# Optim Finance

Whitepaper - Version 1
October 13, 2021

[https://optim.finance/](https://optim.finance/)

We appreciate the dedication and effort of our core team members and the larger Cardano community for making this project possible. As the DeFi ecosystem grows and improves we look forward to serving our users and staying on the cutting edge of what's possible. As we finish the technical spec and get further into our build we expect improvements, iterations, and more clarification regarding the implementation details provided in this document. We will continually update this document to reflect these changes.

# Table of Contents

# 1. Abstract

Simply put, Optim provides crypto holders the means to passively earn optimized returns on their digital assets. Users have access to a portfolio of products across Cardano's decentralized finance (DeFi) ecosystem These smart contract products utilize expertly designed yield farming strategies to optimize and automate yield generation through an intuitive and easy-to-use interface.

Optim simplifies the often complex and burdensome process required to maximize DeFi returns. As the DeFi space continues to grow, tools are needed that allow for automated asset management. Additionally, system-wide capital efficiency is improved by directing assets to higher utilization, yield generating opportunities. For these reasons, a protocol like Optim is integral to the adoption and success of any DeFi ecosystem as it matures and grows.

With rapid protocol development underway, superior security properties, low cost transactions, and a native asset with a top five market capitalization Cardano is well-positioned to quickly realize and grow a large DeFi ecosystem.

# 2. Core Products

The Optim protocol provides users access to optimized yields through vaults. Vaults are pools of deposited assets which utilize investment strategies encoded in smart contracts to allocate funds to yield opportunities. These strategies automatically yield-farm by performing various ordered functions such as deposit, harvest, swap, and mint across many protocols. Automating tedious multi-step processes, reducing fees through pooled transactions, and dynamically shifting assets to better opportunities all contribute to maximize yield.

All of Optim's products incorporate the vault design. Although users lock their funds in vaults, funds are immediately redeemable at any time. To ensure optimal returns for users, multi-strategy vaults automatically rebalance asset allocation based on market opportunities. Oracle integrations are necessary for some core products and are covered in section 9.

## 2.1 Single Asset Vaults

Single Asset Vaults manage a specific asset by deploying funds to yield farming opportunities across the ecosystem. The strategies for these vaults primarily lend assets, collateralize and mint stable coins, stake, and engage with decentralized exchanges using stable swap invariants. DEXs with high impermanent loss exposure are not used in single asset vault strategies.

Each vault consists of one or more strategies into which the pools of deposited assets are deployed. Multi-strategy vault asset allocation is constantly reweighted based on performance and market conditions.

## 2.2 DEX LP Vaults

DEX LP vaults automatically manage LP positions on decentralized exchanges (DEXs). These vaults maximize yields through auto-compounding by staking LP tokens, selling governance tokens earned as rewards, and swapping to LP asset pair tokens to build positions.

DEX LP vault users may also elect to auto-compound yields while retaining a portion of earned governance tokens. In this scenario, users select from predetermined ratios of auto-compounding versus governance token retention. To avoid impermanent loss, users can opt to programmatically liquidate LP positions by setting volatility-based parameters.

## 2.3 LenderOps

LenderOps vaults automatically shift deposited assets between lending protocols optimizing yield in the form of interest paid to the lender. Funds are transferred between Liqwid, Meld, and other whitelisted lenders as interest rates dictate. As such, LenderOps optimizes the interest accrual process across all whitelisted platforms to obtain the highest interest rates at all times on behalf of users. LenderOps also builds users' positions by harvesting governance token rewards and selling them to purchase and deposit additional assets to lend.

## 2.4 KeeperOps

KeeperOps vaults take advantage of arbitrage and similar opportunities across the Cardano DeFi ecosystem. More specifically, KeeperOps deploy capital to capture value from DEX arbitrage opportunities or borrower liquidations on lending protocols. Outside periods of market inefficiencies, idle assets are either staked or lent out across whitelisted protocols to accrue interest. This ensures that KeeperOps pools continually compound value.

## 2.5 StakerOps

StakerOps is a stake optimizer that allows users to efficiently manage their staked ADA based on a number of adjustable parameters. The core features of StakerOps are pool selection, auto-monitoring, and diversification. Users can set pool preferences based on factors such as yield optimization, causes, pool size and Single Pool Operators. If StakerOps monitoring detects a change in pool performance it can automatically re-stake based on your preset preferences. Users can also automatically diversify their staking rewards into other tokens and even enter yield farming opportunities. The fees for using StakerOps are half of normal vault fees.

