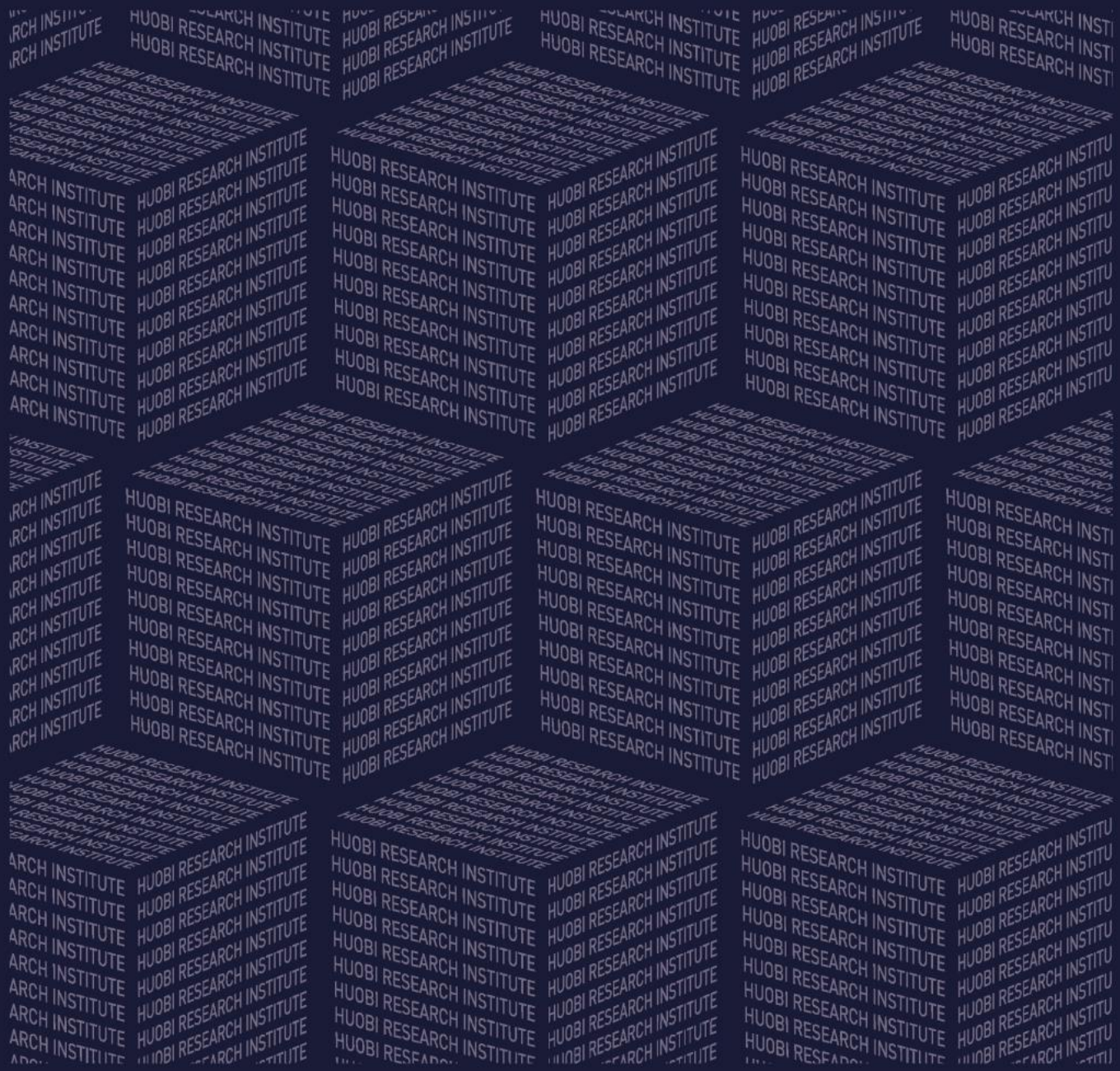


The Birth of ERC-4626 to DeFi: Break of Dawn or Prophet of Doomsday?

