents—and their counterparts in the digital asset space, such as VATPs, tokenization agents, and DA Custodians.

- Part 2 (Section 7) – Case Studies and the Associated Fund Administration Best Practices, inspired by real-world examples (and subsequently generalized for illustrative purposes) of existing DA/TK funds, draws out different fund lifecycle activities where involvement of fund administrators can add value.

	Onshore (OFC)	Offshore
Tokenized Fund	Case study 1 - Authorized retail onshore tokenized fund	Case study 2 - Private offshore tokenized fund
Digital Assets Fund	Case study 3 – Digital assets fund investing in single digital asset (ETF) on a single venue	Case study 4 – Digital assets fund investing in multiple digital assets on multiple venues

By combining theoretical clarity, real-world examples, and pragmatic guidance, this paper equips fund administrators with the tools to support DA/TK funds efficiently.

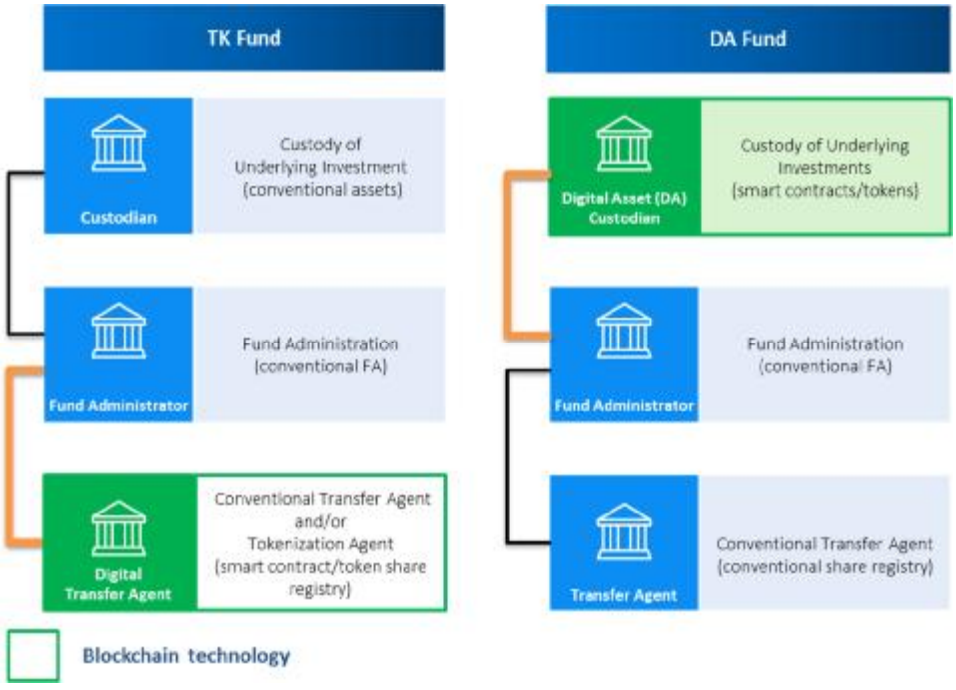
6. Basic Concept of DA/TK Funds

6.1. Clarifying the Difference: Tokenized Funds ≠ Digital Assets Fund

In the evolving landscape of digital finance, the term "Digital Fund" has emerged as a catch-all label for a wide range of investment vehicles. However, this single term describes two fundamentally different operational and risk profiles. To prevent confusion and ensure precise communication, we recommend the industry adopt two distinct terms: Digital Asset Fund (DA Fund) for a fund that invests directly in digital assets, and Tokenized Fund (TK Fund) for a fund that represents its shares on-chain. This clear distinction is critical because while the same underlying on-chain infrastructure is used, the nature and magnitude of their specific risks differ significantly, and therefore, the best practices required to manage these risks are not the same.

- Tokenized funds (**"**TK funds**"**) – These are traditional investment vehicles where the format of the ownership register is "tokenized". Tokenization is the act of representing a fund's ownership register, fully or partially, using on-chain infrastructure (e.g. wallets, smart contracts, tokens, underlying distributed blockchain ledgers). Tokenized funds can be used as a wrapper to house various types of investment strategies which involve traditional financial products as well as digital assets.
- Digital Assets funds (**"**DA funds**"**) – These are funds allocating capital directly into assets that are represented wholly as a smart contract / token entry recorded on a distributed / blockchain ledger. Wallets are associated with the smart contract / token, whereby ownership is evidenced digitally through the possession of a corresponding private key, making the assets both "digital" and "bearer" in nature. The combined "digital bearer" nature of these digital assets introduces novel features into an investment instrument not previously present in the financial sector.

From a fund administration perspective, these two types of funds can be decomposed into their component parts across a typical fund service provision value chain:



The preceding diagram provides a visual supplement to the operational workflows detailed in the following table.

	TK Funds	DA Funds
Custodian	§ Fund manager executes trades of traditional investment assets (e.g. stocks, bonds, etc.) through the fund's brokers. § These investments are managed by conventional custodians like banks or licensed financial institutions ensuring safekeeping, settlement, and reporting of the fund's portfolio.	§ Fund manager executes the digital asset trades through a licensed Virtual Asset Trading Platform (VATP), offshore VATP, or prime broker. Unlike traditional assets, digital assets are digital bearer assets, which are recorded on a distributed ledger / blockchain based book of records. There is no physical form of asset for custody. § When a fund's digital assets are held by a DA Custodian, ownership is represented by the access credentials the DA Custodian manages. The DA Custodian safeguards the private keys controlling the wallets, while the underlying assets remain on the blockchain.
Fund Administrator	§ Conventional fund administration where the fund administrator maintains the accounting book of records and calculates the Net Asset Value of the fund, with holdings that are typically traditional instruments (e.g. stocks, bonds, etc)	§ A core responsibility of the fund administrator is to verify the existence and ownership of the fund's assets. This involves reconciling digital asset trades executed on VATPs, offshore VATPs, or with prime brokers, and confirming holdings with the DA Custodian. Following this, the administrator accrues income/expenses, values the digital assets, and calculates the fund's Net Asset Value (NAV).
Transfer Agent	§ Enhanced Transfer Agency involves orchestrating the interface between on-chain and off-chain infrastructure to maintain shareholder records. Key activities include managing new workflows—such as minting, burning, and transferring tokens—often in coordination with a tokenization agent (sometimes also called a digital transfer agent), and providing investor services through on-chain KYC and whitelisting protocols.	§ Conventional transfer agency services, where the share register is maintained off-chain and investor servicing, which includes KYC, are performed.

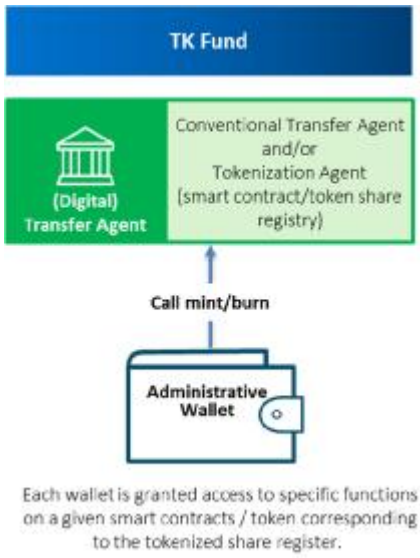
6.2. The Role of Wallets and Wallet Structures

Role of Wallets

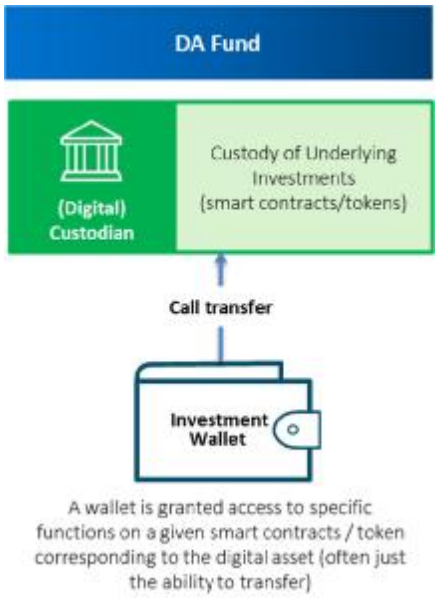
Wallets work the same way for both TK and DA funds. They are the access point used to interact with the on-chain infrastructure—specifically, the smart contracts and tokens on a blockchain. Using a wallet to sign a transaction allows someone to take action on those smart contracts or tokens.

However, while the wallets themselves are technically identical across TK funds and DA funds, their function and what they control are fundamentally different. We can distinguish them as

- Administrative Wallets are used to manage a fund's lifecycle through smart contract interactions. In a TK Fund, the tokenization agent (digital transfer agent) uses this wallet to execute functions like "mint tokens"—creating new tokens on the blockchain to represent additional fund shares—or "burn tokens" to remove tokens from circulation during redemptions.

