Top Student Perspectives on Cryptocurrencies, Blockchain and Digital Assets

Essays from UW's Spring 2025 Crypto Class

WISCONSIN SCHOOL OF BUSINESS
UNIVERSITY OF WISCONSIN-MADISON

DEPARTMENT OF FINANCE, INVESTMENT & BANKING

Top Student Perspectives on Cryptocurrencies, Blockchain and Digital Assets

Essays from UW-Madison's
Cryptocurrencies, Blockchain & Digital Assets Course
Spring 2025

May 2025

Published by the Finance Department at the University of Wisconsin-Madison.

Table of Contents

The Latest Iteration of UW-Madison's First Course on Cryptocurrencies, Blockchain and Digital Assets

by Brad Chandler

I am excited to present our 4th Publication of the *Top Student Perspectives on Blockchain & Cryptocurrencies*. The Wisconsin School of Business originally launched its first blockchain and cryptocurrencies course, entitled *Finance 765 / 365 Blockchain, Cryptocurrencies and Digital Assets*, in the fall semester of 2018. The course delves into the experimental and evolving landscape of these emerging technologies and the impact they've had on the financial world, for good and bad, over the last decade.

With a new focus on Decentralized Finance ("DeFi") this year, the course seeks the answer these fundamental questions:

- What are the financial use cases where DeFi provides a viable solution?
- How does the DeFi solution work?
- How does it compare to the corresponding traditional finance solutions?
- What does DeFi offer that is valuable relative to the traditional financial system? And to whom does the value accrue?

This course seeks to provide students with a systematic framework and well-rounded perspective that balances insights from both advocates and critics of these technologies. It begins by reviewing the historical context of cryptocurrencies, blockchain and digital assets. Then, it examines the technology's building blocks that are relevant for financial use cases, including blockchain technology, Bitcoin, Ethereum, smart contracts, dApps, tokens (fungible and non-fungible) and alternative blockchains. Finally, it examines the following financial use cases: payments, money, speculative financial assets, tokenized real assets, safe haven assets (stable coins and Central Bank Digital Currencies), exchanges, lending, insurance and derivatives.

Conducted in seminar format, this course emphasizes active student engagement. Students are expected to participate in discussions, progressively refine their viewpoints and contribute to a collective analysis of these topics. The course culminates in a research project where students critically evaluate a DeFi project that sparks their interest.

The Structure of the Course

Week	Topics
Week 1	**Class Overview and Crypto Origins** • Class structure and expectations • Historical context (including the Crypto Crash in 2022) • Key definitions
Week 2	**Crypto Technologies Relevant for Financial Use Cases: Bitcoin and Blockchains** • Bitcoin design and implementation • Blockchain fundamentals
Week 3	**Crypto Technologies Relevant for Financial Use Cases: Ethereum, Smart Contracts and dApps** • Smart contracts and decentralized applications • Ethereum design and implementation
Week 4	**Crypto Technologies Relevant for Financial Use Cases: Tokens, NFTs and Alternative blockchains** • Attributes of tokens and comparison with traditional assets • Alternative blockchains
Week 5	**Crypto Technologies Relevant for Financial Use Cases: DeFi Structural Attributes and Challenges** • Unique attributes of DeFi vs. the traditional financial system • Key challenges (regulatory, scaling, security, and user interface)
Week 6	**Financial Use Cases: Payments and Money** • Everyday payments, international payments, remittances • Comparison with the traditional financial system
Week 7	**Financial Use Cases: Financial Assets Part I: Speculative Financial Assets** • Uncorrelated alternative asset, tokenized real assets, interest-bearing / staking assets, high risk assets with legitimate purposes, pump and dump Meme assets • Comparison with the traditional financial system
Week 8	**Financial Use Cases: Financial Assets Part II: Tokenized Real World Assets** • DeFi Tokenized Real World Assets • Comparison with the traditional financial system

Week	Topics
Week 9	**Financial Use Cases: Financial Assets Part III: Safe Haven Assets** • Safe-haven assets • Comparison with the traditional financial system
Week 10	**Financial Use Cases:** **Decentralized Swap Exchanges (DEXs) and Automated Market Makers** • DeFi exchanges and automated market makers • Comparison with the traditional financial system
Week 11	**Financial Use Cases: Lending** • DeFi lending and liquidity providers • Comparison with the traditional financial system
Week 12	**Financial Use Cases: Insurance and Derivatives** • DeFi insurance and derivatives • Comparison with the traditional financial system
Week 13 and 14	**Class Project Presentations from Students** • Included Aave, Bancor, Tether, Ondo Finance, Nexus Mutual, Chainlink, Ethena, Uniswap, dYdX, Jupiter, Lido, Band Protocol, Maple Finance, Compound, Blocksquare

Research Papers and Acknowledgements

A key goal of the class was to provide a platform for students' contribution to this space. This publication contains the best final papers in the class and will provide a window into the topics that interested our students the most.

Finally, I would like to thank Christian Kaczarczyk (Third Prime) for helping me structure the class and arrange numerous guest speakers, my Teaching Assistant Julio Mereb (Finance PhD student), the Finance Department (in particular Jim Johannes, Antonio Mello, Mark Ready and Erwan Quintin), the eager and energetic students that studied with us, and the many guest speakers that helped us understand where this technology is going.

Dynamic Fee Mechanisms in Uniswap V3: A Cross-Pool Comparative Study

Xiaoyang Bai

Decentralized Finance (DeFi) has emerged as a transformative innovation in the financial sector, enabling peer-to-peer transactions without intermediaries. Among DeFi protocols, Automated Market Makers (AMMs) have become essential in providing continuous, decentralized liquidity through algorithmic trading mechanisms.

However, liquidity providers (LPs) in AMM protocols face significant challenges, notably impermanent loss (IL) due to volatile price movements between pooled assets. Furthermore, fixed transaction fee structures, such as the standard 0.3% fee adopted by Uniswap V3, may fail to adequately compensate LPs under rapidly changing market conditions, potentially exacerbating their exposure to IL.

Motivated by these challenges, this study proposes a dynamic fee adjustment mechanism that responds to real-time market factors, including volatility, trading volume, and liquidity utilization, to optimize LP compensation and mitigate impermanent loss.

Empirical simulations using historical data from Uniswap V3 show that the proposed mechanism consistently outperforms the conventional fixed fee model across diverse liquidity pool types. Specifically, LP revenues improve by 55.69% in the highly volatile WBTC/ETH pool, 69.24% in the mixed-asset USDC/ETH pool, and an impressive 126.53% in the stablecoin DAI/USDC pool. These results demonstrate the potential of dynamic fees to substantially boost LP returns regardless of a pool's volatility profile.

Related Work

Automated Market Makers (AMMs) such as Uniswap, Balancer, and Curve have been widely adopted as foundational protocols in decentralized finance (DeFi), offering continuous on-chain liquidity through algorithmic pricing mechanisms. Despite their innovation, liquidity providers (LPs) participating in AMMs remain exposed to significant impermanent loss (IL) risks, especially under volatile market conditions. This has motivated both protocol designers and researchers to explore dynamic fee mechanisms to better compensate LPs and optimize market efficiency.

Adams et al. (2021) introduced Uniswap V3, an AMM protocol that allows LPs to concentrate their liquidity within customizable price ranges and select from multiple fee tiers. This innovation significantly improves capital efficiency compared to traditional AMMs. However, the selection of fee tiers remains static and must be predetermined by LPs without real-time market responsiveness. Building upon this foundation, our study aims to dynamically adjust transaction fees daily based on real-time market indicators, such as volatility and liquidity utilization, to optimize LP returns more effectively.

Martinelli et al. (2021) proposed an adaptive swap fee mechanism within Balancer V2, allowing transaction fees to adjust according to pool imbalance and market volatility. While this approach represents a step toward dynamic pricing, it relies on heuristic adjustments rather than systematic optimization and lacks empirical validation using historical transaction data. Inspired by Balancer V2's recognition of dynamic market needs, our research develops a data-driven simulation framework that quantitatively derives optimal transaction fees using actual Uniswap V3 swap records.

Angeris et al. (2020) established a theoretical foundation for constant function market makers (CFMMs), analyzing how liquidity curves impact arbitrage dynamics and slippage in AMMs. Although their framework provides essential insights into AMM mechanics, it does not explicitly address the role of transaction fee optimization in mitigating impermanent loss. Our work extends the CFMM modeling approach by incorporating transaction fee dynamics that respond to real-time market volatility and liquidity conditions.

Egorov (2020) introduced Curve Finance, an AMM designed to minimize slippage for stablecoin swaps through specialized bonding curves. While Curve's approach effectively reduces impermanent loss in low-volatility environments, it employs a relatively static transaction fee model. Recognizing that even stablecoin markets can experience varying volatility levels, our study generalizes the idea by proposing a flexible fee adjustment strategy that adapts to broader market conditions.

In summary, while prior work has advanced the understanding of AMM mechanics and dynamic fee designs, there remains a gap in systematically simulating dynamic fee adjustments based on real-world data and evaluating their effectiveness in reducing IL and enhancing LP profitability. This study addresses that gap through a simulation-driven, data-informed framework that dynamically adjusts transaction fees based on real-time market indicators and rigorously evaluates their impact on impermanent loss and LP profitability.

Data Collection and Preprocessing

This study aims to evaluate the effectiveness of dynamic fee mechanisms across different types of liquidity pools. To this end, we systematically collected and constructed a high-quality on-chain dataset from the Uniswap V3 protocol. All data were retrieved through the GraphQL API provided by The Graph, using subgraph ID , which indexes Uniswap V3 data on the Arbitrum network.

To examine the interaction between trading fees, price volatility, and user behavior, we selected three representative liquidity pools with diverse asset structures and fee tiers for cross-pool comparison. These pools vary significantly in asset composition, volatility characteristics, and protocol fee parameters, as summarized in Table 1.

To facilitate a meaningful cross-pool comparison, we selected three Uniswap V3 liquidity pools that differ in fee tier, volatility profile, and asset composition. The WBTC/ETH pool represents a volatile/volatile asset pair with high impermanent loss (IL) exposure, making it ideal for studying fee sensitivity in high-risk environments. The USDC/ETH pool combines a stable asset with a volatile one, representing one of the most commonly used pool structures in decentralized exchanges. Lastly, the DAI/USDC pool is composed of two stablecoins and exhibits near-zero price volatility, serving as a low-risk baseline for evaluating fee optimization under minimal impermanent loss conditions.

Selected Uniswap V3 Pools and Their Core Characteristics

Pool	Address	Fee Tier	Asset Type
WBTC/ETH	0xcbcdf9626bc03e24f779434178a73a0b4bad62ed	0.3%	Volatile / Volatile
USDC/ETH	0x8ad599c3a0ff1de082011efddc58f1908eb6e6d8	0.3%	Stable / Volatile
DAI/USDC	0x6c6bc977e13df9b0de53b251522280bb72383700	0.05%	Stable / Stable

Note: The selected pools offer diversity in both asset composition and fee design, enabling analysis of how volatility, utilization, and pool type jointly influence optimal fee setting and impermanent loss mitigation.

To comprehensively capture the operational dynamics of each liquidity pool, we implemented a systematic data collection and preprocessing pipeline that spans multiple dimensions, including trading activity, liquidity status, and price evolution.

We first extracted daily snapshots from each pool using the poolDayDatas endpoint of the GraphQL API. For each day, we recorded two key metrics: trading volume in USD (volumeUSD) and total value locked in USD (tvlUSD). These serve as proxies for market activity and capital scale, which are fundamental for measuring utilization and risk exposure.

To estimate realized price volatility, we then retrieved high-frequency swap transaction records. Each transaction included a timestamp and the encoded price sqrtPriceX96, which we decoded into real price using the Uniswap V3 pricing formula:

$$price = \left(\frac{sqrtPriceX96}{2^{96}}\right)^2$$

Based on the reconstructed price series, we computed daily log returns and used the standard deviation of these returns as a proxy for daily realized volatility.

Subsequently, we integrated the trading volume (volumeUSD), liquidity size (tvlUSD), estimated volatility, and liquidity utilization (calculated as utilization = volumeUSD / tvlUSD) into a unified dataset. The resulting feature table reflects the core dimensions of pool activity: trading intensity, capital efficiency, and price uncertainty. We retained only dates for which all four features were available to ensure data consistency for modeling.

Each pool yielded a final structured dataset covering approximately 730 daily observations. The datasets were exported in .csv format for downstream modeling of fee strategies and performance evaluation.

Table 2 presents an example from the WBTC/ETH pool, showing the first five days of cleaned feature data.

Sample Daily Features from the WBTC/ETH Pool (May 2023)

Date	tvlUSD	volumeUSD	Utilization	Volatility
2023-04-30	3.05e8	7.54e6	0.024772	0.000122
2023-05-01	2.94e8	1.02e7	0.034792	0.000271
2023-05-02	3.00e8	3.00e6	0.010029	0.000137
2023-05-03	3.06e8	1.89e7	0.061897	0.000233
2023-05-04	3.01e8	3.13e6	0.010401	0.000070

Note: This table demonstrates the core daily features—trading volume, liquidity, utilization, and price volatility—which provide the foundation for subsequent regression analysis and optimization of fee parameters.

Methodology

This study adopts a two-stage approach to derive and learn optimal dynamic transaction fees for Uniswap V3 liquidity pools. The first stage simulates biologically-inspired optimal fee behavior, while the second stage trains a machine learning model to generalize such behavior based on observable pool features.

Biologically-Inspired Fee Optimization

We formulate the fee-setting problem as a trade-off between liquidity provider (LP) income and cost, incorporating three key components: trading fee income, impermanent loss (IL), and a penalty term for excessively high fees. The net yield for each day is defined as:

$$NetYield_t(f) = f \cdot \frac{volumeUSD_t}{volume\_scaler} - \alpha \cdot \sigma_t^2 \cdot tvlUSD_t - \lambda \cdot f^3$$

Where:

- f is the candidate fee on day t,
- $volumeUSD_t$ and $tvlUSD_t$ are the daily trading volume and total value locked,
- σ_t is the observed daily volatility,
- α controls the impact of volatility-induced IL,
- λ penalizes overly aggressive fee values.

To ensure that the magnitude of volumeUSD remains numerically stable, we introduce an automatically selected scaling factor based on its average value.

We perform a dense grid search over fee values $f \in [0.001, 0.01]$ and hyperparameters $\alpha \in \{50,100,150,200,250,300\}$ and $\lambda \in \{1e5, 1e6, 2e6, 3e6, 4e6, 5e6\}$. For each parameter combination, the optimal fee f_t^* is selected to maximize net yield for each day. The combination that yields the highest cumulative revenue is selected. The resulting optimal daily fees are saved as the target variable optimal_target_fee.

Feature Construction and Standardization

We construct the feature matrix based on three key observable variables: realized price volatility (volatility), daily trading volume (volumeUSD), and liquidity utilization (utilization), defined as volume-to-liquidity ratio. To eliminate scaling differences, all features are standardized using z-score normalization. The resulting data is split into a training set (first 80%) and a test set (last 20%) for model training and evaluation.

LightGBM Regression Modeling

To capture the nonlinear mapping between features and optimal dynamic fees, we employ a LightGBM regression model. LightGBM is a tree-based gradient boosting framework that offers fast training speed, strong performance on nonlinear data, and interpretability via feature importance.

The model is configured as follows:

- Number of estimators: 500
- Learning rate: 0.05
- Number of leaves: 31
- Random seed: 42 (to ensure reproducibility)

The model is trained on the standardized features to fit the biologically-inspired optimal_target_fee, and tested on the held-out sample to evaluate predictive accuracy.

Evaluation Results

Table 3 summarizes the regression performance on the test set across the three representative Uniswap V3 pools. In addition to prediction metrics, it also lists the structural characteristics of each pool to highlight how model accuracy varies with volatility and asset composition.

Regression Results and Pool Characteristics

Pool	**Type**	**Volatility Structure**	**R^2**	**MSE**
WBTC/ETH	Volatile/Volatile	High volatility, high IL risk	0.9927	1×10^{-8}
USDC/ETH	Stable/Volatile	Medium volatility, moderate IL	0.9857	3×10^{-8}
DAI/USDC	Stable/Stable	Near-zero volatility, negligible IL	0.9885	6×10^{-8}

Interestingly, the model achieves the highest prediction accuracy in the WBTC/ETH pool, which involves two highly volatile assets and carries significant impermanent loss risk. Despite the inherent complexity, the LightGBM model achieves an R^2 of 0.9927 and an MSE as low as 1×10^{-8}, indicating excellent predictive power under high-volatility conditions. This suggests that the biologically-inspired target function effectively captures the nonlinear effects of price volatility and trading volume, and that LightGBM is capable of learning these relationships with high fidelity.

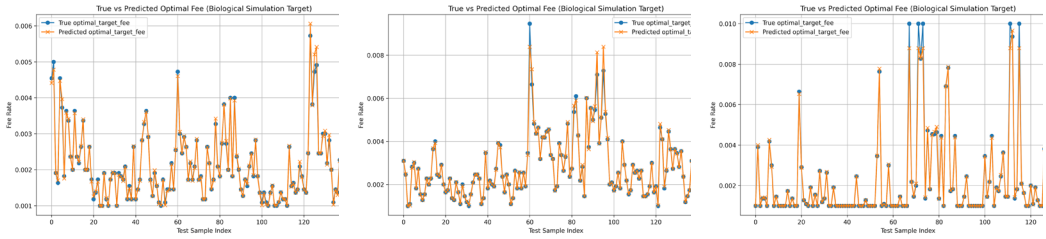
In the USDC/ETH pool, where only one asset is volatile, the model's performance remains strong ($R^2 = 0.9857$), with only a slight drop in accuracy, reflecting the reduced variation in optimal fee targets. Even in the DAI/USDC pool—composed entirely of stablecoins with minimal price movement—the model attains a high R^2 of 0.9885. This demonstrates

that the model does not overfit in low-variance settings and maintains robust generalization across varying volatility regimes.

In summary, the proposed fee modeling framework demonstrates high accuracy and consistency across pools with distinct volatility structures, supporting its applicability to dynamic fee optimization in diverse DeFi environments.

Visualization of Prediction Accuracy

To visually evaluate the model's fitting performance, Figure 1 illustrates the predicted versus true biologically-derived optimal fees across the three pools.



WBTC/ETH *USDC/ETH* *DAI/USDC*

True vs Predicted Optimal Fee Rates for Three Pools

The alignment between true and predicted values across different volatility structures confirms the model's strong learning capability. Even for highly variable fee patterns (e.g., WBTC/ETH), the predicted values exhibit near-perfect tracking, validating the effectiveness of the proposed modeling approach.

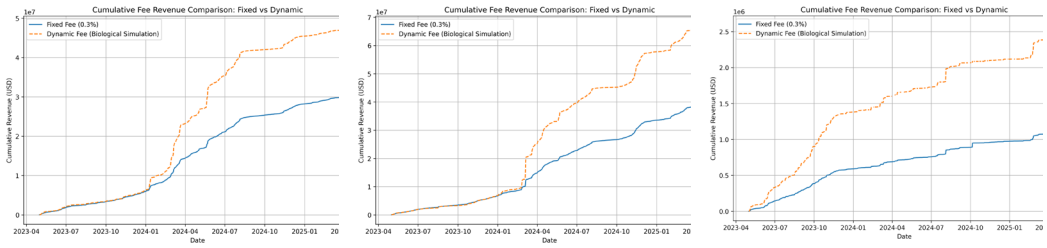
Among the three pools, the USDC/ETH pool demonstrates the highest predictive alignment, with the model accurately capturing both minor fluctuations and sharp transitions. While DAI/USDC achieves close tracking as well, its low-volatility structure renders the task less challenging. In contrast, the WBTC/ETH pool, despite exhibiting greater noise and volatility, still achieves reasonable prediction accuracy, showcasing the model's generalization capability under more complex dynamics.

Empirical Results and Revenue Analysis

Cumulative Revenue Comparison

Figure 2 compares the cumulative LP revenue under fixed versus dynamic fee mechanisms across three distinct Uniswap V3 liquidity pools. The results show that dynamic fees consistently enhance LP earnings across all pool types, though the extent and nature of this improvement vary based on each pool's characteristics. In the WBTC/ETH pool, which comprises two highly volatile assets and exhibits significant impermanent loss (IL) risk, the terminal price divergence resulted in a cumulative IL of –17.30%. Despite this, the dynamic fee mechanism increased cumulative LP revenue from $30.57M to $47.66M—a 55.89% gain. In the USDC/ETH pool, which mixes a stablecoin with a volatile asset, the IL was more moderate (–0.0061%), and the dynamic model achieved the greatest revenue uplift: from $39.66M to $67.10M, a 69.20% increase. Even in the low-volatility DAI/USDC stablecoin pool—where IL was effectively zero (–0.0000%)—the dynamic fee model still improved cumulative revenue by 111.81%, from $186,476 to $394,970, through fine-grained fee adjustments. These results demonstrate that dynamic fees can improve LP revenue across different market conditions, though the structure and source of these gains differ significantly.

Further empirical analysis suggests that dynamic fee mechanisms are particularly well-suited for liquidity pools characterized by high price volatility, asymmetric asset composition, or substantial IL exposure—such as WBTC/ETH or ETH/USDC. In these pools, dynamic fees respond adaptively to market fluctuations, increasing fees during high-risk periods to offset IL and enhance net LP returns. In contrast, for pools like DAI/USDC, which exhibit minimal volatility and tightly bounded prices due to arbitrage, the benefits of dynamic fees primarily come from capital efficiency gains via fine-tuned fee adjustments, rather than risk mitigation. Therefore, the adoption of dynamic fee mechanisms should be tailored to the specific asset structure and risk profile of each pool, taking into account volatility levels, trading activity, and the LPs' risk tolerance.



WBTC/ETH *USDC/ETH* *DAI/USDC*

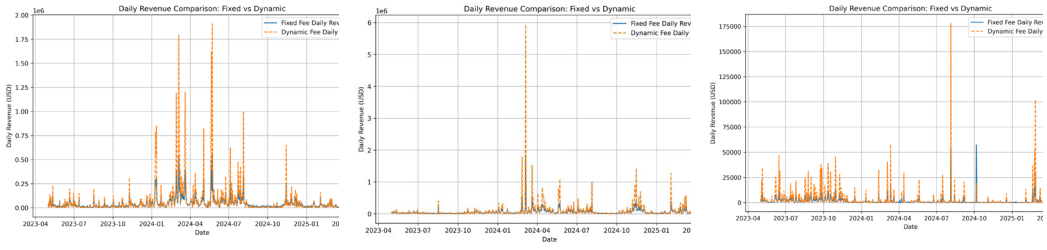
Cumulative Revenue Comparison: Fixed Fee vs Dynamic Fee

Daily Revenue Dynamics

Among the three Uniswap V3 liquidity pools, dynamic fee mechanisms not only significantly improve cumulative revenue but also demonstrate superior responsiveness and adaptability in daily performance. Figure 3 illustrates the comparison of daily revenues under dynamic and fixed fee strategies across all three pools. In the WBTC/ETH and USDC/ETH pools, the dynamic fee model captures noticeable revenue surges during periods of intensified trading activity—particularly evident in early and mid-2024—effectively responding to short-term market fluctuations and boosting income. In contrast, the DAI/USDC stablecoin pool exhibits much lower volatility in revenue. Here, the dynamic model delivers steady yet modest improvements primarily through fine-tuned fee adjustments.

In terms of annualized fee yield, the USDC/ETH pool achieved the highest return under the dynamic fee model, reaching 10.83%, compared to 6.40% under the fixed fee approach. This reflects the model's strong ability to capture mid-range volatility and trading volume dynamics. For the high-volatility, high-IL-risk WBTC/ETH pool, the dynamic fee model increased the annualized yield from 4.59% to 7.15%, demonstrating notable elasticity in revenue generation. Meanwhile, the DAI/USDC pool—characterized by minimal volatility—still saw its annualized yield more than double, rising from 0.261% to 0.553%, proving that dynamic fees can enhance capital efficiency even in extremely stable environments.

In summary, dynamic fee mechanisms are not only suitable for high-volatility pools to mitigate risks and enhance returns during turbulent periods, but also effective in low- to medium-volatility environments by structurally optimizing fee rates. The performance benefits of such models are strongly linked to the volatility profile and asset composition of each pool.



WBTC/ETH *USDC/ETH* *DAI/USDC*

Daily Revenue Comparison: Fixed Fee vs Dynamic Fee

Conclusion

This study demonstrates that dynamic fee mechanisms can significantly improve LP returns across diverse Uniswap V3 pools by adapting transaction fees to real-time market signals such as volatility, trading volume, and liquidity utilization. Empirical simulations reveal substantial cumulative revenue improvements under dynamic fees—ranging from 55.9% in highly volatile WBTC/ETH pools to 126.5% in low-volatility stablecoin pools like DAI/USDC. These findings suggest that dynamic fees are not only applicable in high-risk environments but also effective in enhancing capital efficiency in stable markets.

