UPVAULT FINANCE

UpVault Finance whitepaper version 1.0

help@upvaultfinance.io | info@upvaultfinance.io

UPVAULT FINANCE

Protocol Whitepaper
V1.0 Jan, 2023

Introduction

UpVault Finance is a decentralized exchange and payment settlement protocol based on blockchain technology.

It leverages the characteristics of decentralized blockchain networks.

- Permissionless: Anyone can access without permission.
- Trustless: Based on smart contracts to be transparent and secure without having to trust a third-party.
- Anti-censorship: Based on cryptographic technology that makes value transfer unstoppable.
- Robustness: 24/7 uninterrupted, no single point of operation.

With the innovative development of Decentralized Finance (DeFi), we have seen money markets, lending markets, trading markets, payment networks, insurance markets, derivative markets etc. gradually forming a new and open financial ecosystem based on Blockchain. However, many protocols are still evolving, and there are problems in user experience and separated liquidity.

Thanks to the openness, programmability, and composability of smart contracts, UpVault Finance will integrate various mature financial protocols within the ecosystem and build a global settlement layer on top of them. UpVault Finance will be used as an exchange and payment infrastructure for applications and create a robust and rich global financial market with its ecosystem partners.

We hope that through community building, we will provide developers with a unified and standardized access point to DeFi as well as users with a simple and easy-to-use finance interface, so that everyone can use open financial services freely and equally.

Origin

UpVault Finance, originated in 2022, aiming to offer in-wallet decentralized exchange, with the vision of UpVault Finance becoming an infrastructure of decentralized payment services that provides real-time payment and settlement between different networks and different currencies.

Today, the cryptocurrency payment scenario has not yet arrived, but decentralized exchanges (DEX) have gradually begun to be accepted by the market. As liquidity is an important part of the financial market, the success of DEX will directly affect whether open finance can revolutionize traditional finance and cryptocurrency becoming a more inclusive value store and payment tool.

UpVault Finance is based on an improved off-chain Request for Quotation (RFQ) architecture built on the 0x DEX protocol. With on-chain settlement, UpVault Finance provides users with a trading experience that does not require trust, has neither slippage, nor front running. Thanks to its design, the on-chain settlement success rate is 99.6%, far ahead of other DEX protocols.

As the original vision persists, we are continuing to improve UpVault Finance to make it a payment and settlement infrastructure for open finance.

Future

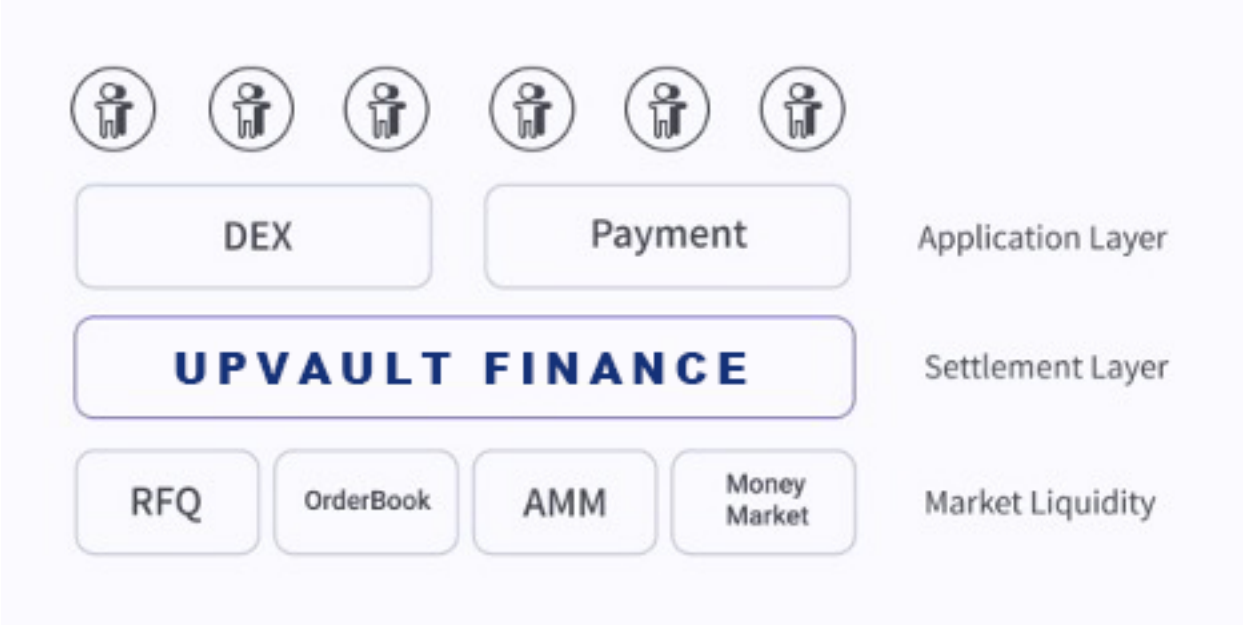
After three years of exploration and practice, UpVault Finance has completed the first milestone, allowing wallet users to easily and reliably complete fast token exchange. In this process, our early users, the core team, Kyber team, 0x team, market makers, and other partners are indispensable. Thus, we aim for more contributors to participate in the construction of the next milestones.