# 3. Key Concepts

### *Vaults*
Pools of capital deployed to generate yield on behalf of depositors.

### *Strategies*
Asset allocation plans, encoded in smart contracts and used to deploy assets towards gainful opportunities in the market. Strategies identify market opportunities among whitelisted protocols. Some vaults have multiple strategies others have only one.

### *Strategists*
Optim team members or active community members who design strategy blueprints minus the associated smart contract programming.

### *Yield Farming*
Staking or lending digital assets to generate returns.

### *Lending and Borrowing Platforms*
DeFi platforms like Liqwid and Meld that connect lenders and borrowers.

### *Ovault Tokens*
Tokens given to vault depositors that represent user assets as proportional shares of a vault. Analogous to deposit receipts.

### *OTM Governance Tokens*
Tokens that represent governance rights on the Optim platform. Users can stake OTM tokens in order to vote while simultaneously accumulating more OTM.

### *Security*
Security is at the center of the Optim protocol. Optim benefits from the robust security of the Cardano blockchain, and smart contracts on the platform undergo rigorous testing and auditing.

## 4. Using Optim

A primary goal of the Optim protocol is to make using and optimizing DeFi as simple and intuitive as possible. As such, the user experience is a key component of the value we provide. Throughout development and after launch we'll be continually testing UI/UX and soliciting feedback from the community. Anywhere we can remove friction and improve the user experience, from features to functionality, we'll consider implementing in short order. In addition, we'll work to provide in-depth technical analysis and detailed documentation on each component of our protocol for more advanced users.

## 4.1 Depositing

Users interested in earning optimized yields on their crypto assets simply deposit funds in an Optim vault through the platform's intuitive UI.

In turn, vaults automatically provide depositors oVault tokens. oVault tokens are LP tokens that function as a deposit receipt. They represent a user's share of the vaulted assets and any yield accrued against that share.

## 4.2 Withdrawing

With the exception of time-locked vaults, depositors can withdraw funds from Optim vaults at any time via the UI. Entering time-locked vaults always requires an additional verification step to ensure users are aware of the withdrawal terms. Moreover, users can always withdraw all or part of their locked funds and accrued yield.

Users submit oVault tokens via the Optim app UI to withdraw their assets and accumulated rewards. Users are able to easily check their redemption token and reward balance prior to withdrawal.

## 4.3 Calculating APY

Annual percentage yield (APY) is the real rate of return earned on an investment, taking into account the effect of compounding interest. The APY displayed next to each Optim vault is the current rate of return based on all historical data. This accounts for all fees and compounding returns.

DeFi protocols where Optim deploys assets for yield generation typically accrue interest every block, with the harvest optionality different for each protocol. The frequency of harvests and resultant compounding schedule for assets in Optim's strategies is carefully optimized to maximize returns. To gain insight into these dynamic parameters users can look at the Optim contracts on CardanoScan to view the exact call and compounding schedule.

## 4.4 OTM: Earn + Staking

OTM tokens are distributed to users of the protocol. We believe that OTM tokens, which dictate the governance and direction of Optim, should be in the hands of community members who have experience interacting with our products. The token emission schedule and distribution mechanism has not yet been determined. Once we release our V1 product more details will be published on this topic.

Staking OTM tokens is an important aspect of governance. Additional OTM tokens as well as higher weights towards governance votes are accrued to stakers. The reason for this is to ensure that decisions made by the community are resistant to short-term manipulation by accumulating OTM in the market. Staking emissions as well as the impact on governance votes will be public as governance vests on the platform.

## 5. Vaults and Strategies

As the key functional components of the Optim protocol, vaults and strategies are a primary area of focus and constant iteration. While the vault structure for asset management in DeFi is originally an Ethereum construct, the implementation on Cardano is unique. The distinction and composition of both off-chain and on-chain components is important. A robust infrastructure that is sufficiently decentralized and persistent to ensure the integrity of all parts of our system is paramount. Validation, transaction construction, and computation are just a few important pieces that the more technically inclined in our community should understand. For those more familiar with Plutus and the eUTXO model we will be providing more extensive documentation on the how and why behind our system architecture and design patterns.