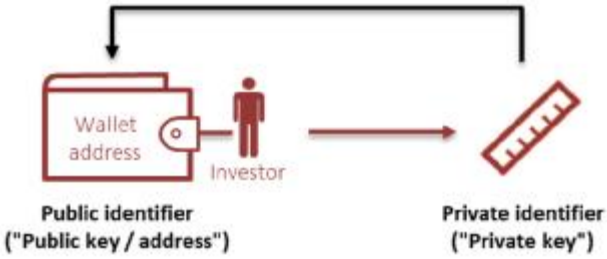


- Investment Wallets – a wallet is used to manage the fund's assets. For a DA Fund, the fund manager instructs a trade. The DA Custodian eventually uses the corresponding Investment Wallet to call the "Transfer" function on the digital asset (smart contract / token), thereby buying or selling the digital asset for the fund's portfolio.



This distinction in wallet purpose—controlling the share register versus the investment assets—defines their role and the associated risks for each fund type.

At a functional level, a digital asset wallet has conceptual similarities to a publicly visible user identifier (i.e. a username or e-mail) and private identifier (i.e. a password). The digital asset wallet's public identifier (i.e. an "address") can be mapped to a smart contract / token (i.e. a "balance") to indicate a relationship of ownership (i.e. address ABC is assigned a balance of 10 tokens in smart contract XYZ). To prove or evidence ownership of the digital asset wallet's public identifier, a valid corresponding private identifier (i.e. a private key) must be presented.



Wallet Structures

The operating models surrounding the management of the private key introduce new concepts relevant for fund administrators:

- Hosted Wallet vs Self-hosted

  A hosted wallet is a setup where a wallet address owner delegates operational and technical control of their private key to a DA Custodian who manages private keys on behalf of the investor. Hosted wallets can be further broken down into different granularity structures:

  - *Omnibus wallets* are a structure where the same wallet address is used for multiple customers. The rationale and preference for the use of omnibus wallet addresses will differ based on the TK/DA fund type / use case – it is generally considered where on-chain operational / transaction cost efficiency, and data confidentiality are required.
  - *Segregated wallets* are a structure where a unique address is used for each customer. The rationale and preference for the use of segregated wallet addresses will differ based on the TK/DA fund type and use cases – it is generally considered where data transparency and on-chain composability and automation are required.

  A Self-hosted wallet is a setup where a wallet address owner retains full operational and technical control of full control of their private keys, eliminating reliance on intermediaries.

- Single vs Multi-party signing

  The private key of a wallet—whether an Administrative Wallet or an Investment Wallet—can be managed under single or multi-signer governance. A single-signer setup is the default, where one entity holds full control. For enhanced security, multi-party approaches can also be explored depending on the use case context. These include multi-signature (multi-sig) wallets, which require approvals from multiple private keys to authorize a transaction, and multi-party computation (MPC), where the private key is split into shares and signatures are computed collaboratively without ever fully reconstructing the key.

This governance is critical for authorizing transactions such as "mint" or "burn" functions in a Tokenized Fund or "transfer" functions in a Digital Asset Fund.

6.3. Summary of Key Risk Management Implications for Fund Administrators

The following diagram provides a high-level framework for characterizing the use of on-chain infrastructure (i.e. the operational "where, why, who, what, and how") of both TK funds and DA funds. They illustrate the core rationale, technological environment, processes, key participants, and critical interactions for each fund type. For a detailed breakdown of the specific operational dimensions and control points, please refer to the table that follows. This concluding table further synthesizes the risk implications of these two distinct fund structures for all market participants, with a specific focus on the critical role and exposure of fund administrators.

Feature	TK Fund	DA Fund
Where is it	A fund where the shareholder register is fully or partially represented using on-chain technologies	A fund invests in digital assets which are transacted and managed using on-chain technologies
Why use it	Enhance fund distribution through the use case of operational efficiency, enhanced liquidity, and transparency	Gain investment exposure to digital assets market performance
Who is interacting	Typically, fund distribution lifecycle participants (i.e. the fund manager, fund distributors, investors and fund administrators, tokenization agents (digital transfer agents)) are directly interacting with the on-chain technologies	Typically, fund investment lifecycle participants (i.e. the fund manager, fund prime brokers, and fund administrators) are directly interacting with the on-chain technologies
What are they interacting with (Smart contracts/ tokens)	TK funds use smart contracts to execute actions on the shareholder register, enforce compliance rules, and provide real-time transparency and direct access, reducing reliance on manual processes and intermediaries. The smart contracts used in this context are often designed with role-based access permissions as per different fund lifecycle participants.	DA funds – investment activities directly interact with smart contracts / tokens. The execution of investment activities may be through brokers and/or exchanges (i.e. VATP). The smart contracts for these digital assets often have very simple or no built-in administrative controls. For example, a stablecoin's contract might have a "freeze" function, but a contract for an asset like Bitcoin or Ether typically has no special roles or permissions. This means there is little opportunity for "on-chain governance" or administrative oversight built into the smart contract / tokens itself. Therefore, fund administrators must rely on traditional "off-chain" methods—like agreements, policies, and controls—to ensure proper governance of these investments.
How are they interacting	Wallets (Administrative wallets)	Wallets (Investment wallets)
Resulting Risk implications	§ Investment Market risk: Typically, traditional securities (e.g. stocks, bonds, etc.). § Security / Technology risk: The configuration and use of on-chain technologies is often reversible. This means that if a security or technology incident compromises the on-chain ledger (e.g., due to an error or hack), the negative effects can typically be corrected. For example, an erroneous balance of tokens can be restored by re-minting (re-creating) tokens that were lost or incorrectly burned, or by re-burning (cancelling) tokens that were incorrectly minted. § Operational risk: Reconciliation of fund distribution lifecycle information across both on-chain and off-chain sources (e.g. shareholder ownership, NAV, etc).	§ Investment Market Risk: Typically digital assets. § Security / Technology Risk: For digital assets, the configuration and use of on-chain technologies is typically permissionless, and therefore risk events arising from security / technology incidents are typically irreversible (e.g., tokens corresponding to digital assets cannot be burnt / re-minted based on investment transactions). § Operational Risk: Reconciliation of investment lifecycle information across both on-chain and off-chain sources (e.g., investment holding positions / book of records, validation of price reference, etc.).

7. Case Studies and the Associated Fund Administration Best Practices

Four illustrative and generalized case studies are analyzed, inspired by live TK/DA funds in the marketplace. For each case study an indicative investor subscription / redemption workflow is described, alongside the roles and responsibilities of different lifecycle participants. Based on these case studies, best practices and recommendations are provided for fund administrators to consider. These best practices are split by the two types of TK/DA funds, and mapped against the same five-pillar fund administrator capabilities framework (also introduced in Section 4).

Overview of indicative case studies:

Case study 1	Authorized retail onshore TK fund
Case study 2	Private offshore TK fund
Case study 3	Authorized retail onshore ETF DA fund
Case study 4	Private offshore DA fund

7.1. TK Fund Case Studies and Best Practices

Case Study 1 – Onshore Authorized Retail TK Fund

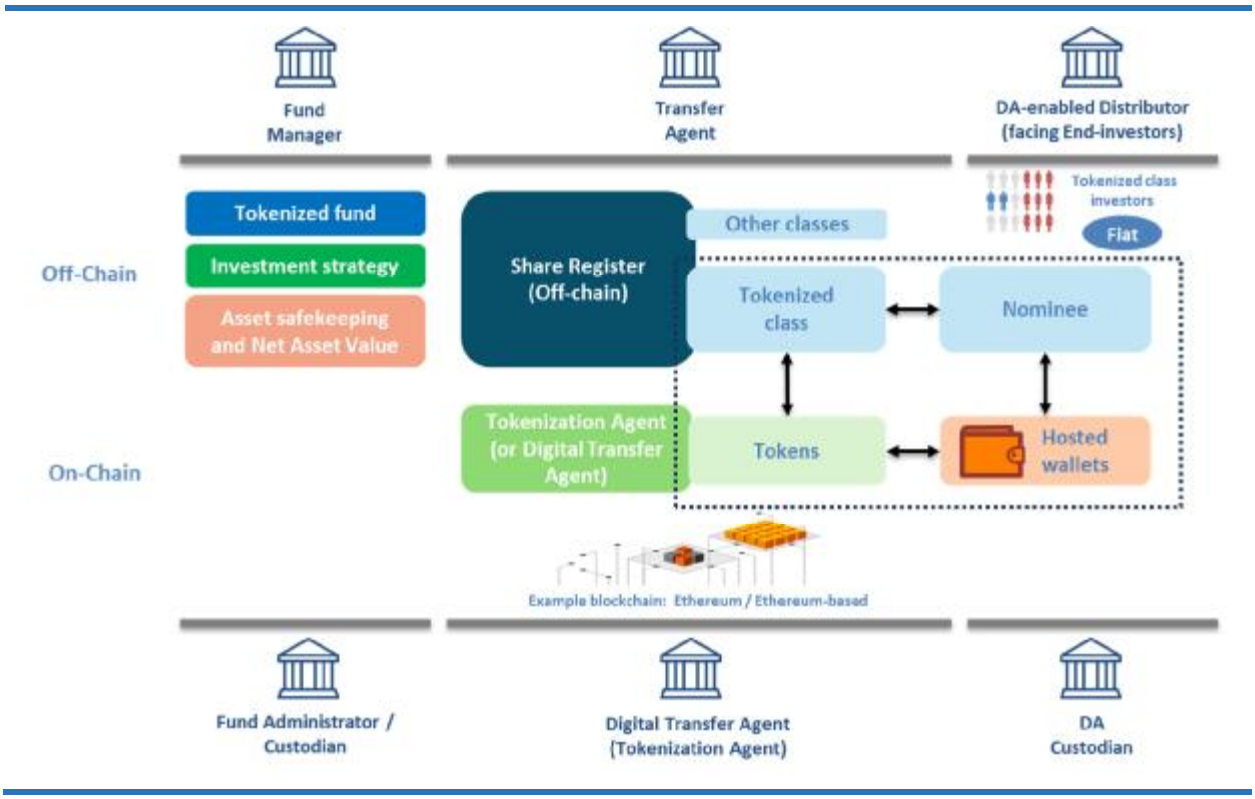
This case study illustrates a commonly observed and generalized TK fund design where the authoritative share register is maintained off-chain. This approach is generally practical where:

- When a fund contains both traditional and tokenized share classes, the transfer agent maintains a single, consolidated off-chain share register to provide a unified view of all investor holdings.
- When a fund contains only a tokenized share class, current market practice still favours maintaining an off-chain register as a safety measure and operational back-up.