Huobi Research

Authored by Tim Chen, Researcher at Huobi Research Institute

Abstract

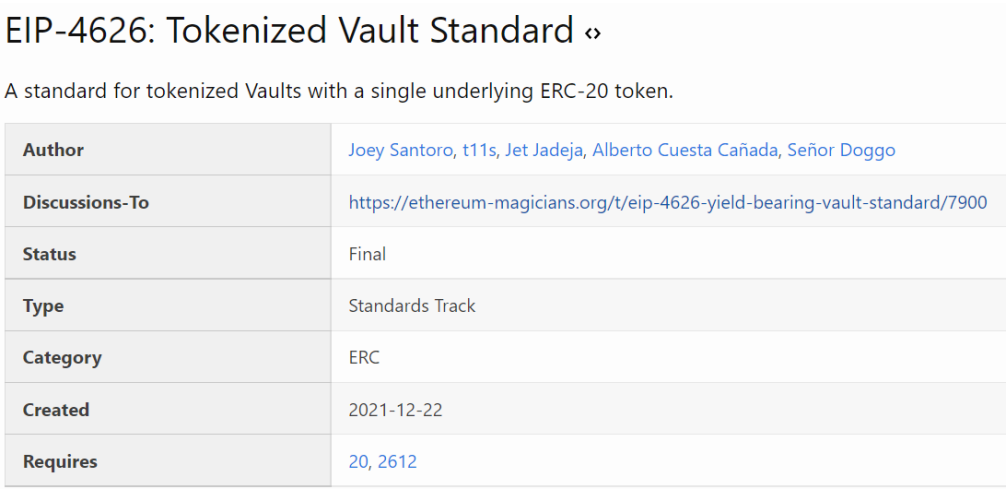
The price of ETH has fallen by 70% from its peak; on-chain activities and other demand have seen a steep decline, and the shock has spread to the whole DeFi industry. However, some claim that the birth of ERC-4626 may reverse the downturn.

As current tokenized vaults are mostly deployed in lending and borrowing, yield aggregators, and stakings in DeFi, yield-bearing tokens minted from those vaults are weak in terms of capital efficiency and liquidity. As a solution, ERC-4626 aims to optimize and unify the technical specs of various vaults in order to establish a standard protocol for all types of yield-bearing tokens. As a result, even though this protocol has not been officially launched on the mainnet yet, it has earned plaudits from early adopters such as Yearn, mStable and Balancer.

In our opinion, the DeFi world would find new opportunities with the birth of ERC-4626. For developers, the cost for development may be cut substantially; for applications, the composability between various DeFi protocols could be improved; for users, capital efficiency would become higher; for the whole DeFi world, it may accelerate the shift to DeFi 2.0. Nevertheless, ERC-4626 is a double-edged sword: if not properly executed, it may become the catalyst to trigger a collapse of the system.

We shall wait and see how ERC-4626 performs in the near future.

Since 2022, many economies have been dealing with inflation with nearly all central banks introducing contractionary monetary policy to counter this threat. Under these circumstances, global liquidity has shrunk beyond expectations, and it is reflected first in risky assets, including cryptocurrency. As the price of ETH fell by over 70%, the overall on-chain environment became less active. Activities, the demand for borrowing, and the desire for speculation cooled down. Accordingly, the whole DeFi world is in distress in 2022. However, the birth of EIP-4626: Tokenized Vault Standard in Ethereum, may signal the first light of dawn.



EIP-4626: Tokenized Vault Standard ‹›

A standard for tokenized Vaults with a single underlying ERC-20 token.

Author	Joey Santoro, t11s, Jet Jadeja, Alberto Cuesta Cañada, Señor Doggo
Discussions-To	https://ethereum-magicians.org/t/eip-4626-yield-bearing-vault-standard/7900
Status	Final
Type	Standards Track
Category	ERC
Created	2021-12-22
Requires	20, 2612

Figure 1: Contents of EIP-4626

Source: eips.ethereum.org

As a key complement to ERC-20, ERC-4626 aims to optimize and unify all technical specifications of various tokenized vaults, and to establish a standardized and simplified protocol for all yield-bearing tokens minted from the vaults. This means such tokens could be compatible with any protocols or applications, further improving the flexibility and accessibility of DeFi.

Prior to the upgrade of EIP-4626, this article provides insights and elaboration on the motivation, contents and possible outcomes of this development.

