GBBC
Global Blockchain Business Council

STANDALONE REPORT

# DECENTRALIZED FINANCE (DEFI) & VAULTS

## GLOBAL STANDARDS MAPPING INITIATIVE (GSMI) 7.0

GBBC GSMI 7.0

**GLOBAL BLOCKCHAIN BUSINESS COUNCIL**

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland

## THANK YOU TO OUR CO-CHAIRS

**Lee A. Schneider**
Ava Labs

**Sadia Halim**
Galaxy

**A full list of GSMI 7.0 contributing organizations can be found on page 43.*

TABLE OF
# CONTENTS

SECTION I

# INTRODUCTION

DeFi vaults have emerged as one of the most significant developments in decentralized finance, transforming blockchain applications from simple yield-generating tools into programmable asset management infrastructure. A vault is a smart contract that accepts user deposits and automatically executes predefined strategies according to rules encoded at deployment. The strategies can run the gamut of DeFi, including allocating capital across lending protocols, liquidity pools, staking platforms, and tokenized real-world assets.

Depending on the strategy, a vault may lend assets on decentralized lending protocols, provide liquidity to decentralized exchanges, stake tokens, reinvest earned rewards (auto-compounding), or rebalance positions as market conditions change. More advanced vaults can optimize collateral positions, hedge risk, or execute algorithmic trading strategies, all through transparent, onchain smart contracts. By automating these activities, vaults abstract away operational complexity, socialize transaction costs, and make sophisticated financial strategies accessible to a broader range of participants.

When DeFi participants provide capital to DeFi protocols, they can earn yield: a financial return generated entirely onchain and in a decentralized manner. While this can be compared to earning interest in a traditional bank account, DeFi yield lacks the deposit-like protections, fixed returns, low volatility, and principal protection typically associated with a bank account. DeFi vault returns may arise from lending, staking, trading fees, incentives, leverage, derivatives, or RWA cash flows.

A vault may rely on custodians, oracle operators, bridge providers, token issuers, off-chain servicers, governance bodies, etc. The smart contract may reduce certain intermediary functions without eliminating all intermediation.

From an institutional perspective, the opportunity is substantial. Boston Consulting Group projects that digital real-world assets could reach roughly 16% of global investable assets by 2035, following approximately 300% growth in tokenized RWAs on public blockchains in 2025 alone.[1] This trajectory is already visible in vault-specific activity: Morpho reported $13 billion in total deposits by the end of Q3 2025, up from $5 billion at the start of the year, with its Coinbase integration generating $960 million in active loans and $1.7 billion in posted collateral.[2] Separately, Coinbase disclosed more than $1 billion in cumulative bitcoin-backed loan originations through Morpho as of October 2025, with CEO Brian Armstrong publicly targeting $100 billion in onchain borrow originations going forward.[3]

Traditional asset managers are entering directly: Apollo Global Management, which crossed $1 trillion in assets under management in Q1 2026, agreed in February 2026 to acquire up to 90 million MORPHO tokens over 48 months to support onchain lending markets on Morpho's protocol.[4] Centralized exchanges are moving the same direction: Kraken launched "DeFi Earn" in January 2026, offering yield up to 8% APY by routing deposits into curated onchain vaults.[5]

The analytical starting point for understanding vaults is the distinction between software development (a type of infrastructure) and intermediation. Vaults, like all DeFi applications, are built on decentralized systems.

## OPPORTUNITY FOR DEFI ACROSS INSTITUTIONS

ACCORDING TO BOSTON CONSULTING GROUP & MORPHO

**16%**

GLOBAL INVESTABLE ASSETS COMPRISED OF DIGITAL RWAS BY 2035

**300%**

GROWTH IN TOKENIZED RWAS ON PUBLIC BLOCKCHAINS IN 2025

**$13B**

TOTAL DEPOSITS BY END OF Q3 2025, UP FROM $5B AT START OF YEAR

**$960M**

IN ACTIVE LOANS FROM MORPHO'S COINBASE INTEGRATION

**$1.7B**

IN POSTED COLLATERAL FROM MORPHO'S COINBASE INTEGRATION

**$1B**

IN CUMULATIVE BITCOIN-BACKED LOAN ORIGINATIONS THROUGH MORPHO AS OF OCTOBER 2025

In their simplest form, the code executes, the strategy runs, and no single person directs what happens to any particular user's assets. But as vaults have grown more sophisticated, a new category has emerged called "curated" vaults. There, a designated curator can do one or more of numerous activities, such as managing strategy parameters, selecting approved protocols, and exercising ongoing discretion over the deployment of user assets. This shift from full automation to some or a lot of human discretion is the key analytical divide, because it can be what changes the regulatory analysis, the risk profile, and the accountability structure of the vault.

One distinction that is essential to maintain throughout that analysis is the difference between the software developer who programs the vault protocol and the curator who engages in ongoing activities related to or including the vault's investment strategy. These are distinct functions. The same person or entity may perform both, but that does not make them the same thing. A developer who writes and deploys the smart contracts that govern a vault is encoding rules that execute autonomously.

A curator who subsequently exercises varying types of discretion over which protocols the vault deploys capital to, which risk parameters apply, and how the strategy evolves over time might be performing an investment management function.

Conflating the two produces analytical errors with significant regulatory and accountability consequences. Where the same entity performs both functions, the analysis must assess each function separately.

This paper builds on GBBC's December 2024 **Global Standards Mapping Initiative (GSMI) 5.0, "Decentralized Finance—Opportunities, Risk Considerations, and Key Principles for Growth**,"[6] which established a foundational taxonomy of DeFi concepts, identified the risks associated with different categories of DeFi participants, and proposed a set of principles and standards to guide the responsible development of decentralized finance.

This paper extends that analysis, focusing specifically on the vault ecosystem, its participants, and the governance, risk, and regulatory considerations that vault structures present. It covers the spectrum of curated to uncurated vaults, the assets they involve, their smart contract architecture, the ecosystem of participants that support them, the risks they present, and the regulatory and compliance considerations they raise. Throughout, the nature of the activity, and in particular the degree to which human discretion is exercised over user assets, is the lens through which each of these topics should be understood across all dimensions.

SECTION II

# OVERVIEW OF VAULTS & CURATED VAULTS

## WHAT ARE VAULTS?

A vault can be referred to as a blockchain-based structure, typically implemented through one or more smart contracts, that allows users to transfer a particular token (most commonly, a stablecoin) to the vault and receive in return a ‘receipt’ token that permits the holder to receive back a proportional amount of the assets held in the vault at a later time.[7]

This smart contract automatically executes predefined rules or strategies governing deposited assets on behalf of users according to a predefined strategy (e.g., investment, lending, rebalancing, collateral allocation, yield generation and optimization, managing leverage, liquidity provision, risk management). A pooled structure automatically deploys the assets deposited from multiple users.

This way, rather than requiring users to actively move funds between DeFi protocols to access different lending platforms, liquidity pools, or other yield-generating opportunities, a vault automates these activities. This allows users to benefit from financial strategies without actively managing every transaction. Moreover, as users can pool their funds into a vault that executes onchain strategies to pursue a defined investment or financial objective, transaction fees can be socialized, splitting gas costs among all users in a given pool rather than having each user pay the full fee individually.

A vault may also be designed for liquidity preservation, hedging, collateral efficiency or risk control, beyond just maximizing profit. Users deposit assets into a vault and receive a token or accounting record representing their share of the pooled assets, as well as any gains or losses generated from the activities deployed by the vault. Vaults are designed to abstract away operational complexity for users by accepting user deposits and automatically executing predefined blockchain-based yield strategies without manual intervention.[8]

Importantly, a vault actively deploys these pooled assets into a yield-generating strategy—such as lending, liquidity provision, staking, looping, or auto-compounding—rather than simply holding them. A contract that only custodies assets without deploying them, such as a static escrow, would not meet this definition. Because returns depend on the performance of that underlying strategy, a vault's receipt token is subject to the performance and risk of the strategy it is deployed into, and its value is not guaranteed to hold or increase.

Many vaults today implement this receipt-token mechanism through a common technical standard, discussed further in the Smart Contract & Programming Considerations section below.

# WHAT IS THE PURPOSE OF VAULTS?

The main purpose of vaults is to generate yield based on digital asset collateral (e.g., stablecoins, crypto) deposited by users. This is carried out by automating the management of digital assets in ways that optimize yield generation. In the context of vaults, yield refers to passive returns generated by depositing cryptocurrency into automated, strategy-driven smart contracts. The most basic form of this is simple yield, described below. What makes vaults attractive is largely this automation.

The yield generated is typically variable, fluctuating with factors like borrower demand and protocol utilization, rather than fixed or guaranteed.[9]

A smaller subset of vaults does offer a fixed, pre-defined yield for a set term, but this is a specialized structure rather than the default.[10]

Simple yield in DeFi vaults is the baseline return earned directly from fundamental, low-complexity activities. It remains stationary in one proven strategy, usually with no active rebalancing. For instance, single action deposits may involve users depositing a token into a vault (e.g., Aave Simple Earn Vault) that can route the funds directly into a single lending market.