## 5.1 Vault Creation

Initially, vault creation will be managed by the Optim founding team. Experienced developers are responsible for coding the Plutus smart contracts which run vault strategies. The team will also guide contracts through audit, code revisions, and necessary iterations.

Throughout development, however, the Optim team will incorporate the ideas of finance strategists. Finance strategists are active community members who propose vault strategies separate from the associated smart contract programming. In future versions of the protocol, this process will be entirely decentralized and under the direction of community governance. We

anticipate the decentralization of coding strategies to be gradual due to the lack of experienced Plutus developers and available tooling from IOG.

Depositors with particularly long investment time horizons (six months, a year or longer) may choose to apportion funds to Optim's time-locked vaults. Similarly to how CDs benefit credit unions and banks, long term deposits benefit Optim's yield generating strategies. As such, users depositing into time-locked vaults will receive lower service fees, increasing their realized return.

## 5.2 Vault Fee Structure

Fees are an important consideration of any investment. Ensuring Optim users earn the highest risk-adjusted Cardano DeFi yields, while providing the convenience of passive investments through automated vaults, is our aim. The fee structure is intended to incentivize user adoption, strategist compensation, and the operational integrity of the protocol.

The Optim protocol is a platform for every investor. As such, Optim's vault fee structure seeks a balance between accessibility and ease of use with platform security.  Vaults only harvest yields if doing so is profitable after fees so users don't withdraw less than their initial deposit.

Fees are subject to change based on governance voting. *The fees listed below are an example of the structure we are considering and will likely be lower at protocol launch.

| Deposit | Withdrawal | Performance fee Unlocked Vaults | Performance fee Locked Vaults | Management fee |
|---------|------------|--------------------------------|------------------------------|----------------|
| 0.05% | 0.2% | 5.0% | 3.0% | 1.5% |

Minimal deposit and withdrawal fees help prevent malicious actors from spamming the platform with exploitive transactions. Performance fees help incentivize innovation and management fees incentivize participants, keepers, and smooth operational functions. Initially, a portion of vault performance fees will be allocated to the treasury. Once the Optim DAO is fully active, OTM token holders may choose to allocate a portion of treasury funds to incentivize OTM token dynamics.

## 5.3 Strategies

Strategies are at the center of yield generation on Optim. Yet, they provide end users with much more: community engagement, assurance, rewards, and transparency.

As mentioned, strategies are hard-coded into smart contracts. These smart contracts outline the discrete actions that yield generating tactics execute to produce returns. Strategies must specify the deposit currency, yield currencies, script state datum, the harvest redeemer, and other crucial components. Naturally, strategy smart contracts are publicly available for investors to review.

Optim's initial vault strategies will be developed by the founding team. However, future strategies will also incubate among the community. Finally, bot networks will help automate vault housekeeping for most Optim vaults. Bots will manage selling reward tokens, reinvesting rewards, managing collateral, and other administrative duties to manage funds in a capital efficient manner.

While all strategies must be discrete, hard-coded contract paths which undergo audits, there is dynamic asset allocation between specific vault strategies. Oracle data feeds power off-chain computation which feeds back to our vault re-weighting process. Based on the spec we are currently writing, we'll soon clarify the re-weighting process between strategies and its automated and manual components.

## 5.4 Strategists

Akin to YFI's yBrain, Strategists are Optim team members who deploy and monitor pre-programmed vault strategies, alongside a Custodian, to realize optimized returns. On the other hand, community members can serve as Finance Strategists by providing their ideas on generating yield.

Optim's Discord forum hosts a #strategy channel as a place for open discussions as well as a venue for finance strategists to propose ideas. Our governance forum is where strategies are formally submitted and voted on by the community. A provided template will help streamline submissions. While there is no guarantee that every strategy proposal will be incorporated into production, there will be a formal proposal and voting process. Furthermore, Finance Strategists whose proposals are successfully enacted will be entitled to a portion of the vault fees associated with their strategy.

## 5.5 Vault Management

*Functions*

Vaults will be managed by a variety of bots and keepers, wherever possible and safe to do so. These bots will be open sourced for community members to help maintain the platform in exchange for OTM tokens. At regular meaningful intervals, our bots will automatically review and notify strategists and custodians of optimizations for each vault's holdings. Interactions involving trust can either be centralized with multi-sig requirements or require proportional holdings of staked OTM tokens to keep the interactions trustless.

