Adapter-based ERC-4626 compliant vaults

ehjc@adapter.fi

26th May 2024

Abstract

ERC-4626 standardizes tokenized Vaults, offering a unified API and guidelines to ensure consistency and interoperability across DeFi platforms. Adapter vaults, compliant with ERC-4626, bridge Vaults with external markets through registered adapters and strategies, enhancing functionality and accessibility. Embedded governance mechanisms within ERC-4626 empower users with control over protocol upgrades and strategic decisions, bolstering security and integrity. Investigating the modular adapter-based approach to ERC-4626 vaults, this paper presents their flexibility through case studies in protocols like Pendle and Balancer. By automating processes and simplifying interactions with external markets, our vaults present a promising avenue for maximizing yields and advancing the DeFi landscape. Through practical examples, we demonstrate how adapter vaults streamline financial operations, improve user experience, and contribute to the democratization of finance in the decentralized era.

1. Introduction

Decentralized finance (DeFi) revolutionizes traditional financial systems by leveraging blockchain technology to create open, permissionless, and trustless financial services. DeFi encompasses a wide range of financial applications and services, including lending, borrowing, trading, and asset management, all executed without intermediaries like banks or brokers.

Vaults, within the context of DeFi, are smart contracts designed to optimize users' yield on their cryptocurrency assets. These vaults typically operate by automatically reallocating user deposits across various strategies, such as lending, liquidity provision, or yield farming, to maximise returns while minimizing risks and costs. Users deposit their tokens into these vaults, and the smart contracts manage the tokens according to predefined strategies.

Users interact with vaults through decentralized applications (dApps) or platforms that facilitate access to DeFi protocols. They can deposit their tokens into vaults using digital wallets, and the vaults automatically generate yield by participating in various DeFi activities. Users can monitor the performance of their investment and withdraw their tokens in accordance to the rules of the vault and available liquidity. This process allows users to earn passive income on their tokens while maintaining custody of their tokens and without relying on traditional financial institutions.

Yearn (Yearn, 2024) was one of the pioneering protocols to take advantage of automating DeFi strategies through vaults. Their business model relies on taking a cut of the generated yield in exchange for fully managed capital migrations.

1.1 Tokenizing Vaults

Tokenizing vaults in DeFi introduces complexities and risks. Managing the tokenization process, tracking ownership, and securing tokens with smart contracts can lead to bugs, vulnerabilities, and hence to potential financial losses for users. Custom implementations of tokenized vaults often lack interoperability with other DeFi protocols, increasing development effort, and leading to inconsistent user experiences. Developing such solutions requires significant resources and expertise, resulting in longer development cycles and higher maintenance costs.

The mentioned disadvantages motivated the creation of the ERC-4626 tokenized vault standard (Santoro et al., 2021) that allows for the implementation of a standard application binary interface (ABI) for tokenized vaults representing shares of a single underlying ERC-20 (Vogelsteller & Buterin, 2021).

1.2 ERC-4626

ERC-4626 serves as a standardized framework designed to optimise and streamline the technical aspects of yield-bearing vaults. It establishes a common ABI for tokenized yield-bearing vaults, representing shares of a single underlying ERC-20 token. Additionally, ERC-4626 offers guidelines for extending tokenized vault functionality using ERC-20, facilitating essential operations like depositing, withdrawing tokens, and checking balances.

Within the realm of yield-bearing vaults, various platforms such as lending markets, aggregators, and tokens inherently bearing interest employ diverse strategies to maximize yields. However, these strategies often vary slightly, potentially leading to errors or inefficient resource utilization during development.

ERC-4626's role in yield-bearing vaults is pivotal as it standardizes these processes, reducing integration complexities and granting broader access to yield across different applications. By establishing consistent and robust implementation patterns, ERC-4626 minimizes development efforts required from developers, fostering a more efficient and accessible DeFi landscape. In the following section, we describe how a modular adapter-

based approach enables the creation of generalised ERC-4626 vaults that target different markets simultaneously based on strategies that can be proposed in a decentralised way.