At a high level, the following strategies can be executed by vaults to provide common sources of yield:

**Lending Interest**

Users can lend capital to borrowers or borrowing pools to generate interest. With base interest rates, returns come strictly from borrower demand on foundational protocols (e.g., Aave, Compound)

**Staking Rewards**

Users can lock up tokens to help secure a blockchain network and earn rewards in the form of network staking yields

**Trading Fees**

Users can provide liquidity to decentralized exchanges and earn a portion of trading/swap fees

**Incentive Tokens / Steward Rewards**

Protocols may provide users with governance tokens for using their platform

Another purpose of vaults is to pool capital and achieve economies of scale. By combining deposits from many participants, vaults can access investment opportunities, reduce transaction costs through batching, automatically compound rewards, and rebalance positions more efficiently than individual users. This creates a more streamlined and scalable way to participate in decentralized financial markets.

# WHAT ARE CURATED VAULTS AND THE ROLE OF CURATORS?

Curated vaults are DeFi vaults in which the investment strategy, eligible assets, counterparties, and risk parameters, among other elements, are actively selected and governed by a designated curator rather than being fully automated or open-ended. A vault curator can be referred to as "an independent team or entity—not part of [a given protocol]—that designs, deploys, and manages onchain vaults."[11]

More specifically, "the assets held in the vault are generally pre-programmed to be deployed in one or more yield-generating strategies determined by a 'curator.'"[12] Notably, the curator is not a direct custodian, but instead influences allocation and risk management through predefined permissions and parameters. They emerged as a response to two related issues in early DeFi lending. The first was the risk profile of broad shared liquidity pools, which exposed lenders to cross-asset contagion, governance risk, and shared insolvency.

The second was the fragmentation created by increasingly permissionless protocol design. Anyone could create lending markets with customized parameters, but few users had the expertise to evaluate the resulting proliferation of options.

The curator steps in as a risk management and capital allocation layer: evaluating protocols, establishing approved strategies and counterparties, setting concentration limits and liquidity thresholds, and managing multi-asset portfolios on behalf of depositors. Rather than deploying funds to any available market offering the highest yield, the curator assesses protocol security, liquidity, collateral quality, counterparty exposure, and market conditions before approving investment opportunities.

This allows vaults to pursue more stable, risk-adjusted returns while reducing exposure to weaker or untested protocols. This model has become especially prominent in decentralized lending ecosystems such as Morpho and Euler. The introduction of a curator, however, places a vault on a spectrum that purely automated vaults do not occupy. Where a vault's curation sits on that spectrum is the primary determinant of its regulatory treatment, risk profile, and accountability structure. At one end, a curator's discretion is tightly constrained by smart contract guardrails.

For example, the code enforces which protocols the vault may use, what the concentration limits are, and the frequency or availability of changes, including giving users the chance to exit. In these structures, the smart contract, not the curator, is the primary decision-maker and implementer; the curator suggests or influences the system within boundaries the protocol itself enforces.


A vault curator may select:

- acceptable collateral assets
- loan markets
- concentration limits
- risk parameters
- liquidity allocation rules
- rebalancing logic
- oracle and valuation requirements
- allocators or other authorized execution roles

At the other end, a curator exercises essentially unconstrained active discretion, dynamically reallocating capital across protocols and strategies based on ongoing judgment about risk and return, which begins to resemble active portfolio management.

Most curated vaults sit somewhere between these poles, combining hard-coded constraints with areas of genuine curator judgment.
The analytical question for regulatory purposes, for risk assessment, and for accountability, is what the curator actually does and how much genuine discretion or control they exercise over user assets and the decisions related to where those assets are utilized or invested.

That question requires maintaining a distinction between the software developer who builds the vault protocol and the curator who manages the vault. These are distinct functions (see page 6).

Conflating software development with vault curation produces regulatory and accountability errors that can be consequential.

Where the same entity performs both functions, each must be assessed separately: the developer role on its own terms, the curator role on its own terms, and the combination assessed for whether the developer's technical access amplifies or changes the curator's effective control over user assets.

# PURPOSE OF CURATED VAULTS

Curated vaults address several related needs in DeFi lending: risk exposure in early shared-liquidity models, the fragmentation and complexity created by increasingly permissionless market design, the difficulty individual users face evaluating and allocating capital across many markets, differentiated risk appetites among depositors, and demand for professional delegation and distribution of DeFi-based products.

One of the clearest drivers was the risk profile of early DeFi lending models (e.g., pooled systems like Aave and Compound) that used broad shared liquidity pools. While efficient, they exposed lenders to risks like cross-asset contagion, governance risk, and shared insolvency.

Across DeFi systems, protocols themselves may have become highly permissionless, meaning that anyone could create applications (e.g., lending markets) with customized parameters. This created fragmentation and varying risk quality. Newer modular lending systems (e.g., Morpho Blue) introduced isolated markets, customizable risk parameters, and permissionless market creation.

While users faced too many fragmented markets to evaluate on their own, curated vaults became increasingly relevant as a risk management layer. The rise of curated vaults is particularly evident in decentralized lending, where increasingly permissionless and modular market structures created a need for an additional risk-selection and capital-allocation layer.

Hence the primary purpose of curated vaults is to improve risk management and capital allocation. Rather than deploying funds to any available lending market or liquidity pool offering the highest yield, the curator evaluates factors such as protocol security, liquidity, collateral quality, counterparty exposure, smart contract risk, and market conditions before approving investment opportunities.

This allows depositors to delegate market selection and risk management according to a defined mandate, rather than independently evaluating each underlying market while also allowing vaults to pursue more stable, risk-adjusted returns while reducing exposure to weaker or untested protocols.

SECTION III

# LANDSCAPE OF VAULT ACTIVITIES

As the vault landscape has evolved from simple yield optimization tools into a diverse ecosystem of onchain asset management solutions serving retail users, DAOs, crypto-native funds, and increasingly institutional investors, vaults now differ not only by the assets they manage, but also by their investment strategies, governance models, risk controls, and target users. This evolution reflects the broader maturing of DeFi from experimental applications toward more structured financial infrastructure.

The vault ecosystem also includes a range of governance models. Permissionless (often simple yield) vaults allow anyone to deposit assets and participate, reflecting the open nature of DeFi. In contrast, curated and permissioned vaults introduce investment oversight, approved protocol lists, identity verification, and compliance controls that make them more suitable for regulated financial institutions. Many newer vaults also incorporate decentralized governance through DAOs, while others rely on professional asset managers or specialized risk committees to oversee strategy decisions.

Vault yield mechanisms can be categorized as follows:

**TABLE 1: VAULT YIELD STRATEGIES**

| Family | Strategy | How it Generates Yield | Typical Assets |
|---|---|---|---|
| Lending & leverage | **Lending** | Deposits are lent to borrowers on decentralized money markets; yield is the interest borrowers pay | Stablecoins, BTC, ETH |
| | **Leverage & looping** | Collateral is borrowed against and the proceeds recycled into the same or a correlated position, repeated to amplify exposure (includes leveraged yield farming); magnifies gains and losses | Stablecoins, ETH, LSTs |
| | **Collateral optimization** | Collateral is reallocated across lending/borrowing markets to improve yield while holding target risk and health levels | Stablecoins, ETH, wrapped assets |
| Staking & restaking | **Staking** | Assets are staked to help secure a proof-of-stake network; validator rewards (block rewards and fees) flow to depositors | ETH, SOL, other PoS tokens |
| | **Liquid staking** | Assets are staked while the depositor holds a liquid staking token (LST) that remains usable elsewhere in DeFi | ETH, SOL, LSTs |
| | **Restaking** | Staked assets or LSTs are re-pledged to secure additional protocols for incremental rewards and incremental risk | ETH, LSTs |

| Family | Strategy | How it Generates Yield | Typical Assets |
|---|---|---|---|
| Liquidity provision & market making | **Liquidity provision (AMM/LP)** | Assets are supplied to automated market-maker pools, earning a share of swap fees, often auto-compounded | LP tokens, stablecoins, ETH/crypto |
| | **Market making** | Liquidity is quoted on DEX or order-book venues, earning spreads and fees from facilitating trading | Stablecoins, ETH/crypto |
| Incentives & protocol rewards | **Yield farming / liquidity mining** | Positions earn a protocol's newly issued governance or incentive tokens on top of base yield | Stablecoins, ETH, LP tokens |
| | **Governance & protocol revenue sharing** | Deposited assets accrue governance/voting tokens or a share of protocol revenues distributed to participants | Governance tokens, stablecoins |
| | **MEV capture** | The vault captures a share of maximal extractable value (e.g., from transaction ordering) and distributes the proceeds | ETH, stablecoins |
| Market-neutral & derivatives | **Market-neutral / delta-neutral** | Offsetting long/short positions minimize directional exposure while capturing funding rates and basis spreads (includes basis trading and funding-rate arbitrage) | Stablecoins, spot crypto (hedged with perpetual futures) |
| | **Options / structured products** | Systematic options strategies (covered calls, cash-secured puts) or packaged risk-return products generate premia or engineered payoffs | ETH, BTC, stablecoins |
| | **Cross-protocol arbitrage** | Capital moves between protocols to capture temporary differences in rates, prices, or incentives | Stablecoins, ETH/crypto |
| Real-world assets & treasury | **RWA yield** | The vault holds tokenized traditional assets and distributes their off-chain cash flows to depositors | Tokenized treasuries, money market funds, private credit |
| | **Tokenized fund exposure** | Capital is allocated to professionally managed onchain funds pursuing diversified strategies | Tokenized fund units/shares |
| | **Treasury management** | Idle DAO or enterprise capital is allocated to conservative, policy-constrained yield opportunities | Stablecoins, tokenized deposits, tokenized treasuries |

**TABLE 2: CROSS-CUTTING APPROACHES AND MECHANISMS**

| Item | What it is | Applies to |
|---|---|---|
| **Yield optimization / active rebalancing** | A portfolio-level approach that dynamically allocates capital across strategies to maximize risk-adjusted yield | Multi-strategy and actively managed/ optimized strategies |
| **Auto-compounding** | Earned rewards are automatically claimed, converted, and reinvested to compound returns | Most yield strategies |
| **Price-per-share accounting** | Yield accrues by increasing the value of each vault share rather than by distributing tokens (the common ERC-4626 mechanism) | Vault share/receipt token |

# MULTI-STRATEGY VAULTS

Vaults can increasingly leverage composability by integrating multiple DeFi protocols into a single investment strategy. A single vault may simultaneously use lending markets, decentralized exchanges, staking protocols, derivatives platforms, and tokenized real-world assets to optimize returns and manage risk. Advances in automation, oracle infrastructure, interoperability, and smart contract security have enabled vaults to become significantly more sophisticated than early yield farming applications.