*Interventions*

Each vault has two designated individuals , a custodian and strategist, who have the authority to make adjustments to the vault. Clear incentives will ensure the interests of these parties are aligned with the community members they serve.

Adjusting asset allocation in multi-strategy vaults, ongoing optimizations, minor adjustments, and necessary interventions in black swan events are the responsibility of designated individuals for Optim vaults. The strategist, who is the vault creator, and the custodian jointly share maintenance privileges. Any changes to the script that affects the conditions by which a redeemer can consume pooled UTXOs must have authorization by the multisig wallet to execute this function.

## 5.6 Vault Tokens

Optim depositors receive oVault tokens upon locking funds in vaults. For instance, ADA placed in an oVault will be represented by oVada. The yield generated from an oVault strategy is reflected in the share price of an oVault token. The price increases due to more underlying tokens representing each oVault token as yield accumulates to the vault. oVault tokens are burned as users withdraw funds.

Naturally, oVault tokens will be native tokens on Cardano, meaning they will enjoy the same functionality as ADA and other assets on the blockchain. For Optim users, this means oVault tokens can be traded frictionlessly while incurring minimal transaction costs.

## 5.7 EUTXO Vault Architecture

DeFi protocols first experienced significant use on Ethereum, an account-based blockchain with smart contract functionality. Unlike Ethereum, however, Cardano's EUTXO model more closely resembles that of Bitcoin. This implies inherently different architectures between Optim and its counterparts on Ethereum.

Cardano's EUTXO model encourages separating on-chain and off-chain logic and delegating most calculations off-chain, and so is Optim. When we talk about a vault, we are talking about a validator script which contains some strategy details as state, two or more minting policies for NFTs and oTokens, and the accompanying off-chain code to prepare the transactions correctly. The off-chain code can be further used and extended by bot operators who wish to participate in Optim protocol

Briefly, when users deposit funds in Optim vaults they are tied to the script of an EUTXO transaction, which in turn allocates these funds to a yield farming strategy. A withdrawal transaction in turn spends the outputs of the allocating EUTXO transaction effectively signaling a "claw back" of funds, and the associated assets, plus yield, are retrieved from the vault and returned to the user.

The design of our "batching" solution will effectively manage any contention that might arise from multiple users trying to withdraw from a vault simultaneously. Our approach to efficiently processing concurrent transactions will be explained at length in a separate document.

Considerations relating to this aspect of protocol design are being made from the outset and will be integrated into our core contracts and larger system.

# 6. Security

The security of the Optim protocol is our number one priority, followed by performance. From an extensive multi-step audit process to multi-signature time-locked vaults, Optim puts the security of user funds at the forefront of everything we do. We're constantly iterating and adding to our security measures and expect to further improve this infrastructure prior to launch. We'll provide the community updates regarding this topic and solicit feedback on our Discord and governance forum.

## 6.1 Smart Contract Audits

All smart contracts deployed on Optim for yield strategies go through an extensive audit and review process. Contracts are first analyzed by internal smart contract engineers and security experts who did not in any way contribute to coding the contracts. The contracts are then reviewed by  the audit team at MLabs. This preliminary review, fast-tracked by our close partners, expedites the audit process by ensuring standardization and adherence to core Plutus best practices as outlined by IOHK. Contracts are then forwarded to unaffiliated third party auditors for further review. Optim is in talks with two leading audit firms which will be on retainer in order to guarantee new strategies are audited quickly and implemented without undue delay.

## 6.2 Multi-Signature Vaults

Multi-signature (multisig) is a cryptographic security scheme wherein numerous parties individually control the cryptographic keys used to control funds. The simplest analogy is a safety deposit box that requires several key turns -- say three keys from a set of five -- to open. Due to its enhanced security, multisig is a common tool throughout the cryptocurrency space.

Optim uses multisig security for many of its vaults to ensure the safety of user funds, protocol changes, and OTM token emissions.

*Administrative multisig*

Admin functions that change the MintContract which distribute OTM tokens to vault depositors are controlled by a 24-hour timelock contract that requires two of five signatures. All admin functions that control Optim vaults are controlled by 10-hour timelock contracts requiring two of

five signatures. Timelock contracts will trigger an alert on the Optim app notifying users of upcoming changes.