1. Background and Motivation of ERC-4626

Some concepts must be clarified before the analysis of ERC-4626:

1.1 What is a Vault?

A vault is a multi-sig solution born earlier than EIP-4626; it is inherently a token pool created by a smart contract. When external tokens are deposited into the vault, the smart contract would mint several vault tokens to users in accordance with the amount in deposit; the minted vault token represents proof of "IOU" or partial equity that is eligible to receive interests over time; upon exit or expiration, original tokens could be redeemed by burning corresponding vault tokens.

In macro, two types of tokenized vaults are most commonly seen in the market. One is a tokenized vault that returns yield-bearing tokens, which are ERC20 compatible and guaranteed free transfer and circulation. The other is a non-transferable vault, which is not the main focus of this article.

1.2 The issue ERC-4626 attempts to tackle

It takes sophistication to create a tokenized vault. For DeFi, if a protocol desires to be compatible with other tokens, it is only viable when each economic model is properly researched so that special API adapters could be constructed in the codes to complete the integration.

In other words, the smart contract of a tokenized vault could be deemed a manufacturer of plugs and power outlets, minted tokens are various models of plugs manufactured by various factories in this case. Usually, a plug can only be plugged into a power outlet manufactured from the same factory; the power outlet is only functional with other plugs when converters are available after due research on other plugs. When the number of manufacturers increases, it would be difficult for a single power outlet to be the universal one to fit all plugs on the market, without proper converters provided.

In real life, tokenized vaults are deployed in three scenarios in DeFi: lending and borrowing (i.e., Compound, AAVE, Fuse, etc.), aggregators (i.e., Yearn, Rari and Idle, etc.) and staking

(i.e., xSushi, stETH, etc.). Analysis will be provided respectively in the next section.

a) Tokenized vaults in lending and borrowing: Compound

Being a famous lending and borrowing platform on Ethereum, Compound provides crypto deposit and lending/borrowing service to users, which is similar to that of banks, by autonomous interest pricing with the help of the decentralized and opensource Compound protocol. Users could receive a certain amount of interest in accordance with the amount deposited, or lend cryptocurrency with collateral.

The process certainly does not involve a free lunch. The following graph demonstrates the core interest pricing model of USDC on Compound, including borrowing and lending rates, which are both adjusted according to the adoption rate of the pool. The technical specifications will not be elaborated on in this article. In short, the interest rate is adjusted with floating pricing based on the degree of demand and supply and market adoption rate; it is updated every 15s to be consistent with the time range for producing a block on Ethereum.

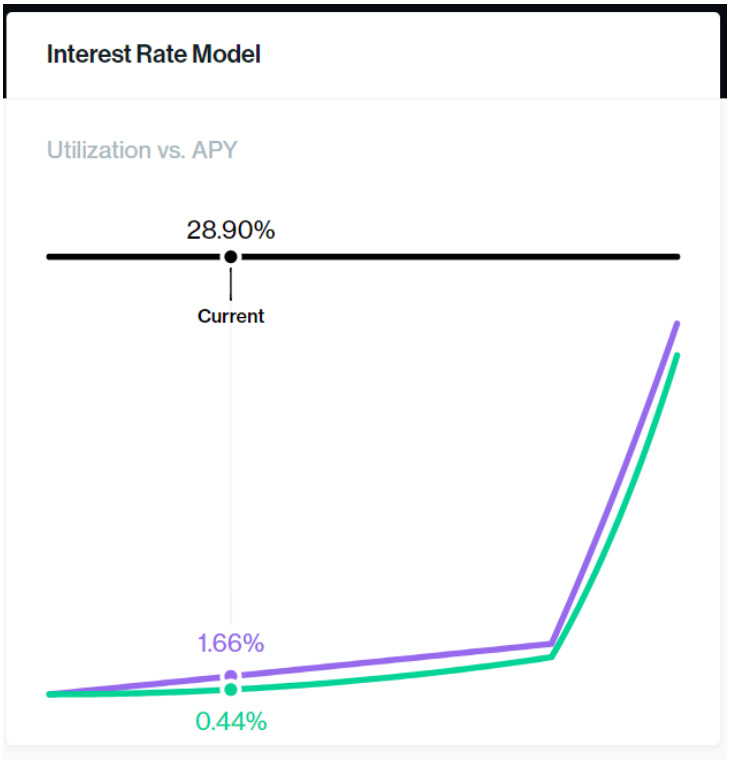


Figure 2: Core interest pricing model of USDC on Compound

Source: Compound finance

Both lenders and borrowers are able to deposit any crypto asset into the vault assigned by Compound, and mint corresponding cToken via the smart contract, cETH, cDAI, cUSDT, for instance.