Many DeFi vaults combine several of these mechanisms simultaneously. For example:

- **Yield optimizer vault:** Lending + auto-compounding + liquidity mining
- **Liquid staking vault:** Staking + liquid staking + lending of the liquid staking token
- **Institutional treasury vault:** RWA yield + treasury management + collateral optimization
- **Market-neutral vault:** Delta-neutral trading + funding rate arbitrage + basis trading
- **DeFi index vault:** Diversified allocation across lending, staking, liquidity provision, and tokenized funds

SECTION IV

# ASSETS HELD AND MANAGED BY DEFI VAULTS

DeFi vaults can hold and manage a wide range of digital assets, determined by their mandate, underlying investment strategy, and the blockchain protocols involved. The most common assets include native cryptocurrencies (e.g., ETH, SOL, BTC), stablecoins (e.g., USDC, USDT, or other fiat-backed stablecoins), and governance tokens issued by decentralized protocols. These assets may be deposited directly into the vault or acquired as part of the vault's strategy.

Many vaults also manage yield-bearing and derivative assets in the form of tokenized positions that continue generating yield while remaining composable across the broader DeFi ecosystem. The digital assets involved for these activities include liquid staking tokens (LSTs), such as tokenized representations of staked assets, liquid restaking tokens (LRTs), liquidity provider (LP) tokens received from decentralized exchanges, lending tokens representing deposits in money markets, and vault receipt tokens that may represent a user's proportional claim on the vault's underlying assets.

More sophisticated vaults are increasingly incorporating tokenized real-world assets (RWAs) (e.g., tokenized U.S. Treasuries, money market funds, private credit, commercial paper, commodities, real estate interests, and other financial instruments), which enable strategies combining traditional sources of yield with blockchain-based automation, settlement, and transparency. Institutional-focused vaults may also hold tokenized deposits, digital cash equivalents, or regulated investment fund tokens.

Ultimately, the mandate plays a central role to determine digital assets to be held in a vault. For instance, a conservative treasury vault may primarily hold stablecoins and tokenized Treasury securities, while a yield optimization vault may actively manage ETH, liquid staking tokens, LP tokens, and governance tokens across multiple protocols. As institutional adoption expands, vaults are expected to support an increasingly diverse range of tokenized financial assets, enabling programmable portfolio management across both native digital assets and traditional financial instruments.

# VAULTS FOR TOKENIZED RWA

Tokenized RWA vaults, as one of the most promising categories of vaults for institutions at the moment, can be used to invest in, manage, and distribute returns from tokenized representations of traditional financial assets. These vaults are expected to become an important component of institutional blockchain infrastructure by offering, beyond investment products alone, programmable asset management vehicles that provide exposure to the economic characteristics of traditional financial assets with the automation and interoperability of decentralized finance.

Tokenized RWA vaults hold blockchain-based tokens that represent ownership or beneficial interests in off-chain assets that traditionally generate returns for investors (e.g., U.S. Treasuries, money market funds, private credit, corporate bonds, real estate, commodities, or other off-chain financial instruments). The management of these tokenized assets can be automated, while providing investors with transparent, programmable, and onchain access. This enables a range of opportunities including:

- Off-chain traditional yield-bearing assets onchain
- Programmable portfolio and treasury management
- Improved settlement speed, transparency, and operational efficiency
- Increased capital mobility (easier to transfer, collateralize, and integrate into other onchain financial applications)
- Providing a foundation for AI-driven treasury management, where autonomous agents can allocate liquidity across tokenized money market funds, Treasury vaults, repo facilities, and other regulated onchain investment vehicles based on predefined risk and investment policies

The primary purpose of RWA vaults is to pool investor capital and allocate it to one or more tokenized real-world assets under a predefined investment strategy.

For example, a vault may accept deposits of USDC and automatically invest them in tokenized U.S. Treasury funds to generate yield from government securities. The vault can distribute interest payments, reinvest proceeds, rebalance allocations, and process subscriptions and redemptions through smart contracts, reducing operational complexity and improving efficiency. The liquidity profile of different forms of tokenized RWA may differ significantly, with treasuries and publicly traded stocks among the most liquid. It may not yet be clear if adding venues to trade on may change this liquidity profile.

For institutions, tokenized RWA vaults can bridge traditional finance (TradFi) and decentralized finance (DeFi) in a way that combines the economic characteristics and cash flows of traditional financial assets with blockchain-based automation, transparency, and composability to carry out many activities resembling existing financial processes in a more efficient manner (e.g., treasury management, cash optimization, collateral management, liquidity management, and diversified investment portfolios). Because the underlying assets are tokenized, they can also integrate with other onchain financial services such as lending, collateralization, and programmable settlement, given the right interoperability mechanisms.

Many institutional RWA vaults also incorporate curation and permissioning, where curators select approved assets, define investment mandates, and monitor portfolio risks, while permissioned access may restrict participation to verified investors and enforce compliance requirements (e.g., KYC, AML, sanctions screening, and securities regulations). Institutional RWA vaults typically rely on regulated custodians or qualified custodial arrangements to safeguard tokenized assets and associated private keys. This governance model makes tokenized RWA vaults more suitable for regulated financial institutions than fully permissionless DeFi strategies.

**TABLE 3: EXAMPLES OF TOKENIZED RWAS HELD IN VAULTS**

| Tokenized RWA | Vault Use Case |
|---|---|
| **U.S. Treasuries** | Generate low-risk yield and manage institutional cash reserves |
| **Money Market Funds** | Provide liquidity with short-duration and income-generating investments |
| **Private Credit** | Earn yield from tokenized loans to businesses or infrastructure projects |
| **Corporate Bonds** | Generate fixed-income returns through diversified bond portfolios |
| **Real Estate** | Provide fractional exposure to income-producing commercial or residential properties |
| **Publicly Traded Stocks** | Provide price exposure to equities and income streams attached to them, such as dividend payouts |
| **Commodities** | Hold tokenized gold or other commodities as inflation hedges or portfolio diversifiers |
| **Trade Finance Assets** | Invest in tokenized invoices, receivables, or supply chain financing assets |
| **Carbon Credits** | Support sustainability strategies through tokenized environmental assets |

SECTION V

# SMART CONTRACT & PROGRAMMING CONSIDERATIONS

Smart contracts are self-executing programs deployed on blockchain networks that automatically perform predefined actions when specified conditions are met. DeFi vaults rely on smart contracts to automate the execution of predefined strategies for the management of digital assets, following a transparent logic that is carried out deterministically on the blockchain. A vault contract, designed to manage user deposits and accounting, accepts user deposits, issues receipt tokens or records ownership shares, and calculates each participant's proportional claim on the vault's assets. This calculation defines the subsequent deposits, withdrawals, fee collection, and reward distribution without requiring manual intervention.

Most vaults also include strategy contracts, designed to implement investment logic. Strategy contracts define how assets are deployed to generate yield, interacting with a wide range of DeFi protocols through standardized interfaces, (e.g., lending markets, decentralized exchanges, staking platforms, derivatives protocols, and liquidity pools) to carry out predetermined functions. These functions may automatically rebalance portfolios, harvest and reinvest rewards (auto-compounding), manage collateral ratios, execute swaps, or migrate funds when governance or predefined conditions trigger strategy updates.

From a technical perspective, DeFi vaults are designed to be modular and upgradeable. A common architecture separates the vault contract from the strategy contract, allowing strategies to be added, replaced, or retired without requiring users to withdraw their assets. This modular design improves flexibility, supports evolving market conditions, and enables governance to adapt investment strategies while maintaining transparency and minimizing operational disruption.

Moreover, because vaults may manage highly valued assets, the underlying smart contracts must incorporate extensive security and risk management features. These may include role-based access controls, multisignature administration, emergency pause ("circuit breaker"), withdrawal limits, timelocks for governance changes, oracle integrations for price data, slippage controls, liquidation protection, and automated health checks. Many institutional-grade vaults also have permissioning controls, identity verification hooks, compliance checks, and detailed event logging to improve auditability and adherence to any regulatory requirements.

SECTION VI

# VAULT ECOSYSTEM MAP

Below is an ecosystem map of the major stakeholders involved in the DeFi vault ecosystem, including both crypto-native participants and the emerging institutional ecosystem, representing the landscape of DeFi vault activities and services. The table below also includes examples of leading providers, noting that the landscape evolves rapidly and these examples are likely to continue to evolve.