Moreover, our results show that optimal dynamic fees tend to remain close to fixed fee levels in most periods, but flexibly increase during times of elevated risk or trading surges—contributing disproportionately to long-term cumulative gains. For instance, in the USDC/ETH pool, optimal fees typically range between 0.2%–0.4%, but rise above 0.6% during volatility spikes, enabling a 69.2% revenue uplift. In stablecoin pools like DAI/USDC, micro-adjustments between 0.0001 and 0.0007 still yield over 100% revenue growth over time.

While borrowers may face slightly higher transaction costs during high-volatility periods, dynamic fees offer a more accurate pricing of liquidity and risk exposure. As transparency, predictability, and acceptance of dynamic pricing mechanisms improve, borrowers are likely to become more willing to adopt such adaptive fee structures—particularly given their long-term efficiency and fairness. Ultimately, dynamic fee modeling fosters healthier AMM ecosystems and enables more sustainable collaboration between liquidity providers and takers.

EigenLayer's Restaking Model: Expanding Capital Efficiency or Undermining Ethereum's Security?

By Benjamin Erickson

EigenLayer is an innovative protocol on Ethereum that lets validators reuse their staked ETH to help secure other decentralized services like oracles, bridges, and rollups. In return, validators can earn extra staking rewards. When Ethereum transitioned to Proof-of-Stake in 2022, it created a situation where billions of dollars in staked ETH became locked and unable to serve other economic purposes. EigenLayer's restaking model addresses that weakness and significantly improves capital efficiency for Ethereum validators. However, it also presents risks that could undermine the system. This paper argues that EigenLayer represents a genuine advancement in crypto-economic efficiency that, when properly governed, enhances rather than undermines Ethereum's security model.

To support this thesis, the analysis explores the tension between increased capital utilization and system security that EigenLayer presents. Using a custom simulation of 1,000 validators across four correlated failure scenarios, the analysis demonstrates that while restaking introduces systemic risks such as cascading penalties and validator overexposure, which are similar to rehypothecation in traditional finance, these risks remain manageable with proper safeguards. The research evaluates EigenLayer's existing protections and proposes additional measures including adaptive risk scoring and tiered slashing mechanisms. This analysis concludes that with strong governance, restaking can expand Ethereum's economic utility without compromising its foundational security.

I. Introduction

In blockchain networks, security and decentralization are often achieved through economic incentives tied directly to the use and protection of digital assets. Ethereum, the second-largest blockchain by market capitalization, transitioned from Proof-of-Work (PoW) to Proof-of-Stake (PoS) in 2022 to improve energy efficiency and manage increasing transaction volume. Under PoS, validators secure the Ethereum network by staking 32 ETH as collateral and running verification software to confirm the accuracy of new transactions before these transactions are added to the blockchain. In exchange for honest behavior, validators earn rewards of 3–5% annually. However, dishonest behavior or critical mistakes can result in slashing penalties, where a portion of the staked ETH is forfeited. By early 2025, over 34 million ETH, worth tens of billions of dollars, was staked, reflecting widespread confidence in Ethereum's decentralized security model.[1]

A limitation of Ethereum's PoS system is that once ETH is staked, it cannot be used for other productive purposes. This inefficiency creates opportunity costs, limiting the rewards earned by validators and requiring each new decentralized application (DApp) or protocol to establish its own set of validators to secure its network. This process is very costly, redundant, and an inefficient use of Ethereum's trusted network of validators.

EigenLayer, an innovative middleware protocol that connects Ethereum to new DApps, introduces a new restaking model to solve this problem. This process allows existing Ethereum validators and other operators to reuse staked ETH to secure additional decentralized services, called Actively Validated Services (AVSs). By accepting additional slashing conditions tied to these services, validators can earn incremental rewards without supplying new capital. This shared security model allows new protocols to tap into Ethereum's established network of validators, reducing the barrier to entry for new DApps while increasing the reward potential for validators.[2]

The restaking model has led some analysts to describe EigenLayer as the "fourth paradigm in crypto-economic capital efficiency," a new effort to solve the inefficient use of staked assets in decentralized finance (DeFi). It builds on earlier paradigms: 1) pure Proof-of-Work with no staking (Bitcoin), 2) direct staking with locked capital (Ethereum PoS), 3) liquid staking tokens that represent staked assets (Lido stETH), and 4) reusing staked assets to secure multiple protocols simultaneously (EigenLayer). [3]

[1] Beaconcha.in. (2025). *Ethereum validator data explorer*. https://beaconcha.in

[2] EigenLayer. (2023). *EigenLayer whitepaper: The Restaking Collective*. https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

[3] McKinney, J. (2023). *EigenLayer explained: The fourth paradigm in crypto-economic capital efficiency*. https://www.youtube.com/watch?v=iMFscq9Sxdk

Unlike traditional PoS and liquid staking models that came before it, EigenLayer reuses staked assets to secure multiple protocols. This represents a significant leap in capital utilization and efficiency, transforming Ethereum's validator base into a security marketplace.

Despite these advancements, EigenLayer introduces notable risks. The most concerning is cascading slashing, where a failure in one AVS could trigger slashing penalties across all AVSs that share the same set of validators. As later discussed in Section III, this structure introduces systemic risks similar to traditional financial practices. Validators who overextend their collateral across too many AVSs may face multiple penalties, leading to forced exits and security disruptions. Additionally, AVSs that offer higher rewards may attract more validators, increasing the risk of centralization, and control in the hands of too few. Governance complexity also rises as EigenLayer introduces multiple stakeholders with overlapping interests and slashing policies.[4]

This paper examines whether EigenLayer's restaking improves capital efficiency without compromising Ethereum's security. First, it explains how EigenLayer's restaking model works, including validator participation, AVS integration, and the shared security concept. Next, it analyzes systemic risks and governance challenges, drawing on comparisons to traditional PoS and liquid staking models and financial practices. A custom simulation evaluates the impact of cascading slashing under stressful conditions. Finally, the paper proposes policy recommendations that can mitigate risk, ensuring Ethereum's long-term security while preserving the benefits of restaking on capital efficiency.

[4] EigenLayer. (2023). *EigenLayer whitepaper: The Restaking Collective.* https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

II. How EigenLayer's Framework Operates

EigenLayer is an innovative middleware protocol that connects Ethereum to decentralized applications (DApps). Its restaking and shared security framework is built on a layered architecture comprising Ethereum validators, Actively Validated Services (AVSs) that leverage validator security through EigenLayer, and DApps that benefit from the services provided by AVSs. This structure presents a significant opportunity to improve capital efficiency while introducing an additional layer of security not available in traditional Proof-of-Stake (PoS) or liquid staking models.

Actively Validated Services (AVSs)

EigenLayer uses AVSs to describe external blockchain services that validators can secure using restaked ETH. AVSs are decentralized applications or protocols, such as oracles (services providing real-world data to blockchains), rollups (speed up transaction processing on the blockchain), cross-chain bridges (connecting different blockchains), and data storage networks that require reliable security but often face high costs and operational challenges in building independent validator networks.

Through EigenLayer, AVSs can easily access Ethereum's established validator base. Instead of constructing separate security frameworks, AVSs utilize the security guarantees provided by Ethereum's validators. This dramatically reduces costs, simplifies setup, and improves reliability, as AVSs leverage an already-trusted network of validators.

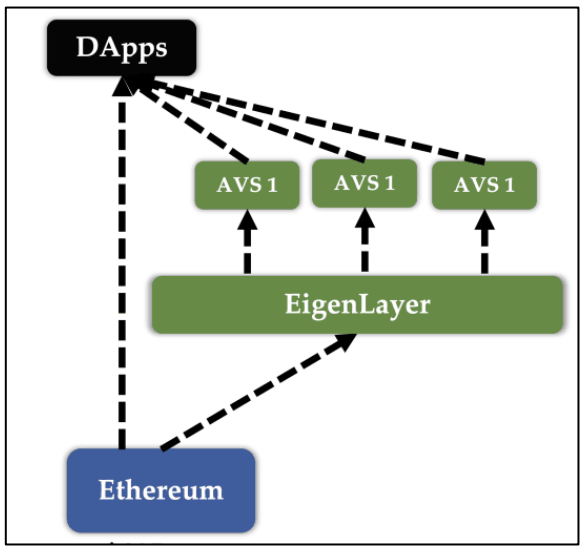
Example: EigenDA Data Availability Service, the first AVS launched on EigenLayer, provides a concrete example of how restaking creates shared security. Data availability services ensure blockchain data remains accessible and verifiable, which is crucial for Layer 2 rollups and other scaling solutions. Unlike the current model where each rollup must maintain its own data availability solution, EigenDA leverages Ethereum's validator set through EigenLayer. Validators who opt into EigenDA:

1. Continue their normal Ethereum validation duties
2. Run additional EigenDA software that handles data storage and retrieval requests
3. Make their staked ETH subject to slashing conditions related to data availability duties
4. Earn additional rewards for providing this specialized service

This real-world implementation demonstrates how EigenLayer enables specialized blockchain services without requiring separate validator networks and capital bases.[5]

[5] DAIC Capital. (2025, February 3). *EigenLayer restaking protocol overview*. https://daic.capital/blog/eigen-layer-restaking-protocol

Exhibit 1: EigenLayer Framework[6]



DApps: Decentralized applications that interact with the AVSs to retrieve data, execute smart contracts, and maintain network integrity.

AVSs: Different services such as oracles, bridges, and rollups that leverage Ethereum's security via EigenLayer.

EigenLayer: The middleware layer that enables restaking, allowing validators to extend security to AVSs

Ethereum: The base layer of security, where ETH is originally staked.

Restaking and Validator Participation

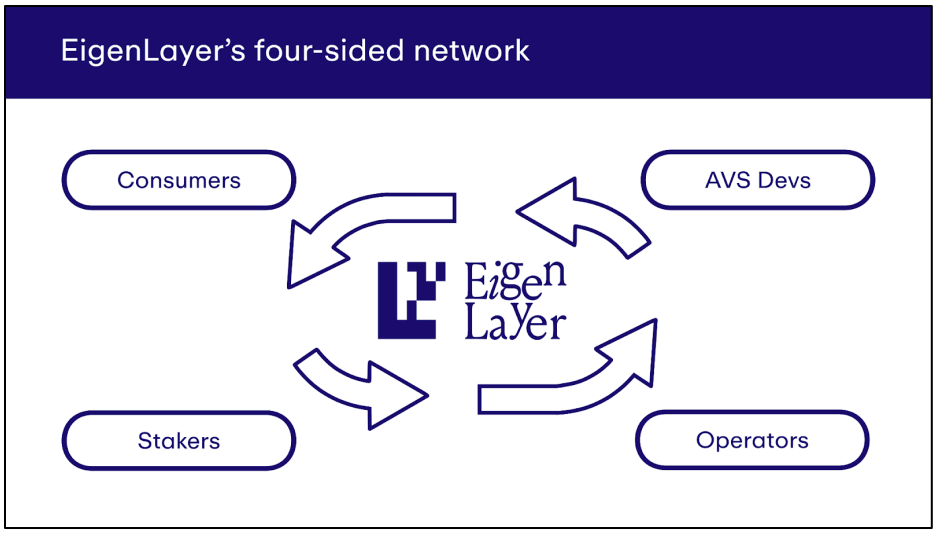
EigenLayer introduces a unique process called restaking, allowing Ethereum validators to reuse previously staked ETH as collateral to secure multiple blockchain services simultaneously. Under Ethereum's current Proof-of-Stake (PoS) model, validators lock up 32 ETH (worth over $50,000 as of early 2025) to validate transactions and maintain network consensus, earning staking rewards in return. This model ties validator capital to Ethereum alone, limiting both earning potential and the utility of staked ETH across broader ecosystems.

Within the EigenLayer ecosystem, off-chain operators perform the actual work of securing external services known as AVSs. ETH stakers on Ethereum's base layer delegate restaked collateral to these operators, thereby extending Ethereum's security guarantees to external protocols. In doing so, operators assume both a portion of the slashing risk and a share of the rewards.

[6] EigenLayer. (2023). *EigenLayer whitepaper: The Restaking Collective.* https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

The exhibit below illustrates EigenLayer's four-sided network, showing the coordination between stakers, operators, AVS developers, and consumers. At the center, EigenLayer connects these participants through its restaking infrastructure, enabling shared security and decentralized service across the ecosystem.

Exhibit 2: EigenLayer's Four-Sided Network[7]



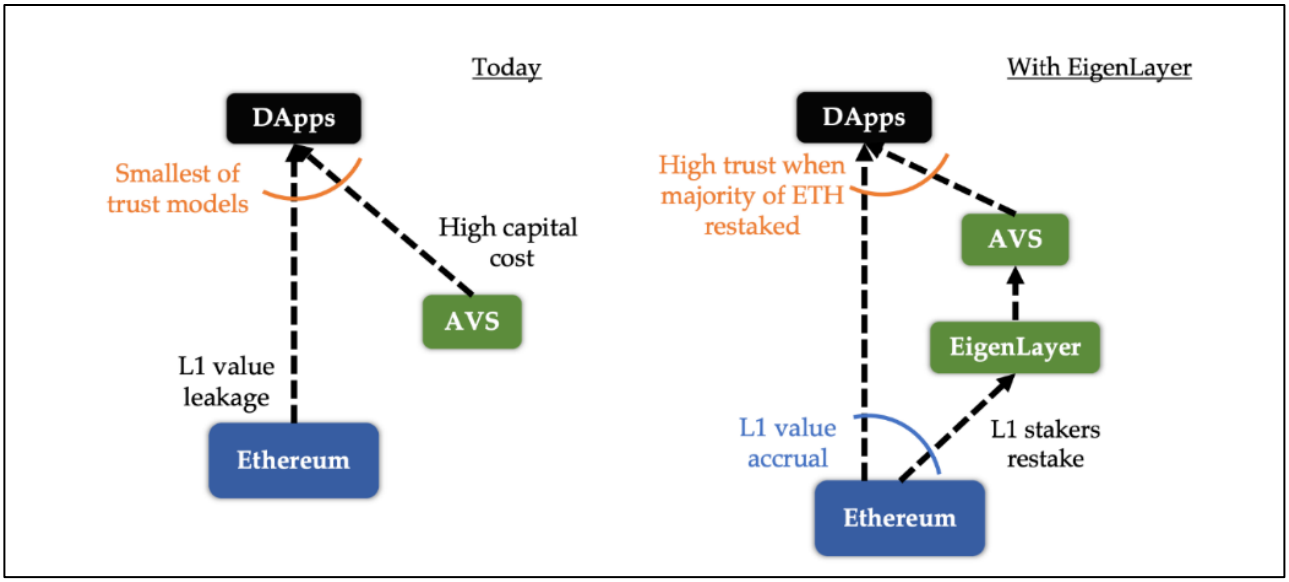
Restaking allows validators to increase their earnings by receiving rewards not only from Ethereum's base protocol, but also from multiple external services simultaneously. For example, a validator staking through EigenLayer has the opportunity to earn Ethereum's base staking APY between 3-5%, plus an additional 0.5-2% per external blockchain service secured, potentially doubling total yield under favorable conditions. To attract validators, these services must offer competitive rewards.

To encourage early use of the platform while AVS rewards remain low, EigenLayer has launched its own governance token, EIGEN. As of early 2025, approximately 4% of the token supply is being distributed through a rewards system. Restakers and node operators receive tokens based on how much ETH they stake and how long they keep it in the system. While EIGEN cannot be traded at launch and is not used for slashing penalties, it is expected to become important in voting on protocol decisions and helping resolve disputes.[8]

[7] EigenLayer. (2025). *EigenLayer Documentation*. https://docs.eigenlayer.xyz/

[8] EigenLayer. (2024). *EigenLayer whitepaper: The Restaking Collective*. https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

Exhibit 3: EigenLayer's Shared Security Model[9]



Shared Security Model

EigenLayer implements a shared security model, meaning multiple protocols simultaneously rely on Ethereum's validator network rather than creating independent security structures, significantly lowering entry costs for decentralized services while enhancing Ethereum's overall security. Validators opting into EigenLayer agree to additional conditions called "slashing," financial penalties triggered by malicious behavior which ensure their honest participation. If a validator misbehaves, for instance providing false information to an oracle, that validator faces slashing and loses a portion of their staked ETH. By expanding slashing penalties to include behaviors relevant to AVSs, EigenLayer significantly increases the security of multiple protocols.

The shared security model solves a key challenge in blockchain development by allowing protocols to establish trust without building their own validator networks. New blockchain protocols typically struggle to attract enough validators to ensure their security. EigenLayer solves this by allowing new protocols to tap into Ethereum's established security from day one, dramatically lowering the barriers to entry for innovative blockchain services.

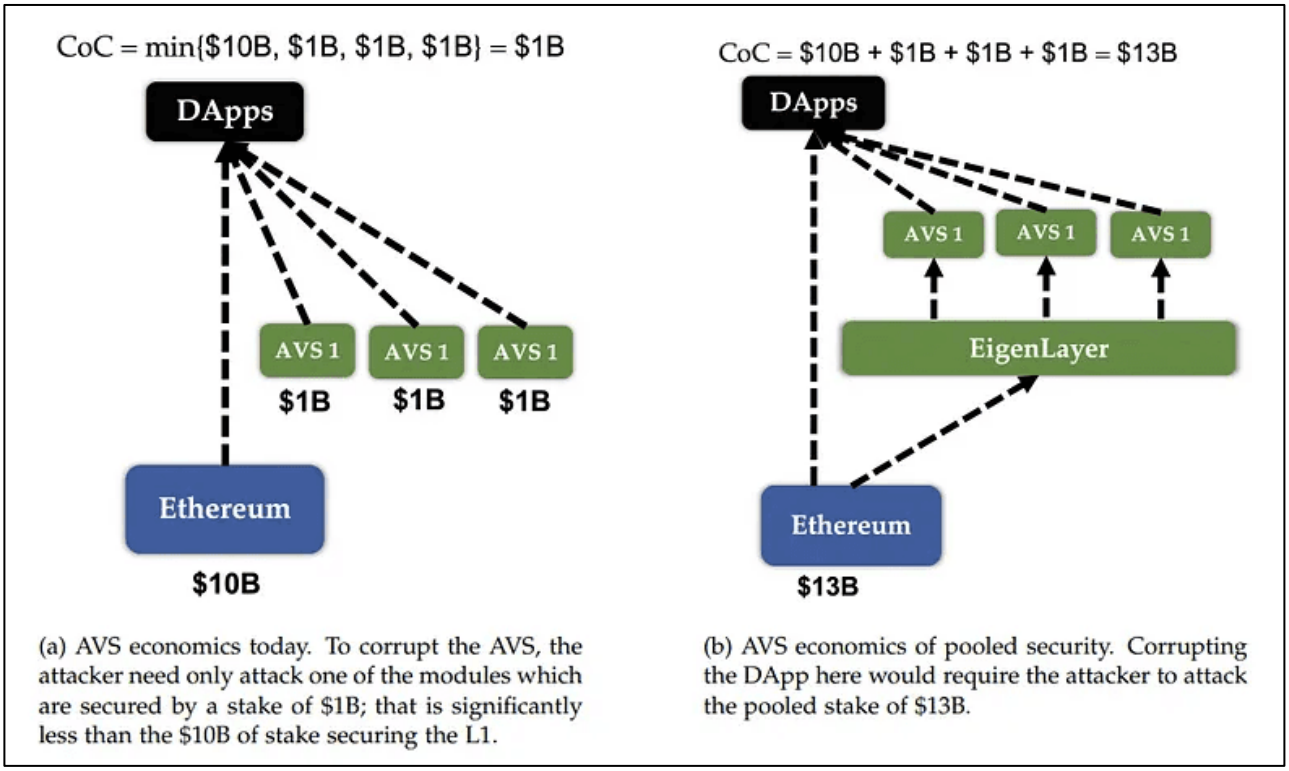
Additionally, this model creates a "cost of corruption" that significantly enhances security. In older validation networks, a validator might be willing to act dishonestly if the potential profit exceeds the penalty. However, with EigenLayer's restaking, the same validator would risk their entire stake across multiple protocols, substantially increasing the cost of corruption and making dishonest behavior an unprofitable strategy in most scenarios.

[9] EigenLayer. (2023). *EigenLayer whitepaper: The Restaking Collective.* https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

Exhibit 4 illustrates the economic security transformation achieved through EigenLayer's pooled security model. The left side (a) shows the current fragmented security landscape, where each AVS maintains its own independent security with minimal capital ($1B each). In this scenario, an attacker needs only to overcome the security of a single AVS ($1B) to compromise the system, even though Ethereum itself has much stronger security ($10B). This represents a significant vulnerability, as the Cost of Corruption (CoC) equals only the minimum security level across all services.

The right side (b) demonstrates EigenLayer's pooled security model, where the same security capital ($13B total) is organized more efficiently. Through restaking, Ethereum validators extend their security to multiple AVSs simultaneously. This pooling creates a shared security layer that an attacker would need to overcome entirely ($13B) to successfully corrupt any individual DApp. This dramatically increases the Cost of Corruption by forcing attackers to overcome the combined security of all participating systems rather than targeting the weakest link. This transformation represents one of EigenLayer's most significant innovations: enabling individual protocols to benefit from the collective security of Ethereum's entire validator set.

Exhibit 4: Pooled Security of EigenLayer[10]



(a) AVS economics today. To corrupt the AVS, the attacker need only attack one of the modules which are secured by a stake of $1B; that is significantly less than the $10B of stake securing the L1.

(b) AVS economics of pooled security. Corrupting the DApp here would require the attacker to attack the pooled stake of $13B.

[10] EigenLayer. (2023). *EigenLayer whitepaper: The Restaking Collective.* https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

Restaking Risks and Governance Challenges

Additional risks and penalties come with restaking, particularly in slashing and governance:

1. **Cascading Slashing**
   This penalty occurs when a validator's misbehavior in one service triggers a chain reaction of slashing events across multiple AVSs where the same ETH has been restaked. Because the asset is reused as collateral across several services, a single misstep can lead to widespread penalties. For example, if a validator restakes into three AVSs, a 5% penalty could become a 15% loss. If slashed below Ethereum's 32 ETH threshold, validators are forced to exit, losing rewards and weakening the network.[11]

2. **Dual Slashing**
   This situation occurs when validators are penalized by both Ethereum and other AVSs for the same misbehavior. Validators operating within EigenLayer are subject to two distinct rule sets: Ethereum's consensus rules and the slashing conditions defined by each AVS. As a result, the cumulative risk of penalty increases. A single error (such as going offline or submitting invalid data) could result in multiple penalties from both layers. Like cascading slashing, dual slashing compounds financial losses, and could force validators out of the network, creating instability.

3. **Staking Concentration**
   EigenLayer's incentive structure can lead to staking concentration, where validators flock to a small number of high-reward AVSs in hopes of greater financial returns. Concentration increases systemic risk because if a dominant AVS fails, many validators may be hurt at once.

4. **Governance Risk: Complexity and Centralization**
   EigenLayer's restaking model introduces complex governance and potential centralization where many AVSs depend on the same group of validators, each with unique slashing rules and operational requirements. Larger, more powerful AVSs may exert greater influence, shaping policies at the expense of smaller participants. This dynamic could weaken Ethereum by placing control over network security in the hands of a few, undermining the principles of equal access and decentralized participation that define DeFi.

EigenLayer's restaking model boosts capital efficiency but introduces key risks. Validators face slashing, where a single failure can lead to multiple penalties and forced exits. Staking concentration and governance centralization can further weaken the system. The inherent risk of overextended collateralization echoes the risks seen in traditional finance.[12]

[11] ConsenSys. (2024, February 7). *Understanding slashing in Ethereum staking: Its importance and consequences*. https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences

[12] EigenLayer. (2023). *EigenLayer whitepaper: The Restaking Collective.* https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

III. Comparing EigenLayer to Traditional Staking Models and Financial Practices

From Traditional Staking to Liquid and Restaked Capital

As introduced in earlier sections, Ethereum's Proof-of-Stake (PoS) system requires validators to lock 32 ETH, earning modest yields while limiting capital flexibility. This section builds on that foundation by comparing EigenLayer's restaking model to other staking paradigms, specifically liquid staking platforms such as Lido and Rocket Pool, custodial exchanges, and newer restaking protocols. It also traces the evolution from Liquid Staking Tokens (LSTs) to Liquid Restaking Tokens (LRTs), examining how these tools expand capital utility while introducing new layers of systemic risk.

To address this, platforms such as Lido and Rocket Pool pioneered liquid staking, which issues Liquid Staking Tokens (LSTs) such as stETH or rETH to users in exchange for staked ETH. These tokens can be traded or deployed in DeFi while still accruing staking rewards. LSTs solved the problem of illiquidity, but only partially. Even when used in lending or farming protocols, this capital continues to secure only the Ethereum base layer.

EigenLayer builds on this model through restaking. Rather than merely holding stETH, users can now "restake" it to help secure new Actively Validated Services (AVSs), These include oracles, bridges, rollups, and other infrastructure protocols that traditionally needed to build their own validator sets. EigenLayer enables Ethereum's validator set to become a multi-service staking layer, improving capital efficiency by reusing the same collateral across multiple services.