UpVault Finance is committed to becoming the infrastructure of the global financial market and connecting the blockchain ecosystem in an open and inclusive manner. The development of a decentralized community is the only way to go. A well-designed and dynamically evolving token economic mechanism can align incentives for all participants and contribute to the creation of an open network protocol and community ecology.

UPVAULT, UpVault Finance’s token, will play this vital role, and UpVault Finance will also open the way to decentralized community governance.

System Architecture

Layered Architecture



UpVault Finance protocol defines a financial service network that provides users with payment and exchange settlement. In essence, it connects users with the market liqudity to achieve safe, efficient, and low-cost transactions.

The supply side of the liquidity is not only diverse, but also fragmented, and even full of uncertain risks.

The satisfaction of user needs requires solving the asymmetry of time, information, subject matter, and payment medium.

UpVault Finance's three-tier structure meets the needs of all parties:

Market Liquidity

Defines settlement strategies for different liquidity sources through smart contracts, which can not only aggregate different liquidity sources to create the best exchange rate, but also resolve unknown counterparty risks. An atomic settlement ensures that the transaction can be concluded without trust between the two parties.

Settlement Layer

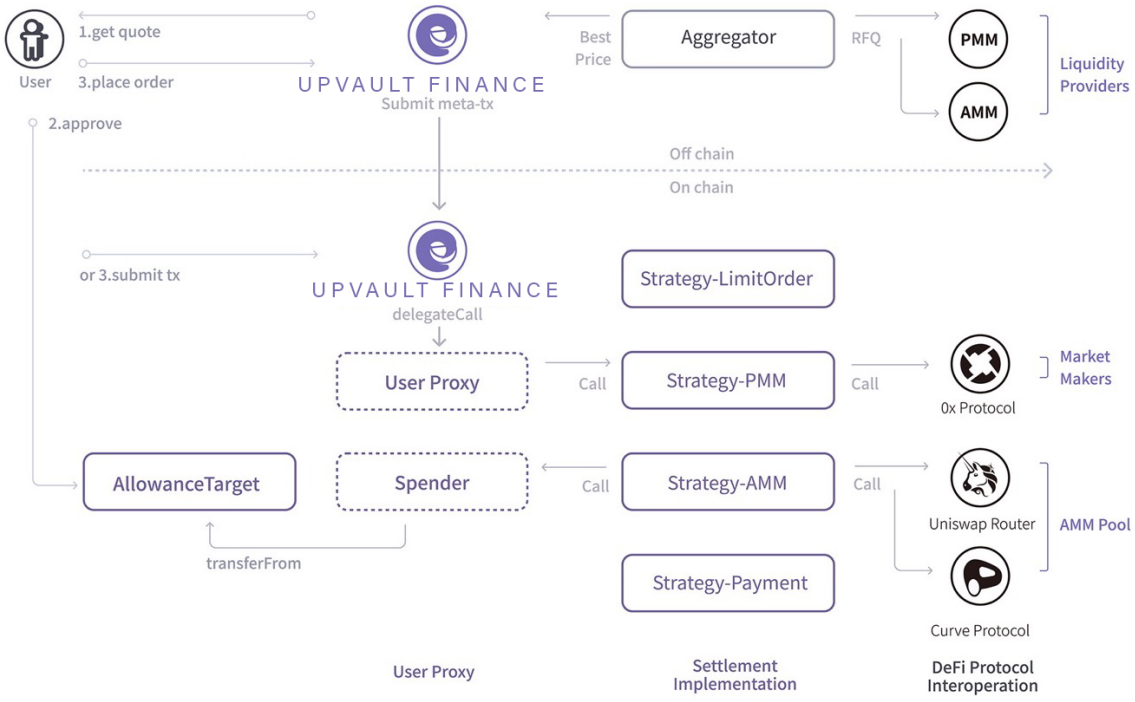
UpVault Finance network connects both trading parties, and based on digital signatures, the trade is finally settled through smart contracts. The settlement logic is based on the pre-defined strategy with trade conditions, liquidity sources, and agreed fees.