*User multisig*

Vaults of any kind (Single asset, LP, KeeperOps) can incorporate multisig. Designated Cardano wallets act as signatories, and smart contract validators can additionally be required to validate transactions that withdraw funds. These flexible yet robust security schemes make Optim an ideal platform for developers, third-party platforms, and institutions to build upon.

## 7. OTM Token

Effective governance is essential to the success of the Optim protocol. As the platform decentralizes, responsibility will shift from the founding team to the community. Future governance will rely upon the DAO, or decentralized autonomous organization, structure.

OTM tokens are there to bridge the gap. To effectively coordinate the efforts of community members with the long-term success of Optim, these governance tokens will convey voting rights and benefits to holders.

The Optim (OTM) token is strictly a utility token that will launch when the protocol is live and sufficiently decentralized. As an open-source, decentralized protocol, any future changes to the token and its utility is strictly the purview of the community and not in the control of any one person or small group of people.

### 7.1 Utility

OTM holders enjoy certain voting rights. Token holders are entitled to vote on fee structures and to approve new strategies that hold an auditor's verifiable signature. Furthermore, the amount of staked OTM holdings will determine a community member's voting power, with more influence evolving from greater stakes.

A successful proposal will initially require a quorum of four percent of issued OTM tokens to enter a period of deliberation. This is to ensure a basic level of community oversight over changes to the protocol. A subsequent approval vote will determine whether proposals are adopted. Here, in favor votes need only outnumber votes against.

### 7.2 Staking

OTM holders are eligible to participate in governance decisions. Staking OTM tokens grants users voting rights. OTM stakers can signal initial support for proposals as well as participate in subsequent for-or-against governance decisions

Future OTM token holders may also choose to alter treasury dynamics in order to benefit themselves. This development may occur only after Optim has fully decentralized. In this scenario, any potential rewards would likely be accrued every five days, in line with the epochs of Cardano. Depending on future governance decisions, users could be able to claim accumulated rewards at the end of these periods.

## 7.3 Token Distribution

Overall, OTM tokens provide a means for active community members to make the Optim protocol their own. OTM tokens will be awarded for several types of participation in the community:

- Users who create and use Optim vaults
- Bot operators and keepers who provide utility and performance to others
- Participants in staking and governance

As mentioned, OTM holders will enjoy voting rights and other benefits on the Optim protocol.

## 8. Governance

The initial protocol will be built and maintained by the founding team. However, future versions will incentivize independent developers to run and maintain the platform. Optim will accomplish complete protocol decentralization through governance and reward systems using its native OTM token. A DAO and formal governance structure will be live upon protocol launch to ensure an appropriate degree of decentralization and distributed decision making from the outset.

Optim's governance system outlines the roles and responsibilities of the founding team as well as mechanisms for community members to engage with the protocol. We believe strongly in decentralisation and autonomy. As the Optim protocol matures, we will foster an active community that will grow into a fully functioning DAO.

## 8.1 Structure and Participants

Optim's governance structure is similar in form to that of a representative democracy. The decision making process begins and ends with OTM holders. The Optim community, through our voting system, designates oTeam "representatives" to help consolidate the decision making process. oTeams in turn execute proposals developed and voted on by the community.

***oTeams***

oTeams are small groups of protocol developers who work independently or in conjunction with contributors from the community. These specialized individuals are responsible for protocol changes that affect their areas of interest. oTeams are elected by OTM holders and serve at the discretion of community members.

oTeams have certain decision-making and emergency powers that cover a range of protocol functions:

| Team | Object | Power | Responsibilities |
|---|---|---|---|
| oGuard | Protect oVaults | Emergency Powers | Intervene during attacks or shutdown recalcitrant strategies or vaults |
| oBrain | Manage strategies | Control strategy operations | Fine-tune strategies and direct their maintenance |
| oDev | Manage protocol | Maintain protocol codebase | Manage Optim's development process |
| oPeople | Curate team | Payroll | Manage team payroll |
| oBudget | Manage protocol funds | Set protocol budgets | Set budgets for platform operations |
| oFarm | Grow Treasury | Deploy treasury | Use treasury for yield farming and manage airdrop reinvestments |
| oTx | Write transactions | Design transactions | Create transactions for the multisig to sign |
| oSignatories | Coordinate contributions | Ratify oTeam signers | Control the approval and removal of oTeam signers |