While there is no direct regulatory mandate for an off-chain ledger, its necessity depends on a number of factors assessed by regulators. In our case study, we observe that an off-chain register is employed as a prudent risk mitigation measure to provide clarity on ownership.

In this model, smart contracts and tokens are minted or burned on-chain to mirror subscription and redemption activity for the tokenized class. This hybrid structure is sometimes referred to in the industry as a digital twin-style tokenized fund model.

A role-based diagram detailing the responsibilities of each participant:



Fund Flow Overview

1. *Subscription and Redemption Orders* – Distributors (on instruction from their investor clients) submit subscription or redemption orders to the transfer agent and approved by fund manager as part of the existing off-chain flow. The tokenized share class is fiat-denominated, and as such all subscription and redemption proceeds between the distributor and the tokenized class are based on fiat cash. The transfer agent receives and records these orders, acting as the central coordinator.

2. *Order Confirmation* – The manager works with the transfer agent to review and confirm the orders. Paired with NAV (in step 3), the transfer agent unitizes the order and determines the amount of shares to be created or redeemed and subsequently the number of tokens to be minted (in the case of subscription) or burned (in the event of redemption) (in step 4).

3. *NAV Calculation / Publication* – The Fund administrator, based on the received orders, and the fund's holdings, calculates the NAV for the fund off-chain. Once completed, the NAV is published through existing publication channels.

4. *Token Creation and Burning / Allocation* – Upon confirmation and unitization off-chain, the transfer agent instructs the tokenization agent (digital transfer agent) to mint / burn the tokens and deposit to the distributor's hosted wallet with the DA Custodian.

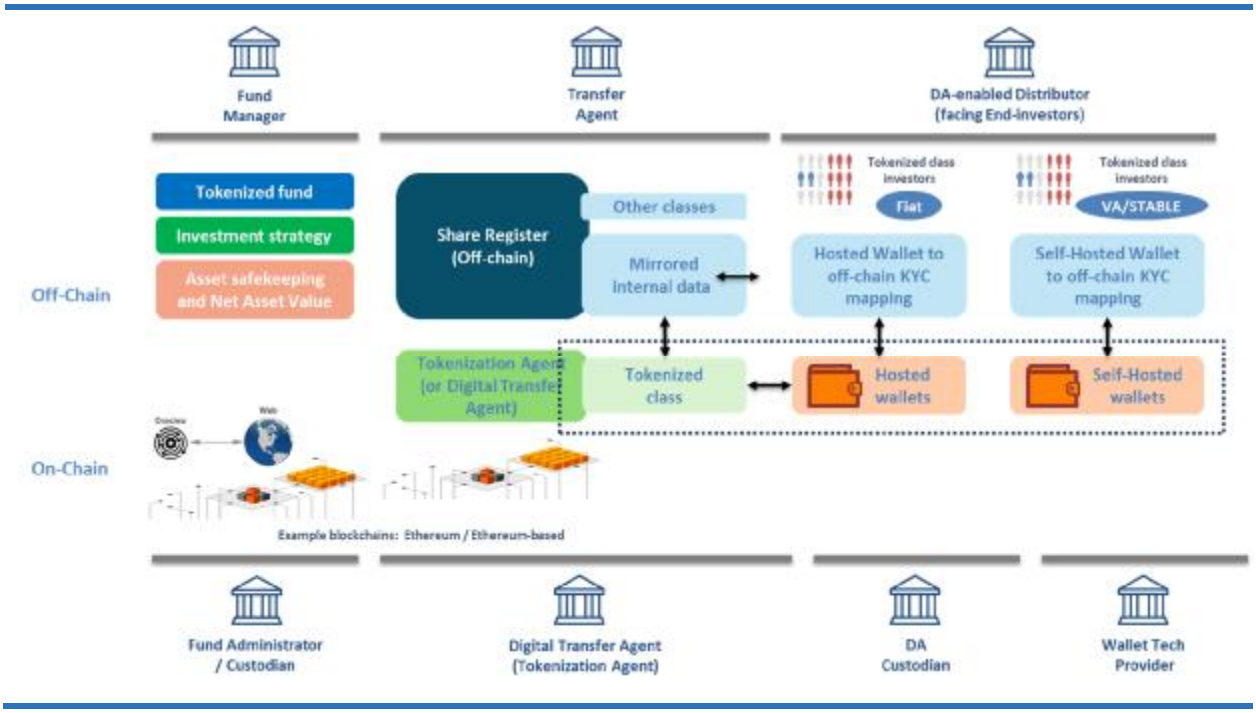
5. *Reconciliation and Recordkeeping* – Due to the internal wallet management structure of the DA Custodian, the fund administrator does not reconcile data directly from the blockchain. Instead, the DA Custodian provides a statement generated from its internal ledger. Reconciliation is therefore performed by comparing this DA Custodian-issued statement against the off-chain share register maintained by the transfer agent.

Case Study 2 – Off-Shore Private Money Market TK Fund

This case study illustrates a newer observed and generalized TK fund design where the authoritative share register is maintained on-chain utilizing smart contracts / tokens, representing a 100% tokenized share class. In this setup, off-chain data is limited to KYC mapping information and mirrored data records needed for downstream fund lifecycle processing (i.e., for fund accounting, risk reporting, etc.). This is sometimes referred to in the industry as a digital native (registered) tokenized fund model.

It should be noted that even in this on-chain native model with a fully tokenized class, current market practice still favours maintaining an off-chain register as a safety measure and operational back-up. This hybrid approach provides business continuity in case of technical issues with the on-chain infrastructure.

A role-based diagram detailing the responsibilities of each participant:



Fund Flow Overview

1. *Subscription and Redemption Orders* – Distributor submits subscription or redemption orders to the transfer agent and approved by the fund manager. The tokenization agent (digital transfer agent) coordinates with a traditional transfer agent off-chain to share the relevant data needed to update downstream systems that are potentially required by the fund administrator and/or fund custodian. The tokenization agent (digital transfer agent) receives and records these orders, acting as the central coordinator.

2. *Order Confirmation* – The manager and transfer agent reviews and confirms the orders. Paired with NAV (in step 3), the transfer agent unitizes the order and determines the amount of tokens to be minted (in the case of subscription) or burned (in the event of redemption) (in step 4).

3. *NAV Calculation / Publication* – the Fund administrator, based on the received orders, and the fund's holdings, calculates the NAV for the fund off-chain. Once calculated, the NAV is then published on-chain channels, usually through an oracle solution.

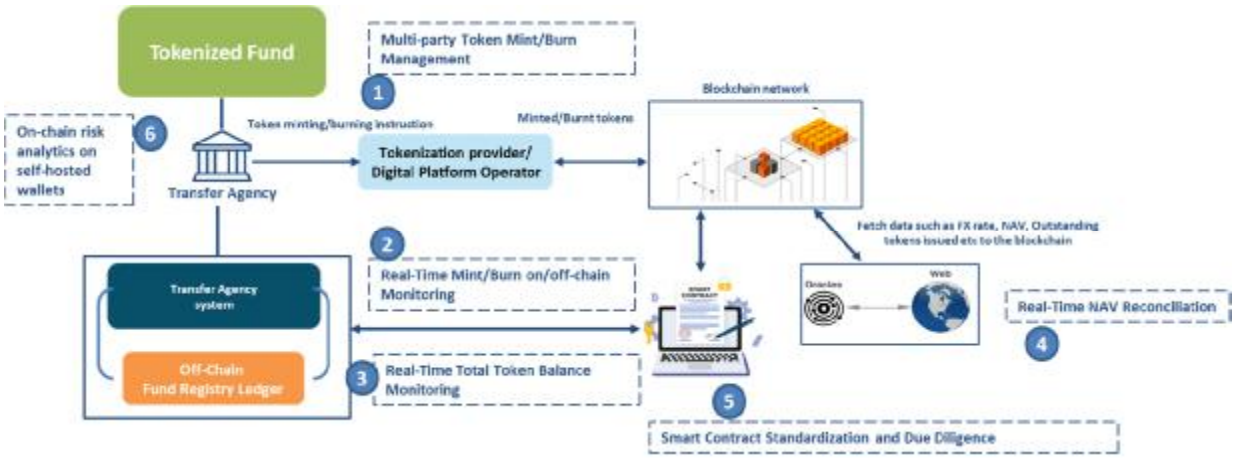
4. *Token Creation and Burning / Allocation* – Upon confirmation and unitization (which can be on or off-chain), the tokenization agent (digital transfer agent) calls the smart contracts and associated functions (on-chain) to update the smart contract. Tokens are minted/burned from the fund smart contract to a distributor's hosted wallet managed by their DA Custodian or self-hosted wallet. Depending on the nature of the business model and contractual arrangement between the distributor and their end-investor clients, there may be onward re-allocation of the tokens from the distributor's address to the end-investor self-hosted addresses whitelisted by the tokenization agent (digital transfer agent), which may be required to conduct Know-Your-Transaction (KYT) checks on self-custody wallets, supplementing standard Know-Your-Customer (KYC) procedures.