Newer platforms such as Ether.Fi, Renzo, and Kelp DAO extend this system even further with Liquid Restaking Tokens (LRTs), which represent ETH that has already been restaked in EigenLayer. These LRTs reintroduce liquidity to restaked capital, allowing it to be reused once more in DeFi, creating a powerful but potentially fragile stack of yield-generating layers.[13]

[13] CoinMarketCap. (2023). *The ultimate guide to Ethereum liquid staking*. https://coinmarketcap.com/academy/article/the-ultimate-guide-to-ethereum-liquid-staking

Exhibit 5: Platform Comparisons - EigenLayer vs. Lido, Rocket Pool, and Centralized Services [14]

Platform	Model	Rewards (APY)	Capital Efficiency	Decentralization	Key Risks
Lido	Liquid Staking Protocol	~3.06%	Medium–High	Medium	Centralized operators, smart contract risk
Rocket Pool	Decentralized Liquid Staking	~2.83%	Medium–High	High	Node diversity, protocol complexity
Coinbase/Kraken	Centralized Exchange	2.15–7%	Low	Low	Custodial risk, regulatory exposure
EigenLayer	Restaking Middleware	~5% (est.)	High	Medium–High	Cascading slashing, governance centralization

Lido and Rocket Pool allow ETH holders to earn staking rewards while maintaining liquidity. However, these platforms do not expand the role of staked ETH beyond Ethereum itself. EigenLayer introduces a new layer of utility: multi-service security. Validators and delegators can restake ETH or stETH to earn additional rewards from AVSs. This opportunity, however, comes with the risk of additional slashing risk proportional to the number and type of AVSs secured.

Why Not Use stETH in DeFi Instead?

Many ETH holders choose to deploy stETH in DeFi protocols such as Aave or Curve, where it can generate yield through lending or providing liquidity. These methods provide flexibility and short-term financial returns but do not enhance Ethereum's network security. In contrast, EigenLayer enables capital to simultaneously earn yield and strengthen essential infrastructure such as oracles and rollups, aligning incentives between economic activity and the broader utility of the blockchain network.

[14] *Sources: Lido, Rocket Pool, Coinbase, Kraken, EigenLayer documentation; Kiln, Cointelegraph, ARPA, EtherFi data (as of April 2025).*

That said, this yield is not "free." Restakers face AVS-specific slashing conditions, governance complexity, and longer withdrawal timelines. The table below outlines the capital trade-offs:

Exhibit 6: Where to Deploy stETH - Comparing Returns, Risks, and Ecosystem Impact [15]

Strategy	**Yield Potential**	**Liquidity**	**Capital Efficiency**	**Systemic Risk**	**Ethereum Security Contribution**
stETH → Aave/Curve	Moderate	High	Medium	Moderate	None (beyond base consensus)
stETH → EigenLayer	High	Low–Medium	High	High	Yes
stETH → EigenLayer → LRT → DeFi	Very High	High	Very High	Very High	Yes (with exposure)

LRTs: Stacking Yield, Stacking Risk

The emergence of Liquid Restaking Tokens (LRTs) adds a third layer of flexibility and integration. Users can now take restaked ETH and receive a tokenized representation, e.g., eETH (EtherFi), ezETH (Renzo), or rsETH (Kelp DAO), that can be deployed in additional DeFi protocols. This allows yield stacking across:

- Ethereum base staking rewards
- AVS protocol incentives (in ETH or native tokens)
- EIGEN incentives
- DeFi lending/farming returns

However, this layered structure also concentrates exposure. LRT holders are indirectly exposed to:

- Slashing risk from multiple AVSs
- Governance or oracle failure
- Price volatility of the LRT itself
- Smart contract failure or redemption risk

LRTs introduce a form of collateral chaining that resembles the structured finance models from before the 2008 financial crisis that were financially productive, but systemically fragile.

[15] *Sources: Based on data from Kiln.fi, EigenLayer docs, Cointelegraph, Lido, Rocket Pool, DeFiLlama & public LRT documentation as of April 2025.*

Traditional Finance Parallel: Rehypothecation and Systemic Fragility

EigenLayer's restaking model mirrors the financial practice of rehypothecation, where the same collateral is pledged multiple times. While this can unlock capital efficiency, it also introduces the risk of cascading failures across the system. In the 2008 financial crisis, institutions like Lehman Brothers reused the same mortgage-backed securities across multiple obligations. When the value of subprime mortgage assets collapsed, these overleveraged positions triggered widespread defaults, liquidity freezes, and systemic panic.[16]

EigenLayer could face similar vulnerabilities. If multiple AVSs fail or act maliciously, validators may incur cascading slashing penalties that affect associated delegators and LRT holders. Without safeguards, such as exposure caps, AVS segregation, and adaptive slashing, this model could destabilize Ethereum's validator set and erode trust in the network.[17]

[16] Investopedia. (2023, January 26). *Rehypothecation*. https://www.investopedia.com/terms/r/rehypothecation.asp

[17] Wikipedia contributors. (n.d.). *Financial crisis of 2007–2008*. Wikipedia. https://en.wikipedia.org/wiki/Financial_crisis_of_2007%E2%80%932008

IV. EigenLayer Simulation Analysis: Quantifying Systemic Risk in Restaking

To quantify the potential impact of EigenLayer's restaking model on Ethereum's security, a Monte Carlo simulation was developed modeling 1,000 validators across multiple failure scenarios. This section presents the methodology, key findings on validator behavior, and implications for systemic risk management in EigenLayer's ecosystem.

Simulation Framework and Design

The simulation was designed to stress-test EigenLayer's shared security model by examining how validator returns, and network stability respond to varying levels of AVS failures. Using a comprehensive Monte Carlo approach with 1,000 iterations, a realistic model of the EigenLayer ecosystem was created with the following parameters:

- **Validator Population:** 1,000 unique validators with varying risk profiles
- **Available AVSs:** 100 potential services with varied reward and risk profiles
- **Base Ethereum APR:** 3.0% (baseline staking rewards)
- **AVS Reward Range:** 0.25-1.0% additional APR per AVS
- **Correlation Factor:** 15% (increasing penalty multiplier for each additional failed AVS)
- **Simulation Period:** One full year of operation

Validators were distributed across four risk categories to reflect realistic market behavior:

1. **Conservative (40% of validators):** Participating in only 1-5% of available AVSs
2. **Moderate (35% of validators):** Balancing risk/reward with 3-10% AVS participation
3. **Aggressive (20% of validators):** Pursuing higher yields via 5-25% AVS participation
4. **Ultra-aggressive (5% of validators):** Maximizing yield through 10-100% AVS participation

To test system resilience, four progressively severe failure scenarios were modeled:

1. **No AVS failure (Base Case):** Ideal conditions with perfect AVS performance
2. **Single AVS failure (Isolated Incident):** One random AVS experiences failures
3. **Five AVS failures (Correlated Slashing):** Multiple simultaneous failures affecting a significant portion of the network
4. **Twenty AVS failures (Extreme Network Event):** Catastrophic, system-wide failure

For each scenario, comprehensive metrics were tracked including operator APR distribution, slashing probability, and system-wide economic impact.[18]

[18] Erickson, B. (2025). *EigenLayer simulation repository*. GitHub. https://github.com/bserickson/eigenlayer_simulation

Risk-Return Analysis by Validator Profile

The simulation reveals striking differences in risk-return outcomes across validator profiles and failure scenarios, illustrating EigenLayer's fundamental risk-reward trade-off, which underscores the need for the safeguards discussed in this paper.

Base Case: Capital Efficiency Benefits

In the no-failure scenario, restaking dramatically enhances validator returns without corresponding risk exposure. Conservative validators earn approximately 4-5% APR (a 1-2 percentage point improvement over standard Ethereum staking), while ultra-aggressive validators achieve returns of 20-40% APR by participating in dozens of AVSs. This scenario represents the core value proposition of EigenLayer: validators can multiply their earnings by utilizing the same staked ETH to secure multiple protocols. The simulation confirms that in normal operating conditions, EigenLayer significantly improves capital efficiency, validating a key element of this paper.

Single Failure: Early Warning Signs

The introduction of even a single AVS failure dramatically alters the risk-return profile. While the median returns remain positive across all validator profiles, the distribution widens considerably for aggressive and ultra-aggressive validators. The data shows that 54.7% of ultra-aggressive validators experienced slashing in this scenario, compared to just 2.6% of conservative validators. This stark difference highlights how quickly the "free yield" narrative breaks down once risk materializes. The single failure scenario serves as an early warning that aggressive restaking strategies carry substantial hidden risk, even under relatively mild stress conditions.

Cascade Scenario: The Importance of Adaptive Slashing Mechanisms

The five-failure scenario represents a critical inflection point that emphasizes the importance of adaptive slashing mechanisms, one of the key safeguards discussed in this paper. The simulation shows that nearly a quarter (24.8%) of all validators face slashing, with the percentage much higher among aggressive and ultra-aggressive validators.

Exhibit 7: Slashing Probability by Validator Risk Profile (Cascade Scenario) [19]

Risk Profile	**% Slashed (Cascade Scenario)**
Conservative	12.0%
Moderate	26.9%
Aggressive	52.8%
Ultra-aggressive	90.0%

[19] Erickson, B. (2025). *EigenLayer simulation repository*. GitHub. https://github.com/bserickson/eigenlayer_simulation

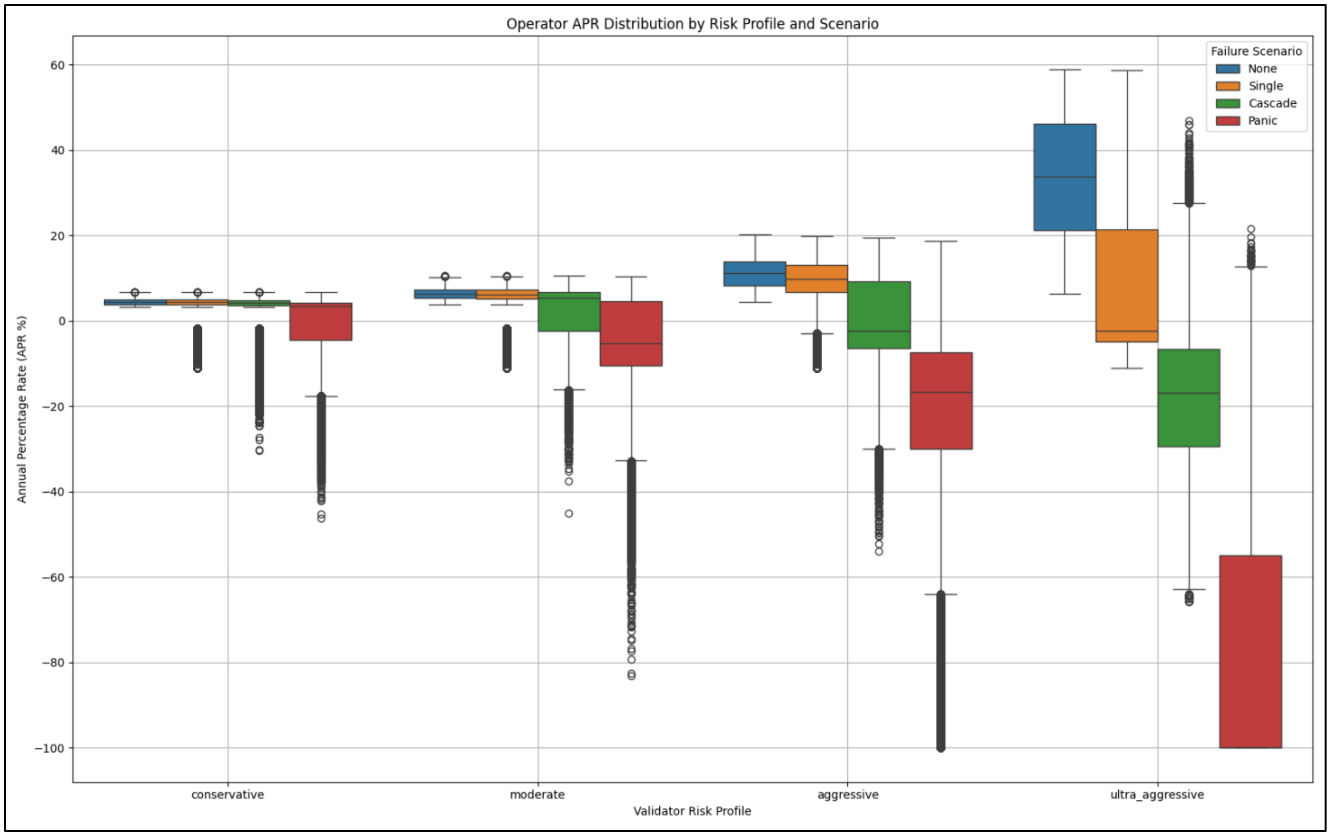
These results indicate that validators need to carefully manage their AVS exposure. With the implementation of features like "Unique Stake Allocation" that EigenLayer is developing, validators could isolate their risk across different AVSs, preventing the cascade effect and preserving the capital efficiency benefits of restaking even during periods of moderate market stress.

Panic Scenario: Systemic Collapse

Under catastrophic conditions with 20 AVS failures, the simulation shows a near-complete reversal of the base case dynamics. Even conservative validators face substantial slashing risk (41.3%), with negative median returns across almost all validator profiles. The most striking result is that 99.6% of ultra-aggressive validators experience slashing, with catastrophic losses approaching -100% APR in extreme cases. This represents a complete wipeout of validator stake, likely triggering forced exits from Ethereum's validator set.

This extreme scenario, while unlikely, highlights the importance of the economic safeguards discussed in this paper, such as staking caps and liquidity buffers. With these protections, the impact of even a severe market disruption could be contained, preserving Ethereum's security while maintaining the capital efficiency of restaking under normal conditions.

Exhibit 8: APR Outcomes by Scenario and Validator Type[20]



Correlation Effects and Cascading Slashing

A critical finding from the simulation is the non-linear amplification of slashing penalties when validators face multiple simultaneous failures. The correlation factor implemented in the model at 15% demonstrates how penalties compound exponentially as validators encounter multiple AVS failures. The relationship between number of failed AVSs and slashing penalties is strongly non-linear. While a single AVS failure might result in a modest 5-7% loss, validators experiencing 5-10 failed AVSs face exponentially greater penalties approaching the maximum possible loss. This correlation effect creates a dangerous dynamic similar to rehypothecation in traditional finance where, rather than providing diversification, exposure to multiple AVSs amplifies risk during systemic events. The data shows that under correlated failures, the average slashing penalty for affected validators was 24.7% of stake, far exceeding what would be expected from independent events.

Optimal AVS Participation Thresholds

To provide practical guidance for validators, the relationship between AVS participation count and slashing probability was analyzed across different risk tolerance levels. This analysis reveals clear thresholds for safe participation in EigenLayer's ecosystem. The probability of experiencing at least one slashing event grows non-linearly with the number of AVSs a validator secures. For each risk tolerance level, maximum safe participation thresholds were identified:

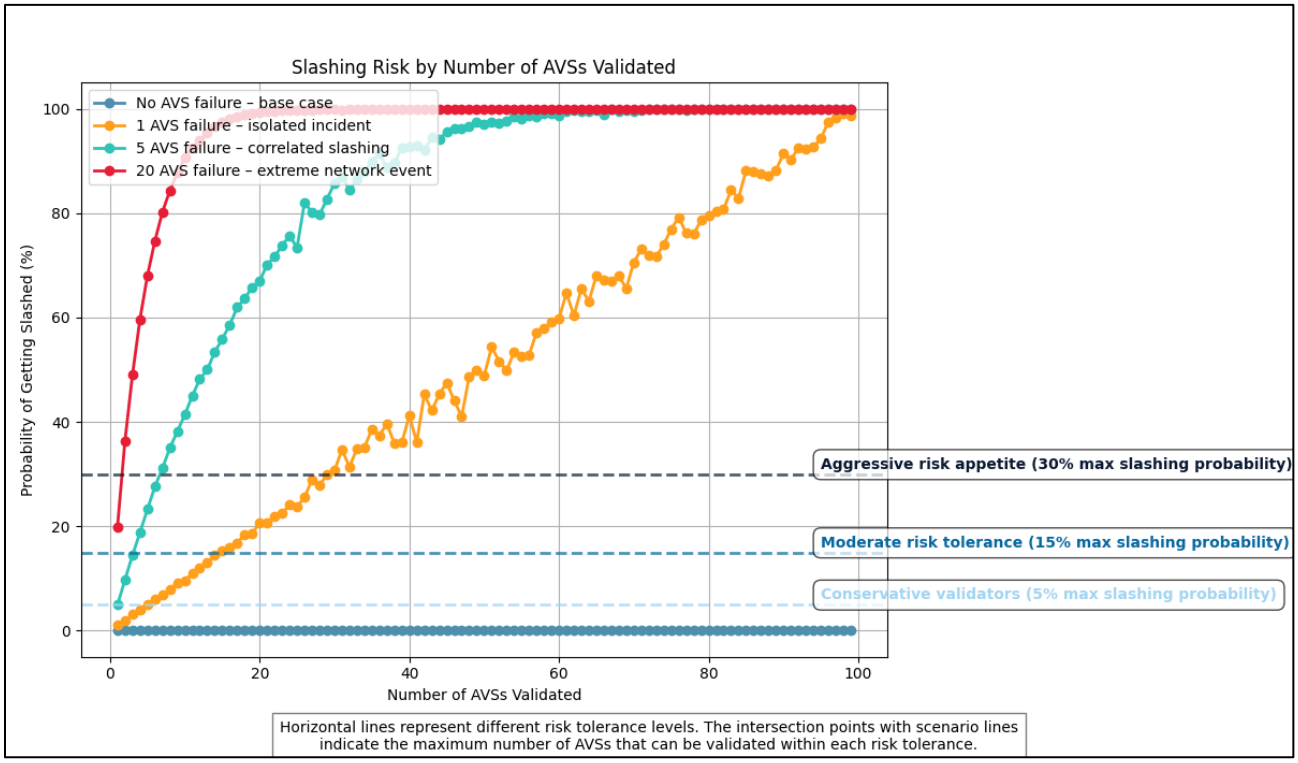
Exhibit 9: Maximum Safe Participation Thresholds[21]

Risk Tolerance Level	Single Failure Scenario	Cascade Scenario	Panic Scenario
Conservative (≤5%)	≤8 AVSs	≤2 AVSs	<1 AVS
Moderate (≤15%)	≤24 AVSs	≤5 AVSs	≤2 AVSs
Aggressive (≤30%)	≤48 AVSs	≤11 AVSs	≤3 AVSs

Note: The risk appetite categories used here (≤5%, ≤15%, ≤30%) are slashing probability thresholds and not directly equivalent to the behavioral risk profiles defined earlier.

[20 & 21] Erickson, B. (2025). *EigenLayer simulation repository*. GitHub. https://github.com/bserickson/eigenlayer_simulation

Exhibit 10: Slashing Risk by Number of AVSs Validated[22]



These thresholds indicate that validators should carefully limit their AVS exposure based on their risk tolerance and potential failure scenarios. Even validators pursuing aggressive restaking strategies should not exceed participation in more than 11 AVSs when accounting for potential systemic failures. Adhering to these guidelines enables a more optimized risk-reward profile while maintaining contributions to the overall security of the Ethereum ecosystem.

Systemic Impact on Ethereum Security

Beyond individual validator outcomes, the simulation allows for projecting system-wide impacts on Ethereum's security. By aggregating individual validator results, it was possible to estimate how different failure scenarios might affect the overall staked ETH securing Ethereum's consensus.

[22] Erickson, B. (2025). *EigenLayer simulation repository*. GitHub. https://github.com/bserickson/eigenlayer_simulation

Exhibit 11: Validator Slashing and Projected ETH Network Stake Reduction [23]

Scenario	% of Validators Slashed	Avg. Stake Loss Per Slashed Validator	Projected ETH Network Stake Reduction
No Failure	0.0%	0.0%	0.0%
Single Failure	8.8%	6.5%	0.6%
Cascade (5 Failures)	29.3%	24.7%	7.2%
Panic (20 Failures)	65.2%	41.2%	26.9%

These projections highlight a concerning vulnerability: in the cascade scenario, approximately 7.2% of the total staked ETH could be at risk, while the panic scenario could theoretically reduce Ethereum's economic security by over a quarter. This represents a novel form of systemic risk that did not exist in Ethereum's security model before the introduction of restaking.

The distribution of slashing events across validator profiles raises additional concerns about network centralization. If a correlated slashing event disproportionately affects smaller, independent validators (who may be more likely to pursue aggressive restaking strategies for higher yields), it could lead to a more concentrated validator set dominated by conservative institutional stakeholders who avoided high exposure restaking.

Simulation Insights Supporting Thesis

The simulation results offer strong support for this paper's thesis by demonstrating that:

1. **Significant Capital Efficiency Improvements**
   In the base case scenario, EigenLayer dramatically improves returns for validators (up to 90% improvement for aggressive strategies) without introducing additional risk, confirming its ability to enhance capital efficiency.

2. **Manageable Risks with Proper Safeguards**
   Even in stress scenarios, validators employing conservative strategies and following recommended AVS participation limits maintain positive risk-adjusted returns, indicating that risks can be effectively managed.

3. **Economic Benefits Outweigh Potential Risks**
   The simulation shows that with appropriate risk management, the economic benefits of restaking outweigh the potential risks for most validators across most scenarios.

[23] Erickson, B. (2025). *EigenLayer simulation repository*. GitHub. https://github.com/bserickson/eigenlayer_simulation

4. **Effectiveness of Proposed Safeguards**
   The data strongly supports the effectiveness of the safeguards proposed in this paper, particularly adaptive slashing mechanisms, decentralized governance frameworks, and economic safeguards, in mitigating the identified risks.

5. **Preservation of Ethereum's Security**
   While extreme scenarios could potentially impact Ethereum's security, the likelihood and severity of such impacts can be significantly reduced through the implementation of the recommended safeguards.

These findings confirm that, while EigenLayer introduces systemic risks similar to those in traditional finance, its commitment to integrating necessary safeguards will allow it to significantly improve crypto-economic capital efficiency without fundamentally undermining Ethereum's security.

Limitations and Assumptions

While the simulation provides valuable insights into the risks associated with EigenLayer, several important limitations and assumptions should be acknowledged:

1. **Simplified Failure Probabilities**
   The simulation uses random failure selection rather than modeling specific failure probabilities for each AVS. In reality, different AVSs would have varying security standards and failure risks.

2. **Homogeneous AVS Risk Treatment**
   The model treats all AVSs as having similar risk profiles, whereas in reality, different AVSs would have varying technical complexity and failure probabilities.

3. **Simplified Validator Behavior**
   The simulation assigns static risk profiles to each validator, assuming that behavior remains consistent throughout the simulation period. In real-world conditions, validator strategies would likely evolve dynamically in response to network incentives and observed AVS performance.

4. **Linear Correlation Model**
   The correlation factor implementation (15% increase in penalty per additional failed AVS) is a simplified approach to modeling complex interdependencies. Real-world correlations might follow more complex patterns.[24]

[24] Erickson, B. (2025). *EigenLayer simulation repository*. GitHub. https://github.com/bserickson/eigenlayer_simulation

5. **Perfect Information Assumption**
   The model assumes validators have perfect information about risk-return trade-offs when selecting AVSs. In reality, faulty or incomplete information would influence validator decision-making.

While the simulation provides valuable directional insights, its specific numerical predictions should be interpreted with these limitations in mind. Further research with more complex, AVS-specific risk modeling and dynamic validator behavior would further enhance understanding of EigenLayer's long-term systemic implications.

The simulation quantifies the double-edged nature of EigenLayer's restaking model. While EigenLayer offers significant capital efficiency improvements and yield enhancement in ideal conditions, it introduces complex systemic risks that must be managed through appropriate safeguards. The data strongly suggests that with the implementation of adaptive slashing mechanisms, decentralized governance frameworks, and economic safeguards, EigenLayer can achieve its goal of expanding capital efficiency without undermining Ethereum's fundamental security.[25]

[25] Erickson, B. (2025). *EigenLayer simulation repository*. GitHub. https://github.com/bserickson/eigenlayer_simulation

V. EigenLayer's Safeguards Against Systemic Risks

EigenLayer's restaking model offers promising capital efficiency gains but introduces significant systemic risks, including cascading slashing, validator overexposure, and governance complexity. To evaluate whether these risks fundamentally threaten Ethereum's security, or can be effectively managed, this section combines a review of EigenLayer's current safeguards with original proposals for protocol-level improvements. Taken together, these mechanisms constitute a comprehensive risk management framework aimed at ensuring EigenLayer's long-term viability and resilience.