cToken is a certificate of deposit or the status as liquidity provider; as long as cToken lies in the wallet, rewards will find their way there. In other words, cToken is the sum of the principal and interest after deposit. The exchange rate to the underlying token is not fixed at 1:1, but is based on the following formula which has various inputs, such as total borrow balance, cToken supply, etc.:

$$Exchange\ Rate = \frac{Underlying\ Balance + Total\ Borrowed\ Balance - Reserves}{cTokenSupply}$$

Normally, the larger the amount borrowed, the faster the increase of the exchange rate, and thus the more profits to be redeemed.

➢ How Compound vaults works

When certain assets are deposited, the vault would return a commensurate amount of cToken in proportion to the exchange rate. Upon redemption, the number of underlying assets to be returned would be calculated again according to the latest exchange rate before the return is initiated.

When borrowing, users must burn cToken as collateral to borrow any token supported by the protocol. Although the collateral factor varies on the market, the fundamental rule applies. The total loan amount must not exceed the total market value of the collateral assets. For lenders and borrowers, operations on underlying assets or cToken are available round-the-clock to pay off debts or redeem assets in staking if liquidation is not triggered.

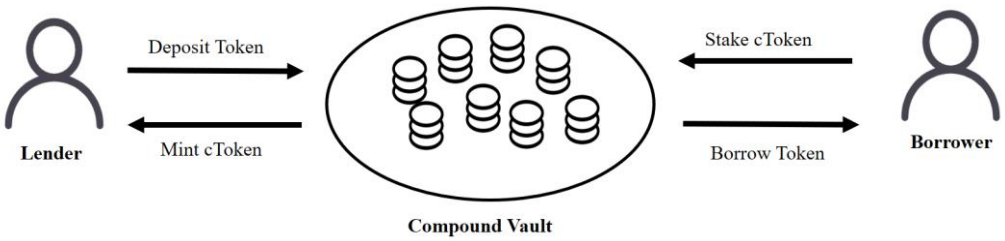


Figure 3: Process of lending and borrowing on Compound

Source: Huobi Research

To sum up, cToken can be deemed as both a proof of "IOU" with floating rate after deposit, and as a prerequisite for lending and borrowing; it is a ticket and a bridge to enter Compound.

b) Tokenized vaults in aggregators: Yearn.finance

Vaults on Yearn.finance are inherently yield aggregators: yield potential is maximized by a smart contract executing various investment strategies on the market.

It is not just one strategy that is executed in an individual vault; the smart contract will modify the execution path from time to time, such that when the current strategy is facing a

downturn, another strategy with a higher yield will replace it. So far, most vaults adopt an investment strategy of compounding where interest from the pool will be reinvested for compounding interest.

Users who deposit to yVault will receive yToken minted by smart contract as a representative for principal and interest. In terms of liquidity from the deposit, it will be injected into other revenue streams to generate yields, such as yield farming, lending, and transaction fees.

For average users, it is rocket science to invest in a reliable project with higher returns in the ocean represented by DeFi; it is not only time-consuming, but also possible to be deferred. But with vaults, it cannot be safer and simpler. Besides, for individual users, switching between protocols must be done by various on-chain actions, which consumes Gas every time. In yVaults, Gas only needs to be paid once as the smart contract would aggregate all funds from users and execute only once even though yVaults may switch between various DeFi protocols.

- How Yearn Vaults work

Taking one strategy in yvETH as an example, users could receive yETH when depositing ETH to yvETH. When the deposit reaches a certain amount, the smart contract would utilize the deposit to interact with MakerDAO and create a margin of DAI based on the over-collateral rate. The DAI lent out could receive extra CRV by adding liquidity to the Y pool via the interaction with yvDAI. Finally, CRV will exchange to ETH to pay off the interest to yETH holders periodically.