**TABLE 4: MAJOR STAKEHOLDERS IN THE DEFI VAULT ECOSYSTEM**

| Stakeholder | Primary Role: Activities | Service Providers |
|---|---|---|
| End Users / Investors | Deposit assets into vaults to earn yield, gain diversified exposure, or delegate portfolio management to automated or curated strategies | • Retail investors |
| Institutional Investors & Infrastructure | Use vaults and set strategies for treasury management, collateral optimization, yield generation, and exposure to digital assets within defined risk and compliance frameworks | • Financial institutions<br>• **Institutional DeFi Infrastructure:** Canton Network, ClearToken, M^0 |
| Curators / Asset Managers | Actively manage curated vault strategies (design investment mandates, select approved protocols and assets, establish risk limits, monitor performance, etc.) | • Professional asset managers<br>• **Curated Vault Management services:** Gauntlet, Steakhouse Financial, Re7 Labs<br>• **Onchain asset management services for curators:** Enzyme Finance, Lagoon Finance, dHEDGE<br>• **Treasury Management Services:** Karpatkey, Avantgarde Finance (Enzyme), StableLab |
| Vault Protocols & Protocol Developers | Build and maintain the vault smart contracts, accounting systems, automation logic, and user interfaces that enable vault operations | • **Vaults:** Yearn Finance, Morpho Vaults, Beefy Finance<br>• **Curated Vaults:** Morpho, Gauntlet, Steakhouse Financial, Euler |
| DeFi Protocols | Provide the underlying lending, trading, derivatives, staking/restaking, or liquidity infrastructure that vaults integrate into their investment strategies | • **Yield Optimization:** Yearn Finance, Beefy Finance, Re7 Labs<br>• **Lending Markets:** Aave, Morpho, Spark, Compound<br>• **Liquidity Provision:** Uniswap, Curve, Balancer<br>• **Liquid Staking:** Lido, Rocket Pool, Binance Staked ETH<br>• **Restaking:** EigenLayer, Symbiotic, Karak<br>• **Market-Neutral Strategies:** Ethena, Neutral Trade, Aperture Finance<br>• **Basis & Funding Rate Strategies:** Ethena, Rage Trade, Contango<br>• **Decentralized Exchanges (DEXs):** Uniswap, Curve, Balancer<br>• **Derivatives Protocols:** Hyperliquid, dYdX, GMX<br>• **Insurance/Smart Contract Cover:** Nexus Mutual, Sherlock, InsurAce |

| Stakeholder | Primary Role: Activities | Service Providers |
|---|---|---|
| Oracle Providers | Supply external price feeds and market data used for valuation, collateral management, liquidations, and automated investment decisions | • Chainlink, Pyth Network, RedStone |
| Smart Contract Automation | Smart contract functions and automated execution | • Chainlink Automation, Gelato, OpenZeppelin Defender |
| Cross-Chain Messaging, Interoperability, and Bridge Providers | Enable vaults to move assets across blockchains, expanding access to investment opportunities while introducing interoperability risks | • **Interoperability:** LayerZero, Wormhole, Chainlink CCIP<br>• **Bridges:** Across, Stargate, Wormhole |
| Stablecoin Issuers | Issue stablecoins that serve as the primary settlement and investment assets for many vault strategies | • Circle, Tether, Paxos |
| Tokenized Asset Issuers & Infrastructure | Issue tokenized treasuries, money market funds, private credit, commodities, and other real-world assets increasingly used within institutional vaults, and provide the underlying infrastructure for tokenized assets. Offer regulated investment products and bring traditional financial assets onchain | • **Tokenized Treasuries/RWA Issuers:** BlackRock (BUIDL), Franklin Templeton (BENJI), Ondo Finance<br>• **Tokenization Infrastructure:** Tokeny, Canton Network, ERC-3643 ecosystem<br>• **Tokenized Fund Infrastructure:** Superstate, Securitize, Dinari |
| Custodians (Qualified or Self-Custody Infrastructure) | Secure cryptographic keys and digital assets, particularly for institutional participants or hybrid custody models. Qualified custodians safeguard institutional assets | • **Institutional Custody:** Fireblocks, Copper, BitGo<br>• **Wallet Infrastructure:** Safe, MetaMask Institutional, Rabby<br>• **MPC Wallet Infrastructure:** Fireblocks, Fordefi, ZenGo X (threshold-cryptography research and OS projects) |
| Maximal Extractable Value (MEV) Infrastructure Providers | Optimize transaction execution and reduce front-running while capturing or minimizing MEV | • Flashbots, bloXroute, Titan Builder |
| Identity & Compliance Providers | Support KYC, AML, sanctions screening, decentralized identity, and permissioning for regulated or institutional vaults. Identity and programmable compliance providers enable permissioned participation | • **Identity & Compliance:** Quadrata, Ethereum Attestation Service (EAS), SpruceID, TRM Labs, Chainalysis<br>• **AML & Blockchain Analytics:** Chainalysis, TRM Labs, Elliptic |
| Security Auditors | Perform smart contract audits, code reviews, penetration testing, and formal verification to reduce technical vulnerabilities. Auditors and assurance providers support operational resilience and regulatory confidence | • **Smart Contract Auditing/Assurance:** OpenZeppelin, Trail of Bits, CertiK, Certora<br>• **Formal Verifications:** Certora, Runtime Verification, Veridise<br>• **Bug Bounty Platforms:** Immunefi, Hats Finance, HackenProof |
| Risk Management Providers & Governance Specialists | Assess protocol risk, monitor exposures, model scenarios, and establish risk limits for vault strategies and portfolios. Risk and governance specialists oversee investment mandates | • **Risk Management:** Gauntlet, Chaos Labs, Block Analitica<br>• **Risk Monitoring:** Chaos Labs, Gauntlet, OpenBlock Labs<br>• **DAO Governance Platforms:** Tally, Snapshot, Boardroom |
| Analytics & Data Providers | Supply dashboards, onchain analytics, performance metrics, portfolio reporting, and risk monitoring for vault users and managers | • **Onchain Analytics:** Artemis, Nansen, Dune<br>• **Portfolio Analytics:** DeBank, Zapper, Arkham |
| Regulators & Policymakers | Establish legal and regulatory frameworks governing digital assets, investment products, custody, AML/CFT, securities, and consumer protection | • Global financial services regulatory bodies |
| Standards Organizations | Develop technical, governance, cybersecurity, identity, interoperability, and operational standards that improve consistency and institutional adoption | • Global financial standards and technical standards bodies |



**Examples in each category are illustrative and not exclusive*

# INSTITUTIONAL ECOSYSTEM EVOLUTION

As DeFi matures, the ecosystem is expanding beyond retail participants toward a more institutional model. This evolution is further contributing to the transformation of DeFi vaults from simple yield optimization tools into programmable asset management infrastructure that connects decentralized finance with traditional capital markets.

These providers form the core infrastructure needed to support institutional-grade DeFi vaults, where governance, security, compliance, and operational resilience can be as important as yield generation.

Among institutional players, stakeholders that are becoming increasingly important include:

- Professional asset managers
- Tokenized fund issuers and other RWA issuers
- Qualified custodians
- Identity and programmable compliance providers
- Risk and governance specialists
- Auditors and assurance providers

For institutional adoption, several activities have become especially relevant:

- Curated vault management
- Risk management
- Tokenized real-world assets
- Institutional custody
- Identity and compliance
- Smart contract assurance

SECTION VII

# RISKS & HOW TO UNDERSTAND THEM

DeFi vaults are subject to a combination of technical, financial, operational, and governance risks because they rely on interconnected smart contracts, external protocols, and onchain market infrastructure. Since vaults often deploy assets across multiple decentralized applications, a failure in any component of the strategy can affect the entire portfolio. These risks can affect performance or lead to losses. Understanding these risks is essential for both individual and institutional participants. Many of these risks can be mapped against the risk assessment approach proposed in the GSMI 5.0 report on **"Decentralized Finance—Opportunities, Risk Considerations, and Key Principles for Growth**."[13] For basic vaults seeking simple yield, risks include the following:

- **Variable Yield Rates:** Yields float up and down based on market utilization rather than staying fixed.
- **Smart Contract Risk:** Even simple vaults carry baseline code vulnerability risks from the underlying protocol.
- **Lower Return Profiles:** Conservative stablecoin simple yields typically hover in a lower, more predictable baseline range.

Curated vaults, due to their more complex operations, can introduce new layers of smart contract vulnerabilities, flawed strategy design, oracle failures, governance attacks, market volatility, and liquidity shocks.

One of the most significant risks for vaults overall is smart contract risk. Vulnerabilities in the vault's code, or in any protocol with which it interacts, can be exploited, potentially resulting in partial or total loss of assets. A well-documented example specific to tokenized vaults is the donation or inflation attack affecting ERC-4626-based vaults, in which an attacker manipulates the vault's share-to-asset ratio, particularly around initial deposits and through rounding, to disadvantage other depositors. It is an especially acute risk for newly launched or low-liquidity vaults. Some implementations mitigate this by requiring a non-zero initial deposit at launch to raise the cost of manipulation. Aave's own vault deployment documentation, for example, requires such an initial locked deposit specifically to prevent this type of share-price manipulation.[14] Other technical risks include oracle failures that provide inaccurate market data, blockchain network congestion or outages, bridge vulnerabilities for cross-chain strategies, and integration failures between protocols. Because many vaults compose multiple DeFi services, they may also face composability risk, where a security weakness in one external protocol can cascade into the vault.