2. Adapter Vaults

Adapter vaults comply with the ERC-4626 standard and expose its ABI to allow easy integration with other projects. In addition to the standard functionalities, the vault has been customised to use a strategy based on registered adapters for deploying assets that are available in the vault. An adapter represents the modular integration to another project (e.g. AAVE (AAVE, 2024), Compound (Compound, 2024), Pendle (Pendle, 2024), or similar). A strategy specifies the proportions in which existing assets are allocated to the active adapters (e.g., deploy a ratio of 1:1 to AAVE and Compound). Strategies can be proposed in a decentralised manner, but rejected by guards that are part of the vault's governance smart contract. We pursue with optimistic strategy control in which strategies must be rejected rather than explicitly approved. Figure 1 exemplifies an user interacting with an Adapter vault. Upon deposit the tokens are converted into vault shares. Tokens are deployed to different markets according to the active strategy. The funds allocator smart contract is responsible for dividing the tokens into parts to generate yield for liquidity providers.

3. Applications

Figure 1 shows the high-level architecture of an Adapter vault. Once a user deposits a token into the ERC-4626 vault, they receive shares that represent their ownership. The currently active strategy is used within the funds allocator smart contract, to deploy tokens through the registered adapter into different markets. In the following, we discuss adapters, strategies, and governance in more detail.

3.1 Adapters

Adapters form the basis for making tokens of the Adapter vault available in an external project and offer basic functionalities for interacting with it. A generic adapter interface has been created that implements basic functionalities (e.g., *maxWithdraw*, *maxDeposit*, *totalAssets*, *deposit*, *withdraw*). Adapters can be added and removed within an Adapter vault by its owner. In principle, any type of protocol that provides atomic transactions can be integrated using adapters. Examples include lending markets, liquidity pools, vaults, and staking contracts. Tokens in the vault are distributed to the respective markets based on the currently active strategy.

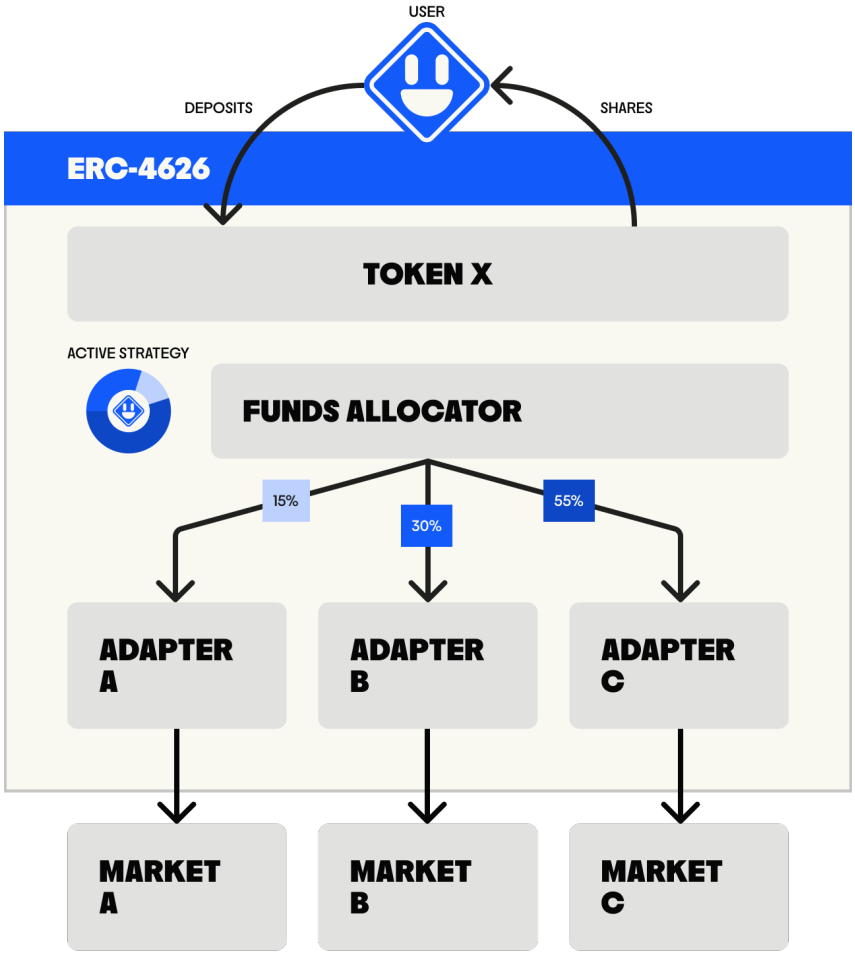

Figure 1: High-level functionality of an Adapter vault having three registered adapters. The active strategy generates yield by allocating 15% of the tokens to market A, 30% of the tokens to market B, and 55% of the tokens to market C.