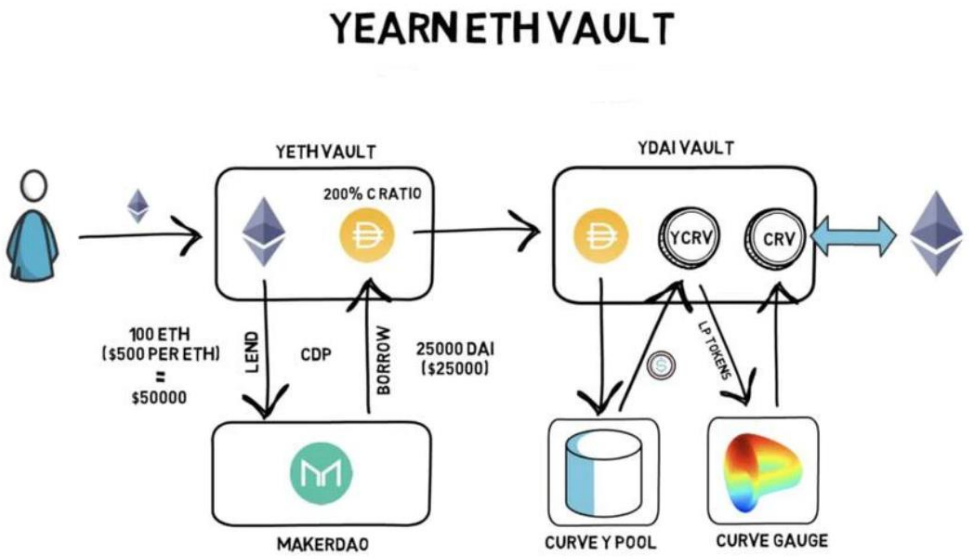


Figure 4: Strategy of yETH Vault

Source: Yearn.finance

It is evident that yToken is merely a certificate for receiving interest in the continuously optimizing yVault and a tool for liquidation upon exit; it is not flowing in the whole process.

c) Tokenized vaults in staking: Sushiswap

Similar to the aforementioned two types of vaults, vaults in staking also require an initial deposit in order to receive a corresponding token certificate, returned from the smart contract. However, some vaults may set strict rules on the duration of staking, such that only at maturity can the collateral be redeemed and interest claimed. For example, in Ethereum POS, all ETH for validation must wait for the first fork upgrade after the Merge to be released in line; in other words, the liquidity of sport ETH on hand is forfeited. As a response, some protocols, such as Sushiswap, have started to work on modifications of staking rules.

- How Sushibar works

In Sushibar, users could stake Sushi and receive xSushi at the current exchange rate. For every transaction on Sushiswap, 0.05% of the transaction fee would be deposited as LPs to

the Sushibar Vault. Finally, vaults would exchange these LPs to Sushi periodically (at least once a day), and distribute yields to each user who participated in staking according to their proportion. During the process, users could withdraw and retrieve the original amount of Sushi anytime.