DeFi vaults also face market and liquidity risks. Asset prices can decline rapidly, leveraged positions may be liquidated, liquidity pools may experience significant withdrawals, and strategies may underperform due to changing interest rates or incentive structures. Participants in automated market maker (AMM) vaults may also be exposed to impermanent loss, while arbitrage and market-neutral strategies may become less profitable as market conditions evolve.

Finally, governance and operational risks play an increasingly important role, particularly for institutional adoption. These include poor strategy selection, ineffective risk controls, malicious or compromised governance decisions, concentration of decision-making authority, key-person dependencies, and inadequate monitoring or incident response. Moreover, misalignment of objectives between curators and investors can also lead to subpar performance, or deviation from investment mandates or intent. Additional concerns include regulatory uncertainty, cyber threats, and counterparty risk, where centralized service providers, custodians, or permissioned infrastructure are involved.

When designing or participating in DeFi vaults, particularly for institutional users, best practices to mitigate these risks typically require:

- smart contract audits
- formal verification
- continuous monitoring
- diversification
- robust and transparent governance
- transparent reporting
- clear operational controls
- risk limits
- clearly defined risk management policies

SECTION VIII

# AGENTIC & AI CONSIDERATIONS

Agentic AI has the potential to transform how DeFi vaults are managed by enabling autonomous financial decision making within predefined governance, risk, and compliance frameworks. What does it mean when an AI agent makes the decision to post liquidity in a vault? The convergence of agentic AI and DeFi vaults is a key factor in the evolution of vaults from passive investment products into autonomous financial infrastructure. Rather than a human manually deciding where to allocate capital, or in addition to human insight in the case of vaults managed by professional curators, an AI agent can continuously observe market conditions, evaluate risk and return, and execute transactions according to the vault's predefined objectives and constraints. In this model, the vault can play a role as one of many financial tools and services that an AI agent can use to optimize a portfolio, treasury, or payment strategy.

When an AI agent decides to post liquidity into a DeFi vault, it is effectively making an investment decision. The agent analyzes several factors (e.g., expected yield, smart contract security, protocol reputation, liquidity, historical performance, token incentives, market volatility, and counterparty risk) before determining whether the vault best satisfies the user's objectives. Once the decision is made, the agent can automatically take a variety of actions (e.g., sign and submit blockchain transactions, deposit assets into the selected vault, monitor the position over time, harvest rewards, rebalance capital into alternative vaults if conditions change, and ultimately withdraw funds when appropriate).

For institutions, this decision-making process is expected to become significantly more sophisticated than simply selecting the highest annual percentage yield (APY). Enterprise AI agents may evaluate risk-adjusted returns, diversification requirements, liquidity needs, concentration limits, collateral eligibility, regulatory requirements, treasury policies, and operational constraints. For example, an institutional treasury agent may decide to allocate excess USDC into a permissioned Treasury-backed vault because it satisfies the organization's liquidity policy and investment mandate, while avoiding a higher yield but riskier permissionless strategy.

# ROLE OF AI AGENTS FOR DEFI VAULTS

**INVESTMENT DECISIONS**
Selects the most appropriate vault based on risk, return, liquidity, and policy objectives rather than simply maximizing yield

---

**PORTFOLIO OPTIMIZATION**
Continuously reallocates assets across multiple vaults to optimize overall portfolio performance

---

**RISK ASSESSMENT**
Evaluates smart contract security, protocol health, market volatility, oracle dependencies, and concentration risk before allocating capital

---

**REAL-TIME MONITORING**
Continuously monitors vault performance, liquidity, protocol governance changes, and emerging threats

---

**AUTONOMOUS REBALANCING**
Moves assets between vaults as yields, risks, or liquidity conditions evolve

---

**POLICY ENFORCEMENT**
Ensures allocations comply with investment mandates, treasury policies, and governance constraints defined by users or institutions

---

**PROGRAMMABLE COMPLIANCE**
Screens counterparties, verifies identities, enforces jurisdictional restrictions, and checks sanctions or regulatory requirements before investing

---

**EXPLAINABILITY**
Records why a vault was selected, what factors influenced the decision, and how the recommendation aligns with policy

**HUMAN OVERSIGHT**
Supports configurable approval workflows where high-value or higher-risk allocations require human authorization before execution

**OPERATIONAL RESILIENCE**
Responds to market disruptions, protocol incidents, smart contract exploits, or governance attacks by automatically reducing exposure or exiting positions

**MULTI-AGENT COORDINATION**
For more sophisticated institutional treasury operations, a single agent may be insufficient. Specialized agents, for example, one focused on risk assessment, another on execution, another on compliance screening, may need to coordinate with each other, potentially under an orchestrating agent, to manage the full vault allocation lifecycle rather than concentrating every function in one system

Agentic AI has the potential to make DeFi vaults into dynamic capital allocation engines rather than static investment products. AI agents could continuously optimize capital across various platforms and mitigate risk. AI-driven vault management could become a core component of institutional treasury management, asset management, and cash optimization. When it comes to institutional treasury management, rather than finance teams manually deciding where to park excess liquidity each day, AI agents could continuously evaluate onchain investment opportunities, allocating capital in accordance with organizational objectives while maintaining full transparency, governance, and compliance.

As treasury operations scale in complexity, this is likely to involve multi-agent systems with specialized agents coordinating on risk, execution, and compliance rather than a single agent managing the entire process. This is likely to become a significant application of agentic AI in digital asset markets over the coming decade.

Ultimately, the emergence of autonomous financial agents also has implications on governance and accountability. Rather than asking *"Who chose this investment?"*, organizations must ask *"Who designed the decision policy?"* Human stakeholders establish the objectives, guardrails, and authorization levels, while the AI agents execute decisions within those boundaries. This introduces new requirements for explainability, auditability, transaction approvals, policy enforcement, and oversight to ensure that these autonomous decisions remain aligned with fiduciary responsibilities and regulatory obligations.

SECTION IX

# CYBERSECURITY CONSIDERATIONS

Recent regulatory developments have not yet explicitly stated cybersecurity requirements. Yet cybersecurity is one of the most critical considerations for DeFi vaults because of their nature as fully digital, programmable financial tools that often manage significant amounts of capital through smart contracts. Unlike traditional financial institutions, where unauthorized transactions can in most cases be reversed, exploits on public blockchains are often irreversible once executed.

As a result, vault security must address both the vault's smart contracts and the broader ecosystem of protocols, wallets, bridges, oracles, and other infrastructure upon which the vault depends. Best cybersecurity practices include comprehensive code reviews, independent security audits, formal verification, continuous monitoring, bug bounty programs, and secure software development practices.

The primary cybersecurity concern is smart contract security. Vulnerabilities (e.g., reentrancy attacks, access control flaws, arithmetic errors, logic bugs, flash loan exploits, oracle manipulation) can provide avenues for attackers to drain assets or manipulate vault behavior.

In addition, vaults that integrate with multiple DeFi protocols also face composability risk. Cybersecurity also extends to the operational infrastructure supporting vaults.

Private key compromise, wallet attacks, phishing, malicious software, compromised administrator credentials, DNS hijacking, front-end website attacks, and supply chain compromises can all lead to unauthorized transactions or loss of control over vault operations. Institutional deployments often mitigate these risks through multi-party computation (MPC), hardware security modules (HSMs), multisignature authorization, role-based access controls, privileged access management, network segmentation, and secure key lifecycle management.

Moreover, as DeFi vaults become increasingly AI-driven and institutionally managed, cybersecurity must also address autonomous decision making and operational resilience. AI agents interacting with vaults should operate within clearly defined authorization limits, verify transaction integrity, validate external data sources, and maintain detailed audit logs of their actions. Institutions should implement continuous threat detection, real-time anomaly monitoring, incident response plans, disaster recovery procedures, and governance mechanisms capable of pausing or restricting vault activity during a cyber incident.

Together, these measures help ensure that vaults remain resilient against both technical exploits and operational threats while supporting institutional trust and regulatory expectations.

For institutional DeFi vaults especially, cybersecurity should be treated as a defense-in-depth discipline that spans applications, infrastructure, governance, and operations. Alignment with established cybersecurity frameworks such as the NIST Cybersecurity Framework (CSF 2.0), NIST Secure Software Development Framework (SSDF), ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and the CIS Critical Security Controls is key, while incorporating blockchain-specific practices such as smart contract assurance, cryptographic key management, oracle security, and onchain monitoring.

Below is a mapping of cybersecurity tools and their functions, as relevant for DeFi vaults:

**TABLE 5: DEFI VAULT CYBERSECURITY TOOLS AND FUNCTIONS**

| Cybersecurity Tool | Function |
|---|---|
| **Smart Contract Security** | Audits, formal verification, secure coding, bug bounty programs |
| **Access Management** | Multisignature wallets, MPC, HSMs, role-based access control, least privilege |
| **Infrastructure Security** | Secure APIs, node security, cloud security, network segmentation |
| **Third-Party Risk** | Oracle providers, bridges, external protocols, software dependencies |
| **Transaction Security** | Transaction simulation, phishing protection, address validation, slippage controls |
| **Monitoring & Detection** | Onchain monitoring, anomaly detection, SIEM, security operations centers (SOC) |
| **Incident Response** | Emergency pause mechanisms, recovery procedures, communication plans, forensic capabilities |
| **Operational Resilience** | Backup infrastructure, disaster recovery, business continuity, redundancy |
| **Governance Security** | Timelocks, governance monitoring, proposal review, protection against governance attacks |
| **AI Security** | Guardrails for autonomous agents, explainability, approval workflows, protection against data and prompt manipulation |

SECTION X

# REGULATORY CONSIDERATIONS

The threshold regulatory question for any DeFi vault is not whether a smart contract is involved, or whether the structure is described as decentralized, automated, or non-custodial. It is what activity is actually being performed and by whom. Automation does not eliminate legal or regulatory obligations. As SEC Commissioner Hester Peirce put it in a statement specifically addressing crypto vaults, "[m]oving activities that fall within the scope of the federal securities laws onchain, as a general matter, does not take those activities outside the scope of the laws the Commission administers."[15] Accordingly, the starting point for regulatory analysis should be the activity being performed. With vaults, that often means assessing the degree to which human discretion is exercised over user assets to determine when regulatory obligations attach.