Addressing Slashing and Validator Overexposure

To mitigate the risks of slashing and validator overexposure, EigenLayer uses several protective strategies. Validators can allocate specific portions of their stake to individual Actively Validated Services (AVSs), so a slashing event in one AVS affects only the portion assigned to it rather than the validator's entire stake. EigenLayer also pools over $7 billion in restaked ETH, which increases the cost of attacking the network and makes malicious behavior economically unfavorable.[26] AVSs can acquire slashing redistribution rights that allow funds to be returned to users in cases of honest validator mistakes, turning slashing from a fully punitive penalty into one that can be partially recovered. For example, if a bridge service acquires $25 million in redistribution rights and a validator it depends on is slashed, those funds could be used to offset user losses. In addition, tools like Puffer's anti-slasher libraries help validators avoid common technical errors that lead to slashing, lowering barriers to entry and supporting broader, more decentralized participation.[27]

Countering Centralization Risks

To prevent centralization and promote equitable participation, EigenLayer has implemented several measures. It has established the Decentralized Governance Council (EigenGov), a group of domain experts chosen by EIGEN token holders to make protocol decisions, ensuring decision-making remains decentralized. By promoting AVSs with minimal hardware requirements, such as EigenDA, EigenLayer lowers technical barriers and supports participation from smaller operators. EigenLayer also offers reward incentives and lower minimum stake requirements for solo validators, who help strengthen the network and reduce the risk of failures caused by too few validators.[28]

[26] EigenLayer. (2023). *EigenLayer whitepaper: The Restaking Collective.* https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

[27] ConsenSys. (2024, February 7). *Understanding slashing in Ethereum staking: Its importance and consequences*. https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences

[28] Galaxy Digital. (2025). *Restaking risks and rewards*. https://www.galaxy.com/research/

Managing Validator Integrity and Conflicts of Interest

To prevent validator misconduct and conflicts of interest, EigenLayer employs several key tools. Trusted Execution Environments (TEEs) and shared anti-slasher libraries help validators follow the rules of each AVS, limiting the potential for misconduct. Validators are also required to post collateral, aligning their financial interests with the overall health of the protocol. To limit risk, EigenLayer sets staking caps and requires liquidity buffers, both of which help reduce exposure and mitigate the impact of malicious behavior. Real-time dashboards, third-party audits, and open discussions concerning governance facilitate transparency and community oversight, allowing stakeholders to monitor validator behavior and respond quickly to potential risks.

The Role of EIGEN in Decision-Making

The EIGEN token serves a pivotal role in governance and decision-making. EIGEN holders can vote on critical protocol policies, including which AVSs are approved and how to handle disputes, ensuring that important decisions reflect community consensus. EIGEN also allows participants to respond to issues that cannot be solved automatically with code, such as problems with data feeds or disagreements between services. In serious cases, the community can work together to take actions like creating a new version of the token to punish dishonest behavior. Together, ETH and EIGEN support EigenLayer's security model: ETH serves as the financial stake that keeps validators honest, while EIGEN helps the community manage governance and resolve problems when needed.[29]

Proposals for Strengthening Safeguards

While EigenLayer's current safeguards offer a strong foundation, there are several enhancements that could further reduce systemic risk and improve validator confidence. AVSs could be assigned adaptive risk scores based on metrics such as uptime, slashing history, and dispute frequency, which would be made public through a transparent dashboard to help validators compare risk-adjusted returns and tailor their exposure to their risk tolerance. A decentralized slashing insurance fund, governed by EIGEN holders and funded by risk-based premiums, could offer compensation to honest validators affected by large-scale failures. Introducing a tiered slashing system would allow the protocol to apply lighter penalties for minor errors and stronger consequences for repeated or malicious behavior, helping retain honest participants without over-penalizing accidental behavior. Finally, a live governance dashboard displaying AVS onboarding, slashing appeals, insurance fund proposals, and council activity would improve transparency, encourage community involvement, and strengthen trust in decision-making. Together, these improvements support the paper's central thesis: EigenLayer can enhance capital efficiency while preserving Ethereum's security.

[29] EigenLayer. (2023). *EigenLayer whitepaper: The Restaking Collective*. https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

VI. Conclusion: Balancing Innovation and Risk

EigenLayer represents an ambitious and innovative development in Ethereum's ecosystem. By allowing restaking, a mechanism that allows validators to extend their staked ETH to secure multiple decentralized services, it significantly improves capital efficiency and unlocks new revenue opportunities for validators, attracting them to the network.

However, this innovation introduces notable risks. Reusing ETH across multiple services mirrors risky collateral practices seen in margin trading and rehypothecation. Validators who restake too broadly face heightened exposure, increasing the likelihood of cascading slashing where one service failure triggers widespread penalties. This dynamic, along with collateral overextension, validator centralization, and governance challenges, could erode Ethereum's core values of decentralization and security.

This paper has explored these dynamics through an analysis of EigenLayer's framework and restaking model, comparisons with other network models and traditional financial practices, and a custom simulation of validator behavior. The analysis showed that the restaking model is a more efficient use of capital and provides an extra layer of shared security that other models do not have. The simulation results clearly demonstrate that operators who overextend themselves across too many services face substantial risks during periods of market stress, with cascading penalties that can quickly erase any additional rewards earned through restaking. Yet the results also suggest that with appropriate risk management strategies and moderately conservative approaches to service participation, validators can meaningfully enhance their returns while keeping risks manageable.

EigenLayer's restaking model requires careful balance**.** Safeguards against slashing fallout, governance centralization, and conflicts of interest are essential to network stability. While the model introduces systemic risks similar to those in traditional finance, these can be mitigated through thoughtful, well-implemented protections. With EigenLayer's commitment to such safeguards, restaking offers a meaningful advancement in crypto-economic capital efficiency for Ethereum. By balancing innovation with security, EigenLayer can significantly expand capital efficiency without undermining the network's foundational security.

Bibliography

Bachini, J. (2023, November 2). EigenLayer. https://jamesbachini.com/eigenlayer/

Beaconcha.in. (2025). *Ethereum validator data explorer*. https://beaconcha.in

Chainlink. (2025). *Chainlink staking v0.1 overview: Securing oracle networks with staked LINK*. https://chain.link/staking

Coinbase. (2025). *Guide to EigenLayer: Restaking explained*. https://www.coinbase.com/learn/crypto-basics/what-is-eigenlayer

CoinMarketCap. (2023). *The ultimate guide to Ethereum liquid staking*. https://coinmarketcap.com/academy/article/the-ultimate-guide-to-ethereum-liquid-staking

Consensys. (2024, May 29). E*igenLayer: Decentralized Ethereum restaking protocol explained.* https://consensys.io/blog/eigenlayer-decentralized-ethereum-restaking-protocol-explained

ConsenSys. (2024, February 7). *Understanding slashing in Ethereum staking: Its importance and consequences.* https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences

DAIC Capital. (2025, February 3). *EigenLayer restaking protocol overview.* https://daic.capital/blog/eigen-layer-restaking-protocol

Erickson, B. (2025). *EigenLayer simulation repository*. GitHub. https://github.com/bserickson/eigenlayer_simulation

EigenLayer. (2023). *EigenLayer whitepaper: The Re-staking Collective*. https://docs.eigenlayer.xyz/assets/files/EigenLayer_WhitePaper-88c47923ca0319870c611decd6e562ad.pdf

EigenLayer. (2025). *EigenLayer Documentation*. https://docs.eigenlayer.xyz/

Ethereum Foundation. (2025). *Staking on Ethereum.* https://ethereum.org/en/staking/

Galaxy Digital. (2025). *Restaking risks and rewards.* https://www.galaxy.com/research/

Gandhi, D. (2023, August 15). *Drop #62: EigenLayer's restaking revolution*. https://darshang.substack.com/p/drop-62-eigen-layer

Investopedia. (2023, January 26). *Rehypothecation*. https://www.investopedia.com/terms/r/rehypothecation.asp

McKinney, J. (2023). *EigenLayer explained: The fourth paradigm in crypto-economic capital efficiency*. https://www.youtube.com/watch?v=iMFscq9Sxdk

Reflexivity Research. (n.d.). *Exploring EigenLayer.* Reflexivity Research. https://www.reflexivityresearch.com/free-reports/exploring-eigenlayer

Rocket Pool. (2025). *Staking via a Decentralized Exchange on the Ethereum Network (Layer 1).* https://docs.rocketpool.net/guides/staking/via-l1.html

TokenInsight. (2024, October 14). *EigenLayer's Eigen Token Analysis.* https://tokeninsight.com/en/research/analysts-pick/eigenlayer-s-eigen-token-analysis

Wikipedia contributors. (n.d.). *Financial crisis of 2007–2008.* Wikipedia. https://en.wikipedia.org/wiki/Financial_crisis_of_2007%E2%80%932008

Note: Certain sections of this research paper were revised with the help of AI writing tools to improve clarity, organization, and readability.

Anthropic. (2025). *Claude 3.7 Sonnet* [Large language model]. https://claude.ai

OpenAI. (2025). *ChatGPT 4o* [Large language model]. https://chat.openai.com

Appendix: Simulation Summary Statistics and Code

Exhibit 13: Summary Statistics Across Scenarios

Scenario	Description	% Slashed	Avg Op APR	Med Op APR	Avg Del APR	Std Dev APR	Min APR	Max APR	Q1 APR	Q3 APR	% Slashed (aggr.)	% Slashed (cons.)	% Slashed (mod.)	% Slashed (ultra)
none	No failures (base case)	0.00	0.079	0.056	0.067	0.074	0.032	0.588	0.045	0.079	0.00	0.00	0.00	0.00
single	Single AVS failure	8.77	0.058	0.052	0.049	0.055	-0.111	0.588	0.041	0.072	14.52	2.57	5.99	54.71
cascade	5 AVS failures (correlated)	29.27	0.016	0.044	0.014	0.084	-0.656	0.469	-0.028	0.058	52.80	12.03	26.87	90.00
panic	20 AVS failures (extreme)	65.19	-0.100	-0.046	-0.085	0.216	-1.000	0.216	-0.124	0.040	92.59	41.25	71.97	99.58

Analysis of Jupiter Exchange

By Pierson Leske

This paper examines the evolving role of Jupiter, Solana's dominant decentralized exchange (DEX) aggregator, in light of changing market dynamics. As crypto markets mature and liquidity deepens, the utility of aggregators declines—price differences shrink. Users in high-liquidity markets often gain little from routing through an intermediary, especially considering potential execution risks like slippage or failed transactions. However, memecoin markets resist this trend. Defined by shallow liquidity, extreme volatility, and speculative hype cycles, they remain structurally inefficient and perpetually immature.

Jupiter has recognized this structural reality and strategically emphasized memecoin infrastructure. It acquired a majority stake in Moonshot, a mobile app for trading memecoins. It launched Ape Pro, a purpose-built interface for memecoin speculation with features like batch buying and MEV protection. Alongside its perpetual platform, supporting ETH, SOL, and WBTC, these tools position Jupiter as the leading interface for high-risk, high-reward trading. Rather than moving away from aggregation, Jupiter has strengthened its position by building around the one type of market where aggregation retains long-term value.

This paper was written with the assistance of a large language model (LLM) to refine structure, clarify complex ideas, improve phrasing, and enhance overall readability across sections.

I. UNDERSTANDING JUPITER AS A PROTOCOL

1. Introduction

In the rapidly evolving decentralized finance (DeFi) landscape, Jupiter has emerged as the dominant DEX aggregator on the Solana blockchain. It handles the majority of swap volume and serves as the most popular interface for trading on Solana. While this growth has been primarily driven by the explosive popularity of memecoins—tokens often dismissed as unserious or fleeting—Jupiter's embrace of this segment reflects a deeper understanding of market structure and user behavior.

As crypto markets mature, liquidity[1] improves, and pricing becomes more efficient across DEXs. In these conditions, aggregators lose relevance: price discrepancies narrow, and routing through an intermediary often fails to justify added execution risk. Memecoins, however, defy this pattern. Defined by volatility, low liquidity, and rapid narrative shifts, they operate in a state of permanent immaturity. In this context, aggregation remains not only useful but essential.

Rather than resisting the chaotic nature of meme trading, Jupiter has embraced it. The protocol has expanded beyond aggregation by acquiring tools like Moonshot, launching a perps[2] platform, and building Jupiter Mobile.

This paper argues that Jupiter's integration with memecoin trading is not a liability but a forward-looking strategy. By focusing on a market segment that resists maturity, Jupiter secures long-term relevance in an industry where many aggregators may become obsolete. Jupiter will remain indispensable if retail users seek high-risk, high-reward opportunities in fragmented markets.

2. What is Jupiter? A Dex Aggregator For Solana

Jupiter is a decentralized exchange (DEX) aggregator built on the Solana blockchain. It offers users the most efficient and cost-effective token swaps by routing trades through decentralized liquidity providers.[3] Unlike traditional DEXs that maintain their own

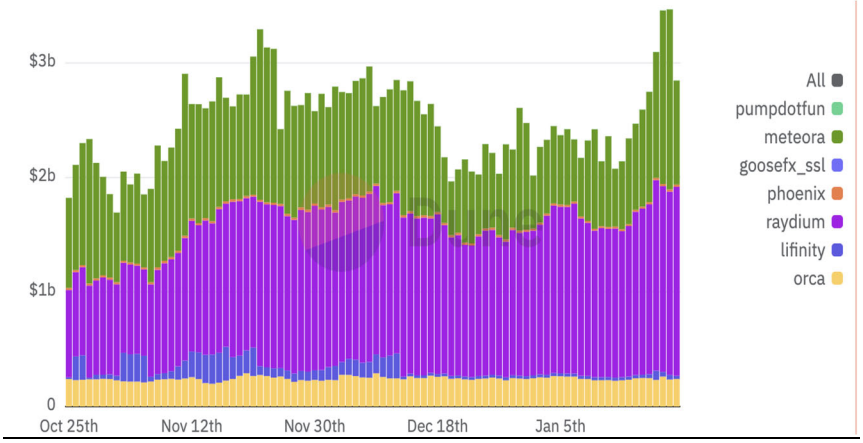
[1] Liquidity: The ease with which an asset can be bought or sold in a market without affecting its price significantly.
[2] Perpetuals (Perps): Derivatives that allow traders to take long or short positions on an asset without an expiration date, often with leverage.
[3] https://www.youtube.com/watch?v=8rddKvHjkJ0

liquidity pools,[4] Jupiter scans pools across Solana-based DEXs—such as Orca, Raydium, Lifinity, and Meteora to determine the optimal path for each trade. It evaluates slippage,[5] liquidity depth,[6] route complexity, and execution reliability in real time. This routing process is critical on Solana, where liquidity is often fragmented across many small pools. By combining multiple routes or splitting large trades across different DEXs, Jupiter delivers better pricing and less slippage than a single-platform trade. This functionality has made Jupiter the backbone of token trading on Solana. At the time of writing, it handles over half of all swap volume on the network[7]—a dominance unmatched by aggregators on other major blockchains.

3. Liquidity Fragmentation and the Need for Routing Engines

At its core, Jupiter solves one of DeFi's most persistent inefficiencies: fragmented liquidity. On Solana, tokens are traded across a range of DEXs—such as Orca, Raydium, and Lifinity—each with its own pools and pricing. This causes token prices to vary between platforms, especially during high volatility or low liquidity periods. Jupiter's aggregator solves this by scanning all available pools and routing trades through the most efficient paths.[8]

Figure 3.1 Solana DEX USD Liquidity by Platform (Oct 25, 2024 – Jan 25, 2025)



[4] Liquidity Pools: A collection of crypto assets locked in a smart contract, used to facilitate trading on DEXs without relying on order books.
[5] Slippage: The difference between the expected price of a trade and the price at which it is actually executed.
[6] Liquidity Depth: Refers to how easily an asset can be traded without causing a significant change in its price. Greater depth means large trades have less impact on price.
[7] https://solscan.io/analytics#programs
[8] https://support.jup.ag/hc/en-us/varticles/18735544617628-How-Jupiter-Swap-Works

As Figure 3.1 illustrates, liquidity is fragmented across Solana's DEX ecosystem, leading to inconsistent pricing across different pools. Aggregators like Jupiter capitalize on this by dynamically routing trades to reduce slippage and improve output.

4. Swap Aggregator: Jupiter's Core Routing Engine

Jupiter's swap aggregator is the backbone of its platform. It scans Solana's major DEXs—including Raydium, Orca, Lifinity, and Meteora—to find the best execution path for every trade. Intelligently splitting transactions across multiple liquidity pools minimizes slippage and maximizes output.[9] Figure 4.1 illustrates this process: Jupiter routes a $1000 USDC trade into Jailstool by splitting across Bonk on ZeroFi and SOL via Raydium, demonstrating how its routing engine constructs complex, multi-hop paths to secure the best price in low-liquidity markets.

Figure 4.1 Split Route Optimization by Jupiter Aggregator

5. Limit Orders and DCA: Advanced Tools for Volatile Markets

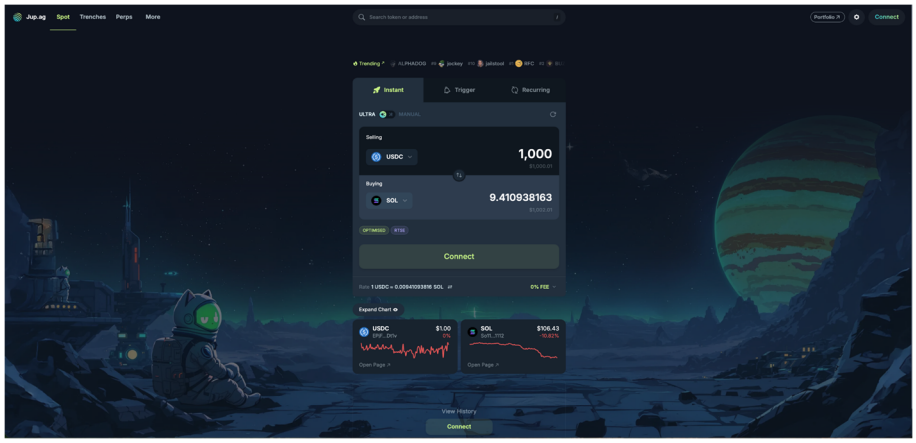
Jupiter offers limit orders and dollar-cost averaging (DCA) features to give users greater control in volatile markets. Limit orders allow users to specify a price at which they want to buy or sell a token, executing if the market hits that level. DCA enables recurring buys over time, helping mitigate volatility and reduce the emotional timing of entries.

These tools are particularly useful in memecoin markets,[10] where price swings and thinning liquidity are frequent. Limit orders let users wait out volatility, while DCA spreads out risk.[11]

[9] https://support.jup.ag/hc/en-us/articles/18735544617628-How-Jupiter-Swap-Works
[10] https://support.jup.ag/hc/en-us/articles/18734698136604-How-Recurring-works-in-depth
[11] https://www.bitstamp.net/en-gb/learn/cryptocurrency-guide/what-is-jupiter-jup/

Both features contribute to protocol revenue through small execution fees, making them essential to Jupiter's broader monetization strategy.

Figure 5.1 Jupiter Swap Interface: Instant, Limit, and Recurring Trade Options



As shown in Figure 5.1, these features are integrated directly into Jupiter's swap interface. This streamlined presentation ensures users can access advanced tools without switching platforms, reinforcing Jupiter's position as the most intuitive front end for traders on Solana.

6. Perpetuals Platform: Expanding Into On-Chain Derivatives

Jupiter has launched a perpetual futures (perps) platform, allowing leveraged trading on assets like SOL, ETH, and BTC. Trades are backed by the JLP pool, a vault where users provide liquidity in exchange for a share of trading fees, funding payments, and potentially token rewards.[12]

Though relatively new, the perps platform has already attracted billions in TVL, rapidly positioning itself as one of the largest perpetual platforms on Solana. Its success highlights Jupiter's ability to expand from aggregator to multi-product exchange. Integrated directly into the main interface, the Perps platform enables users to transition seamlessly from spot swaps to leveraged positions.

[12] https://support.jup.ag/hc/en-us/articles/19356216696860-JLP-Economics

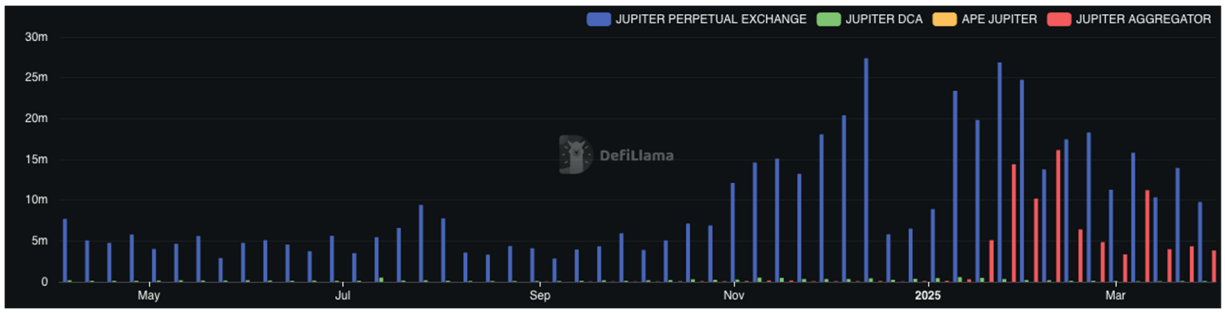
Figure 6.1 Jupiter Perpetual User Interface

As shown in Figure 6.1, the perps interface mirrors the simplicity of Jupiter's swap engine while offering advanced controls for leveraged trading. Users can easily toggle between long and short positions,[13] adjust leverage from 1.1x up to 100x, and view real-time fees, funding rates, and price impact[14]—all within a single, intuitive dashboard.

7. Jupiter's Revenue and Fee Structure

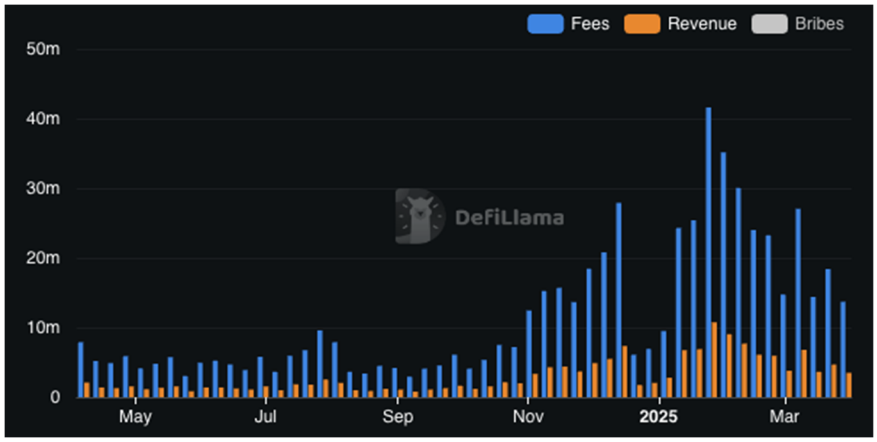
Jupiter's monetization strategy spans a growing suite of trading products. While standard swaps on the base interface are mostly fee-free, users who enable Ultra Mode—a premium routing tier—pay between 0.05% and 0.1%,[15] depending on the token pair. This feature improves execution and generates steady revenue. Additional income comes from the perpetual exchange, limit orders, and DCA tools, all of which apply execution-based fees.

Figure 7.1 Jupiter Weekly Revenue by Product: Perps, DCA, Aggregator, and Ape Pro



[13] https://support.jup.ag/hc/en-us/articles/19209043643036-How-limit-order-works-on-Jupiter-Perps
[14] https://support.jup.ag/hc/en-us/articles/18735045234588-What-are-the-fees-associated-with-Jupiter-Perps
[15] https://dev.jup.ag/docs/ultra-api/#:~:text=FAQ%E2%80%8B,swap%20amount%20as%20a%20fee

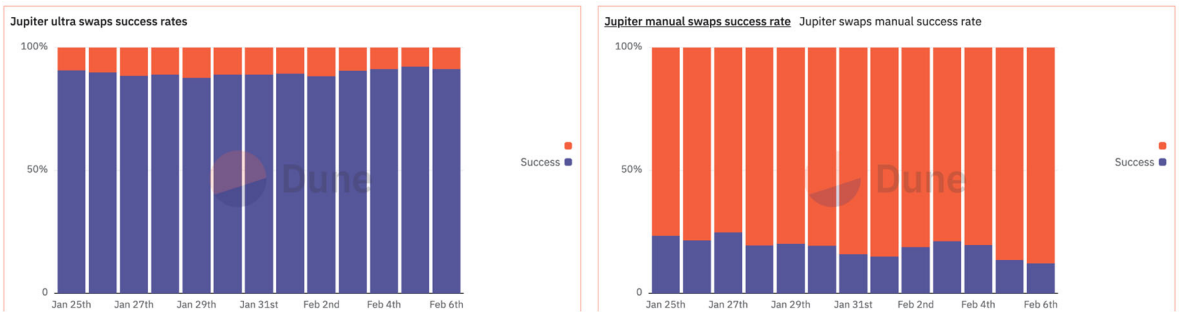
Figure 7.2 Jupiter's Weekly Revenue vs Fees



Figures 7.1 show that Jupiter's Perpetual Exchange quickly became its top revenue driver, surpassing swap aggregation. At the peak, weekly perp fees topped $30 million, reflecting growing demand for leveraged trading in speculative markets. However, Figure 7.2 reveals a gap between total fees and retained revenue, indicating Jupiter shares revenue with LPs, partners, or incentive programs. This reflects a common challenge in DeFi: balancing ecosystem growth with sustainable protocol capture.