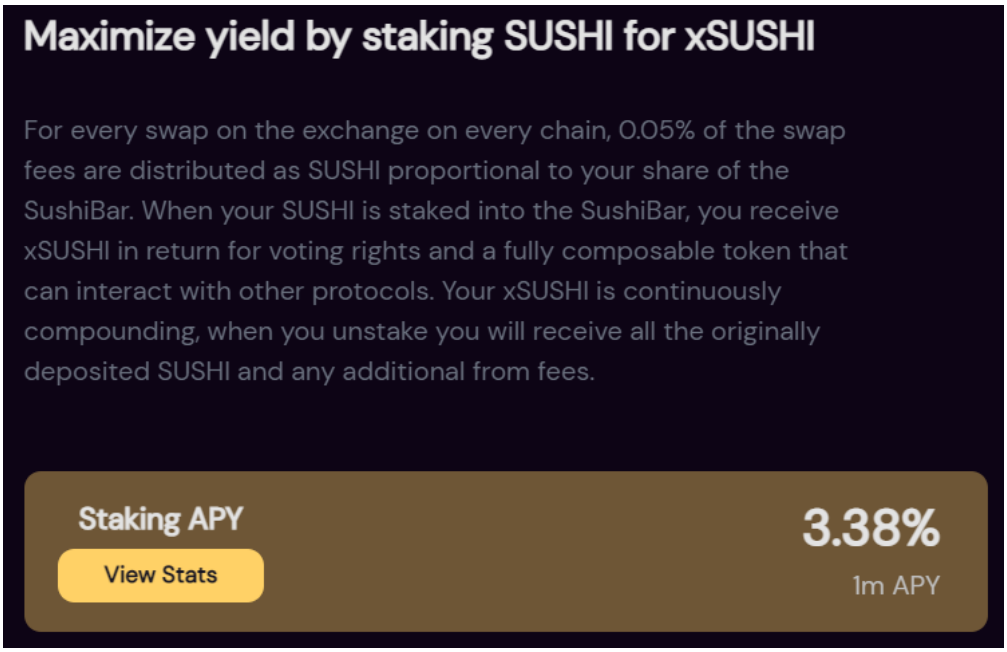


Figure 5: Staking rules for xSushi

Source: SushiSwap

As xSushi represents real assets, SushiSwap endows more viable functions for xSushi such as liquidity mining, lending and borrowing, as well as voting in community governance, etc.

Further, xSushi is not only eligible to receive yields as a certificate for staking, but is also feasible for subprime lending. The versatility of xSushi points to a brighter future with more possibilities for DeFi.

Through detailed analysis of the status quo of the mainstream DeFi protocols, we found that current yield-bearing tokens in tokenized vaults suffer from low capital efficiency and low liquidity. ERC-4626 may be the solution: it is intent on becoming the new infrastructure in DeFi

so that developers could configure tokenized vaults and yield-bearing tokens economically, and promptly.

2. ERC-4626: Tokenized Vault Standard

As mentioned above, the mission of ERC-4626 is to improve the poor liquidity of yield-bearing tokens, which are all ERC-20 compatible. To put it another way, ERC-4626 is not a brand-new standard to renounce and replace ERC-20, but rather an extension, or a portal.

ERC-4626 provides a universal development foundation for vaults with single ERC-20 tokens to represent shares so that holders can be eligible for more options in the vaults.

It proclaims the following criteria to be standardized:

1. The way users deposit and withdraw from the vaults;
2. The functions to calculate the amount of yield-bearing tokens and underlying assets;
3. An interface to confirm the address of underlying assets;
4. Events that take place when interacting with vaults, including deposits and withdrawals.

As a result, standardized vaults could enable every yield-bearing token to interact with each other across various DeFi protocols quickly without boundaries, ushering a new era of interoperability between different protocols. Therefore, ERC-4626 has already been at the center stage even though it is not officially launched. Figure 6 shows some early adopters.