## THE ACTIVITY-BASED FRAMEWORK

For vaults, the regulatory analysis begins with two sequential questions. First, does anyone exercise meaningful control over the vault's activities? Second, if so, does that control amount to the provision of financial services?

These are distinct questions, and the answer to the first does not automatically determine the answer to the second. In other words, contrary to what some policymakers and regulators have proposed, the existence of control does not create a presumption that financial services are being performed.[16] Rather, one must inquire into the nature of that control to ensure that it is control over a regulated activity. Only then is the application of regulation warranted and justified.

A fully automated vault executing a predefined, immutable strategy with no curator exercising ongoing discretion presents a different regulatory profile than a curated vault in which a human decision-maker actively manages capital allocation. For the fully automated vault, answering the first question likely will find that no person controls the strategy, because the code executes autonomously according to predefined rules, and users can only act according to the vault's terms. As such, no analysis of the second question is needed because control is absent.

For the curated vault, however, the first question is likely answered affirmatively because the curator’s activities allow it to, among other things, direct assets. In this case, the second question becomes essential and turns on the nature of the curator’s actual powers and actions.

The capabilities that characterize financial intermediation and that connect control to the provision of financial services include the ability to execute or alter orders or transactions on behalf of users, the ability to affect how and where user assets are deployed, the ability to change the terms on which users participate, and the ability to determine what happens to user assets in a material way.

A curator empowered to exercise those capabilities is doing something that financial services law has long recognized as intermediation, regardless of whether the mechanism is a smart contract or some other technology. A fact specific analysis of the curator's powers is necessary to a determination of whether the curator is conducting, or has the power to conduct, regulated financial services.

# REGULATORY FRAMEWORKS THAT MAY APPLY

Because vaults can combine numerous investment strategies, asset types, and governance models, regulatory classifications are highly fact-specific and will continue to evolve. Several overlapping frameworks warrant consideration.

Whether vault receipt or share tokens constitute securities depends on the economic reality of the arrangement, including the expectations of depositors, the role of the curator or operator in driving returns, and the degree to which users are relying on the efforts of others. Where a curator actively manages strategy to generate returns for passive depositors, the arrangement begins to resemble a collective investment in many jurisdictions, including an investment contract in the US.

Whether a pooled vault constitutes an investment company, collective investment scheme, or equivalent regulated structure depends on the jurisdiction, the assets involved, and whether the vault is holding or investing in securities or other regulated instruments.

Institutional and permissioned vaults that hold tokenized securities or RWAs are particularly likely to engage these frameworks.

Whether a curator functions as an investment adviser, discretionary portfolio manager, commodity pool operator, or commodity trading advisor depends on the degree of ongoing discretion exercised, the nature of the assets managed, and the jurisdiction. Where a curator actively reallocates user assets across protocols based on ongoing judgment about risk and return, the functional resemblance to discretionary asset management is difficult to avoid.

Broker-dealer, futures commission merchant, virtual asset service provider (VASP), and money transmission or money services business frameworks may also be relevant depending on the vault's activities, particularly where vaults facilitate the exchange or transfer of assets on behalf of users.

For RWA vaults, securities, derivatives, and tokenization-specific laws and regulations introduce additional layers of analysis that are highly dependent on how the underlying assets are structured and offered.

Across all of these frameworks, sanctions compliance and AML obligations are necessary considerations. Vaults that interact with user assets, even on a fully automated basis, may not be categorically exempt from financial crime compliance requirements, and curators and operators should assess their obligations accordingly.

# THE DEVELOPER AND CURATOR DISTINCTION IN REGULATORY ANALYSIS

As discussed above, the software developer who builds the vault protocol and the curator who manages its investment strategy perform distinct functions that must be assessed separately.

This distinction matters in the regulatory context because the two roles carry different potential obligations. A developer who deploys immutable smart contract code is performing an infrastructure function, simply encoding rules that execute autonomously without ongoing human direction. That function does not, by itself, constitute financial intermediation or investment management.

A curator who exercises ongoing discretion over the deployment of user assets is doing something analytically different, and, as outlined above, the regulatory analysis attaches to the nature of those activities rather than to the underlying technology.

Where the same entity performs both functions, the regulatory analysis must assess each separately.

The developer function does not insulate the curator function from scrutiny, and the existence of smart contract constraints on the curator function does not automatically insulate it either. The question is whether the constraints are substantive and enforceable, or whether the curator retains effective authority to direct user assets in ways that constitute financial services or intermediation.

# INFRASTRUCTURE PARTICIPANTS

The ecosystem supporting DeFi vaults includes participants whose role is infrastructural rather than intermediary: validators, oracle providers, bridge operators, smart contract automation providers, auditors, and analytics services. These participants enable DeFi and vault protocols to operate without themselves exercising discretion over user assets or controlling financial outcomes.

Long-standing regulatory practice across financial markets does not treat infrastructure providers as financial intermediaries solely because their services are involved in (or even essential to) the execution of transactions or provision of financial services.

That principle applies in the DeFi context as well and vaults do not disrupt it.

The regulatory analysis changes only where an infrastructure participant crosses into exercising meaningful control over user assets or financial outcomes. But that is a change in activity from infrastructure to intermediation and does not alter the well-established principles that infrastructure provision and financial intermediation are distinct activities.

# REGULATORY UNCERTAINTY AND THE PATH FORWARD

Regulatory frameworks for DeFi vaults remain at an early stage in most jurisdictions. In the United States, for example, recent regulatory developments leave genuinely decentralized activities largely outside the direct regulatory perimeter, though the boundaries of that perimeter continue to be tested and refined through guidance and interpretation, as well as, if passed, the Digital Asset Market Clarity Act (H.R. 3633). Jurisdictions like the EU and UK have moved in broadly related directions, though through different mechanisms: MiCA currently exempts fully decentralized activity,[17] subject to a formal EU review opened in May 2026 that may narrow it,[18] while the UK's incoming FCA regime applies regulation wherever an "identifiable controlling entity" can be found.[19]

The ERC-4626 tokenized vault standard has become the dominant technical approach, but technical standardization does not resolve legal classification questions.

A vault that complies with ERC-4626 may still constitute a securities offering, an investment company, or a discretionary managed account depending on its structure and activities.

The most defensible approach for vault designers, curators, and institutional participants is an activity-based analysis conducted at the outset and revisited whenever the vault's strategy, assets, governance structure, curator authority, or user population changes materially. Labels such as decentralized, automated, or non-custodial are useful descriptors but are not legal conclusions.

The regulatory analysis begins with what is actually happening—who is doing what, with whose assets, under what constraints, and with what degree of human discretion—and works outward from there to the applicable frameworks. That approach is more likely to produce defensible, durable conclusions than one that starts from the label and works backward to justify it.

SECTION XI

# RECOMMENDATIONS

DeFi vaults should be treated as programmable asset-management infrastructure whose governance, risk controls, legal responsibilities, and disclosures must evolve with the complexity of the activities they perform. Automation can reduce transaction costs and operational complexity, but it does not remove financial risk, cybersecurity exposure, regulatory obligations, or accountability for investment decisions.

## 1. DEFINE A CLEAR VAULT MANDATE

Each vault should publish a clearly defined mandate covering its investment objective, eligible assets, permitted protocols, yield mechanisms, liquidity requirements, risk tolerance, leverage limits, and rebalancing rules. For curated vaults, the mandate should also specify the curator's authority, including which parameters the curator may modify and which changes require governance or investor approval.

Vaults should distinguish clearly between simple, stationary yield strategies and more complex strategies involving active rebalancing, derivatives, leverage, looping, cross-protocol allocation, or tokenized real-world assets. This distinction would help users understand that vaults with similar headline yields may have materially different risk profiles.

## 2. PRIORITIZE RISK-ADJUSTED RETURNS OVER HEADLINE YIELD

Vaults should not be evaluated or marketed solely on the basis of annual percentage yield. Operators and curators should identify the sources of yield—including borrower interest, staking rewards, trading fees, incentive tokens, leverage, derivatives, or underlying RWA cash flows—and explain the risks associated with each source.

As is best practice, performance reporting should distinguish between base yield and returns generated through incentives, leverage, looping, or temporary market conditions. Vaults should also disclose whether yields are variable, whether principal is exposed to loss, and how market or liquidity conditions may affect withdrawals.

## 3. ESTABLISH FORMAL CURATOR GOVERNANCE AND ACCOUNTABILITY

Curators should operate under documented governance frameworks defining their responsibilities, permitted actions, conflicts of interest, risk-management duties, monitoring requirements, and procedures for modifying or terminating strategies. Because curators may influence capital allocation without directly holding assets, their functional control over investment decisions should be transparent.