Meanwhile, Ultra Mode, which launched in early 2025, has contributed $3–10 million per week. While it operates within the main aggregator interface, Ape Pro is a separate, purpose-built memecoin trading terminal. It features MEV protection, batch buying, and sign-less execution[16]—tools tailored to high-frequency, narrative-driven speculation. While Ape is still growing in usage, it represents a strategic bet on the persistence of memecoin activity.

Figure 7.3 Success Rate of Ultra Swap Vs. Manual Swap



[16] https://support.jup.ag/hc/en-us/articles/18601340971804-Will-my-order-get-frontrun

The success rate is a key revenue lever. Figure 7.3 shows that Ultra Mode consistently achieves over 90% execution, while manual swaps often fall below 20%, primarily due to slippage protection. In volatile or low-liquidity markets—especially memecoins—Ultra's ability to route around failed trades means more volume, trust, and fees earned.

Together, these products demonstrate how Jupiter transforms volatility into value. It doesn't just route trades; it captures speculative flow and converts it into revenue by building tools designed for the behaviors that drive crypto's most active markets.

II. ANALYSIS: MEMECOINS AND THE VALUE OF AGGREGATION

1. Why Memecoins Are the Perfect Fit for Aggregators

Tokens like SOL and USDC are among the most established on Solana, trading across numerous decentralized exchanges with deep liquidity. This liquidity causes prices across platforms to align closely, reducing the benefit of routing through an aggregator. Users often face similar outcomes whether they route or not while still taking on potential execution risks like slippage, latency, or failed transactions.

This reflects the behavior of automated market makers (AMMs) like Raydium or Orca, which operate on the constant product formula ($x * y = k$). As liquidity increases, the price curve flattens, allowing for larger trades with minimal price movement. Figure 8.1 illustrates this clearly: price impact is negligible in high-liquidity environments. But when liquidity is low, even modest trade sizes cause steep price swings. This is when routing becomes most valuable and when aggregators like Jupiter shine.

Figure 8.1 Price Impact in Low vs. High Liquidity Markets

The following trade routes illustrate how liquidity differences play out in practice.

Figure 8.2 Jupiter Routing in High Liquidity Markets

Figure 8.3 Jupiter Routing Low Liquidity Markets

Low liquidity defines memecoin markets because, unlike blue-chip tokens, memecoins rarely sustain deep liquidity and are driven by fast-moving hype cycles. Each coin creates a short-lived, inefficient micro-market with high slippage and extreme volatility. As shown in Figure 8.3, the complexity of routing into Fartcoin, a popular memecoin, reflects how liquidity is often spread thinly across multiple venues and token pairs. Aggregators like Jupiter are essential in these environments—not because of price volatility alone, but because no single DEX offers complete access. Jupiter reduces friction by stitching together fragmented liquidity and delivering a route that would otherwise be inaccessible to the average trader.

Figure 8.4 Jupiter Swap Volume by Token Category

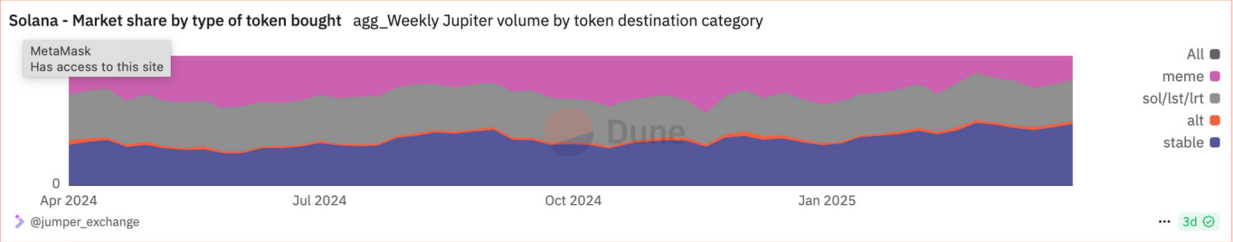


Figure 8.4 shows that memecoins consistently account for at least one-third of Jupiter's volume. These trades aren't isolated events but part of a broader behavioral pattern. Retail traders chase narrative-driven tokens, and memecoins provide the volatility and payoff structure they seek.

Jupiter hasn't just responded to this; it has built around it. The protocol acquired Moonshot in 2025,[17] an app to easily purchase memecoins, and launched Ape Pro in 2024, a dedicated memecoin execution terminal. These products are part of a larger strategy to own the speculative flow that drives on-chain volume. By investing in tools for this chaotic, persistent market segment, Jupiter ensures that its aggregator remains critical—even as the rest of DeFi becomes more efficient.

Memecoins may never mature, but that's why they matter. Their churn, volatility, and inefficiency guarantee a long-term need for routing infrastructure. And no protocol is better positioned to serve that need than Jupiter.

2. Speculation as Product: Memecoins as a Psychological Engine

Memecoins are often dismissed as jokes—lacking fundamentals, roadmaps, or utility, but their appeal is psychological. They tap into the brain's dopamine system, activating the universal desire for sudden wealth, excitement, and cultural status. Memecoins are not traditional investments. They are entertainment, identity, and community packaged in volatile financial wrappers. As Meow, the founder of Jupiter, argues, memecoins function less like financial assets and more like symbolic rallying points. Like sports teams, national flags, or online fandoms, they give people a sense of shared identity and belonging. Their speculative energy is charged with emotional resonance, offering what Meow describes as "emotional ups and highs that usually require actual individual

[17] https://www.youtube.com/watch?v=2pR8903YT-c

achievement and actualization."[18] They don't just offer profit—they offer participation in a broader cultural moment. As Meow puts it, "Memecoins are, in essence, social infrastructure."[19]

Behavioral finance helps explain this. In his 2007 study, Kumar found that retail investors exhibit lottery-like preferences, especially those with lower income or financial literacy. They chase asymmetric bets: low-cost assets with slim chances of massive returns.[20] Memecoins mimic that structure exactly. A 2015 Harvard study[21] outlines core behavioral economics principles, including present bias, overconfidence, and social reference framing, that help explain why traders are drawn to speculative assets like memecoins. This helps explain why memecoin investments often bypass fundamentals entirely: the appeal lies not in intrinsic value but in the narrative. A few dollars in the right token offers a 1000x return, status, identity, and participation in a cultural moment.

Figure 9.1 Fartcoin (Blue) vs. S&P 500 (Red): ROI Performance (Nov 2024 – Apr 2025)

Figure 9.1 reflects that dynamic. While traditional assets like the S&P 500 move slowly, memecoins swing wildly. That volatility is not a bug—it's the feature users are chasing.

Social media fuels this cycle. Platforms like X and Telegram act as trading floors, hype machines, and echo chambers. Viral screenshots of $10K-to-$1M flips create FOMO.

[18] https://meow.bio/symbols-and-gods.html
[19] https://meow.bio/meme-coins.html
[20] http://www.econ.yale.edu/~shiller/behfin/2005-04/kumar.pdf
[21] https://scholar.harvard.edu/files/laibson/files/aer_principles_2015.pdf

Traders pile in not because of fundamentals but because others already have. This reflexivity makes prices go up simply because people believe they will.[22]

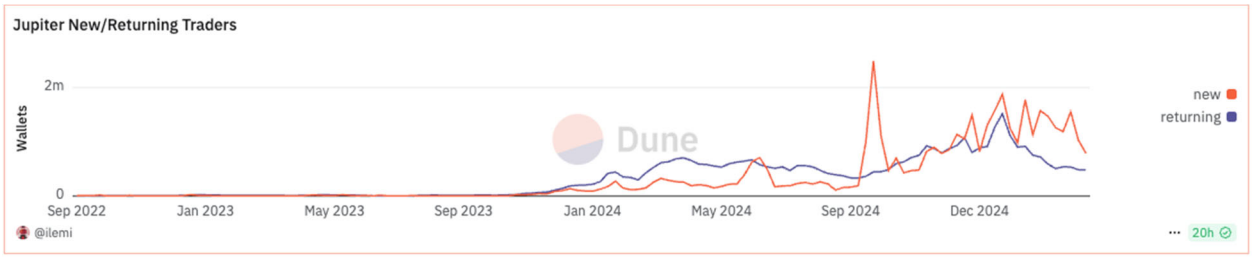
This behavior scales fast. Dogecoin, created as a joke, is in the top 10 in market cap.[23] More recently, $TRUMP hit a $15 billion market cap within 24 hours, with daily volume peaking at nearly $50 billion.[24] Neither had meaningful utility. They succeeded because they were seen as wealth generators, not financial infrastructure.[25]

Unlike gambling, memecoin speculation is decentralized, permissionless, and participatory. There's no house edge or central authority. Users feel empowered choosing the right coin, the right timing, and the right group chat. The experience is more engaging than passive betting.[11]

Even sophisticated traders participate. Why? Because people will buy anything they believe might make them money. The line between investing and gambling blurs, especially when quick, asymmetric returns take precedence over fundamentals.

Platforms like Jupiter don't just benefit from meme-driven speculation—they optimize for it. Tools like Moonshot and Ape Pro streamline discovery and execution, funneling users toward trending tokens. This design supports user behavior and converts attention into transaction volume. Meme trading also serves as a powerful onboarding mechanism: many users first discover Jupiter through volatile tokens and continue using it as their primary platform for future trades.

Figure 9.2 Number of Returning and New Users on Jupiter



[22] https://www.psychologytoday.com/us/blog/the-human-algorithm/202501/why-crypto-memes-hijack-your-brain-and-how-to-resist
[23] https://coinmarketcap.com/currencies/dogecoin/
[24] https://coinmarketcap.com/currencies/official-trump/
[25] https://www.prnewswire.com/news-releases/meme-coins-or-meme-gamble-the-risky-world-of-trump-coin-and-other-crypto-memes-with-jamie-bungaree-from-casinoaus-302384807.html

Figure 9.2 shows that memecoin surges drive repeat engagement. Once users see low-friction execution during speculative runs, they're more likely to return for future trades. Memecoins function as a revenue stream and a customer acquisition funnel.

For many, memecoins are the first touchpoint in crypto. Not because of their utility—but because of the opportunity they represent. They combine speculation, community, and entertainment into one high-volatility experience. By designing for this behavior, Jupiter becomes the platform users remember when the next wave of hype arrives.

3. Jupiter's Strategic Positioning and Long-Term Risks

As Jupiter cements its role as Solana's premier trading interface, it is actively repositioning for long-term dominance beyond the aggregator model. While it began by routing trades across DEXs like Orca, Raydium, and Lifinity, Jupiter has evolved into a vertically integrated product suite. This shift reflects a clear understanding that aggregation alone may not remain a defensible moat in increasingly efficient markets. By developing its wallet, perps exchange, memecoin platforms, and eventually a cross-chain bridge, Jupiter aims to control the full lifecycle of on-chain trading—from discovery to execution and custody.

10.1 From Aggregator To Solana Frontend

One of Jupiter's most important strategic advantages is its evolution into the default front-end for trading on Solana.[26] Rather than simply routing swaps in the background, Jupiter has become the interface through which most users interact with decentralized markets. Whether executing swaps, setting limit orders, using DCA tools, or speculating through Moonshot and Ape, users increasingly engage with Solana through Jupiter—not the underlying DEXs.

[26] https://www.youtube.com/watch?v=2pR8903YT-c

Figure 10.1. Interaction Volume by Program On Solana

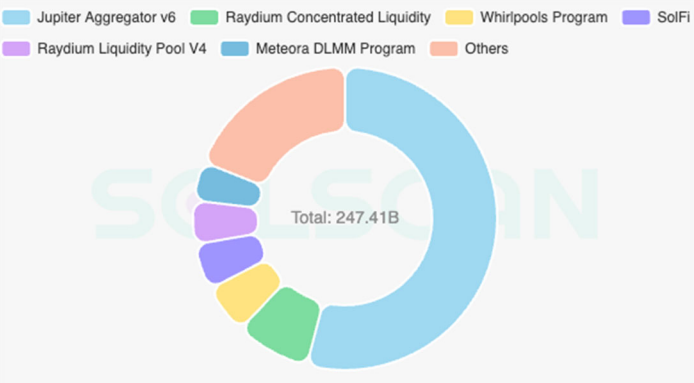


Figure 10.1 shows that Jupiter Aggregator v6 leads in volume routed across Solana DEX programs, surpassing direct interactions with platforms like Raydium. This dominance reinforces Jupiter's status as the front-end gateway to trading activity on Solana. Most users first interact with Solana through Jupiter, often via speculative meme coin trades. In an environment where code can be copied and features duplicated, Jupiter's edge lies in capturing users early and forming habits that increase the likelihood they continue using its broader ecosystem of tools.

10.2 Owning The Speculation Funnel

Jupiter's acquisition of Moonshot and the development of Ape Pro demonstrate a clear understanding of where crypto volume originates. Rather than building for theoretical DeFi users, Jupiter builds for actual ones—users who chase tokens, act on narratives, and want the fastest possible execution. Moonshot simplifies memecoin discovery, while Ape enables users to buy in bulk, batch trades, and vault assets without leaving the Jupiter ecosystem.

Jupiter is not just a DEX aggregator—it is a speculation funnel. From the moment a user hears about a token on X to the moment they trade, Jupiter wants to be the shortest and smoothest path. As Jupiter's founder, Meow, explains, "A 'normie' is not coming into this market because you did some math they can't decipher, and now your DEX routes orders better. But they will come into the market because some memecoin they can buy

100,000,000 of, with a cute animal picture, is pumping."[27] This philosophy shapes Jupiter's product decisions—from memecoin-focused tools to mobile-first interfaces.

By controlling both the discovery and execution layers, Jupiter increases retention, captures more fees, and positions itself as the core infrastructure layer for the market's most active behavior. This strategic alignment reduces the risk of being replaced by more user-friendly DEXs and ensures users turn to Jupiter when meme coins are trending.

10.3 Preparing for a Post-Aggregator World

While Jupiter is dominant today, the team recognizes that aggregation may not be a defensible moat forever. As Solana matures and DEX liquidity consolidates, price discrepancies shrink. In high-liquidity environments, routing loses value, and aggregators may introduce friction through swap failures, latency, or slippage risk.

Jupiter is proactively addressing this risk. Its launch of a perpetual platform and Jupiter Mobile, a full-featured wallet,[28] signal an intent to become Solana's all-in-one trading super app. These products capture new fee streams—such as trading, staking, and liquidity provision—and reduce dependence on swap volume alone.

The proposed Jupnet project, an omni-chain liquidity and data layer, expands this vision further. If successful, Jupnet would allow Jupiter to route trades and aggregate liquidity across multiple blockchains.[29] This would increase its relevance and insulate the protocol from being tied too closely to Solana's performance.

By building across layers—routing, trading, execution, and now infrastructure—Jupiter is preparing for a future where aggregators need to do more than just compare prices. Regardless of where that volume originates, it is positioning itself as the central interface for speculative volume.

[27] https://meow.bio/meme-coins.html
[28] https://support.jup.ag/hc/en-us/articles/18287955471772-About-Jupiter-Mobile
[29] https://meow.bio/jupnet.html

10 Risks and Limitations

Jupiter's strategy is bold but not without risk. Its growing reliance on memecoin volume exposes it to speculative cycles that are inherently unpredictable. Memecoins attract attention, but they also fade quickly. If user behavior shifts or retail interest moves elsewhere, a major source of Jupiter's volume and fees could evaporate.

Moreover, Jupiter is deeply tied to Solana. While this has allowed for exceptional performance, it also creates platform risk. If Solana suffers downtime, regulatory scrutiny, or ecosystem contraction, Jupiter could face a sudden drop in usage or credibility.

There are also concerns about centralization. Despite its alignment with DeFi principles, Jupiter's product development, branding, and user interface are controlled by a relatively small team. This introduces potential governance concerns, especially as Jupiter evolves from an aggregator into a full trading stack and wallet provider.

Lastly, the shift from aggregator to front-end introduces user experience (UX) and security risks. As Jupiter expands into more user-facing tools—such as wallets, mobile apps, and leveraged trading—it must deliver the smooth, intuitive interfaces users expect from centralized exchanges (CEXs) while still preserving the transparency and safety of a decentralized system. Any security exploit or failed product rollout could severely damage user trust and undermine the entire ecosystem.

11 Conclusion and Outlook

Jupiter's dominance in the Solana ecosystem may appear tightly tied to the memecoin trend, but a closer look reveals strategic foresight—not dependence. As decentralized markets mature, liquidity deepens, and price discrepancies narrow, the role of aggregators becomes less valuable. In efficient environments, routing adds complexity and risk without a meaningful payoff.

Memecoins, however, are structurally different. Their inherent volatility, fragmented liquidity, and narrative-driven trading behavior create the perfect environment for aggregation to remain useful. Jupiter has not only identified this reality, but it has built for it.

Through acquisitions like Moonshot and the development of purpose-built tools like Ape Pro, Jupiter has expanded its role from a routing engine to the primary interface for speculative trading. In doing so, it has redefined what an aggregator can be: not just a technical optimizer but an enabler of cultural and behavioral market patterns.

The behavioral mechanics behind memecoin trading—FOMO, status-seeking, and the pursuit of sudden wealth—are deeply human and unlikely to disappear. At the core is a simple truth: people want to be rich but don't want to work for it. Memecoins may lack fundamentals, but they fulfill emotional needs that engage users. As Meow, the founder of Jupiter, writes, "You can't kill memes on the internet, and you can't kill memecoins."[30] This resilience is precisely what makes them a long-term asset class—and what keeps Jupiter relevant.

Memecoins are not just a byproduct of crypto—they are central to how it spreads. As Meow puts it, they are "a vital component of the cryptocurrency landscape," bridging emotional resonance with speculative structure.[24] This cultural persistence is what Jupiter is designed to support.

Jupiter's roadmap signals continued evolution in the months ahead. From omnichain aggregation with Jupnet to a seamless trading experience through Jupiter Mobile and Perps, the protocol is positioning itself as a speculation super app. Its success will hinge not on capturing every user—but on capturing the users who matter most in DeFi's high-volume, high-volatility corners.

Crypto narratives will rise and fall. Liquidity will move. But speculation will remain constant. In that chaos, Jupiter isn't just surviving—it's thriving.

[30] https://meow.bio/meme-coins.html

The DeFi Illusion: Why Compound Will Never Solve Financial Exclusion

By Dawson Gulley

Abstract: This paper challenges the belief that decentralized finance (DeFi) platforms like Compound can solve financial exclusion. While these protocols promise open and permissionless[1] access to credit, their reliance on overcollateralization structurally favors existing asset holders and excludes those most in need of capital. More critically, only relying on overcollateralization is destined to fail as a long-term approach to risk management due to contagion risk[2], leverage[3], and the inability to differentiate borrower risk. Platforms like Compound are exposed to systemic failures. Moreover, attempts to implement protections such as insurance funds, safety modules, or capital buffers are often unworkable in these systems, since they rely on undifferentiated borrower risk and offer no way to prevent adverse selection. This paper argues that without incorporating risk-tiered lending, or protocol-level protections, collateral-based DeFi platforms will not democratize finance, but instead replicate and amplify the failures of traditional lending systems[4].

[1] A permissionless blockchain allows any user to participate in network activities (e.g., transacting, validating) without prior approval, unlike permissioned networks that restrict access to verified actors.
[2] Contagion risk refers to the spread of financial distress from one entity, asset, or protocol to others, often through interconnected exposures. In DeFi, liquidation cascades, shared collateral assets, or leveraged positions can transmit shocks across an entire ecosystem.
[3] Leverage refers to the practice of using borrowed funds to amplify returns. In DeFi, users often recycle borrowed assets to increase their exposure, multiplying both potential gains and losses.
[4] Portions of the wording and sentence structure in this paper were refined using OpenAI's ChatGPT (April 2025 version) to improve clarity and coherence. The ideas and arguments are my own.

Introduction

Background on Financial Exclusion

Access to affordable credit is one of the most significant barriers to economic opportunity. In traditional finance, this access is often reserved for those who already hold wealth. Individuals with substantial assets—real estate, securities, or income—benefit from lower interest rates and favorable loan terms, while those without such backing face prohibitively high borrowing costs or outright rejection. This dynamic perpetuates wealth inequality by making it easier for the rich to invest and harder for the poor to build wealth.

Banks act as gatekeepers, relying heavily on credit scores, employment history, and asset verification to evaluate borrowers. These requirements systematically exclude many low-income individuals, immigrants, gig workers, and young people with limited credit histories. The financial system, in effect, favors those who are already established.

Introduction to Compound

Compound is a decentralized finance (DeFi) protocol built on the Ethereum blockchain. Launched in 2018 by Compound Labs, it allows users to lend and borrow cryptocurrency assets without relying on traditional intermediaries. Instead of relying on banks or credit institutions, Compound uses smart contracts[5] to manage lending pools, calculate interest rates, and enforce collateral requirements.

At its core, Compound is a money market protocol. Users can supply supported assets (e.g., ETH, USDC, DAI) to earn interest or use their deposits as collateral to borrow other assets. Interest rates are determined algorithmically based on the supply and demand of each asset. When more users are borrowing a specific asset, the interest rate rises to attract more lenders. When there is excess supply, rates fall to encourage borrowing.

Borrowers do not need to undergo credit checks, provide identification, or interact with a central authority. All they need is a compatible crypto wallet, collateral in the form of supported tokens, and enough gas (Ethereum transaction fees) to interact with the protocol. This permissionless approach allows anyone in the world to participate, theoretically democratizing access to financial services (Lesniewski & Hayes, 2019).

[5] Smart contracts are computer programs that automatically execute predefined instructions once specific conditions are met, typically without needing human intervention.

However, there is a major caveat. In order to borrow on Compound, users must overcollateralize their loans. That means if a borrower wants to take out $100 in USDC, they might need to deposit $150 worth of ETH or another volatile asset. The protocol enforces these collateral ratios through automated liquidation mechanisms—if the value of a borrower's collateral falls below a certain threshold, it is sold off to repay the debt. The collateral factor represents the threshold at which liquidation becomes mandatory. It is defined as the ratio of the borrowed amount to the value of the posted collateral. As of April 13, 2025, Ethereum's collateral factor on Compound was 75%. In this example, that means if the value of the borrower's ETH collateral falls from $150 to $133.33, the position would hit the 75% threshold and trigger automatic liquidation by the protocol (Compound Labs, n.d.).

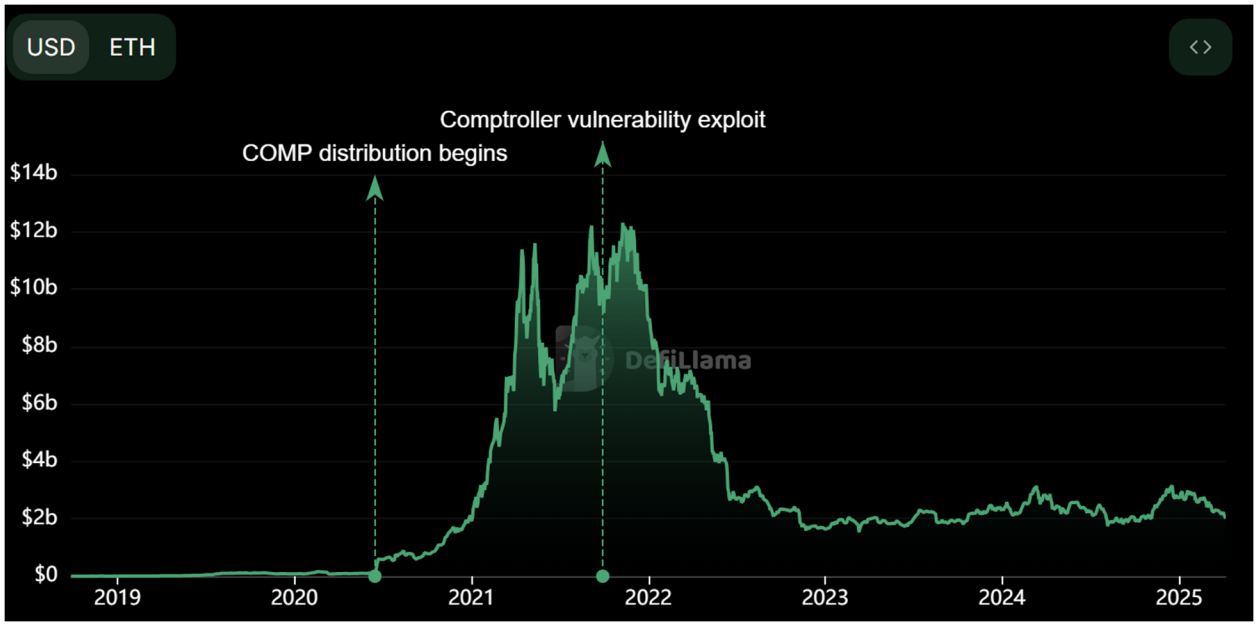
While it may seem counterintuitive to borrow less money than the value of the collateral being posted, many users turn to Compound for liquidity without wanting to sell their assets. For example, an investor holding ETH who expects it to appreciate in value may prefer to use it as collateral rather than sell it outright, which could trigger taxable events or reduce their exposure to potential gains.