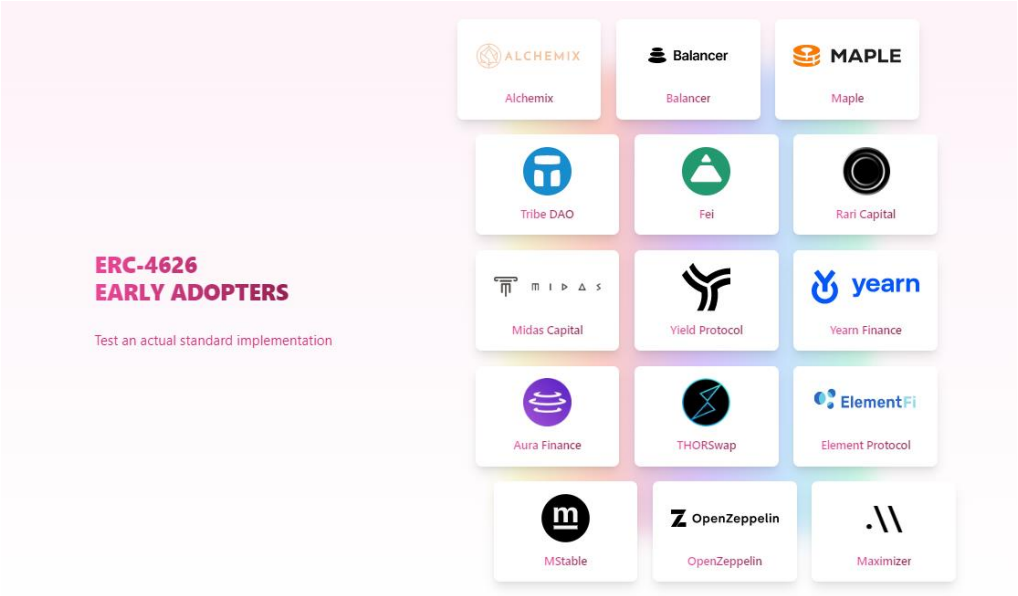


Figure 6: Early adopters of ERC-4626

Source: ERC4626.info

3. ERC-4626: Break of Dawn or Prophet of Doomsday?

From the above, ERC-4626 is a new solution to solve the current incompatibility of yield-bearing tokens to each other and the corresponding lack of application scenarios. Practically, the following influences may emerge:

3.1 Break of Dawn: New opportunities

a) Cost savings. As mentioned, ERC-4626 provides a universal development framework for developers. In the future, if new yield-bearing vaults are desired, only a standardized API is necessary to connect existing vaults to other protocols instead of a special adaptor or socket. Meanwhile, unnecessary auditing costs can be saved due to the standard coding rule that prevents errors to some extent.

b) Further improve the composability of DeFi protocols. The most attractive thing about DeFi is that developers can combine various protocols of free will without centralized permission to pursue higher profits by continuous innovations. As a complement, DeFi is frequently called

"Finance Lego" – by structuring all kinds of frames via certain combinations of modules, each module could enjoy a stronger network effect with augmented functions and practicality. At the same time, synergies will arise between various modules that further elevate the value. **Nonetheless, ERC-4626 merely reduces the friction of integration between various DeFi protocols, which facilitate the functions of yield-bearing tokens, rather than being a must for composability.** For instance, stETH is a staking certification provided by Lido to those who participate in the validation in Ethereum Beacon Chain: it is nothing more than a reimbursement solution to remedy the liquidity loss of staking users. Yet Aave desires more than just a structured product, namely a stETH/ETH regressive leverage strategy, which enables stETH holders to amplify earnings by multiple lending. ERC-4626's philosophy has been rooted in some protocols long before the mainnet was deployed.

c) Improve capital efficiency. When yield-bearing tokens are not just lying in the wallet and waiting for predetermined and fixed yields at a fixed date, but circulating all over other protocols similar to the underlying assets, the capital efficiency of users is bound to be optimized. For instance, Sushiswap enables xSushi holders to receive staking rewards of Sushi as if they were still in staking status, even though the original xSushi deemed as a certificate for rewards are already serving as underlying assets elsewhere. Hence, when ERC-4626 is officially launched, more applications are expected to embrace external yield-bearing tokens, promoting more innovations on products with embedded earnings.

d) Promote the DeFi 2.0 era. In the past two years, DeFi has grown rapidly with TVL of over US$200 billion at its peak. However, issues were exposed in the DeFi 1.0 era: low capital efficiency, poor liquidity, and high slippage rate, etc. As a result, DeFi 2.0 was proposed by some protocols in response to fix the existing defects. **We predict that ERC-4626 will be the major force to accelerate the shift of DeFi to a new era. Along with the implementation, lending and borrowing and yield aggregators may become the first to undergo a revolution and innovation.** For lending and borrowing, collateral assets may become more abundant with higher flexibility for composability, dramatically lifting the adoption rate of lending and borrowing protocols. For aggregators, each token may be compatible with more vaults, paving the way to new strategies which are higher in risk and products to emerge in the market.

3.2 Prophet of Doomsday

Although higher yields are promising by composability, these opportunities present certain issues. Originally, higher earnings come from the high leveraged earnings of single collateral via multiple implantations. In a bull market, a certificate of staking could be utilized as liquidity in most scenarios as long as the value of underlying assets continuously increases; the leverage increases synchronously. **However, yield-bearing tokens are generally less popular in a bear market, and the leverage cannot reach such a high level. Meanwhile, high leverage comprises multiple layers of risk such that once the price fluctuates over a certain range, multiple forced liquidation may be triggered by a single default.** With the launch of ERC-4626, various products are expected to enter the market, which can continuously amplify earnings. However, if the mechanism does not feature any form of risk management, products with high leverage will become unsustainable, leading to systematic risk.