Application Layer

The application layer offers APIs and provides standard SDKs for developers to integrate the functionality into other applications and provide users with an alternative, easy-to-use interface.

It is our core concept to develop with users as the center, and to then add protocol and network layers.

System design



System architecture diagram

Modules

User

Users use digital wallets with their own private keys to access the DApp provided by UpVault Finance or third-party integrators to trade.

On-chain Contracts

Users need to authorize Tokens to **AllowanceTarget** before officially submitting the order for the on-chain settlement. This is a small step for the user to authorize. The design takes into account long-term validity (to avoid contract upgrades requiring users to authorize again) and the security hierarchy. Before on-chain settlement, UpVault Finance will verify the order and user signature[2]. Only when the verification is successful, a token deduction can be made with **Spender**.

UpVault Finance Proxy

Following the EIP1967 Proxy[3] standard, UpVault Finance Proxy acts as a protocol entry to proxy specific business logic code, and it separates business logic from persistent storage, making future protocol upgrades more convenient and secure.

UserProxy

Acts as an agent for the interaction between users and on-chain contracts, routing to different contracts according to user instructions, such as

- Fill Order: Submits an off-chain order for on-chain atomic settlement;
- Swap: Designates an on-chain automatic market maker to perform token exchange;
- Payment: Specifies how many tokens to pay to the recipient;

At the same time, it is responsible for managing the life cycle of agency contracts and strategic contracts.

Liquidity Strategy

Implements liquidity settlement strategies for smart contracts to adapt to different types of liquidity providers. At the same time, it helps liquidity partners to customize their different trading strategies.

Off-chain System

Relayer

UpVault Finance off-chain network relay service provider that operates relay nodes in a peer-to-peer network and provides services such as order routing, transaction matching, and on-chain settlement.

Aggregator

Responsible for integrating multiple liquidity sources to find the best order for users.

Liquidity Providers

Liquidity sources in the market that are integrated to UpVault Finance, including:

- On-chain automated market maker
- Off-chain professional market maker
- Order book with orders submitted by users
- Centralized exchange order book

Our strategy is to integrate liquidity providers from various sources, with the system automatically selecting the best route for users.

Security

Transaction Atomicity

For a user's on-chain transaction, the smart contract design guarantees the atomicity of transaction settlement, that is, either the transaction conditions are met to complete the settlement or the transaction fails, and the user's assets are always kept in the wallet, under the user’s control.

Contract Authorization Control

UpVault Finance protocol involves upgrading and configuration, which requires an administrator account for execution. The administrator account is a ⅗ multi-signature account[4] to avoid a single point of failure. At the same time, for operations related to user assets, the contract is designed with a timelock to delay update time, and for the administrator to make corrections within the period of delay.

Minimizing Trust

For the trust relationship between users and the protocol, we follow the principle of minimizing dependence. In the first version of UpVault Finance 5.0 design, users need to trust the verification and settlement logic of the strategy contract. We opened source all contract code publicly verifiable on chain. Anyone can audit the contract, thus establishing trust based on transparency.

3rd-Party Security Audit

The first round of security audit will be done by a professional security audit team before it goes live on mainnet, while the launch time will be based on the results of the audit report.

After the version is released on mainnet, a second round of security audits will be conducted for the contract deployed on the mainnet.

Before every contract change and upgrade, a third security audit will be submitted. In addition, we will continue to provide a Bug Bounty and encourage the community to submit security risk reports.

Tokenomics

Decentralizing UpVault Finance

In order to achieve a neutral and robust exchange and payment settlement protocol, UpVault Finance itself needs to be integrated with the blockchain ecosystem and become a part of the entire decentralized network. The design of the tokenomics and the decentralized governance model aligns all ecosystem participants' incentives, and sustainably promotes the positive development of UpVault Finance.

Ecosystem Overview

Participants of the network include:

- **Users**, including: Users of the protocol and referrers
- **Liquidity providers**, including: Market makers, brokers, asset providers
- **Developers**, including: Core development team, community developers, relay operators, and third-party integrators
- **Governance participants**, including: TIP proposer, reviewers, and token-holding voters

As developers come together to build a valuable protocol, a product and service that solves real pain points, more traders are attracted.