Suppose a user deposits $15,000 worth of ETH into Compound. With a 150% collateralization ratio, they could borrow up to $10,000 in USDC while still maintaining their ETH position. If ETH increases in price, they would benefit from the appreciation while still having access to spendable funds. Some users go a step further and use the borrowed $10,000 in USDC to purchase additional ETH, effectively leveraging their position. This strategy can amplify returns in a rising market, but it also significantly increases exposure to price volatility and the risk of liquidation if ETH's value drops.

Compound introduced the COMP token in 2020 to decentralize governance. Token holders can vote on changes to the protocol, such as adding new assets, adjusting interest rate models, or modifying collateral factors. While this move aligns with the ethos of decentralization, it has also led to questions about the influence of early investors and the technical barriers to participating in governance (Compound Labs, n.d.; Compound Governance Forum, n.d.).

Compound has been one of the most prominent and widely used DeFi platforms, and at its peak in 2021, the protocol had over $10 billion in total value locked (TVL). However,

its TVL has declined significantly in recent years as users have migrated to more flexible or capital-efficient protocols like Aave and Morpho (DeFiLlama, 2025).



Source: DeFiLlama

It was one of the first DeFi applications to offer a relatively simple and composable interface, paving the way for integrations into wallets, aggregators, and DeFi asset managers. Compound's design also inspired numerous competitors—including Aave and Morpho.

Thesis Statement

Compound and similar collateral-based DeFi lending platforms are fundamentally incapable of solving financial exclusion. First, their requirement for overcollateralization inherently excludes individuals without substantial existing assets, replicating the barriers of traditional finance. Second, even with excess collateral, these systems remain vulnerable to collapse due to leverage, contagion risk, and the Lemon Problem. Third, implementing protections like insurance funds, safety modules, or capital buffers is often unfeasible in collateral-based systems like Compound, since they rely on undifferentiated borrower risk.

The Problem of Credit Access in Traditional Finance

Case Study: Elon Musk vs. the Average Borrower

One of the clearest illustrations of unequal credit access can be displayed by comparing how Elon Musk borrows versus the average working individual. Musk has repeatedly used his shares in Tesla as collateral to secure loans worth billions of dollars—at interest rates close to the risk-free rate. Because he holds a massive portfolio of liquid, high-value assets, lenders consider him a low-risk borrower, even if his actual income is relatively modest. These loans are typically structured with low interest, minimal oversight, and favorable terms. For wealthy individuals, borrowing is frictionless and strategically beneficial.

In contrast, a middle-class borrower seeking a personal loan must often undergo rigorous credit checks, provide detailed income documentation, and post personal assets like a home or car as collateral. Even then, the interest rate may range from 10% to 30%, depending on the borrower's credit history and income stability.

The 3 Major Consequences of This System

1. Risk Profile Bias

While Musk might lose a portion of his equity holdings if the market turns, a typical borrower could lose their home. This asymmetry highlights how the credit system is built to favor those who already have wealth, while imposing far greater relative risks on those who do not. This leads less wealthy investors to justifiably adopt a much lower risk tolerance, as they cannot afford to lose the limited assets they already have.

2. Rate of Return Advantage for the Wealthy

This bias extends beyond risk tolerance into return expectations. Wealthy borrowers often access capital at interest rates as low as 2% or 3%, significantly lowering their cost of debt. That means any project or investment that generates returns above this low hurdle rate becomes profitable. Conversely, if the average borrower is offered a loan at 15%, their cost of debt is substantially higher. They must find an investment with a much greater return just to break even. This raises the bar for entrepreneurship and economic mobility among non-wealthy individuals and further entrenches financial inequality.

While the theoretical cost of equity is the same for all investors operating in the same market—based on factors like the risk-free rate and market volatility—in practice, it often differs depending on the investor’s financial position. Wealthier individuals typically

have greater diversification, access to better information, and higher risk tolerance, which allows them to pursue investments with lower expected returns. Meanwhile, less wealthy investors may demand higher returns to justify the personal financial risk involved, especially when investing a significant portion of their limited assets. As a result, even though the formal cost of equity may be equal, the effective cost of capital is often lower for the wealthy, further reinforcing their ability to access and profit from investment opportunities (Campbell, 2006).

Over time, this creates a self-reinforcing cycle. Wealthier individuals borrow cheaply to invest, earn predictable returns, and expand their wealth. Those without access to cheap credit are forced to either take on more risk or opt out of borrowing altogether, limiting their ability to build assets or start businesses.

3. Stifles Innovation

Because of these financial barriers, even highly capable individuals from low-income backgrounds may be unable to act on transformative ideas. A person could have the knowledge and vision to develop a cure for cancer, but without access to affordable capital or a safety net, they may never be able to fund research, start a business, or bring their innovation to market. In this way, financial exclusion doesn't just harm the individual—it imposes a cost on society by stifling innovations that could benefit everyone. Talent alone is not enough—opportunity requires resources, and the current credit system often denies opportunity to those who need it most.

Why Compound Was Created

Compound emerged as a response to this inequality by attempting to democratize access to credit through decentralized finance. This model treats all users equally—interest rates are not based on personal profiles, but on real-time market dynamics. For example, if there is a high demand for borrowing USDC and a limited supply, the interest rate for borrowing USDC will rise accordingly. If more users supply USDC to the pool, the rate will fall to reflect the increased availability of capital. This pricing mechanism aims to be transparent, efficient, and fair—at least in theory.

The Lemon Problem: How Compound Fails to Overcome Asymmetric Information

What is the Lemon Problem?

The "Lemon Problem" originates from economist George Akerlof's seminal 1970 paper, The Market for Lemons, which analyzed quality uncertainty in the used car market. Akerlof explained that when buyers cannot distinguish between high-quality cars ("peaches") and low-quality ones ("lemons"), they are only willing to pay an average price. As a result, sellers of high-quality cars withdraw from the market because they cannot command a fair premium, leaving behind more lemons. This creates a self-reinforcing cycle: as more peaches leave the market, the overall quality declines, which further discourages high-quality sellers from participating, ultimately leading to market failure since only lemons are left, and no one wants to pay for a lemon. This principle of asymmetric information—where one party has more knowledge about the quality of an asset than the other—applies directly to credit markets. In lending, borrowers know more about their own risk profile than lenders do. If lenders cannot accurately assess that risk, they may charge higher average interest rates to cover potential losses. But just like in the used car market, this drives away the "good" borrowers who deserve lower rates, leaving only higher-risk participants (Akerlof, 1970).

In traditional finance, institutions mitigate this problem through mechanisms like credit scoring, income verification, and other underwriting procedures. These tools allow banks to separate high-risk from low-risk borrowers and offer differentiated loan terms accordingly. While imperfect, these practices help keep interest rates in line with actual borrower risk and preserve the integrity of the lending pool.

Compound, however, makes no such distinction. As a decentralized protocol, Compound does not perform identity verification, credit assessments, or any evaluation of borrower behavior. Instead, it uses a market-based interest rate that adjusts purely based on supply and demand for each asset. This means all borrowers receive the same rate for a given token, regardless of their creditworthiness, financial history, or behavior on-chain. The absence of risk-based pricing leaves Compound unable to effectively screen borrowers or reward low-risk participants with lower borrowing costs.

Invisible Risk: Why Compound's Stable Rates Conceal a Deteriorating Borrower Pool

The result of this design is a self-reinforcing cycle that mirrors the lemon market's unraveling. Because Compound does not evaluate borrower quality, creditworthy individuals—those who might qualify for lower rates in a traditional system—have no incentive to borrow at the average or above-average rates imposed by the protocol. Instead, they may seek more efficient lending platforms or abstain from borrowing altogether. This leaves behind a borrower pool that is increasingly composed of users willing to pay high rates, which typically means they are riskier borrowers, more desperate for capital, or engaged in speculative activity.

In theory, as the composition of the borrower base deteriorates, the protocol should raise interest rates to compensate for the increased utilization and perceived risk. But this only reinforces the trend: higher rates further drive out low-risk borrowers and attract even more high-risk ones, exacerbating the problem.

While Compound's model creates conditions for adverse selection, its interest rates do not necessarily reflect this growing risk. As of April 13, 2025, the net borrow APR on Ethereum was 2.39%—notably lower than the prevailing risk-free rate[6] (Compound Labs, 2025). Unlike traditional lenders or DeFi platforms that incorporate credit scoring or borrower vetting, Compound sets rates purely based on asset utilization, not borrower quality. As a result, even if low-risk users exit the platform and riskier borrowers remain, interest rates may stay relatively stable—masking the systemic risk beneath the surface. This keeps Compound's rates competitive, but it shifts risk into borrower pool composition and increases the protocol's vulnerability during market volatility. Without tools to assess or segment borrower risk, Compound doesn't fully experience rate inflation—but the fragility introduced by asymmetric information still remains.

[6] The risk-free rate is typically represented by U.S. government securities or overnight secured lending benchmarks. As of April 14, 2025, the Secured Overnight Financing Rate (SOFR)—a widely used proxy for the risk-free rate—was 4.33%.

Compound's Competitors

In contrast, some of Compound's competitors have introduced models that attempt to address this information gap. Platforms like Maple Finance use off-chain underwriting or institutional diligence to assess borrower quality and issue undercollateralized loans to vetted entities (Maple Finance, 2021). Aave, another leading DeFi protocol, has introduced risk-tiered models in its Version 3 update, enabling more nuanced collateral and borrowing structures (Aave, 2020). While these systems are far from perfect and often still rely on reputation and trust, they at least begin to tackle the core issue of borrower differentiation. Compound, by offering identical terms to all users, treats high-risk and low-risk borrowers as interchangeable—a decision that invites adverse selection. Instead of assessing borrower quality, Compound relies solely on overcollateralization as its primary risk management tool, which does little to mitigate the effects of asymmetric information.

Why Overcollateralization is NOT a Perfect Solution

Excludes the People Who Need Credit the Most

Overcollateralization automatically excludes anyone who doesn't already have significant assets. In theory, DeFi was supposed to unlock credit access for the underbanked—people without access to traditional financial infrastructure or without credit scores. In practice, however, Compound only offers loans to those who already have valuable crypto holdings. If you already possess $15,000 in ETH, and the protocol allows you to borrow $10,000 against it, you likely have other financial tools at your disposal. Meanwhile, an individual without such holdings cannot access any credit at all, regardless of how trustworthy or productive their intended use of funds may be. Therefore, Compound's model favors existing wealth, repeating the very barriers it was supposed to eliminate.

Overcollateralization Does NOT Prevent Lender Losses

There's a common misconception that overcollateralized loans are risk-free for lenders. But even in traditional finance, secured loans can default—especially in volatile markets. For example, mortgage-backed securities were technically overcollateralized, yet lenders suffered massive losses during the 2008 financial crisis when the underlying assets collapsed in value. Similarly, in DeFi, the value of collateral can drop so quickly that automatic liquidation mechanisms can't keep up. A 20% price drop in ETH over a single

day can cause a cascade of margin calls, where multiple positions fall below the required collateral ratio at once.

DeFi Lending Assumes 100% Liquid Markets—But That's a Dangerous Assumption

Compound's design assumes there will always be liquidity—that someone will be willing to buy discounted collateral when liquidation is triggered. But crypto markets are notoriously thin during moments of crisis. In a black swan event such as an exchange hack, regulatory announcement, or even a coordinated sell-off, liquidity can vanish instantly. When that happens, the protocol cannot execute liquidations at fair prices, and lenders are left holding undercollateralized debt. Crypto's extreme volatility[7] makes this even worse: unlike real estate or corporate bonds, assets like ETH and DAI can experience double-digit percentage swings within hours. A system built on the assumption of stable liquidation conditions is fundamentally brittle when exposed to real-world volatility.

The Chain Reaction of Liquidations – How Compound Can Collapse in a Market Crash

The theoretical risk of illiquidity becomes a very real threat during a sharp market downturn. In a cascading liquidation event, a sequence of automated reactions can drive prices lower, shake confidence, and lead to systemic failure across the platform.

Step 1: A Sharp Price Drop Triggers Liquidations

The process begins with a sharp decline in the value of a major collateral asset, such as ETH. Because Compound requires borrowers to maintain a fixed collateral ratio, any price movement that causes that ratio to fall below the threshold automatically triggers liquidation. Using the example mentioned earlier, assuming a 75% collateral factor, if someone deposits $15,000 worth of ETH to borrow $10,000 USDC, and the total value of their ETH drops to below $13333.33, the smart contract will then automatically liquidate a portion of their collateral to repay the loan.

Step 2: Collateral Floods the Market

These liquidations are not isolated. In a downturn, many users are holding ETH or other volatile tokens as collateral. As price drops trigger mass liquidations, the protocol dumps large amounts of ETH onto the open market at once. This selling pressure further drives down the price of ETH, which causes even more loans to fall below collateralization

[7] As of early 2024, ETH's 30-day realized volatility has often exceeded 60%, far higher than most traditional assets like U.S. equities (15–20%).

thresholds, creating a feedback loop. With each round of liquidations, the market becomes more fragile, and price declines accelerate.

This risk is further amplified by the widespread use of leverage within Compound's ecosystem. Many users don't just borrow to spend — they recycle borrowed funds back into the platform to farm COMP rewards or amplify their exposure to crypto assets. For instance, a user might supply collateral, borrow ETH, and immediately reinvest it to earn more yield, effectively leveraging their position multiple times. While profitable in stable markets, this behavior drastically increases the system's fragility. In a downturn, even a small drop in asset prices can trigger liquidations across several layers of leveraged positions. When users are highly leveraged and chasing yield incentives, they are more likely to panic-sell or mass-liquidate when volatility hits, accelerating the liquidity crunch and deepening the contagion risk. Leverage doesn't just increase individual exposure—it creates a network-wide feedback loop, where one user's liquidation can cascade across the protocol, threatening its overall solvency.

This dynamic is worsened by the Lemon Problem, which concentrates the riskiest borrowers on the platform. As safer participants exit in search of better terms elsewhere, Compound is left with highly leveraged, high-risk users who are the first to collapse in a downturn, magnifying the severity of liquidation cascades and systemic instability.

Step 3: Lenders Start Taking Losses

In theory, liquidators buy collateral at a discount to repay a borrower's loan and pocket the difference, creating an arbitrage opportunity that helps maintain the protocol's solvency. Per our example, if a user borrows $10,000 in USDC backed by $15,000 worth of ETH, and the price of ETH drops—bringing the collateral value below the safe threshold say $13,000—a liquidator can repay part or all of the loan and receive ETH worth slightly more than what they paid, such as $10,200. This extra $200 is the liquidation incentive, and the $2,800 would go back to the borrower. This profit incentive ensures that liquidators act quickly to prevent undercollateralized positions from causing losses. However, in fast-moving crashes, the price of collateral like ETH can plummet before liquidators can react. If ETH drops rapidly enough, the protocol may not be able to liquidate assets in time to fully cover loan balances. In such cases, the ETH may sell for far less than the remaining debt, leaving the lending pool with a shortfall—also known as bad debt. For example, if a user owes $10,000 and the value of their ETH collateral suddenly falls to $9,000, liquidators have no incentive to step in. Since repaying the loan

would only earn them $9,000 in ETH—less than the $10,000 they spend—executing the trade would be unprofitable. As a result, liquidations may not occur, and the protocol is left absorbing the loss. This ultimately impacts lenders, who were led to believe their deposits were protected due to overcollateralization but may find their funds partially unrecoverable during market-wide liquidation spirals (contagion risk).

Step 4: Borrowers and Lenders Panic (Liquidity Crisis)

As the protocol begins to absorb losses and confidence deteriorates, rational actors on both sides panic. Borrowers scramble to repay loans before their positions are liquidated, sometimes buying back crypto at unfavorable prices. Simultaneously, lenders rush to withdraw their funds, fearing the lending pool will become insolvent or frozen. This creates a liquidity crunch where capital leaves the system faster than it can be replenished, potentially forcing Compound to pause operations or enter governance discussions to stabilize the protocol.

Historical Example: MBS Crisis – 2008

A more apt analogy may be the 2008 mortgage-backed securities (MBS) crisis. Like Compound, the MBS market was built on the assumption that collateralized loans—in that case, home mortgages—were inherently safe as long as they were overcollateralized. However, when housing prices fell across the entire US, all at the same time, the value of the collateral eroded faster than the system could react. Liquidity vanished, defaults soared, and investors who believed they were protected by structural safeguards faced massive losses. Similarly, Compound assumes that excess crypto collateral and automated liquidation will prevent lender losses — but this logic fails in the face of sharp, systemic price declines. In both cases, overreliance on collateral creates a false sense of security and underestimates the effects of contagion and feedback loops in stressed markets.

Historical Example: Terra-Luna Collapse 2022

Another relevant example is the collapse of the Terra-Luna ecosystem in 2022. Terra's algorithmic stablecoin, UST, relied on a circular collateral model where value was supposedly maintained through a mint-and-burn mechanism with its sister token, Luna. Like Compound, the system promised automated, collateral-driven stability — but without real, external assets backing it, the platform was structurally fragile. When confidence faltered and redemptions spiked, the feedback loop between UST and Luna

triggered a death spiral. Luna's value plummeted, UST lost its peg[8], and the entire system unraveled in a matter of days. This mirrors the risk in collateral-based DeFi platforms: the belief that code and collateral alone can ensure stability ignores behavioral panic, reflexivity, and systemic interdependence. Terra proved that algorithmic or overcollateralized stability mechanisms can amplify, rather than absorb, shocks (Rai, 2022).

Other Platforms

Feature	Compound (COMP)	Aave (AAVE)	Maple Finance (MPL)	Morpho
Collateral-Based Lending	☑ Yes (Overcollateralized)	☑ Yes (Overcollateralized)	✗ No (Undercollateralized for institutions)	☑ Yes (Overcollateralized, layered on Compound/Aave)
Risk-Based Interest Rates	✗ No	☑ Partially (Aave V3 tiers)	☑ Yes (Creditworthiness assessed)	✗ No
On-Chain Credit Scoring	✗ No	✗ No	☑ Yes (Off-chain underwriting)	✗ No
Reputation-Based Borrowing	✗ No	✗ No	☑ Yes (Institutions only)	✗ No
Dynamic Collateralization	✗ No (Fixed levels)	☑ Yes (Isolated markets)	☑ Yes (Based on risk)	✗ No (Inherits Aave/Compound levels)
Insurance or Risk Pooling	✗ No	☑ Partially (Aave Safety Module)	☑ Yes (Insurance pools)	✗ No
Safety Module	✗ No	☑ Yes (Staked AAVE slashing)	✗ No	✗ No
Capital Buffer	✗ No	✗ No	☑ Yes (Protocol treasury buffer)	✗ No
Rate Optimization	✗ No	✗ No	☑ Yes (Protocol treasury buffer)	☑ Yes (Peer-to-peer matching)

Source: (Maple Finance, 2021), (Lesuisse & Morpho Labs, 2022), (Aave, 2020), (Lesniewski & Hayes, 2019)

Other decentralized lending protocols use different mechanisms to protect lenders from losses during market downturns or loan defaults. A Safety Module, such as the one used by Aave, is funded by users who stake tokens (e.g., AAVE) in exchange for yield, typically 4–10% APY. In a shortfall event, up to 30% of these staked assets can be slashed to cover bad debt. For example, if Aave has $500 million staked and suffers a $100 million shortfall, the protocol can slash enough tokens to repay lenders in full. Essentially, stakers[9] are selling a credit default swap[10] contract to the protocol—earning yield during stable conditions in exchange for absorbing risk during times of distress (Aave, 2020).

[8] A peg refers to the fixed exchange rate a stablecoin aims to maintain, typically $1 USD. When a coin "loses its peg," it deviates significantly from that target.

[9] Stakers are users who deposit (or "stake") their tokens into a protocol to support its security or financial stability. In return, they earn yield, but they also accept the risk of partial loss if the protocol experiences a shortfall or default event.

[10] A credit default swap (CDS) is a financial derivative that allows one party to insure another against the risk of default on a debt instrument. In DeFi, stakers in safety modules take on a similar function by agreeing to absorb losses in exchange for periodic returns, effectively acting as decentralized risk insurers.

An Insurance Fund, on the other hand, is typically protocol-funded using fees or treasury reserves. If Maple Finance maintains a $20 million insurance fund and a borrower defaults on a $10 million loan with only $7 million recovered through liquidation, the fund absorbs the $3 million shortfall without impacting user funds. Insurance funds are usually capped and may not cover system-wide losses—they're useful but limited in scope (Maple Finance, 2021).

A Capital Buffer operates similarly but is more passive—an internal pool of protocol-owned assets reserved to absorb losses. If Compound had a $25 million buffer and faced a $4 million bad debt event, the buffer would cover it, and lender funds would remain untouched.

Compounds Weaknesses

However, it is ultimately unfeasible for Compound to implement any of these stopgap solutions effectively. If Compound were to implement a Safety Module, it would still face the lemon problem—borrowers are not screened for creditworthiness, so the protocol cannot prevent high-risk users from dominating the platform. This makes it more likely that stakers would eventually be slashed, reducing the appeal of staking and discouraging participation. Meanwhile, building an insurance fund or capital buffer would likely require raising protocol fees or redirecting yield, making borrowing more expensive and potentially driving users to cheaper competitors who use on-chain credit scoring. In all cases, these mechanisms come at a substantial cost, and without borrower differentiation, Compound's flat-rate, permissionless model remains especially vulnerable to systemic risk without these stopgaps.

Counterarguments and Their Weaknesses

"Other Reputation-Based Models Have Also Failed"

Critics of undercollateralized or reputation-based lending often point to failed or struggling DeFi platforms like Goldfinch or TrueFi as evidence that credit-based models simply don't work. They argue that if those systems failed, Compound's model is justified in avoiding them (Castillo, 2023; Sandor, 2022).

While it's true that many early experiments in reputation-based DeFi lending have struggled, this argument is a form of false equivalence. The fact that others have not yet succeeded doesn't mean Compound's model is working—it simply means innovation in this area is still ongoing. Credit scoring, reputation staking, and off-chain underwriting

are still developing, and dismissing them now is like dismissing early attempts at online banking because early apps were clunky. More importantly, Compound hasn't tried to solve borrower differentiation. Its refusal to assess borrower risk isn't a limitation of blockchain—it's a design choice. Failing to experiment doesn't count as a safer model; it just locks Compound into the status quo of capital-based access.

"Compound Has Proven Resilient in Market Crashes"

Finally, some argue that Compound has already survived significant market volatility—including the March 2020 crash, the May 2022 Terra collapse, and other periods of high volatility—suggesting that the protocol is inherently resilient and well-designed.

It's true that Compound has not collapsed during prior market events. However, that doesn't prove the model is structurally sound—it may simply reflect that conditions happened to favor the protocol at the time. In several cases, Compound relied on the quick response of independent liquidators to prevent systemic damage. But this assumes that liquidators will always be present, that liquidity will always be available, and that markets will always move slowly enough for automated systems to react. None of those are guaranteed in future black swan events. Without an insurance fund, capital buffer, or safety module, Compound's model remains acutely exposed to the kind of cascade failure that has taken down other protocols. Its resilience may be less about design and more about luck. Assuming the protocol will always hold because it hasn't broken yet is not resilience — it's survivorship bias[11].

Misconceptions

"Overcollateralization Prevents Risky Borrowing"

A common defense of Compound is that overcollateralization protects against defaults by requiring borrowers to lock up more value than they borrow. While this appears safe, it creates a false sense of security. The model doesn't assess borrower risk—it simply demands wealth up front, excluding the underbanked and failing to address systemic risk. Even worse, in volatile markets—like March 2020, the 2008 housing crisis, or Terra's 2022 collapse—even overcollateralized loans can fall below liquidation thresholds before protocols react, resulting in losses.

[11] Survivorship bias occurs when we focus only on entities that have "survived" a selection process, ignoring those that failed. It can lead to incorrect conclusions about resilience or success.

"Algorithmic Interest Rates Reflect Risk"

Unlike traditional finance, where risk-based pricing is central to underwriting, Compound's model uses supply and demand mechanics for each asset pool — not borrower behavior. This means it prices liquidity scarcity, not creditworthiness.

Permissionless = Inclusive

DeFi protocols like Compound are often praised for being permissionless, meaning anyone can access them without approval. But open access doesn't equal true inclusion. If borrowing requires substantial collateral, only those who already hold wealth can participate. The undercollateralized—often the financially excluded—remain locked out. So while the system is open, it's not accessible to those who need it most.