## 8.2 Proposals

OTM holders will determine the development of Optim through proposals. While it is incumbent upon the community to create and vote for proposals, they convey significant decision-making powers to users. There are three categories of Optim proposals:

- Optim Improvement Proposal (OIP): motion to enact platform changes

- Optim Delegation Proposal (ODP): motion to reallocate decision making powers, for example, among oTeams
- Optim Signaling Proposal (YSP): non-binding motions to signal community sentiment

Enacting and voting for Optim proposals allows users to reassign or revoke oTeam powers, alter the OTM token contract, set fees, and so on.

Proposals will require an initial quorum of four percent of token holders to be eligible for deliberation. Discussions and debates will be hosted on our #proposal channel, and a template for submission will be made available. A simple for-or-against vote among holders determines the final outcome of a proposal. Tooling for voting and confirming the staked token holders

# 9. General Technical Overview

Upon launch, DEX LP Asset Vaults will be most prominent followed by StakingOps, and a few Single Asset Vaults. Lender Ops will be possible once there are two or more lenders in the space

In order for LenderOps and KeeperOps to work efficiently, we need robust and accurate oracles to indicate whether a lending protocol or a stake pool has a higher APY. We are planning to integrate with Chainlink or build our own oracle solution with the upcoming read-only UTxO in Plutus hard-fork.

Oracle integrations will enable vault validator scripts, wherever necessary, to adhere to off-chain parameters that can distinguish and appropriately adjust to dynamic market conditions.

**DEX LP Asset Vaults**

*Basic Functions*

Deposit Options
1) Deposit LP token into pool and mint oToken as receipt that represents share of underlying asset pool
2) Once users select a pool, users can provide liquidity with just one token. For instance, if users select ADA/LQ pool, users can provide liquidity by just supplying ADA. Optum will automatically and optimally swap the tokens to make sure users have equal value of both ADA and LQ to supply to ADA/LQ pool on SundaeSwap.

Adjustable Auto-Compounding Options

1) 100% reinvest: Harvest all governance token LP staking rewards from DEX and swap them for underlying LP asset pair to build user's position.
2) 50%/50% OR 25/75 - reinvest/hold native gov token.

<u>Functions Executed In/By Pools</u>

1) Call harvests
2) Withdraw harvested tokens
3) Route harvested tokens to DEX
4) Swap harvested tokens for LP asset pair
5) Generate new LP token on designated DEX
6) Add new LP tokens to the DEX LP token pool

### *Single Asset Vaults*

Basic Functions

<u>Deposit Options</u>
1) Deposit individual token into pool and mint oVtoken as a receipt that represents a share of the underlying asset pool, including any yields accrued on that pool.
2) Pools are limited to a single token type, the user can deposit additional funds at any time, or withdraw for a small fee.

<u>Adjustable Auto-Compounding Parameters</u>
- Adjust and tune strategies to be used within the vault and initial weights.  (strategies are limited to those that start with the vault's indicated asset)
- Choose to allow automatic reweighting across strategies, or to lock in existing strategies.
- Choose to allow Reinvestment level

### *Strategies*

A Strategy is a flattened data representation of a series of contract interactions that must be performed to execute various critical operations that form a *strategy interface*.
Each strategy must specify the following:
- Deposit currency
- Yield currencies
- Yield swap mapping (if yield currency is different than deposit currency)
- Yield reinvestment frequency
- Deposit validator and Redeemer
- Pre-deposit steps
- Withdrawal redeemer
- Harvest redeemer
- Dex pairing for reinvestment of yield

These serve as validation instructions which will be used by Optum keepers & bots to perform automated operations based on user settings.

## 9.1 Performance Considerations

Plutus's performance issues occur mainly when state needs to be shared among users. Fortunately, the contracts necessary for Optum do not require this kind of *immediate* and *shared* user state, instead, this data can be aggregated by trusted actors within the system.

Optum is designed to keep almost all transaction-specific data in vaults or user-specific structures to reduce contention on any kind of central state. Global state will be based on bot, rather than user actions, allowing for a highly responsive smart contract for all user-facing interactions, at a small increase in overhead used for keeper/bot interactions.