5. *Reconciliation and Recordkeeping* – Reconciliation of the records directly between the on-chain (token balances from the fund smart contract, recorded on the blockchain) and off-chain (TA account identifiers for the fund recorded in the TA internal systems) records is completed.

Fund administrator key capabilities and Best Practices

As tokenized funds grow in popularity and become increasingly explored in Hong Kong's TK/DA ecosystem, fund administrators can help shape the commercial innovation and risk management practices for this next evolution of the fund format. To do this, fund administrators will be increasingly expected by their clients (fund managers) to extend their current capabilities to support the latest on-chain infrastructures underpinning these new products. This, in turn, will enable the seamless extension of existing fund administration services for tokenized funds.

The following best practices have been identified for the current market landscape for tokenized funds. As the current iteration of tokenized funds still operates across both on-chain and off-chain infrastructure, it is perhaps not surprising that many of the best practices for fund administrators exploring support for tokenized funds to be focused on robust and streamlined reconciliation processes, alongside providing trusted infrastructure to minimize risks in smart contract management.



Fund Administration Capabilities	Best Practices (BP)
1 Due Diligence	§ Best Practice#5 – Smart Contract Due Diligence
2 AML/KYC	§ Best Practice#6 – On-chain risk analytics on self-hosted wallets
3 NAV	§ Best Practice#4 – Real-Time NAV Reconciliation
4 Transfer agency	§ Best Practice#1 – Multi-party Token Mint/Burn Management
5 Reconciliation	§ Best Practice#2 – Real-Time Mint/Burn on/off-chain Monitoring § Best Practice#3 – Real-Time Total Token Balance Monitoring

Best Practice #1 – Multi-Party Token Mint/Burn Management

It is important for all related parties to establish a secure, transparent, and straight-through processing (STP) joint framework for the minting and burning of digital tokens. This ensures that these critical actions, which directly impact the total outstanding share count and per unit value of the fund, are never executed by a single party, thereby mitigating operational risk, preventing fraud, and enforcing robust internal controls.

The exact design of this joint authorization and execution mechanism can vary – in part driven by jurisdictional considerations where tokenized products are subject to prescriptive requirements around tokenization arrangements/designs, as well as business/operating model considerations of a particular tokenized fund ecosystem of participants.

At a minimum, the mechanism should involve coordinated approval from at least the transfer agent, and the tokenization agent (digital transfer agent). The minting and burning of tokens ideally utilizes a multi-party process – be it an application-based maker checker, multi-signature (multi-sig), or multi-party computation (MPC) process. This formalizes the hand-off between off-chain operational functions and on-chain automated execution.

Best Practice #2 – Real-Time Mint/Burn on/off-chain Monitoring

The reconciliation of token minting and burning events is a critical function in maintaining the integrity of tokenized fund operations.

Upon a successful function call on a smart contract, a transaction is recorded, and/or events are potentially emitted depending on the design of the smart contract. Collectively, these transaction records and/or events, form the "on-chain datapoints" that can be used in subsequent reconciliation processes.

As these on-chain datapoints are created and stored automatically on the blockchain, immediately after a successful smart contract function call, there is the potential to implement real-time automated reconciliation workflows that take this on-chain data and compare it to the transfer agent's off-chain records. This real-time reconciliation ensures that the on-chain token supply accurately reflects the authorized changes. Any discrepancies between the blockchain record and the off-chain ledger trigger an alert, prompting a suspension of further token operations until the issue is resolved.

Best Practice #3 – Real-Time Total Token Balance Monitoring

Ensuring that the total number of tokens created by the smart contract, as well tokens mapped to various wallets matches the corresponding off-chain records at the transfer agent is another critical component of the reconciliation process. Depending on the business / operating model design of the tokenized fund, there may need to be different data transformations on the on-chain data in order to properly line it up to the off-chain data. The transfer agent records shareholder balances at a TA ID level, and given the flexibility for different wallet configurations by distributors, there may need to be different data transformations performed to combine various token-bearing wallets' balances to arrive at a TA ID. It is important to not only ensure that the aggregated totals match, but also the distributor-level / shareholder balances.

In the event of a mismatch, the tokenization agent (digital transfer agent) and transfer agent need to coordinate on reconciliation procedures. This procedure may include automated checks and manual review, with administrative functions implemented on-chain (e.g. to burn and re-mint) potentially requiring additional documented approvals (either off-chain, or on-chain if the smart contract is designed by the manager to permit additional metadata / reasoning fields as part of the function call). Depending on the joint mechanism design, additional roles (i.e. additional keys, key shards, or off-chain role-based access designations) can be defined as part of execution requirements / policy. This approach ensures that token holdings are accurately reflected both on-chain and off-chain, thereby safeguarding investor assets and maintaining operational integrity.

Best Practice #4 - Real-Time NAV Reconciliation Using Oracle Integration

Where NAV and related fund data are published on-chain for DA ecosystem use via a secure oracle solution, the reconciliation of off-chain calculated NAV and related fund data and the on-chain published versions within the oracle solution should be considered.

The exact design of this reconciliation can vary – in part driven by the manager's design of the tokenized fund (particularly, the use of smart contracts), as well as the transfer agent's and fund administrator's own internal systems. Similar to the mint / burn reconciliation best practice, the publication of NAV and fund-related data on-chain are created and stored automatically on the blockchain, immediately after a successful smart contract function call – thereby allowing for the potential to implement real-time automated reconciliation workflows that take this on-chain data and compare it to the transfer agent and fund administrator's off-chain records. Any discrepancies between the blockchain record and the off-chain ledger trigger an alert, prompting a suspension of further token operations until the issue is resolved. This final reconciliation step ensures that the fund data presented on the blockchain is consistent with the authoritative source, thereby reinforcing investor confidence and regulatory compliance.

The consideration of the roles and responsibilities surrounding who performs the NAV reconciliation needs to be clarified by fund administrators in such a setup. In conventional NAV-related roles and responsibilities, the fund administrator is typically responsible for valuation / NAV calculation and production of the related fund data, while the fund manager generally specifies and engages the publication practices, including the use of any NAV publication vendors. However, for tokenized funds where there is the use of an on-chain oracle solution, it can be possible that the NAV publication vendor contracts with either the fund manager or the fund administrator, or a tri-party arrangement for the NAV publication logistics and setup. Fund administrators should specify clearly in service provider agreements with the manager the operational responsibility for such an activity and cater for the risk associated with incorrect publication of NAV and fund data.

Best Practice #5 – Smart Contract Standardization and Due Diligence

Smart contract standardization

To mitigate operational risk and ensure sustainable growth, we recommend the industry develop and adopt standardized smart contract templates for tokenized fund operations. The proliferation of custom, non-standard smart contract implementations introduces potential risks. The current environment, characterized by numerous unique contract variations, directly increases the likelihood of operational errors during critical functions and drives up the cost and complexity of the required security audits. Adopting secure, well-audited standard templates would dramatically reduce these risks, lower costs for all participants, enhance interoperability between service providers, and ultimately accelerate the safe and efficient adoption of tokenized funds.

Smart contract due diligence

The role of a fund administrator also extends to ensuring the accuracy, integrity, and security of fund operations and investor assets. In a tokenized fund, a significant portion of the fund's core business logic, by way of the share register, is embedded directly into the smart contract code. This code acts as an automated ruleset that governs the permissible fund lifecycle activities on the blockchain.

This shift from traditional, human-administered processes to code-executed logic which introduces a new and critical operational risk: the risk of vulnerabilities within the smart contract itself. The use of the smart contract code in unforeseen ways can lead to adverse fund and investor outcomes. Therefore, it is recommended as a best practice that fund administrators extend their operational due diligence efforts to also cover the smart contracts governing the fund. This can include a review of the code itself, or at minimum ensuring that independent audits conducted by a specialized third-party blockchain security firms have been undertaken ensuring:

- *The code matches the business logic*: The audit verifies that the deployed smart contract accurately reflects the fund's stipulated rules and offering documents.

- *Vulnerabilities have been identified and remediated*: The audit process is designed to uncover critical security flaws, logical errors, and inefficiencies before the contract goes live.
- *Best practices are followed*: Auditors confirm the code adheres to industry development standards, minimizing the risk of unforeseen issues.

Best practice #6 – On-chain risk analytics on self-hosted wallets (addresses):

Where self-hosted wallets (addresses) are involved, enhanced due diligence on DA-related activities may be required in addition to traditional due diligence dimensions, which can include:

- Self-hosted wallet ownership verification through appropriate proof of ownership approaches
- Direct on-chain risk analytics assessment of wallets (KYT / KYW) directly interacting with the fund - including selection of appropriate vendors covering relevant token and blockchain scope.