Conclusion: DeFi's Promise and Its Pitfalls

This paper set out to answer a central question: Can Compound truly expand access to credit and solve financial exclusion, or does it simply reproduce the same barriers under a decentralized framework? After examining its architecture, incentive design, and risk management limitations, the answer appears clear. While Compound removes some of the gatekeeping found in traditional finance—such as identity checks and credit scores—its reliance on overcollateralization and lack of credit assessment ultimately recreate the same structural exclusions. Those without assets remain locked out, and those who borrow face substantial systemic risks, including liquidation spirals and market contagion. Without addressing core issues like asymmetric information and borrower differentiation, Compound risks systemic instability despite its transparent and permissionless design.

Looking forward, the future of DeFi lending will likely depend on more sophisticated tools—such as on-chain credit scoring, risk-tiered lending, and protocol-level protections—to foster true financial inclusion without compromising sustainability. However, it's also important to recognize that financial systems alone cannot solve wealth inequality. Like many inequality challenges, meaningful solutions require public-sector action—such as low-rate government loans, targeted fiscal policies, and structural reforms. Financial institutions, whether traditional banks or decentralized protocols like Compound, were never designed to address these broader societal gaps. Crypto may offer new tools, but without thoughtful innovation and policy alignment, it may only replicate the same systems it aims to disrupt.

Sources

Aave. (2020). Aave protocol whitepaper v1.0. https://github.com/aave/protocol-v1/blob/master/Aave_Protocol_Whitepaper_v1_0.pdf

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. The Quarterly Journal of Economics, 84(3), 488–500. https://doi.org/10.2307/1879431

Campbell, J. Y. (2006). Household finance. Journal of Finance, 61(4), 1553–1604. https://doi.org/10.1111/j.1540-6261.2006.00883.x

Castillo, M. (2023, October 19). Real-world asset loan worth $20M at risk of losing $7M on DeFi platform Goldfinch. CoinDesk. https://www.coindesk.com/markets/2023/10/19/real-world-asset-loan-worth-20m-at-risk-of-losing-7m-on-defi-platform-goldfinch/

Compound Governance Forum. (n.d.). https://www.comp.xyz

Compound Labs. (n.d.). Compound documentation. https://docs.compound.finance

Compound Labs. (2025). WETH Market on Compound Finance (Mainnet). https://app.compound.finance/markets/weth-mainnet

DeFiLlama. (2025). Compound Total Value Locked (TVL) Chart. https://defillama.com/protocol/compound

Lesniewski, G., & Hayes, R. (2019). Compound: The Money Market Protocol (White Paper). Compound Labs. https://compound.finance/documents/Compound.Whitepaper.pdf

Lesuisse, P., & Morpho Labs. (2022). Morpho: Hybridizing P2P and Pool-based lending. https://docs.morpho.org/pdf/morpho-whitepaper.pdf

Long, K. (2022, December 22). Crypto's horrible, no good, very bad year. Investopedia. https://www.investopedia.com/cryptos-horrible-no-good-very-bad-year-6835076

Maple Finance. (2021). Maple protocol whitepaper v1.0. https://maplefinance.gitbook.io/docs/resources/maple-whitepaper-v1.0

OpenAI. (2025). ChatGPT (April 2025 version) [Large language model]. https://chat.openai.com (Used to improve sentence structure, clarify arguments, and test the core thesis against counterarguments)

Rai, R. (2022, May 17). The death spiral: How Terra's algorithmic stablecoin came crashing down. Forbes. https://www.forbes.com/sites/rahulrai/2022/05/17/the-death-spiral-how-terras-algorithmic-stablecoin-came-crashing-down/

Sandor, K. (2022, November 2). Lending protocol TrueFi issues notice of default to Invictus Capital for failing to repay loan. CoinDesk. https://www.coindesk.com/markets/2022/11/02/lending-protocol-truefi-issues-notice-of-default-to-invictus-capital-for-failing-to-repay-loan/

Band Protocol's Future Outlook in the Oracle Space

By: Will Heuer and Brady Moll

We examine the value of oracle platforms in the decentralized finance space. We focus on Band Protocol and its largest competitor Chainlink. Our analysis identifies where Band Protocol will be most effective in competing with Chainlink. Band Protocol is superior to Chainlink when speed, cost, and long-term scalability are more important than breadth of data accessibility such as in the areas of high frequency transactions, instant data feeds for gaming platforms, and specialized data pulls that require efficiency.

We used ChatGPT to support the development of the essay by generating citations in MLA format, refining sentence structure, and aiding in the cohesion of ideas.

Background on Oracles

Toshendra Sharma from Blockchain Council explains the importance of an oracle by saying, “As smart contracts cannot access data from outside their network, they need access to information from the outside world. Blockchain oracles are the services that send and verify real-world occurrences and submit information to smart contracts, triggering state changes on the blockchain” (Sharma). Thus, an oracle serves as the connection between on-chain code and off-chain reality. Blockchains and smart contracts by themselves cannot access data like market prices, weather information, or random numbers due to their isolated and deterministic nature. Oracles solve this by feeding external data into blockchain environments in a secure manner, enabling a much wider range of decentralized applications.

Oracles have become very important in DeFi because they can greatly increase the power of smart contracts which allows further progression of decentralized finance. Many lending and trading protocols, such as MakerDAO, Aave, and Compound, rely on oracles for asset prices. For example, a lending smart contract needs the up-to-date price of collateral (like ETH or BTC) to know when to trigger liquidation. Oracles provide these price feeds by collecting data from multiple exchanges and sources, ensuring the contract uses an accurate price (Liu et al.).

Another massive use case for oracles is within blockchain gaming and for NFTs. The Blockchains need oracles to supply verifiable random numbers to ensure fairness. For instance, in many games there are mystery boxes which need to be randomized to ensure the integrity of the game. Oracles like Chainlink VRF (Verifiable Random Function) deliver randomness that is unpredictable and fair, which has been used in high-profile projects such as the Bored Ape Yacht Club (Chainlink). This use of oracles for randomness ensures games and NFT drops cannot be rigged by insiders or miners (BlockPegnio Insights).

Oracles can also enable interoperability between different blockchains, which is a need in a multi-chain DeFi ecosystem. An oracle has the capability to send data to other blockchains based on the formation of its layer 1 network. Cross-chain oracles thus help coordinate actions in multichain deployments (Cryptopedia Staff). Band Protocol for example, utilizes Cosmos' IBC to be blockchain-agnostic and serve data to many different blockchains (Band Protocol).

In summary, oracles allow decentralized apps connection with the real world. They enable smart contract innovation by providing external data that can't be accessed by on-chain code. Without oracles, decentralized applications would be limited to on-chain data, which would severely limit use cases. With oracles, however, blockchains can host complex financial instruments, games, interoperable tokens, and more. This can all be done while maintaining the security and automation of smart contracts.

The Oracle Problem

Relying on oracles introduces what researchers call the oracle problem: how can we trust that the external data fed into a blockchain is accurate and not tampered with? If an oracle is centralized or compromised, it becomes a single point of failure that can undermine the security of the entire smart contract (DuPont). One of the main features of the blockchain is that it tries to remove trust intermediaries, but if a single oracle is feeding data, then we have added an intermediary. Centralized oracles pose serious risks, a malicious or incorrect data feed can trigger wrong contract outcomes, leading to financial loss or system failure (Teex.).

One famous example of this risk was the bZx exploit in 2020, where a DeFi lending platform was attacked because it used a single-source price oracle. The attacker took out a complex flash loan and manipulated the price of an asset on a decentralized exchange; bZx's smart contract was reading that DEX price (via an oracle) as the "true" price.

Because bZx relied on one data source for prices, the manipulated price was accepted, enabling the attacker to profit about $1 million (Immune Bytes.). This incident showed that even a perfectly coded smart contract can be undone by a flawed oracle input.

More recently, oracle manipulations have become a common attack method in DeFi. In 2022 alone, over $400 million was stolen from various DeFi protocols through oracle manipulation attacks, in at least 41 separate incidents (Chainalysis). In these attacks, manipulators don't break the smart contract code itself but instead trick the oracle or exploit its design. The October 2022 Mango Markets exploit on Solana involved an attacker pumping the price of Mango's thinly traded token and using that inflated price (accepted by Mango's oracle) to borrow against, ultimately draining about $117 million (Chainalysis).

The solution to the oracle problem is to make data feeds as trustless and reliable as the blockchains themselves. This is why a major focus for modern oracles is decentralization as well as ensuring a secure design (Techround). Instead of one source, decentralized oracles can gather data from many independent providers, so that no single source could possibly falsify the outcome. They will also often incorporate cryptographic proofs or economic incentives to ensure honesty (Garcia).

In summary, trustless data feeds matter because the ecosystem of execution of smart contracts using off-chain data is reliant on accurate data. The "oracle problem" reminds us that decentralization must extend beyond the blockchain itself to the data coming in. Ensuring oracles are decentralized and tamper-resistant is critical to avoid repeats of the costly hacks and exploits that have plagued DeFi when oracles failed.

Background on Chainlink

Chainlink is the pioneering decentralized oracle network on Ethereum and remains the most widely adopted oracle solution in the blockchain ecosystem (Chainlink). Launched in 2017 by Sergey Nazarov and team, Chainlink introduced a framework where many independent oracle nodes deliver data to smart contracts, rather than a single trusted source.

At its core, Chainlink is a network of independent node operators that seek out external data and then feed it to the on-chain contracts which consume the information. First, when a smart contract needs data, it emits a request, and the Chainlink protocol creates a Service Level Agreement (SLA) for that job (Chainlink). Secondly, This SLA in the Chainlink system generates several on-chain contracts, the most important of which being, a Reputation Contract, an Order-Matching Contract, and an Aggregating Contract. The reputation contract checks the track record of oracle nodes and filters out unreliable ones. The order-matching contract then selects a set of available oracle nodes to fulfill the request. Each selected Chainlink node calls the appropriate external API or data source and returns the result to the blockchain. The aggregating contract then collects all the responses from multiple nodes and calculates a single result, often by taking a median or consensus of the values reported (Chainlink).

Chainlink's economic model is powered by the LINK token. LINK is an ERC-20 token used to pay node operators for their services on the network (Chainlink). When a contract requests data, it pays LINK as a reward to the oracles providing the data. Chainlink node operators thus earn LINK for delivering accurate data. Additionally, Chainlink introduced a staking mechanism in 2022—node operators and community members can stake LINK as collateral, which can be slashed if an oracle provides false data (Chainlink).

Chainlink's primary strength is its proven security and broad adoption. It has been the industry-standard oracle for years, trusted by a vast number of projects. By 2024, Chainlink was securing over $9 trillion in transaction value (Chainlink). Virtually all major DeFi platforms on Ethereum, and many other chains, have integrated Chainlink price feeds or data services. The system's design—multiple independent nodes plus aggregation contract—and continuous upgrades, such as off-chain reporting, have solidified its reputation.

Despite its success, Chainlink faces limitations, particularly around cost and speed due to its Ethereum roots. Each oracle update is an Ethereum transaction, which can become expensive during high congestion. A single Chainlink data request in 2020 could cost hundreds of dollars in gas fees (Band Protocol). Chainlink has addressed this with off-chain aggregation and threshold signatures to batch reports and reduce on-chain load. However, Chainlink's Ethereum-based model is not ideal for high-frequency or high-speed applications.

In short, Chainlink's secure but resource-intensive architecture leads to top-tier data quality at a premium cost. This creates an opening for other oracle networks that prioritize speed and efficiency.

Background on Band Protocol

Band Protocol is a decentralized oracle platform that has emerged as one of the main alternatives to Chainlink. Initially launched on Ethereum, Band migrated to its own blockchain built on Cosmos to prioritize scalability and cross-chain capabilities (Band Protocol). Today, Band operates via BandChain, a dedicated blockchain for oracle data, which uses the Cosmos SDK and Tendermint BFT consensus (Band Protocol).

BandChain runs on a Delegated Proof of Stake (DPoS) model with a set of validators who perform dual roles: maintaining the blockchain and fulfilling oracle data requests. When

a user makes a data request, an oracle script on BandChain specifies which data sources to search through and how to aggregate the results. The protocol then selects a subset of validators to handle the request. These validators fetch data from external sources, report it on BandChain, and aggregate it into a result. The result can be relayed to the requesting blockchain with cryptographic proof of authenticity (Band Protocol).

A key aspect of Band's approach is cross-chain interoperability. By building on Cosmos, Band can use the Inter-Blockchain Communication (IBC) protocol to deliver data to other Cosmos-based chains. For non-Cosmos chains like Ethereum or BNB Chain, Band uses bridges or light clients. This blockchain-agnostic model allows Band to serve any public blockchain with oracle data (Band Protocol).

The BAND token is used for staking and fees. Validators and delegators stake BAND to secure the network and earn rewards. If validators misbehave, they can be slashed. Band also supports premium data feeds by allowing data providers to host APIs and charge for access, expanding the range of available data (Band Protocol Whitepaper).

Band's main strengths are speed, cost-efficiency, and scalability. By moving oracle computation to its own high-throughput chain, Band processes requests faster and at lower cost than Ethereum-based solutions. Band's architecture allows it to query any API and deliver responses in seconds. This makes Band well-suited for applications where speed and cost are paramount (Band Protocol Marketing).

However, Band has not yet achieved Chainlink's level of adoption or security record. While Chainlink is used by major DeFi protocols, Band's usage is smaller. Band's validator set is limited to 100 nodes, and for non-Cosmos chains, data is relayed through bridges that may introduce trust assumptions. Additionally, Band's community and ecosystem are smaller than Chainlink's, which could affect long-term network effects and resilience (SmartContent).

In conclusion, Band Protocol offers a compelling alternative for scenarios where speed and efficiency are essential. Its Cosmos-based design and blockchain-agnostic model make it a strong candidate for the future of multichain DeFi.

Band Protocol's Superior Role in Speed, Cost, and Long-Term Scalability

Band Protocol Active Deployments Within Cutting Edge Technology

As the decentralized finance ecosystem expands, scalability, both in terms of technical throughput and cross-chain reach, has emerged as a critical differentiator among oracle providers. Band Protocol has positioned itself at the forefront of this shift through its recent strategic integrations and innovations in infrastructure. In late 2023, Band became the first decentralized oracle solution to launch on the XRP Ledger (XRPL), providing real-time price feeds for assets such as XRP, BTC, and ETH on both the XRPL mainnet and its Ethereum Virtual Machine (EVM) sidechain (Band Protocol Marketing). This partnership can be viewed as something that is only going to further establish Band Protocol as a serious player in the oracle space. By XRP being positioned as a business solutions provider in helping global transactions eliminate exchange fees, Band Protocol's feeds can help solve problems both in automatic trading platforms and other applications that depend on real time data. This can continue to be an opportunity beyond XRP as businesses being satisfied with what Band Protocol has created can encourage continued relationships beyond the involvement of XRP.

The biggest development as of late for Band Protocol is its partnership with Monad which seeks to be a high throughput, low latency layer 1 blockchain (Band Protocol Marketing). Monad is both faster and more scalable than Ethereum (Monad). By Band being the oracle for Monad, it opens the door for high-speed protocols such as lending platforms, high frequency trading, prediction markets, and real-world assets on Monad. This development further solidifies the belief in Band being a go-to provider for quick data

feeds while working with companies aiming to change the space of blockchain technology as we know it.

These real-world deployments serve as concrete examples of Band Protocol's commitment to extending its reach while maintaining the fast, low-cost characteristics that are increasingly demanded by high-volume DeFi applications. Having instant feeds that are accurate can be crucial to various business ventures as analyzing markets and identifying opportunities has become increasingly difficult with the increase in technological advancements to identify optimal prices.

Technical Aspects Elevating Band Protocol's Viability

Band Protocol's technical architecture is deliberately optimized for interoperability and speed. Built using the Cosmos SDK, BandChain utilizes Delegated Proof-of-Stake (DPoS) to efficiently validate data with relatively low computational cost and latency compared to its competitor Chainlink. This approach allows Band to finalize data quickly and push it to external blockchains without congesting the network, a clear advantage in situations where gas fees and block confirmation times must be minimized (Binance Academy). Furthermore, the Cosmos SDK and Inter-Blockchain Communication (IBC) protocol give Band the ability to operate natively across numerous chains—including Ethereum, Binance Smart Chain, Solana, Avalanche, and Polkadot—positioning it as a truly multi-chain oracle solution (Band Protocol Marketing). This makes Band uniquely capable of delivering its services to a wide array of applications, from established DeFi platforms to emerging multi-chain protocols with fast processing capabilities compared to Chainlink. This helps Band in the long term of being able to operate sufficiently without worrying about how they will continue to process large amounts of transactions as more users adopt their system. This long-term scalability is important in creating any DeFi product for it to be a viable solution down the line.

Many DeFi platforms depend on accurate and timely price updates, especially in high-frequency environments such as trading, derivatives, and synthetic asset markets. Traditional oracle models, which often rely on Ethereum's base layer, can be bottlenecked by slow block times and prohibitively high gas fees (Lithium Digital). These issues become especially acute when market volatility demands constant rebalancing and recalculations of collateral or asset prices. Band sidesteps these constraints by offloading computation to BandChain and pushing only the final results on-chain, significantly reducing time-to-finality and transaction costs (Band Protocol Marketing). This is why Band is increasingly appealing to developers looking for streamlined, responsive oracle solutions that can operate across several blockchain environments without sacrificing performance.

Band's design also facilitates user-defined customization in ways that many competitors cannot easily match. By using customizable oracle scripts written in WebAssembly, developers can specify exactly what data to retrieve, from which sources, and how to aggregate it (Band Protocol Marketing). This level of control is particularly useful for businesses that need specific, non-standardized data feed, such as weather inputs for agricultural insurance contracts or location data for supply chain smart contracts. (Lithium Digital). Because the scripts are executed on BandChain, they benefit from the same low-latency, high-throughput environment that defines Band's broader ecosystem. In contrast to more rigid oracle solutions that offer only pre-selected feeds, Band provides the flexibility to scale with business demands as they grow more complex and global.

Ultimately, Band's cross-chain operability, customizable architecture, and ability to deliver fast and inexpensive data feeds enable it to scale alongside DeFi's most dynamic applications. As more projects look to expand across chains, either to capture new user bases or to avoid the bottlenecks associated with Ethereum, Band's design makes it a prominent player in areas like trading, derivatives, and gaming where speed is essential.

Chainlink's Superior Aspects That Pose Challenges to Band Protocol

Despite its technical advantages and growing partnerships, Band Protocol still faces meaningful challenges as it tries to expand its market share in a space dominated by Chainlink and increasingly competitive upstarts. Chainlink, the first major oracle project in the space, has built a massive network effect by integrating with over 17 blockchains, securing tens of billions of dollars in smart contract value, and developing a suite of services such as Chainlink Keepers and Verifiable Random Functions (Metana Editorial). The Chainlink brand has become nearly synonymous with blockchain data infrastructure, making it difficult for newcomers to attract developers or institutional interest, regardless of performance metrics.

Just as Ethereum is often chosen for DeFi development because it is familiar and well-supported, Chainlink is often selected not because it is the fastest or cheapest but because it is the most established. Band must work twice as hard to not only demonstrate its technical edge in areas like speed and cost but also to overcome this psychological barrier within the developer community (Binance Academy). Until Band can achieve deeper integrations with widely used DeFi protocols or become the oracle-of-choice for a breakout new application, it will likely remain in Chainlink's shadow despite its advantages in speed and scalability.

Additionally, Chainlink can access nonpublic API's compared to Band which uses public API's for data pulls (SmartContent). These private API's store data that can be confidential and not intended for public disclosure (3pillar). This can be useful for projects requiring that information to be put on chain and thus allowing for more data sources to be accessed by Chainlink. These challenges for Band and the gap that exists between the two can continue to be tightened with increased partnerships with cutting-edge high-performance platforms. Band staying true to their roots of speed and flexibility as an oracle network, should continue to make big splashes with projects such as Monad.

This will allow Band to continue to create opportunities for themselves to expand into various use applications that primarily relate to their original strength which are the live price feeds and prediction markets.

Finally, the crypto space is one of rapid change. Even the best protocols can be upended by new innovations or shifts in user preference. Layer-2 networks like Arbitrum and Optimism are already challenging the need for fast data on layer-1s by offering cheaper and faster execution environments (Cyrpto News). If Band is slow to support these platforms or fails to adapt to their technical peculiarities, it risks missing out on the fastest-growing areas of DeFi. Band will need to execute successful partnerships at a greater rate than Chainlink while not neglecting continuous improvements to its own protocol in order to truly catch up to the Chainlink status as a very trusted player in the space.

The Outlook for Specialized Oracle Use Cases

While Band faces a daunting competitive landscape, there is strong evidence to suggest that the oracle space will not be winner-take-all. Instead, the market will likely fragment based on use-case specialization, creating space for multiple successful providers that excel in different dimensions. In this emerging environment, Band Protocol is well-positioned to become the go-to solution for applications that prioritize speed, cost-efficiency, and long-term scalability.

In DeFi, the needs of a prediction market will differ dramatically from those of a lending platform or synthetic asset protocol. Chainlink may remain dominant in high-value financial applications where reputational trust, decentralization, and high-quality data aggregation are paramount. With the ability to access more broad data sources than Band, it can be better suited for complex projects that may not need the speed to be at the fastest processing capability in order for it to be successful (SmartContent). Band Protocol’s low-

cost, high-speed model is much better suited to trading apps, games, decentralized exchanges, and financial services where smart contracts need to execute in near real-time and across multiple chains (Binance Academy). Just as Ethereum was created to rival the downfalls of Bitcoin in creating a platform that could handle complex transactions and go beyond the value of the coin, Band has the opportunity to become a large player in the areas that Chainlink falls short in which is providing the highest speed with a high level of compatibility.

There are already signs that this specialization is emerging. For example, in 2021 Band was selected to provide oracle data for Terra's Mirror Protocol, which required frequent, accurate pricing for synthetic assets representing U.S. equities. Chainlink was unavailable on Terra at the time, and Band filled that gap successfully (Band Protocol Marketing). More recently, Band's partnership with Celo on a Layer-2 DeFi testnet reflects a recognition that performance-focused platforms need data partners with similar priorities (McCall). In both cases, Band succeeded not because it was the largest or most established oracle, but because it was the right tool for the job. With Band being able to continue identifying use cases where platforms emphasize speed, low transaction fees and being scalable long term, they can continue to push specialization onward.

Looking forward, Band could also play a key role in cross-chain DeFi protocols and aggregators that need to manage data across multiple blockchains simultaneously. As protocols like THORChain, Osmosis, and Axelar push toward more fluid multi-chain environments, the need for oracles that can deliver consistent data across different networks will grow. Band's native interoperability via Cosmos and IBC is tailor-made for this role (Band Protocol Marketing). It has already demonstrated success on this front, but the potential for growth in this area is still enormous.

Conclusion

The oracle market in DeFi is no longer a single player environment dominated by Chainlink alone. As applications grow more diverse and performance-sensitive, the need for alternative oracle solutions has become evident. Band Protocol has emerged as a serious contender by focusing on speed, efficiency, multi-chain interoperability, and customizability—traits that are increasingly important in today's high-frequency, cross-chain DeFi environment. While Band still faces stiff competition and must overcome significant branding and network effects, it offers unique technical and architectural advantages that position it to lead in a specific and growing segment of the market. In a future where DeFi continues to prioritize speed and cost-effectiveness, Band Protocol is poised to become the go-to oracle solution for many of its most innovative and demanding use cases that emphasize reliance on speed, low cost, and long-term scalability for their data feeds.

Works Cited

Band Protocol. "BandChain." *Band Protocol*, bandprotocol.com/bandchain.

Band Protocol. "Band Protocol Documentation: Band Protocol." *Band Protocol Documentation | Band Protocol*, docs.bandchain.org/.

Band Protocol Marketing. "Band Protocol & XRP Ledger (XRPL): Band Protocol Integrating as the First Oracle Provider for XRPL." *Band Protocol Blog*, 1 Dec. 2023, blog.bandprotocol.com/bandprotocol-xrpledger-oracle-provider/.

Band Protocol Marketing. "Band Protocol 2021 Recap and Vision: Rapid Expansion, BandChain V3, and Beyond Oracle." *Band Protocol Blog*, 22 Apr. 2022, blog.bandprotocol.com/band-protocol-2021-recap-and-vision-rapid-expansion-bandchain-v3-and-beyond-oracle/.

Binance Academy. "What Is Band Protocol (BAND)?" *Binance Academy*, 14 Feb. 2024, academy.binance.com/en/articles/what-is-band-protocol-band.

BlockPegnio Insights. "Blockpegnio Integrates Chainlink's Oracles for on-Chain Verified Randomness in Game Interactions." *Medium*, BlockPegnio, 10 July 2020, medium.com/blockpegnio/blockpegnio-integrates-chainlinks-oracles-for-on-chain-verified-randomness-in-game-interactions-96cef98dcafb.

bZx Protocol Exploit – Sep 14, 2020 – Detailed Analysis. *ImmuneBytes*, 14 Sept. 2020, www.immunebytes.com/blog/bzx-protocol-exploit-detailed-analysis/.