While the value created by the network continues to be invested into further developing the ecosystem, more contributors are encouraged to participate, optimizing and upgrading all layers of the protocol, letting the protocol enter a positive feedback loop.

UPVAULT builds the core of that ecosystem feedback loop.

UPVAULT: UpVault Finance Network Token

UPVAULT is a utility token issued by UpVault Finance, used to align all parties involved in the ecosystem and incentivize participation and expansion of the ecosystem.

Token Utilities

UPVAULT tokens have the following two main use cases:

1. Fee discount: UpVault Finance currently charges a standard 0.30% fee for most transactions. By holding UPVAULT, users can get corresponding fee discounts based on the number of tokens held.
2. Governance: UPVAULT will give the community the right to participate in the governance of UpVault Finance. UPVAULT holders can improve UpVault Finance by initiating UpVault Finance Improvement Proposal (TIP) proposals and voting, such as determining the use of the treasury, fee parameters, buyback parameters, supporting assets, product features, etc.

UPVAULT AMOUNT	Rate
0	0.30%
20	0.29%
50	0.28%
150	0.26%
500	0.24%
1,500	0.22%
5,000	0.20%
10,000	0.18%
30,000	0.15%
100,000	0.10%

UpVault Finance Fee Table

Economic Mechanisms

Buyback

Net fees collected by UpVault Finance will be used to buyback UPVAULT on the open market, and the UPVAULT bought back will be transferred to the treasury and staking reward pool.

Staking

UPVAULT holders will be able to enjoy fee discounts and governance rights by participating in

the staking. In return, the stakers will receive UPVAULT as staking reward. The staking rewards come from the UPVAULT bought back on the open market. The number of UPVAULT used for staking rewards from each buyback will be determined by the following formula.

*stakingRewardUPVAULT = buybackUPVAULT * stakingRewardFactor)*
*UPVAULT Staking amount = UPVAULT buyback amount * Staking Reward Factor*

The default staking reward factor value is 0.6, that is, for every buyback of 1 UPVAULT, 0.6 UPVAULT will be used for staking reward.

Treasury

Treasury is a UPVAULT reserve pool governed by the community, used to develop and promote the development of the UpVault Finance ecosystem. The UPVAULT in the treasury comes from UPVAULT bought

back on the open market. The number of UPVAULT allocated to the treasury in each buyback will be determined by the following formula.

*treasuryUPVAULT = buybackUPVAULT * (1 - stakingRewardFactor)*
*UPVAULT amount in the Treasury = UPVAULT buyback amount * (1 - stakingRewardFactor)*

The default value of the initial staking reward factor is 0.6, that is, for every 1 UPVAULT bought back, there will be 0.4 UPVAULT allocated to the treasury.

Core team is expected to start the governance contract development in the third quarter of 2022, and the specific launch date and implementation plan will be announced to the community in the future. Before the governance contract goes live, the community will be able to participate in early governance through Snapshot[5], conduct off-chain voting, and participate in forming proposals led by the core team.

Risks

Investment risk

UPVAULT is a utility token issued by UpVault Finance, not an investment product. Before making a purchase decision, the purchaser should carefully consider whether it is suitable for its financial situation,

purchase objectives and experience, risk tolerance, and other relevant circumstances, and should also understand the relevant risks involved in the purchase of UPVAULT.

System risk

Security is the highest priority of the UpVault Finance protocol. The core team and the external security audit team have invested a lot of resources to ensure that the protocol is safe and reliable.
UpVault Finance related smart contract codes are public and verifiable, and we also invite external security personnel to join our Bug Bounty program and look for vulnerability.

Glossary

DeFi
Short for Decentralized Finance. Specifically refers to open, transparent and financial agreements and products that are implemented on smart contracts on a blockchain.

DEX
Short for Decentralized Exchange, which part of the DeFi category.

RFQ
Short for request-for-quotation, a trading system where quotes are provided in response to a

request for a quote submitted by a trader.

UPVAULT
The native asset of UpVault Finance ecosystem, which is used to keep all the ecosystem participants aligned.

LIP
The plan to distribute TT to incentivize all the ecosystem participants.

TIP
The proposal that drives the change of UpVault Finance, TT holders can vote on the proposal to participate in the Governance.

Reference

[1] 0x Protocol Specification

[2] EIP-1271: Standard Signature Validation Method for Contracts

[3] EIP-1967: Standard Proxy Storage Slots

[4] dYdX PartiallyDelayedMultiSig
[5] Snapshot is an off-chain gasless multi-governance client