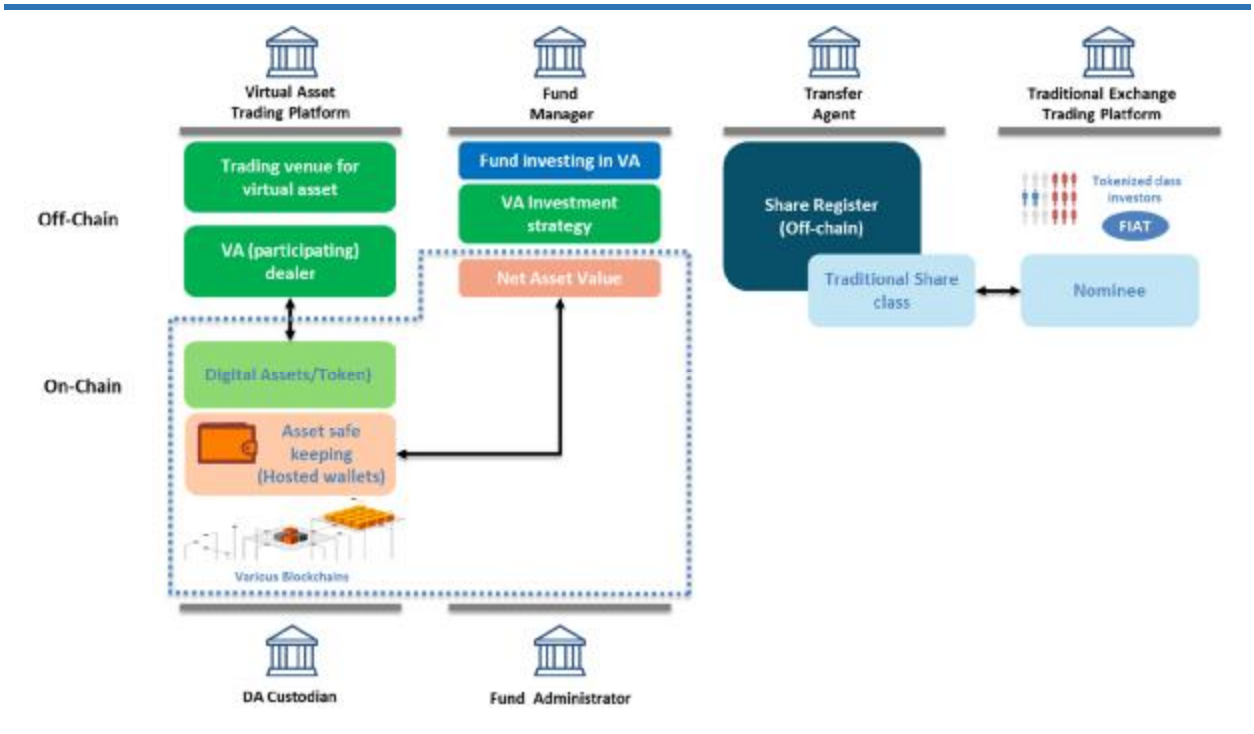
Where interaction with the self-hosted wallets result in direct changes to the shareholder register, the fund manager may rely on fund administrators to operationally carry out on-chain risk analytics activities, which can include upfront and ongoing monitoring. For details of the due diligence, please refer to Appendix 2 - Enhanced Due Diligence Framework for Self-Hosted Wallets.

7.2. DA Funds Case Studies and Best Practices

Case Study 3 – Onshore DA Fund investing into a Single Digital Asset, through Single Venue/Custodian (Spot ETF)

The emergence of Spot Crypto ETFs marks a significant milestone in bridging traditional finance with digital assets. This case study, which illustrates how these ETFs de-tokenize a digital asset by wrapping it in a traditional investment vehicle, is supported by below diagrams:

A role-based diagram detailing the responsibilities of each participant:



Fund Flow Overview

The diagram outlines the intricate process of creating a Spot Ether ETF, highlighting the roles of various stakeholders and the flow of assets and information across both on-chain and off-chain systems.

Primary Market: ETF Creation Process - The primary market is where ETF shares are created through a structured process involving investors, participating dealers, fund managers, fund administrators, the custodian and the exchange.

1. Investor Initiation: The process begins when an investor expresses interest in acquiring ETF shares. If the investor wants to do an in-kind subscription (as in this case, where the investor uses Ether ("ETH") to exchange for ETF shares), the investor must have a whitelisted wallet to ensure compliance with regulatory standards. For ETF, creation must be made via participating dealers ("PDs"). Investor should approach a PD for ETF shares creation.
2. Instruction to Create ETF Shares: The PD sends a request to the fund manager to initiate the creation of ETF shares.
3. Ether Transfer and KYT: The investor (either directly or via the PD) transfers the required amount of Ether to the DA Custodian. The DA Custodian performs the necessary know-your-transaction ("KYT") to ensure secure handling of crypto assets and confirms receipt of Ether to the fund manager and fund administrator for order confirmation.
4. Confirmation of creation order: Upon confirmation of the Ether deposit by the VATP, the fund manager confirms the creation order and sends confirmation to the fund administrator. The fund administrator further confirms the creation order with the VATP.
5. Ledger Updates: The VATP (Virtual Asset Trading Platform) updates its ledger under the fund's name to reflect the deposited Ether. Simultaneously, the Custodian and Fund administrator update the off-chain ledger to record the Ether deposit.
6. ETF Creation Execution: The fund administrator processes the ETF creation and updates the share register.
7. Allocation of ETF Shares: ETF shares are allocated to the PD's CCASS (Central Clearing and Settlement System) account. These shares represent the investor's exposure to Ether without directly holding the crypto asset.
8. Final Allocation to Investor: The ETF shares are then transferred from the PD's account to the investor's CCASS account, completing the creation process.

The above illustrates the in-kind creation process, it is important to highlight the KYT process when the VATP received crypto. Cash creation process is the same as for other traditional ETFs, where the fund manager will instruct the VATP to execute the purchase of crypto. Please note that pre-funding is required for crypto ETF creation. The fund administrator should work with the fund manager and VATP on the pre-funding and refund arrangement.

Secondary Market: Exchange Trading

Once ETF shares are created, they enter the secondary market where they can be traded on the Hong Kong Stock Exchange.

- Market Makers and Brokers: These entities facilitate liquidity and price discovery, ensuring that ETF shares can be bought and sold efficiently.
- ETF Market Price: The market price of the ETF reflects the underlying value of Ether, adjusted for supply and demand dynamics.
- Staking: Ether held by the fund may be staked to generate additional yield, enhancing the fund's performance.

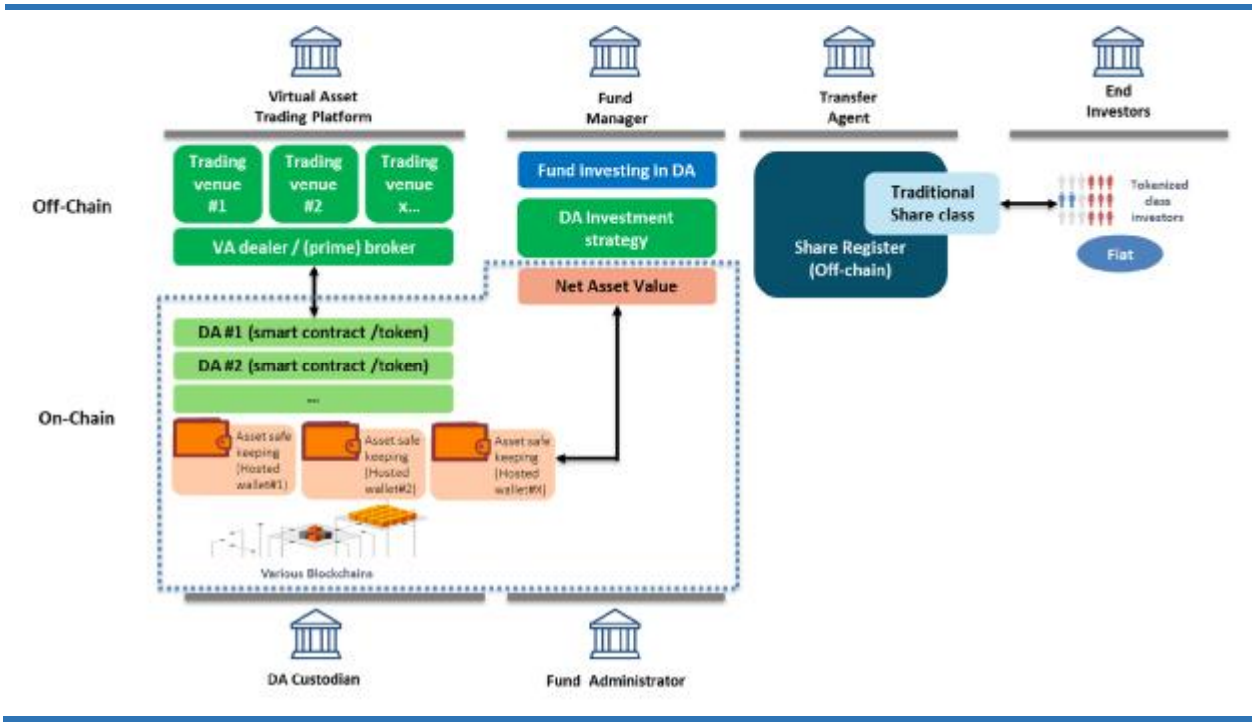
Ledger Reconciliation

Due to the internal wallet management structure of the VATP, the fund administrator does not reconcile data directly from the blockchain. Instead, the VATP provides a statement generated from its internal trading ledger. Reconciliation is therefore performed by comparing this VATP-issued statement against the off-chain share register maintained by the transfer agent.