Curated vaults should disclose who selected the curator, how the curator is compensated, whether the curator has financial interests in underlying protocols or assets, and how the curator may be removed or replaced. Governance arrangements should reduce key-person dependency and ensure that responsibility is not obscured by smart contract automation.

## 4. PRESERVE MEANINGFUL USER AGENCY

Vaults should clearly identify whether users, curators, governance bodies, or autonomous systems have practical control over investment decisions. Users should receive understandable notice of material strategy, fee, risk-parameter, or protocol changes and should have a reasonable opportunity to withdraw before those changes take effect.

Timelocks, withdrawal windows, and governance notifications should be designed to provide genuine user control rather than merely technical notice. In practice, the mechanism for delivering that notice remains an open challenge. Unlike traditional financial institutions, DeFi protocols and vaults generally do not collect email addresses or phone numbers from participants, so there is no default channel through which a curator or protocol can reach users directly.

Current approaches are partial: community channels such as Discord can broadcast changes, but only reach users who have already opted in and are actively monitoring those channels; wallet-native notification protocols such as Push Protocol (formerly the Ethereum Push Notification Service) offer an onchain alternative, but require wallet support and a user habit of monitoring notifications, neither of which is yet standard practice. Until a more universal notification mechanism is adopted across the ecosystem, vaults and curators should be transparent about which notification channels they use and their limitations, rather than treating onchain publication of a change, on its own, as adequate notice to users. Where a curator can actively reallocate assets without meaningful user intervention, the vault should acknowledge that it more closely resembles discretionary portfolio management.

## 5. IMPLEMENT COMPREHENSIVE RISK MANAGEMENT POLICIES

Each vault should maintain a documented risk-management framework addressing smart contract, market, liquidity, leverage, liquidation, oracle, governance, operational, counterparty, bridge, and composability risks. The framework should establish measurable limits by asset, protocol, blockchain, collateral type, strategy, and service provider.

Curated and multi-strategy vaults should conduct scenario analysis and stress testing for rapid market declines, liquidity shocks, stablecoin depegging, oracle failures, protocol exploits, governance attacks, blockchain outages, and correlated failures across integrated protocols. Risk limits should be enforced programmatically where possible.

## 6. CONTROL LEVERAGE AND LOOPING STRATEGIES

Vaults using leverage or recursive borrowing should disclose the full economic exposure created by the strategy, rather than only the amount initially deposited. They should establish maximum leverage ratios, loan-to-value thresholds, liquidation buffers, collateral haircuts, and limits on repeated use of receipt tokens as collateral.

Users should be able to distinguish returns generated by the underlying asset from returns created through leverage. Automated deleveraging, liquidation protection, and emergency unwind procedures should be incorporated into leveraged strategies.

## 7. STRENGTHEN SMART CONTRACT ARCHITECTURE AND ASSURANCE

Vault contracts should be modular, separating user deposits and share accounting from strategy execution. Strategy contracts should have narrowly defined permissions, and the replacement, upgrade, or retirement of strategies should not compromise users' ownership records or withdrawal rights.

Vaults should use independent smart contract audits, formal verification where appropriate, invariant and integration testing, bug bounty programs, secure development practices, and continuous monitoring. Security reviews should cover not only the vault's own code but also every external protocol, oracle, bridge, automation provider, and software dependency used by the strategy.

## 8. APPLY DEFENSE-IN-DEPTH CYBERSECURITY CONTROLS

Institutional vaults should apply cybersecurity controls across smart contracts, wallets, keys, infrastructure, governance, front-end applications, APIs, and third-party integrations. Relevant controls include multisignature authorization, MPC, HSMs, role-based access, least privilege, secure key lifecycle management, network segmentation, transaction simulation, and address validation.

Vaults should establish continuous threat detection, onchain anomaly monitoring, incident-response plans, forensic capabilities, backup infrastructure, disaster recovery, and business-continuity procedures. Cybersecurity programs should align with established frameworks such as NIST CSF 2.0, the NIST SSDF, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and the CIS Critical Security Controls, supplemented by blockchain-specific controls.

## 9. ESTABLISH EMERGENCY AND OPERATIONAL RESILIENCE MECHANISMS

Vaults should define the circumstances under which deposits, strategy execution, rebalancing, or withdrawals may be paused. Emergency powers should be subject to clear authorization rules, multisignature controls, event logging, time limits, and post-incident review.

Each vault should maintain procedures for responding to smart contract exploits, oracle failures, bridge incidents, protocol insolvency, liquidity shortages, governance compromises, and key loss. Recovery procedures should prioritize asset preservation and an orderly withdrawal or unwind of positions.

## 10. INCREASE TRANSPARENCY AND REPORTING

Vaults should provide users with timely information on portfolio composition, underlying protocols, asset allocations, leverage, collateral ratios, liquidity, fees, curator actions, governance changes, and material dependencies. Reporting should allow users to understand how returns were generated and which risks were assumed.

For curated vaults, disclosures should compare actual allocations and performance with the stated mandate. Deviations, risk-limit breaches, emergency interventions, security incidents, and changes to approved assets or protocols should be recorded and communicated.

## 11. CLARIFY RECEIPT TOKEN AND ASSET RIGHTS

Vault documentation should explain what receipt or share tokens represent, how their value is calculated, whether they are transferable, and what rights they provide in relation to the underlying assets. Technical compliance with ERC-4626 should not be presented as resolving legal questions concerning ownership, redemption, custody, creditor status, or regulatory classification.

For tokenized RWA vaults, documentation should also identify the legal relationship between the token, the vault, the issuer, and the off-chain asset. Redemption rights, settlement processes, asset custody, valuation sources, and treatment in the event of issuer or curator failure should be clearly described.

## 12. CONDUCT ACTIVITY-BASED REGULATORY ASSESSMENTS

Vaults should be assessed according to their economic substance and functional activities rather than labels such as decentralized, automated, or non-custodial. Legal analysis should consider the assets involved, promises or expectations of returns, pooling arrangements, receipt-token characteristics, curator discretion, and the degree of user control.

Depending on the structure and strategy, analysis should consider whether receipt tokens may be securities, whether the vault could constitute an investment company or commodity pool, and whether curators or operators may be acting as investment advisers, commodity pool operators, commodity trading advisors, brokers, custodians, or money transmitters. Regulatory analysis should be repeated when strategies, assets, governance, or user populations change.

## 13. INCORPORATE IDENTITY, AML, AND SANCTIONS CONTROLS WHERE APPLICABLE

Institutional and permissioned vaults should incorporate proportionate identity verification, wallet screening, sanctions checks, jurisdictional restrictions, and transaction monitoring. Compliance requirements should be integrated into deposits, withdrawals, asset transfers, and interactions with underlying protocols where technically and legally feasible.

Sanctions and anti-money-laundering considerations remain relevant even where broader DeFi regulation is uncertain. Vaults should therefore establish risk-based compliance frameworks rather than assuming that automation or decentralization eliminates these responsibilities.

## 14. APPLY ADDITIONAL SAFEGUARDS TO TOKENIZED RWA VAULTS

RWA vaults should evaluate the legal, liquidity, settlement, valuation, and counterparty characteristics of each underlying tokenized asset. The liquidity profile of tokenized treasuries, private credit, real estate, commodities, equities, and trade-finance assets may differ significantly and should not be treated as interchangeable.

RWA vaults should align onchain subscriptions, redemptions, and collateralization processes with the transfer restrictions, investor-eligibility rules, and settlement processes of the underlying assets. Curators should maintain approved-issuer lists and monitor issuer, custodian, servicer, and off-chain asset risks.

## 15. CONSTRAIN AND OVERSEE AI-AGENT ACTIVITY

AI agents allocating assets to vaults should operate under predefined investment policies, eligible-asset lists, protocol restrictions, transaction limits, concentration limits, leverage caps, and human-approval thresholds. Agents should optimize for risk-adjusted outcomes and policy compliance rather than simply selecting the highest available yield.

Institutions should maintain records of the data, assumptions, policies, and reasoning supporting AI-driven decisions. Agents should verify transaction details, validate external data, detect abnormal conditions, and escalate high-risk or unusual transactions for human review. Protection against prompt manipulation, corrupted data, compromised models, and unauthorized changes to decision policies should form part of the vault's cybersecurity framework.

## 16. DEVELOP COMMON INSTITUTIONAL STANDARDS FOR VAULT ASSESSMENT

Industry participants and standards bodies should develop a common assessment framework covering vault architecture, strategy complexity, curator governance, asset eligibility, risk controls, cybersecurity, compliance, liquidity, leverage, disclosure, and operational resilience.

Because vaults can support a wide variety of assets and strategies, a single prescriptive standard may not be appropriate. A modular framework could instead classify vaults by strategy, governance model, user type, underlying assets, and risk characteristics, while establishing minimum principles applicable across all vault categories.

It is important to note that a single vault could combine SEC-regulated securities and CFTC-regulated commodities, and no single regulator currently has jurisdiction spanning both. The agencies' March 2026 joint interpretation[20] and the pending Digital Asset Market Clarity Act are steps toward clearer jurisdictional lines, but neither yet resolves how a mixed-exposure vault would be assessed under one framework. A more immediately viable path may be a ratings-agency approach, comparable to established stablecoin rating products such as S&P Global's Stablecoin Stability Assessment,[21] or to quantitative risk-rating methodologies published by blockchain security firms such as Halborn.[22] This gives depositors a comparative reference point alongside, rather than in place of, whatever regulatory framework eventually develops.