In this aspect, the following measures may be considered to avoid the above-mentioned risks:

a) Set a quota for each account where any debt exceeding the limit would be subject to forced liquidation the moment it happens, regardless of the collateral value;

b) Adjust the collateral rate and liquidation ratio in extreme conditions to prevent downward spiral through a large amount of liquidation;

c) Enhance current risk control measures, establish close surveillance on on-chain liquidation activities; and find a reserve with a safe balance for liquidation to be completed within one single system.

4. Conclusion

As a crucial supplement to ERC-20, the absolute advantage of ERC-4626 lies in the standardization of tokenized vaults, so that issues regarding the security of codes are eliminated to enable more convenient integration between various protocols. Even though ERC-4626 has not been officially launched, the general idea is already widely accepted in

whole or in part. In the next few years, the entrenchment of ERC-4626 will drive flexibility in mix and match and interoperability between protocols. It may even be possible for ERC-4626 to become the standard for a new product in Defi to be structured and delivered. However, it can be a double-edged sword: if no proper improvements or upgrades are applied to the product mechanism, there is a possibility it can cause the system to collapse.

ERC-4626 is just around the corner, and we shall see if it will become an angel or a devil.

References:

1. https://eips.ethereum.org/EIPS/eip-4626
2. https://ethereum-magicians.org/t/eip-4626-yield-bearing-vault-standard/7900
3. https://ethereum.org/zh-tw/developers/docs/standards/tokens/erc-4626/
4. https://erc4626.info/
5. https://compound.finance/
6. https://yearn.finance/vaults
7. https://sushi.com/

About Huobi Research Institute

Huobi Blockchain Application Research Institute (referred to as "Huobi Research Institute") was established in April 2016. Since March 2018, it has been committed to comprehensively expanding the research and exploration of various fields of blockchain. As the research object, the research goal is to accelerate the research and development of blockchain technology, promote the application of blockchain industry, and promote the ecological optimization of the blockchain industry. The main research content includes industry trends, technology paths, application innovations in the blockchain field, Model exploration, etc. Based on the principles of public welfare, rigor and innovation, Huobi Research Institute will carry out extensive and in-depth cooperation with governments, enterprises, universities and other institutions through various forms to build a research platform covering the complete industrial chain of the blockchain. Industry professionals provide a solid theoretical basis and trend judgments to promote the healthy and sustainable development of the entire blockchain industry.

Official website：

https://research.huobi.com/

Consulting email:

research@huobi.com

Twitter: @Huobi_Research

https://twitter.com/Huobi_Research

Medium: Huobi Research

https://medium.com/huobi-research

Disclaimer

1. The author of this report and his organization do not have any relationship that affects the objectivity, independence, and fairness of the report with other third parties involved in this report.

2. The information and data cited in this report are from compliance channels. The sources of the information and data are considered reliable by the author, and necessary verifications have been made for their authenticity, accuracy and completeness, but the author makes no guarantee for their authenticity, accuracy or completeness.

3. The content of the report is for reference only, and the facts and opinions in the report do not constitute business, investment and other related recommendations. The author does not assume any responsibility for the losses caused by the use of the contents of this report, unless clearly stipulated by laws and regulations. Readers should not only make business and investment decisions based on this report, nor should they lose their ability to make independent judgments based on this report.

4. The information, opinions and inferences contained in this report only reflect the judgments of the researchers on the date of finalizing this report. In the future, based on industry changes and data and information updates, there is the possibility of updates of opinions and judgments.

5. The copyright of this report is only owned by Huobi Blockchain Research Institute. If you need to quote the content of this report, please indicate the source. If you need a large amount of reference, please inform in advance (see "About Huobi Blockchain Research Institute" for contact information) and use it within the allowed scope. Under no circumstances shall this report be quoted, deleted or modified contrary to the original intent.

THE END