Case Study 4 – Offshore DA Fund Investing in Multiple Digital Assets Across Multiple Venues/Custodians

This case study illustrates a multi-digital assets fund investment strategy, requiring connections to multiple venues / DA Custodians.

A role-based diagram detailing the responsibilities of each participant:



Fund Flow Overview

1. Investor initiation: Investor subscribes into the fund either via fiat or in-kind using stablecoins, leveraging wallets hosted by approved VATPs, or offshore VATP, or their own self-hosted wallets.
2. Investment strategy execution: Fund manager executes a strategy involving investments across multiple types of digital asset and venues
3. NAV Calculation: The fund administrator calculates the NAV of the digital assets portfolios, which may involve sourcing pricing data from various feeds
4. Reconciliation: Fund administrator needs to reconcile fund holdings across multiple wallets – which may be held across various DA Custodians and venues (depending on the fund's operational arrangement).

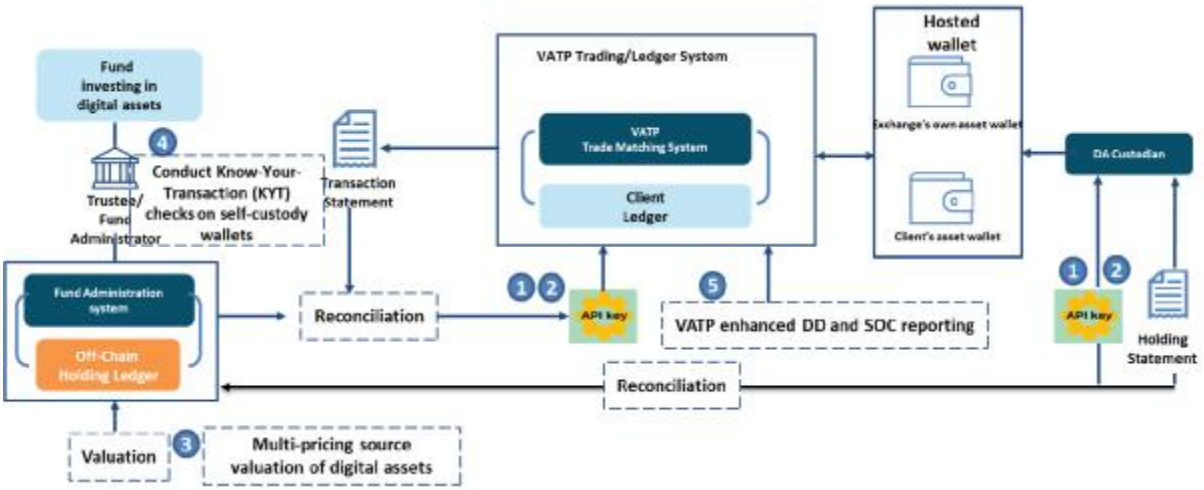
Best Practices for DA funds

Fund administrators face operational and reconciliation challenges when overseeing investments through Virtual Asset Trading Platforms (VATPs). These challenges stem from the platforms' internal wallet arrangements, which often pool client assets, limiting the administrator's ability to directly verify wallet-level balances on the blockchain. During the due diligence process, the custodian and fund administrator would seek to understand the VATP's specific wallet structure. However, depending on the setup, there can be a time lag between the VATP's internal ledger updates and the actual on-chain wallet balances. This lack of real-time, granular visibility means administrators are often compelled to rely solely on the statements provided by the VATP for transaction recording and position reconciliation.

This dependency introduces risk, including potential discrepancies in reported balances and an inability to independently verify the custody of assets. To mitigate these risks and ensure financial integrity despite these constraints, it is imperative to implement robust alternative safeguards. This recommendation underscores the critical importance of independent verification of total client asset holdings and the review of SOC 1 & SOC 2 reports to validate the soundness and internal controls of the VATP counterparty.

In our assessment, we have provided five key recommendations to enhance oversight and security. Four of these recommendations — holding and transaction reconciliation, smart contract audit, and multi-source price verification — are operational controls that can and should be directly implemented and performed by the fund manager or the fund administrator.

The remaining recommendation — Third-Party SOC Report is the fundamental safeguards that rely on external, independent validation. These processes are designed to provide assurance over the VATP's platform-wide controls and overall solvency as a single entity. As they require a holistic review of the VATP's entire operation, they must be conducted by qualified third parties, such as licensed auditors, to ensure objectivity and comprehensive coverage.



Fund Administration Capabilities	Best Practices
1 Due Diligence	§ Best Practice#5: VATP enhanced DD and SOC reporting
2 AML/KYC	§ Best Practice#4: conduct Know-Your-Transaction (KYT) checks on self-custody wallets
3 NAV	§ Best Practice#3: Multi-pricing source valuation of digital assets
4 Transfer agency	§ Best Practice#4: conduct Know-Your-Transaction (KYT) checks on self-custody wallets
5 Reconciliation	§ Best Practice#1: Operational Integrity Through Automated FA-VATP Reconciliation § Best Practice#2: Reconciliation frequency

Best Practice #1 – Operational Integrity Through Automated FA-VATP Reconciliation

To mitigate operational risk and ensure efficiency, fund administrators should move beyond manual reconciliation processes. The established best practice is to implement a secure, API-driven straight-through processing (STP) system to automate the reconciliation of VATP statements and custodian records, focusing human effort on managing exceptions.

- Secure API Integration: Establish secure, read-only API connections directly to the VATP(s) and the DA Custodian's systems. This allows for the automated and real-time pulling of transaction feeds and holding statements, eliminating manual data entry and its associated errors and delays.
- Automated Transaction Matching: The system should automatically match:
  - Trade Executions: VATP trade confirmations against the fund manager's instructions.
  - Cash & Asset Movements: Deposits, withdrawals, and transfers recorded by the VATP against those recorded by the DA Custodian and the fund's general ledger.
- Automated Position Reconciliation: The system should perform daily (or intraday) automated reconciliations of end-of-day holding positions between the VATP's issued statement, the DA Custodian's statement and the fund administrator's internal book of record.
- Exception-Based Management: The primary role of the reconciliation team shifts from manual matching to efficiently investigating and resolving exceptions flagged by the automated system. This includes breaks due to timing differences, missing transactions, or data discrepancies, allowing for quicker resolution and higher accuracy.

In an environment where direct verification is limited, the integrity of the fund administration function hinges on the reliability and efficiency of the reconciliation process. Automating this process via secure APIs is not merely an efficiency gain; it is a critical risk control that provides scalable, timely, and accurate assurance over assets held in third-party VATP ecosystems.

Best practice #2 – Reconciliation frequency

Under the existing model for traditional assets, asset positions are reconciled with the custodian on a periodic basis, at least per valuation cycle (i.e., for a monthly valuation fund, reconciliation should be done at least monthly). Between valuation cycles, more frequent position reconciliation is recommended. The fund administrator shall obtain securities positions from the custodian (via API key or other electronic means) and reconcile them against the accounting book of records. For any unreconciled items, the fund administrator should investigate discrepancies with the custodian and resolve them before the next valuation cycle to ensure an accurate book of records reflecting the actual holdings when calculating the NAV.

Practically, key performance indicators (KPIs) should be outlined in the operating memorandum, requiring the DA Custodian to resolve any discrepancies within a specified timeframe.

Best practice #3 – Multi-source pricing for valuation

Relying on a single source for pricing introduces significant valuation risk, particularly for funds investing across multiple trading venues or holding blended cryptocurrencies (e.g., BTC + ETH). We therefore recommend using professional pricing sources from multiple fintech providers. This is essential because the decentralized nature of digital asset markets and the real-time trading of assets across myriad global exchanges require a specialized solution to calculate an accurate composite price.

These firms employ sophisticated technology to gather real-time trade and order book data directly from hundreds of centralized and decentralized exchanges globally. They cleanse this data, eliminate the outliers, and calculate comprehensive volume-weighted average prices (VWAPs) as a result. After obtaining accurate data from these professional data providers, the median is then taken to serve as the final, reliable fair market price data.

Crucially, we recommend pre-defining an acceptable "deviation threshold" with the fund manager. This threshold is used to establish a price band, which is referenced against the primary valuation benchmark price. If the primary benchmark price falls outside this band, an immediate alert is escalated to management for investigation and resolution before finalizing the NAV. This proactive approach significantly reduces valuation risk and enhances operational control.