SECTION XII

# CONCLUSION

DeFi vaults are not simply another DeFi application. They are a new model for programmable financial infrastructure, one that automates portfolio allocation, treasury management, collateral optimization, and increasingly sophisticated investment strategies. This can blur the line between technology and financial intermediation, which requires a strong analytical framework such as the one developed in this paper. The nature of the activity, and the degree to which human discretion is exercised over user assets, determines how vaults should be understood from a technical, legal, and institutional standpoint.

The spectrum from fully automated vault to actively curated vault is a spectrum from infrastructure to intermediation, and the analysis must follow the activity rather than the label.  A vault described as decentralized may have a curator exercising substantial discretion over user assets. A vault managed by a professional curator may operate within stringent smart contract constraints that significantly limit that discretion. The developer who built the protocol and the curator who manages the strategy may be the same person, but performing different functions, with different analytical and legal/regulatory consequences. Getting these distinctions right is the real work behind getting the regulatory classifications correct.

For regulators, the implication is that vault regulation requires activity-based analysis rather than categorical treatment. Frameworks that attach regulatory obligations to the presence of a smart contract, or that presume financial intermediation from the presence of any degree of human involvement, will produce results that are both over-broad and lacking in a strong legal foundation. Curators who exercise genuine ongoing discretion over the deployment of user assets, on the other hand, are more likely to be conducting regulated functions. The line between those two positions is already drawn; it is the factual analysis that needs to take place to get the implementation right.

For vault designers and curators, the implication is that governance, accountability, and legal clarity are not optional features to be added when institutional adoption demands them. They are foundational design requirements whose absence creates regulatory, operational, and reputational risk that compounds as vaults grow in complexity and scale.

The recommendations in this paper are intended as a starting point for that design work, not a compliance checklist. As the vault ecosystem continues to evolve, incorporating tokenized real-world assets, agentic AI, and increasingly sophisticated multi-strategy architectures, the analytical framework will need to keep pace. But what will not change is the starting point: what is actually being done, by whom, with whose assets, and under what constraints.

# CONTRIBUTORS & REVIEWERS

## Thank you to our team of contributors and reviewers for GSMI 7.0 representing 100+ entities, including:

2Tokens
Accenture
Advanced AI Society
AI 2030
AI MIND Systems
Aleo
Animoca Brands
Association of National Numbering Agencies (ANNA)
Ava Labs
Banca d'Italia
BGIN
Blockchain Arbitration & Commerce Society
Blockchain for Energy (B4E)
Blockchain Foundation
Blockmosaic
Bodin Advisory LLC
British Columbia Public Service
Buenos Aires Government
Business IQ
Cahill Gordon & Reindel LLP
Canton Foundation
Capital Markets Authority (CMA) of Kenya
Central Bank of Jordan
Chainlink
Chronicle Labs
Citibank
Clifford Chance
City University of New York (CUNY)
Curaçao Fintech Association
Dastru Design Labs
DELTA FOODS
Deutsche Börse
DFM Data Corp.
dHub Group
Digital Euro Association
dlt.NYC
DTCC
Digital Token Identifier Foundation (DTIF)
Elliptic
Ethiopian Capital Market Authority (ECMA)
Euroclear
EU Blockchain Observatory and Forum (EUBOF)
Evergon Labs
Financial Services Agency of Japan (JFSA)
Florida Institute of Technology
Florida International University
Folks Finance
Futura Law Firm
Galaxy
GBBC Ambassadors
George Washington University
Global Legal Entity Identifier Foundation (GLEIF)
The Graph Protocol
Hashgraph
Hearts of Change
Hedera
Hong Kong Securities and Investment Institute
IDB Lab
IMHOTEP Consulting
International Securities Services Association (ISSA)
IOTA Foundation
Islandpreneur International
Jitterbits
J.P. Morgan Chase
Kaiko
Kenyan State Department for Investment Promotion
Kinexys by J.P. Morgan
Linux Foundation
Media Luna
Mercy Corps Ventures
Moody's Ratings
National Bank of Romania
Networks for Humanity
New York Blockchain Council (NYBC)
Nigerian Bar Association-Section on Business Law
Nomura Research Institute, Ltd.
NorthStar DAO Foundation
Norton Rose Fulbright US LLP
OKX
OpenID Foundation
Panamá CO
Patomak Global Partners
Qatar Financial Centre Authority (QFCA)
Schulich School of Business
SETAR (Aruban Telecom)
Simpaisa Technologies Limited
Skyrocket Financial Solutions
Sodot
Solidus Labs
Standard Chartered
Stratford Finance International
Sumsub
Unipd
United Nations Joint Staff Pension Fund (UNJSPF)
Università degli Studi di Padova
University of Arkansas
U.S. Blockchain Coalition (USBC)
U.S. House of Representatives
Veridex Alethia
VerifyVASP
World Bank
Wyoming Stable Token Commission

# ENDNOTES


1 BCG, "The Future of Digital Assets" (May 2026) — https://web-assets.bcg.com/fd/19/d52ba9ab4857911cf3650e991ef0/the-future-of-digital-assets-may2026.pdf

2 Morpho, "The Morpho Effect: 2025" — https://morpho.org/blog/the-morpho-effect-2025/

3 The Block, "Coinbase tops $1 billion in bitcoin-backed onchain loans via Morpho" — https://www.theblock.co/post/373032/coinbase-tops-1-billion-in-bitcoin-backed-onchain-loans-via-morpho

4 Morpho, "Morpho Association Announces Cooperation Agreement with Apollo" — https://morpho.org/blog/morpho-association-announces-cooperation-agreement-with-apollo/; Apollo Global Management, Q1 2026 earnings release (May 6, 2026) — https://ir.apollo.com/news-events/press-releases/detail/622/apollo-reports-first-quarter-2026-results

5 Kraken Blog, "Earn up to 8% APY: Get DeFi-like rewards with a simplified experience" — https://blog.kraken.com/product/defi-earn/simplified-defi-rewards

6 https://www.gbbc.io/uploads/reports/gsmi50/DeFi-Stand-Alone.pdf

7 https://www.lexology.com/library/detail.aspx?g=8922c167-410d-4e69-8649-2598582be506

8 https://www.rockawayx.com/insights/defi-vaults-explained-2026-guide

9 Aave Protocol Documentation, "Simple Earn Vaults" — https://aave.com/docs/developers/aave-v3/vaults/overview; "Fixed vs Variable DeFi Yield," Plasma, https://www.plasma.org/learn/fixed-vs-variable-defi-yield

10 "Fixed vs Variable DeFi Yield," Plasma — https://www.plasma.org/learn/fixed-vs-variable-defi-yield

11 https://morpho.org/blog/curators-explained/

12 https://static.cahill.com/docs/CahillNXT_Client%20Alert_7.23_v7.pdf

13 https://www.gbbc.io/uploads/reports/gsmi50/DeFi-Stand-Alone.pdf

14 OpenZeppelin, "ERC-4626 Tokens in DeFi: Exchange Rate Manipulation Risks" — https://www.openzeppelin.com/news/erc-4626-tokens-in-defi-exchange-rate-manipulation-risks; Aave Protocol Documentation, "Vaults" — https://aave.com/docs/aave-v3/smart-contracts/vaults

15 Hester M. Peirce, "Headstands and Summervaults: A Statement on Crypto Vaults and Lending Strategies," U.S. Securities and Exchange Commission (July 22, 2026), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-crypto-vaults-lending-strategies-072226

16 Treasury Department/IRS, "Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales," 89 Fed. Reg. 106928 (Dec. 30, 2024) — https://www.federalregister.gov/documents/2024/12/30/2024-30496/gross-proceeds-reporting-by-brokers-that-regularly-provide-services-effectuating-digital-asset-sales, which classified certain DeFi trading front-end providers as brokers based on control over transaction terms rather than a separate inquiry into financial services performed; overturned by H.J.Res. 25 (April 10, 2025) — https://carey.house.gov/2025/04/10/carey-bill-to-eliminate-burdensome-irs-defi-crypto-broker-rule-signed-into-law-by-president-trump/

17 Regulation (EU) 2023/1114 (MiCA), Recital 22 — "where crypto-asset services are provided in a fully decentralized manner without any intermediary, they should not fall within the scope" of the regulation.

18 CERHA HEMPEL, "Testing the Boundaries of MiCA's DeFi Exemption" — https://www.cerhahempel.com/blog/fintech-ledger/testing-the-boundaries-of-micas-defi-exemption (European Commission targeted consultation opened May 20, 2026 under Articles 140/142 MiCA, deadline August 31, 2026)

19 "UK finalises 2026 crypto rules with DeFi carve-out and 'controlling entity' test," crypto.news — https://crypto.news/uk-finalises-2026-crypto-rules-with-defi-carve-out-and-controlling-entity-test/

20 U.S. Securities and Exchange Commission, "SEC Clarifies the Application of Federal Securities Laws to Crypto Assets" (March 17, 2026) — https://www.sec.gov/newsroom/press-releases/2026-30-sec-clarifies-application-federal-securities-laws-crypto-assets

21 S&P Global Ratings, "Stablecoin Stability Assessment" — https://www.spglobal.com/ratings/en/products/stablecoin-stability-assessment

22 Halborn, "A Framework for Measuring, Assessing, and Rating Risk in Stablecoins" — https://cdn.mainframe.halborn.com/Stablecoin_Framework_and_Methodology_Halborn_50256b7842.pdf