3.2 Strategies

Strategies form the basis of how tokens are distributed based on the registered adapters using a vault-specific funds allocator smart contract. Strategy proposal is a decentralised process and anyone can propose new strategies to optimize the current vault offering. We follow an optimistic governance principle in which a strategy can only be rejected by guards, which are set by the contract owner. This allows everyone to suggest a better strategy. If there are no votes against the strategy after a prescribed time window, it can be activated. We added an optional incentive that grants a strategist a certain share of the profits generated within the active period of their strategy that are claimable from the Adapter vault, which can be nullified.

3.3 Governance

Governance is made possible on the basis of guards that are part of the governance smart contracts. Those guards are added or removed by the governance smart contract owner. Each Adapter vault is associated to a governance smart contract. If a malicious user

proposes a strategy that is exclusively to the detriment of liquidity providers, guards can reject it within a pre-defined time window. This time window from proposing a strategy to activating it is passed in the constructor when the governance smart contract is deployed and is therefore dependent on the underlying governance smart contract. Suggesting a strategy is more gas-intensive than rejecting it, such that an attacker trying to propose several malicious strategies would have the economical disadvantage.

We present the flexibility of Adapter vaults on two example applications. First, we show how we integrate to Pendle, a protocol that offers fixed yield markets through yield stripping. Second, we show how we introduce boosted yields for liquidity provider in liquidity pools.

3.4 Fixed Yield Compounder

Pendle is a permissionless yield trading protocol that wraps yield-bearning tokens into standardized yield tokens (SY). SY tokens are compatible with the original asset and the Pendle automated market maker (AMM). Pendle strips the yield part from SY, by splitting the token into its principal (PT) and yield (YT) component. Both PT and YT can be traded on the Pendle AMM.

$$P_{SY} = P_{PT} + P_{YT} \tag{1}$$

Each PT and YT has a maturity date upon which PT tokens can be redeemed. For YT, the yield of the yield-bearing token is only accrued up until maturity date, after which YT has no value. Equation 1 shows that the asset price is composed of both parts the principal and the yield token. Hence, PT can be purchased at a discount and the fixed yield that a user obtains is dependent on the spread between the PT price and the asset price obtained after maturity is reached.

Pendle users participate in the protocol by making a deposit of their yield-bearing token where a maturity date must be selected. After the maturity date, the user can convert PTs for an unindexed version of the yield-bearing token, e.g., for 1 PT-ezETH, they will be able to redeem 1 ETH worth of ezETH. The inconvenience for the user is that this process is carried out manually.

Adapter vaults automate this previously manual process by rolling-over maturity dates. This is resolved at the adapter level in the vault such that assets auto-compound after the maturity date has reached. A strategy is used that first deploys all assets in the current maturity date t_1. When this maturity date expires, a new strategy is activated, which redeems the assets and deploys them in another maturity period t_2, where $t_2 > t_1$. In this way, the user can be relieved of more work and gas costs are minimised. Figure 2 exemplifies maturity date roll-over which auto-compounds yields for the users. The Adapter strategy is updated to reallocate funds to a Pendle market that is still active.