Best Practice #4 – Conduct Know-Your-Transaction (KYT) checks on self-custody wallets

In addition to traditional due diligence requirements (e.g., AML/KYC and Source of Wealth), enhanced due diligence on digital asset-related activities is required. This enhanced due diligence should include:

- Self-hosted wallet ownership verification using appropriate proof of ownership approaches.
- Direct on-chain risk analytics (KYT) of wallets involved in in-kind subscriptions and redemptions. It is advisable to use multiple KYT tools to compare risk scores, as differing algorithms provide a more comprehensive assessment for informed judgment.

The selection of vendors should cover the relevant token and blockchain scope for the fund's activities.

For detailed procedures on conducting wallet ownership verification and implementing KYT checks using vendor tools, please refer to Appendix 2 – Enhanced Due Diligence Framework for Self-Hosted Wallets.

Best Practice#5 - VATP enhanced DD and SOC reporting

SOC 1 and SOC 2 reports provide essential insights into a VATP's operational controls. The SOC 1 report, focusing on financial controls and client asset safeguarding, should be extended to include independent third-party verification of total client asset holdings to confirm adequate reserves and prevent fractional reserve practices. The SOC 2 report assesses IT infrastructure, security, and data privacy, ensuring the reliability of VATP-issued statements.

Fund administrators should conduct enhanced due diligence, particularly for offshore VATPs, requiring these enhanced SOC reports and assessing ownership structure, regulatory standing, financial health, and cybersecurity. Ongoing monitoring should include reviewing updated SOC reports and tracking material changes in the VATP's control environment.

For detailed due diligence questions, refer to Appendix 1 - Enhanced Due Diligence on VATP/DA Custodians.

Appendix – Sample Due Diligence Frameworks: Industry Best Practices

This section consolidates practical "sample" due diligence frameworks collated from direct industry engagement. The content within has been synthesized from interviews with and materials provided by experienced fund administrators, fund managers, and audit firms that actively support digital asset funds. These frameworks are not theoretical but represent the evolved best practices and critical checkpoints used by professionals navigating the complex risks of digital assets. They are designed to be implemented directly or adapted for your specific due diligence processes.

It contains two comprehensive frameworks:

- Enhanced Due Diligence on VATP / DA Custodians - A detailed checklist for assessing the third-party service providers that form the core infrastructure of any digital asset fund, covering licensing, security, operations, and risk management.
- Enhanced Due Diligence Framework for Self-Hosted Wallets - A specialized protocol for validating and accepting asset transfers directly from investor-controlled wallets, addressing the unique challenges of source of funds, wallet screening, and transaction purity.

Appendix 1 – Enhanced Due Diligence on VATP/DA Custodians

Enhanced Due Diligence is important for VA service providers due to high fraud, regulatory, and operational risks. Fund administrators should check that exchanges, DA Custodians, and distributors are licensed, financially stable, secure, and reputable to protect investors and comply with regulations.

A fund manager should exercise due diligence in selecting their VATPs and DA Custodians. The due diligence process may be delegated to a Fund administrator to conduct the due diligence.

For VATP and DA Custodian

1. Regulatory Verification & Licensing

   The regulatory jurisdiction directly impacts the operation of the VATP or DA Custodian it supervises. Service providers who are under stronger regulatory regimes are usually considered to be more secure. Regulatory jurisdiction can be an indicator of the strength of operational compliance.

   - Confirm licenses / registrations across applicable jurisdictions; monitor ongoing status, enforcement actions, sanctions, and investor-protection alignment. For example, for a HK VATP, one should verify if the VATP is licensed (Type 1 Securities Dealing and Type 7 Automated Trading) by the Hong Kong Securities and Futures Commission (SFC) under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) and complies with the Guidelines for Virtual Asset Trading Platform Operators, confirm SFC approval and check past regulatory audits and findings.

2. Experience and Track Record

   - Review legal entity structure, ownership, related-party arrangements; assess financial strength, liquidity and solvency.
   - Confirm jurisdiction coverage, time zones, language support, local regulatory requirements, cross-border tax implications and client onboarding suitability.

3. Reporting, Audit and Transparency

   - Obtain third party audits (e.g. SOC 1 or 2 reports) and understand its audit frequency and period coverage.
   - Confirm relevant control reports such as ISAE 3000/3402 are available for assessing and monitoring the processes, risks and controls.

4. Legal terms, Contracts and Exit Provisions

   - Understand terms and conditions of the services agreement.
   - Scrutinize master agreements, SLAs, data rights, termination, data return / destroy, transition assistance, review indemnities, liability caps, remedies for breach and reporting mechanism.

5. Anti-Money Laundering Policies

   - Does the VATP conduct effective customer identity verification and due diligence to prevent money laundering and malicious activities?
   - Verify and confirm the VATP's adherence to the SFC's AMLO requirements
   - FATF Travel Rule for crypto transactions, VATPs are mandated to gather, verify, and exchange specific customer information before facilitating any digital asset transfer, which ensures that personal data "travels" with a crypto or fiat transaction, increasing transparency and traceability.

- Does it comply with FATF Travel Rule for cross-border transfers? As per the FATF Travel Rule, the following information is to be verified by the originator VASP before transacting,
  - Originator's name,
  - Originator's account number,
  - Originator's physical address OR
  - Originator's national identity number, or customer identification number, or date and place of birth.
- The below information is to be verified by the beneficiary VASP before transacting,
  - Beneficiary's name,
  - Beneficiary's account number.
- How does the VATP handle the "sunrise issue"?
- Review their KYC / CDD procedure for investor onboarding
- Do they screen investors against sanctions lists (OFAC, UN, EU)?
- Do they monitor for suspicious transactions?
- What is the minimum "purity" threshold accepted:
  - How is self-hosted wallet ownership verified (e.g. Satoshi test, signed message)?
  - Are flagged wallets (hacked / scammed / sanctioned) screened before transactions?

6. Segregation of Client Assets (Crypto & Tokenized Assets)

   In Hong Kong, licensed Virtual Asset Trading Platforms (VATPs) must comply with strict client asset segregation rules under the Securities and Futures Commission (SFC) regulatory framework. Unlike traditional securities, where assets are held in brokerage accounts, crypto assets are stored in wallets, requiring unique safeguards:

   - Conflict of Interest and Interdependence – Does the VATP have any connected party transaction where the counterparty concerned is the group affiliate in managing their digital asset portfolios
     - Is the DA Custodian independent or linked to a VATP or an affiliated distributors? (risk of self-dealing)?
   - Risk Management – Understand the risk management policies and procedures in respect of the proposed digital asset portfolio activities explaining how they manage the technology risk, market risk and liquidity risk in particular under a 24x7 operating environment

7. Wallet Management and Asset Transfer

   - Evaluate the VATP's trading platform's wallet management system and security measures
     - Assess the security and stability of the platform's wallet management system
     - Investigate measures for secure private key storage, such as cold storage, multi-signature, and distributed storage
     - Evaluate the mechanism for secure asset transfer, including security and reliability of fund withdrawals and storage
     - Determine the security controls for key generation, storage, management, and transaction signing

- Wallet's Key Management - To ensure a multi-signature scheme such as a 2-of-3 or 3-of-5 threshold should be used to ensure no single party can control the movement of the VA-assets
    - 2-of-3 threshold - Three keys are required to operate the wallet, with at least two signatures needed to approve a transaction.
    - 3-of-5 threshold - Five keys are required, with at least three signatures needed to approve a transaction.
    - All key holders are independent (i.e. not all controlled by the VATPs), and what types of wallets are used (e.g. hardware wallets, HSMs, etc (not plaintext keys))
    - If one of the keys lost, the remaining keys should still allow migration of VA assets to a new wallet.
    - Keys are securely stored in the required jurisdiction (if applicable, for example in Hong Kong) Hong Kong, with access restricted to authorized personnel only
    - Wallet whitelisting process – describe the procedure for whitelisting new wallet addresses
- Cold and Hot Wallet Allocation
    - According to SFC guidelines, authorised funds are required to hold most of their digital assets in cold wallets. This principle of secure custody is further reinforced for assets held by licensed Virtual Asset Trading Platforms (VATPs), which are mandated to store 98% of client assets in cold storage, limiting hot wallet exposure to only 2%. Although private funds are not subject to these specific regulatory requirements, it is considered a prudent risk mitigation practice to adopt a similar approach by minimizing hot wallet holdings to only what is necessary for liquidity, thereby avoiding the concentration risk associated with storing a majority of assets in a connected environment.
- Cold Wallet Storage
    - The hardware wallet should be safekept (e.g. in a safe deposit box with biometric, PIN access, etc.)
    - Describe how the cold storage is protected by physical hardware and software / cybersecurity infrastructure and operational control processes;

8. Trading System and Liquidity Oversight

   Assess the trading platform's trading system and liquidity management capabilities:

   - Review the trading system architecture, including the trading engine, order matching, and execution capabilities
   - Evaluate the trading process and monitoring mechanisms to ensure fairness, transparency, and compliance
   - Investigate liquidity management measures, including market depth, trading speed, and support for large volume and high-frequency trading
   - Determine whether the platform has high-speed and stable trading execution capabilities and support for large volume and high-frequency trading
   - Investigate the supervision of trading activities and compliance with market regulations.