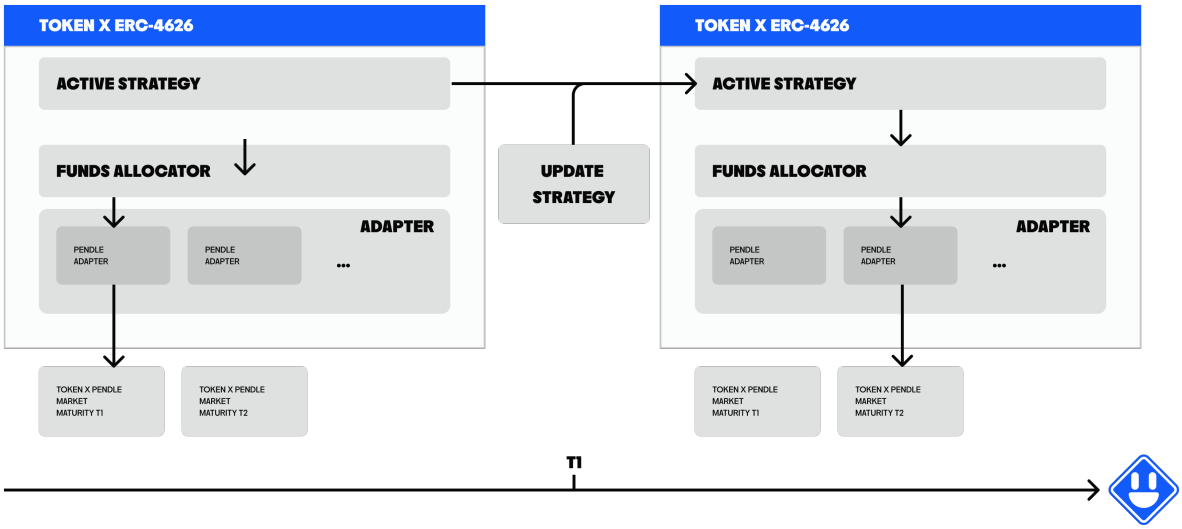

Figure 2: Pendle strategy update upon expiry of a maturity date for one market. The updated strategy will redeem PT tokens and deploys them into a market with an active maturity date.

3.5 Boosted Liquidity Pools

Adapter vaults act as strategy manager for liquidity pools of decentralised exchanges like Balancer (Balancer, 2024) or Curve (Curve, 2024). Idle liquidity is shifted to asset-specific Adapter vaults that use adapters and strategies to generate additional yield. Adapters can integrate to lending protocols, other (ERC-4626) vaults, or staking contracts, and we exemplify lending markets below.

The nature of lending protocols makes the returns on lent assets inversely proportional to the availability of capital in the respective lending markets. In the presence of a surplus of available capital, interest rates on lending protocols decrease. The deployment of assets by different DeFi protocols leads to interest rate imbalances that come as a result of different utilisation rates.

Figure 3 shows interest rate fluctuations for the DAI stable coin token within the AAVE and Compound lending protocols. Adapter vaults can react to interest rate changes in real time by strategy adjustments.

4. Adapter.Fi

Multiple DeFi protocols use a deduction of user profits as an economic model. We take two percent of vault yield and convert them into liquidity pool tokens (LPT) of a 80/20 liquidity pool (LP), which consists of the native Adapter token ($ADAPT$) and wrapped Ether ($wETH$). For this purpose we market buy $ADAPT$ tokens from the LP, provide liquidity in aforementioned LP to obtain LPTs, and take the LPTs as incentives to the Adapter reward vault. Note that $ADAPT$ tokens alone do not provide any rewards. The reward vault is an ERC-4626 vault that holds the 80/20 LPT as base token, where

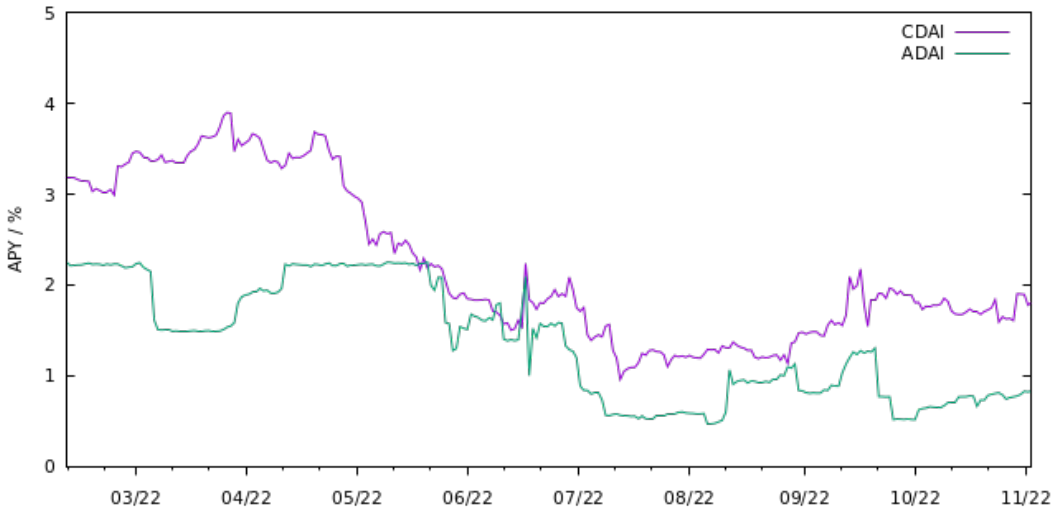

Figure 3: Annual percentage yield (APY) fluctuations for DAI on Compound (CDAI) and Aave (ADAI).

incentives are distributed in form of LPTs to liquidity providers according to their shares in the vault.

A withdrawal fee of 10 basis points is taken, which is distributed (100% of the fee) to remaining liquidity providers of this vault. This way, liquidity provider obtain rewards through liquidity incentives from the protocol as well as through new deposits and withdrawals that auto-compound over time.

4.1 Tokenomics

ADAPT is the native ERC-20 token of Adapter.Fi with a total supply of 1,000,000,000. Figure 4 presents token distributions to different divisions of the protocol in percentages

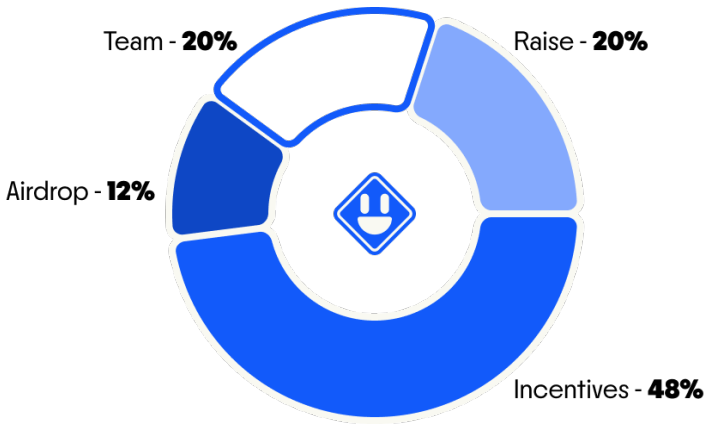

Figure 4: *ADAPT* token distribution.

while exact token allocations are defined in the Table 1.

	%	Allocated tokens
Incentives	48	480,000,000
Airdrop	12	120,000,000
Team	20	200,000,000
Raises	20	200,000,000

Table 1: Exact *ADAPT* token allocations.

4.2 Distribution and Vesting

A points based system is integrated that tracks user actions and rewards them by points in three points seasons. Within these seasons, we distribute a total of 120,000,000 tokens (12% of the total supply). We define the allocated tokens in Table 2 since we expect the demand and growth to scale with token interest.

Season	%	Allocated tokens
1	6	60,000,000
2	4	40,000,000
3	2	20,000,000

Table 2: Airdrop allocation with respect to Adapter points seasons.

This strategy is meant to release the airdrop in parts over a longer period of time and participants can claim their airdrop through a Merkle proof on-chain after we prepared the recipient set accordingly. At the end of each season, we reset the points count to guarantee participants a fair game. Note that partner vaults will receive additional multipliers with respect to points accrual.

Tokens from the treasury are aimed to be distributed within a time range of four years in form of liquidity incentives. Team member token allocations have a linear vesting of 24 months that starts at the token generation event (TGE). Investor token allocations have a linear vesting of 12 months that starts at the TGE.

References

AAVE. (2024). Open source liquidity protocol [https://www.aave.com].

Balancer. (2024). Defi liquidity protocol [https://www.balancer.fi].

Compound. (2024). Compound finance [https://compound.finance/].

Curve. (2024). Stable swap [https://www.curve.fi].

Pendle. (2024). Liberating yield [https://www.pendle.finance].

Santoro, J., t11s, Jadeja, J., Cuesta Cañada, A., & Doggo, S. (2021). Tokenized vaults.

Vogelsteller, F., & Buterin, V. (2021). Token standard.

Yearn. (2024). The yield protocol [https://yearn.fi].