9. Insurance Coverage

   - Ensure the VATP and DA Custodian maintain adequate compensation / insurance arrangements:
       - Who is the insurer underwriting the insurance policy

- Confirm coverage for professional indemnity and cyber liability, with explicit coverage for errors and breaches during VAPT operations
- Does the policy cover theft of digital assets by outside parties or insiders?
- Does the policy cover the loss / destruction of private keys caused by natural disasters or software bugs?
- If staking is offered, does the policy cover slashing loss?
- Are cold wallets, hot wallets, or both covered? Are any losses excluded?
- What legal entities are covered, and does the insured entity match the service agreement?
- Can clients purchase additional insurance?

10. Business Continuity Plan
    - Understand the business continuity and contingency arrangement including disaster recovery sites and recovery time objectives.

11. Incidents History
    - Review incidents related to regulatory, reputational, or cyber issues, including past security breaches and response measures
    - Check for negative news
    - Establish periodic reviews (annual / semi-annual) with trigger-based re-assessments; define KPIs, red flags, and change-notification protocols.

12. Additional Checks on Offshore VATP
    - For a private fund, investment managers may trade on an offshore VATP. It is generally recommended to use only those offshore VATPs that are regulated by the relevant jurisdiction's regulators or backed by regulated service providers. In both cases, the fund has its crypto account and the subscribers have their wallets).
    - These offshore VATPs should provide the relevant regulatory attestations, to ensure that all AML requirements are met.

13. Additional Due Diligence Specific to DA Custodians on Wallet Management and Asset Transfer:
    - How does the custodian's hardware and software infrastructure support wallet arrangements?
    - Assess the security and stability of the platform's wallet management system
    - Investigate measures for secure private key storage, such as cold storage, multi-signature, and distributed storage
    - Evaluate the mechanism for secure asset transfer, including security and reliability of fund withdrawals and storage and the approval mechanism within the DA Custodian. Identify procedures and controls for the transfer of fund assets out of the accounts with the custodians and the controls in place to prevent misappropriation of fund assets. Are there sufficient access log records?
    - Does the custodial facility have sufficient safeguards to protect against external threats?
    - Are the hardware components stored in secure locations? Are there measures for protection against natural disasters?
    - Does the custodian employ reliable authentication methods and technologies to ensure that only authorized personnel can access the platform?

Appendix 2 – Enhanced Due Diligence Framework for Self-Hosted Wallets

Private funds are increasingly accepting in-kind subscriptions from professional investors using stablecoins (e.g., USDC, USDT). While investments through wallets hosted by regulated VATP / DA Custodians often benefit from built-in KYT / KYW checks, the use of self-hosted wallets presents unique challenges for fund administrators. This section outlines due diligence considerations to address the operational, compliance, and security risks associated with these transactions.

Wallet Ownership Verification – The primary challenge is conclusively proving that the subscriber controls the self-hosted wallet address. The absence of a universal technical standard for proof-of-ownership leads to operational inefficiencies, security risks, and a suboptimal investor experience. Observed Verification Methods in the market include:

- Digital Signature (Signed Message) – The investor signs a specific, nonce-generated message from their wallet. This is the most common and secure method but may require technical guidance for the investor.
- Satoshi Test – This is a specific type of micro-transaction. The fund administrator provides the investor with a unique deposit address and a precise, unusual amount to send (e.g., 0.00541321 USDC). The investor must then initiate a transfer for that exact amount from their self-hosted wallet. This proves control over the wallet and definitively links the investor to the specific subscription transaction
- Generic Micro-Transaction – The administrator requests the investor to send a negligible, specific test amount. While effective, this method incurs minor transaction fees and can create accounting complexity.

Note: All these methods introduce manual steps and require secure logging to create a verifiable audit trail.

Wallet Risk Assessment (KYT / KYW) – Once ownership is established, a thorough risk assessment of the wallet's transaction history is mandatory. This "Know Your Transaction / Wallet" (KYT / KYW) process screens for exposure to illicit activities, including interactions with sanctioned addresses, mixers, darknet markets, or addresses associated with stolen funds.

A significant hurdle conducting KYT / KYW is the lack of regulatory consensus on an "acceptable" risk threshold or risk scoring. Leading blockchain analytics providers use proprietary algorithms, which can result in divergent risk scores for the same wallet across different platforms.

To ensure comprehensive coverage and mitigate vendor bias, the following multi-layered approach is advised:

- Primary Vendor Analysis: Conduct a formal risk assessment using a premier blockchain analytics tool.
- Secondary Tool Validation: Where feasible, validate the results using a second analytics provider to compare risk scores and flags.
- Blockchain Explorer Check: Supplement the automated tools by manually reviewing the wallet address on relevant blockchain explorers Scrutinize any warning labels or community-identified suspicious tags associated with the address

Until industry-wide standards for wallet verification and risk scoring are established, fund administrators should employ a rigorous, multi-faceted due diligence process. This framework balances the growing demand for digital asset innovation with the fund's duties of regulatory compliance, operational security, and investor protection.

About the Editors

The development of this best practice paper was overseen by a dedicated editorial team with extensive expertise in the digital asset domain.

Raymond Chung

Raymond Chung is a seasoned financial services executive with over 30 years of distinguished experience across securities services, fund management, and brokerage industries. He has built a robust career within premier global institutions, including HSBC Securities Services, HSBC Asset Management, Nomura, and UBS. Raymond currently holds a key leadership position as General Manager at AFAHKGBA and contributes to industry standards and practices as the Co-Chairperson of the Technical & Regulatory Sub-Committee.

Raymond served as the Chief Editor of this best practice paper, providing strategic direction and editorial guidance for the project. He was dedicated to fostering a collaborative environment, supporting the two co-authors who are recognized experts in the digital fund space, and ensuring the final document was both coherent and rigorous.

Margery Wong

Margery Wong is a finance executive with extensive experience from global custodians, fund administrators, and insurance companies. Her expertise spans the fund industry value chain, including Fund Accounting, Treasury, Client Servicing, and Product Strategy, with a focus on a diverse institutional client base.

Most recently, she was the Head of Finance and Fund Services at BOCI-Prudential Trustee Limited. Her distinguished career includes tenures at State Street, HSBC, BNP Paribas, and Sun Life Financial. She is a qualified accountant (ACCA) and an associate member of The Hong Kong Chartered Governance Institute (HKCGI).

She is a co-author of this paper and a member of the AFA Marketing Committee, contributing to the industry's advancement.

Andrew Wong

Andrew Wong is a global financial services executive with experience spanning Asia Pacific, Europe, and North America.

He was formerly the fund tokenization lead at UBS, where he launched the firm's first tokenized fund, and was responsible for digital asset ecosystem strategy, tokenized product and lifecycle structuring, on-chain risk and compliance analytics design, and technology architecture. Earlier in his career, Andrew was a management consultant (Engagement Manager) at Oliver Wyman, advising leading global financial institutions – including wealth and asset managers, banks, insurers and securities services firms – on a variety of strategic finance, risk and digital transformation topics.

He is a co-author of this paper and a member of the AFA Fintech Committee, contributing to the industry's advancement.

Together, the editorial team managed the end-to-end development process, ensuring the final output is a valuable contribution to the industry's understanding of best practices.

Acknowledgements

This best practice paper was developed through a structured and collaborative multi-stakeholder approach to ensure it is both authoritative and reflective of real-world expertise.

We extend our deepest gratitude to the Advisory Group, comprised of distinguished market experts who provided specialized guidance, practical insights, and validation throughout the development process. Their invaluable contributions from their respective areas of the digital asset ecosystem were essential to the paper's depth and relevance.

Our Sincere Thanks to the Advisors (listed alphabetically by last name):

- Kevin Lam of PwC
- Helen Li of PwC
- Gilbert Ng of Mulana Investment
- Gary Tiu of OSL Group
- Isabella Wong of Deacons
- Wally Yu of Chainlink Labs

The process began with in-depth interviews conducted with these and other market practitioners to gather frontline insights and practical knowledge. The overall direction and framework were then guided and validated by a dedicated committee from the AFA Association, ensuring alignment with the highest industry standards. This synergistic approach guarantees that the paper is a trusted resource for the profession.

Disclaimer: The advisors named herein provided inputs to the paper in their personal capacity voluntarily. Their participation does not constitute an endorsement of the paper's content, and they, together with their affiliated organizations, assume no responsibility for content and inaccuracies of the report.

Disclaimer

The content of this report represents the views of the authors and the AFA, which retain ownership of and all rights (including intellectual property rights) arising from the paper. The content, including any information, recommendations, and guidance contained in the paper (the "Content") is provided based on the public information available to AFA and is for general reference purposes only. While AFA used its best endeavour to ensure the accuracy and reliability of the Content, AFA, its chairman, committee members, officers, members, and agents make no representations or warranties of any kind, express or implied, regarding the completeness, accuracy, reliability, suitability or availability of the Content. AFA shall not be liable for any errors, omissions, or inaccuracies in the Content or for any actions taken or decisions made in reliance thereon. The Content is not intended to constitute and does not constitute professional advice on any matter, including but not limited to sales, tax, operational, legal, or accounting matters. You must not rely on the Content to substitute any advice from qualified professional advisors. You should seek independent professional advice for your specific circumstances. Any use, reproduction, distribution, dissemination, or referencing of the Content in any publication, media, or other format is strictly prohibited without the prior written consent of AFA. By accessing this Document, you acknowledge and agree to be bound by this disclaimer.

afa

The Association of Fund Administrators of
Hong Kong and the Greater Bay Area