Chainalysis Team. "Oracle Manipulation Attacks Are Rising: A Unique Concern for DeFi." *Chainalysis Blog*, 7 Mar. 2023, chainalysis.com/blog/oracle-manipulation-attacks-rising/.

Chainlink. "Chainlink: The Backbone of Blockchain." *Chainlink*, chain.link.

Coindar. "Band Protocol to Be Integrated With XRP Ledger." *TradingView News*, 13 Jan. 2025, tradingview.com/news/coindar:17fc5fa11094b:0-band-protocol-to-be-integrated-with-xrp-ledger/.

Crypto News. "Arbitrum and Optimism: Two Protocols Control 80% of All Ethereum Layer 2 TVL." *World News about Cryptocurrency and Blockchain Technology from Different Sources*, 25 Jan. 2023, cryptonews.net/news/blockchain/19785813/.

Cryptopedia Staff. "Band Protocol: Decentralized Finance (DEFI) Oracles." *Gemini*, www.gemini.com/cryptopedia/band-protocol-oracle-blockchain-defi-band-coin.

Dupont, Laurent. "What Is the Oracle Problem? How Morpher Overcomes It." *Morpher.Com*, morpher.com/blog/oracleproblem#:~:text=Blockchains%20are%20designed%20to%20be, known%20as%20the%20Oracle%20Problem.

Garcia, Mikel. "What Is a Blockchain Oracle? A Guide." *DIA*, 19 Oct. 2023, diadata.org/blog/post/what-is-blockchain-oracle/.

Lithium Digital. "Bridging the Gap: How Band Protocol Powers Blockchain Applications with Real-World Data." *Medium*, Lithium Digital, 19 Mar. 2025, medium.com/lithium-digital/bridging-the-gap-how-band-protocol-powers-blockchain-applications-with-real-world-data-d26b1549f2ee.

Liu, Bowen, et al. "A First Look into Defi Oracles." *arXiv.Org*, 25 June 2021, arxiv.org/abs/2005.04377.

Mccall, Isaiah. "Band Protocol and Celo Launch L2 Testnet for Scalable and Inclusive DeFi." *99Bitcoins*, 11 Dec. 2024, 99bitcoins.com/news/band-protocol-and-celo-launch-l2-testnet-for-scalable-and-inclusive-defi/.

Metana Editorial. "Top 6 Chainlink Alternatives for 2025." *Metana*, 4 Mar. 2025, metana.io/blog/top-6-chainlink-alternatives-for-2025/.

OAK Research. "Overview: Mapping Decentralized Oracle Protocols." *OAK Research*, 2024, oakresearch.io/en/analyses/fundamentals/overview-mapping-decentralized-oracle-protocols.

Sharma, Toshendra. *What Is a Blockchain Oracle? A Detailed Overview*, www.blockchain-council.org/blockchain/what-is-a-blockchain-oracle-a-detailed-overview/.

SmartContent. "Band Protocol and Chainlink: A Comparative Analysis." *Medium*, Medium, 8 Feb. 2021, smartcontentpublication.medium.com/a-comparative-analysis-of-band-protocol-and-chainlink-54b7d14823b5.

TechRound. "How Decentralised, Trustless Oracles Can Solve the 'Oracle Problem.'" *TechRound*, 24 Jan. 2025, techround.co.uk/cryptocurrency/how-decentralised-trustless-oracles-can-solve-oracle-problem/.

TEEX. "What Are Oracles? Smart Contracts, & 'The Oracle Problem.'" *Medium*, 2024, medium.com/@teex/what-are-oracles-smart-contracts-the-oracle-problem.

3Pillar. "Open vs. Closed Apis." *3Pillar*, 15 Aug. 2024, 3pillarglobal.com/insights/blog/open-vs-closed-apis/.

Ondo Finance and the Institutionalization of Real-World Asset Tokenization

By Alex Buchholz and Luke Hupfer

The convergence of blockchain technology with traditional finance is accelerating through the rise of tokenized Real-World Assets (RWAs), enabling regulated institutions to engage with decentralized infrastructure. This paper explores how Ondo Finance is emerging as a leading platform in this transformation by offering a permissioned, compliance-first blockchain ecosystem designed for institutional adoption. Through its proprietary Ondo Chain and core products such as OUSG (Ondo Short-Term US Government Treasurys: tokenized U.S. Treasuries), USDY (U.S. Dollar Yield Token), and Flux Finance (decentralized lending), Ondo enables 24/7, transparent, and secure access to yield-generating assets while maintaining regulatory compliance (Business Wire – Ondo Finance Unveils Integrated Infrastructure Suite to Bring US Financial Markets onto the Blockchain). Its unique validator structure, built-in Know-Your-Customer / Anti-Money Laundering (KYC/AML) protocols, and strategic partnerships with firms like BlackRock position Ondo as a trusted platform for large financial institutions who want exposure to the digital asset space. By prioritizing compliance, usability, and integration with existing TradFi (Traditional Finance) systems, Ondo offers a credible alternative to fully permissionless platforms and is poised to become the default infrastructure for institutional tokenized finance.

Introduction

In the evolution of blockchain technology, DeFi, RWAs, and the growth of institutional interest have been transforming the space. As financial institutions begin exploring blockchain-based systems, there is a growing demand for platforms that merge the programmability and transparency of DeFi with the regulatory structure of traditional finance. RWAs, such as tokenized Treasury bills, corporate bonds, or real estate, can bridge that gap, bringing institutional-grade investment products on-chain while maintaining the compliance standards necessary for regulated entities. Ondo Finance is at the forefront of this transformation. Unlike permissionless blockchains such as Ethereum, which cater primarily to retail users and decentralized experimentation, Ondo is deliberately tailored to institutional needs. **With its permissioned blockchain design, focus on selected financial use cases like tokenized RWAs, and commitment to regulatory compliance for large institutional investors (highlighted by their partnership with Blackrock), Ondo will become the largest institutional partner for TradFi organizations looking to move on-chain.**

Ondo's Structure

Ondo Finance operates through two key pillars: an asset management branch that creates tokenized products and a technology arm that builds decentralized protocols. The launch of Ondo Chain, its proprietary L1 blockchain, marks a strategic move toward creating a fully integrated system designed specifically for institutional investors. Most DeFi platforms (such as Ethereum-based apps), were built to be open and permissionless and only added compliance tools later if they felt the added security outweighed the loss of decentralization (Ethereum.org - Introduction to Ethereum Governance). On the other hand, Ondo Chain was built with compliance in mind from the beginning with features like KYC, regulatory controls, and permissioned access. Since these features were built into the core of the platform from the start, large institutional investors like Blackrock

have become interested, highlighted by their most recent partnership (Ondo Finance Blog – Building on BUIDL). Additionally, validators on the network are not anonymous actors incentivized by block rewards but instead are regulated asset managers, broker-dealers, and other institutional participants. Their activity is monitored, and front-running is proactively prevented through various safeguards (Ondo Finance Docs – Ondo Chain Overview)

Therefore, what differentiates Ondo from generalized blockchains is the combination of transparency, compliance, and usability. These regulatory frameworks add a level of credibility for Ondo, ultimately appealing to large institutional investors who are constantly under strict regulatory scrutiny. The chain also supports a variety of services such as cross-chain issuance, on-chain wealth management, staking, and brokerage services. Together, these tools create a platform that closely mirrors what institutional investors are accustomed to in traditional markets, but with the advantages of blockchain technology such as 24/7 access (Ondo Finance Docs – Ondo Chain FAQ).

Thesis Point 1 – RWAs on Platform

Ondo's growing suite of tokenized products is central to institutional adoption and positions the platform well as the leader in the RWA space. Each product is designed to incorporate blockchain technology without compromising compliance or regulatory standards. A popular offering is OUSG, which provides tokenized exposure to short-duration U.S. Treasuries. Built for institutional users, OUSG allows capital to be allocated into high-quality, low-risk government debt with 24/7 subscription and redemption via USDC (United States Dollar Coin) (Ondo – The Institutional Standard for Liquidity). This marks a significant improvement over traditional fixed-income instruments, which often involve settlement delays (T+1), intermediaries, and limited trading hours. OUSG is also designed to grow in value over time as the underlying Treasury ETF earns interest and

appreciates, allowing holders to passively earn yield over time (Ondo Finance Docs – OUSG Token Overview). This mimics traditional money market funds but operates on chain, removing inefficiencies like T+1 settlement and limited trading hours. As a result, OUSG offers a secure, liquid, and yield-generating asset while maintaining compliance which is crucial for institutional investors.

Ondo's USDY (United States Dollar Yield Token) is another major product (ReflexivityResearch.com). Unlike stablecoins such as USDC or Tether, which are fully reserved but non-yielding, USDY is backed by a combination of U.S. Treasuries, repos, and U.S. bank deposits, offering holders passive income through exposure to short-term and risk-free government securities (Llama Risk – Asset Overview – USDY). USDY is attractive for non-U.S. investors and institutions in emerging markets that face capital controls, limited access to USD-denominated assets, or tax complications. Through USDY, these investors can gain dollar exposure while earning yield within a blockchain format which allows for simplified cross-border investment and 24/7 liquidity.

Another key component of the Ondo ecosystem is Flux Finance which is a decentralized lending platform that allows institutional investors to borrow and lend using high-quality assets (Flux Finance.com). It allows users to lend stablecoins and borrow against permissioned and yield-bearing tokens like OUSG. Loans are overcollateralized and managed via smart contracts that enforce risk parameters (Flux Finance.com). Flux essentially brings the mechanics of traditional secured financing into a blockchain environment. This structure enhances capital efficiency for borrowers, provides yield opportunities for lenders, and ensures transparency through the enforcement of loan terms through smart contracts.

These products do more than simply bring RWAs on-chain. They are re-designing traditional financial functions, like saving and lending, in a way that's automated,

regulatory compliant, and available 24/7. Markets historically settled on physical transfer of securities, until the advent of the Internet, and electronic settlement allowed for consistent T+3 settlement (Investopedia: T+1 (T+2, T+3) Explained: Definitions and Settlement Example). This was increased to T+2 in 2017 to reduce counterparty risk after the Great Financial Crisis (GFC), and T+1 as recently as May 2024. Crypto exchanges and tokenized assets debuted at T+0 with immediate settlement, which has forced the Securities and Exchange Commission (SEC), and off-chain capital markets to accelerate their processes. Conversations have started to speed up TradFi settlement, particularly concerning UST at T+0, but corporate bonds, other fixed-income securities, and equities would likely take longer to transition. Institutions looking to gain access to the future of settlement can work with Ondo and trade established RWAs on chain with immediate clearing.

OUSG, USDY, and Flux Finance make up a strong foundation for institutional investors, offering regulatory-compliant alternatives to TradFi assets like money market funds, bank accounts, and loans. As demand builds for tokenized RWAs, Ondo's emphasis on regulation will give it an edge in attracting institutional investors, just as they did with Blackrock.

Thesis Point 2 – Permissioned Network

A key difference between Ondo and most blockchains, like Ethereum, is the idea that full decentralization is not always beneficial. While decentralization has brought major breakthroughs in openness and user control, it also introduces uncertainty and operational risk for institutional investors who are bound by strict regulations and fiduciary responsibilities to clients. The lack of clear accountability in decentralized systems, such as not knowing who is responsible if something goes wrong, can be a significant barrier. For institutional investors such as asset managers, this lack of clarity is a barrier, not a value proposition.

Ondo addresses these issues with a hybrid model. It retains the main benefits of blockchain (transparency, automation, and fast settlement), but also adds the additional regulatory controls institutional investors are used to. Validators on the Ondo Chain are screened and approved, ensuring the network is operated by known and trustworthy instructional-based entities. Applications must adhere to compliance standards, helping to avoid the unpredictability sometimes evident in fully open blockchain platforms (Ondo Blog -Introducing Ondo Chain: The Omnichain Network for RWAs). Assets are permissioned, meaning only verified participants can access certain financial products, in line with securities laws such as anti-money laundering rules and know-your-customer (KYC) standards (Ondo Finance Docs).

This model is attractive for institutional investors given they operate in a heavily regulated industry. That is, Ondo's structure enables financial institutions to adopt blockchain technology while still being exposed to similar regulatory oversight standards they must adhere to in traditional markets. This includes auditability, enforceability, and risk control which are generally difficult to guarantee on permissionless networks.

Beyond compliance, Ondo is designed to make it easier for institutions to enter and operate in the digital asset space. Instead of dealing with a mix of disconnected tools, like separate wallets, protocols, and custodians, Ondo offers an all-in-one platform (Ondo Blog: Introducing Ondo Chain: The Omnichain Network for RWAs). This creates a smooth and interconnected experience where institutions can move capital, invest, and manage risk more efficiently.

Additionally, collaborations with major players like Coinbase for custody, fiat on/off ramps, and KYC integration streamline the onboarding process. This helps address some key operational challenges such as asset safekeeping, regulatory reporting, and capital flows between fiat and crypto, bridging the gap between traditional finance and blockchain technology. This results in a scalable product that combines the regulatory compliance and trust required for decentralized finance to become mainstream for large intuitional investors.

Thesis Point 3 – Partnerships for Institutional Trust & Accessibility

Ondo has targeted its strategic partnerships to both DeFi and TradFi firms that will help establish credibility and trust in their platform, boosting the adoption of blockchain technology by established TradFi organizations looking to gain exposure to crypto and on-chain assets. Ondo has launched a wave of partnerships and collaborations recently to scale and secure their offerings. The Blockchain Trilemma, where crypto developers theoretically must pick two options from scalability, security, and decentralization, has presented a challenge for new offerings in the field (Binance Academy: What is the Blockchain Trilemma). Ondo is targeting scalability and security, which is appealing to institutions as it mirrors their current business model in existing TradFi. Sacrificing some decentralization for the sake of better compliance, regulatory monitoring, and quicker

ramping for large clients should allow them to convince larger institutions to join their platform. The table below details several recent partnerships that align with this strategy.

Partner	Product/Service	Reason for Collaboration
BlackRock	BUIDL: tokenized UST and other RWAs	Backing by the world's largest asset manager is a huge declaration of trust and adoption for blockchain, a positive signal to markets and other clients about the long-term staying power of Ondo and their offerings
Aptos Foundation	High-performance L1 chain with more customizable language	Boost adoption of USDY cross-chain and bring tokenized UST to new markets and investors
Hex Trust	Regulated custodian, multi-chain compliance	Institutional-grade custody and compliance for USDY and OUSG
Nonco	Crypto-native trading firm	Enhance USDY's market liquidity, price discovery, and trading efficiency cross-chain, deepen liquidity
Polygon Labs	Established dev. team for L2 infrastructure	Expand access to Ondo products cross-chain with an established institutional developer
Rakkar Digital	Institutional-grade custody in APAC	Increase geographic diversification of adoption, increase custody and security

(Table sourced from several press releases and blogs, broken out in sources on page 18)

Ondo's approach is analogous to the difference between renting cloud infrastructure and purchasing a fully managed SaaS platform. Institutions prefer the latter because it minimizes operational complexity and legal exposure. Its narrow focus on RWAs and institutional adoption may limit its appeal in the retail DeFi world, but it enhances its value proposition for its target audience.

Additionally, as institutional investors grow less cautious about on-chain exposure, demand will rise for secure, yield-generating assets in digital formats. Ondo's focus on short-duration government-backed securities positions it as an entry point for cautious institutions seeking familiar risk-return profiles in an on-chain environment. Large TradFi clients exploring crypto would prefer this business model, as well as the assets and products offered; government-backed, stable, and liquid securities are a logical first choice for on-chain RWAs.

Risks and Obstacles to Adoption

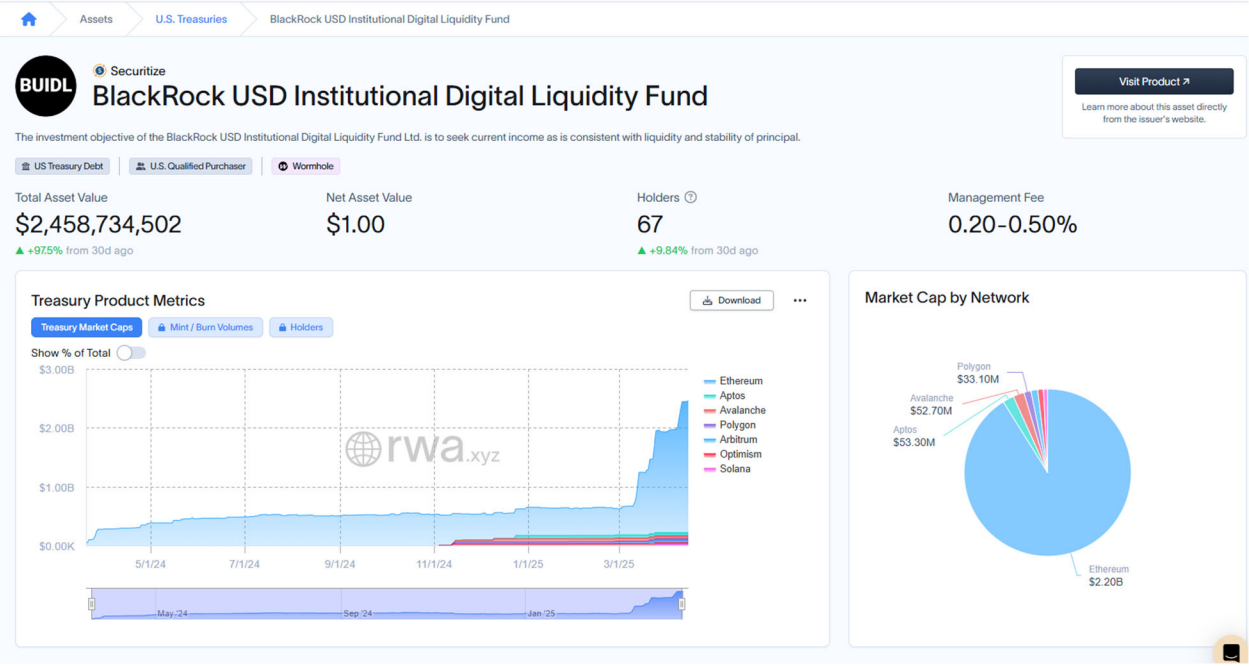
Regulatory uncertainty looms over the entire crypto ecosystem. While Ondo has structured its offerings under Reg D and Reg S exemptions and built-in strong compliance features, shifting laws could impact product availability or investor participation. The current Trump administration has been extremely vocal in their support of the crypto industry broadly, with plans to reduce regulation, encourage innovation, and even establish a government reserve of several tokens (AP News - Trump Tells Crypto Leaders at White House Summit He's Committed to Helping their Industry). However, the current administration has a track record of being fickle with frequent last-minute policy changes, adjustments, or cancellations. The uncertainty around tariffs has rattled markets, and with crypto being a more nascent field, it is likely to face the same policy whiplash.

In addition, smart contract risk is not trivial: despite regular audits, bugs and exploits remain a possibility, and any security breach could erode trust quickly (QuillAudits – Smart Contract Vulnerabilities, Risks and How to Mitigate Them). The largest crypto heist ever was committed in February, where North Korean hackers took advantage of a vulnerability in Bybit's third-party wallet system. Bybit is one of the world's largest crypto exchanges and is still a target for criminal activity (Wired – The Kings of the Crypto Heist). Another potential limitation is ecosystem maturity. Ethereum has a vast developer base, deep liquidity pools, and years of client transactions. Ondo will need time to build comparable depth, especially for applications beyond its core offerings. However, its institutional-first design may shield it from some of the early-stage growing pains experienced by more experimental DeFi platforms.

Tokenization is gaining legitimacy among regulators and financial institutions alike. Asset managers are exploring blockchain-based fund structures, and even central banks are piloting digital currencies. Against this backdrop, Ondo is well-positioned. Its integration of yield-bearing, real-world financial products with programmable infrastructure addresses a genuine gap in the market. By embedding compliance, leveraging strategic partnerships, and offering RWAs in a digitally native format, Ondo Chain has the potential to become the default platform for institutional capital entering the blockchain space. Much like Ethereum was the launchpad for the ICO and DeFi waves, Ondo will become the standard for tokenized finance in the institutional era.

It's true that there are higher fees for tokenized products vs products in TradFi. For example, Blackrock launched their USD Institutional Digital Liquidity Fund (BUIDL) which holds RWA USD bank deposits, repos, and UST. This fund commands a relatively high management fee of 0.2-0.5%. An equivalent ETF of the exact same products in the real world has a fee of 0.05% (Blackrock's iShares U.S. Treasury Bond ETF). This implies the cost of blockchain technology, immediate settlement, and 24/7 liquidity is 4x-10x

higher than the TradFi equivalent. Presumably, there is some premium demanded for the benefits of on-chain funds compared to a symmetrical portfolio of real assets, but this magnitude of differential is unjustified. As more competitors create similar products, the fee would be driven down by supply and demand dynamics which should further increase the demand for on-chain assets. You can see in the chart below that AUM more than doubled around the time the Trump administration announced the creation of a crypto strategic reserve in addition to the standard assets normally held. This signals a big shift towards crypto and RWAs for institutions as legitimate currencies, backed by a supportive administration.



Source: BlackRock - USD Institutional Digital Liquidity Fund

Ondo Finance vs Maple Finance Competitive Analysis

Ondo's main competitor in institutional adoption, Maple Finance, has similar products and offerings as they strive for on-chain market share. Ultimately, Ondo Finance is better positioned to compete for institutional business as they are specifically designed to meet the compliance-focused needs of institutional investors. The protocols, products, and regulations detailed throughout the paper support our analysis of how Ondo is built with and run by trusted, regulated, financial firms. That makes it more appealing to large traditional financial institutions (like BlackRock) that want to invest in crypto without taking on too much risk.

Maple Finance, on the other hand, is more geared toward crypto-native users which could deter institutional investors. It lets investors lend to institutional borrowers through professionally managed lending pools. While it does offer higher potential returns, the loans are often backed by more volatile assets like ETH or BTC. Maple also uses its own token system (MPL, SYRUP, and Drip rewards) but these reward systems are less aligned with the needs of compliance-sensitive institutions. Its lack of built-in identity checks and past defaults (like the $36M Orthogonal Trading default) also make it harder for cautious institutions to trust the platform (Maple Finance FAQs).

Overall, Ondo will serve as a more familiar entry point for institutions that are just starting to explore blockchain investing. Maple may offer higher yields, but it also comes with more risk and less regulatory oversight. For now, Ondo is better suited to meet the needs of traditional investors looking for secure, on-chain exposure to real-world assets.

Conclusion

The rise of RWAs as a category is a transformative trend for DeFi. Tokenization can unlock enormous efficiencies if executed securely and compliant with regulations: 24/7 trading, fractional ownership, global liquidity, and reduced settlement times. Ondo's offering of U.S. Treasuries and dollar-backed yield tokens gives institutions a new way to access these benefits without overhauling their entire operational or compliance frameworks. This shift also has macroeconomic implications, highlighted by Ondo's partnership with Blackrock. In summary, Ondo Chain is positioned to become the dominant platform for institutional investors by combining tailored institutional design (permissioned network), deep integration with traditional financial products (UST and repos), and exclusive, high-profile partnerships (Blackrock) that create early credibility in an emerging market.

Sources:

ChatGPT was used for research, writing support, and general assistance.

https://www.businesswire.com/news/home/20250206421408/en/Wall-Street-2.0-Ondo-Finance-Unveils-Integrated-Infrastructure-Suite-to-Bring-US-Financial-Markets-onto-the-Blockchain

https://www.reflexivityresearch.com/free-reports/ondo-finance-overview-future-of-rwas

iShares U.S. Treasury Bond ETF | GOVT

RWA.xyz | BlackRock USD Institutional Digital Liquidity Fund

Building on BUIDL: How Ondo Leverages BlackRock's Tokenized Treasuries

Ethereum Governance

Eligibility | Ondo Finance

Ondo Chain Overview | Ondo Finance

Ondo Chain FAQ | Ondo Finance

OUSG | Ondo Finance

Overview | Ondo Finance

Asset Overview - U.S. Dollar token (USDY) - LlamaRisk

fluxfinance.com

Introducing Ondo Chain: The Omnichain Network for RWAs

What Is the Blockchain Trilemma? | Binance Academy

T+1 (T+2, T+3) Explained: Definitions and Settlement Example

Trump tells crypto leaders at White House summit he's committed to helping their industry | AP News

The Importance Of Smart Contract Audits And Best Security Practices

Smart Contract Vulnerabilities, Risks and How to mitigate them

TraderTraitor: The Kings of the Crypto Heist | WIRED

RWA.xyz | BlackRock USD Institutional Digital Liquidity Fund

Introduction | Maple

Ondo Partnerships Table Sources:

Rakkar Digital Joins Ondo Finance's Ecosystem as First Custodian Partner in APAC

Ondo Finance and Aptos Foundation Forge Strategic Partnership to Tokenize Real World Assets

Hex Trust Partners with Ondo Finance to Expand Custody Solutions | Hex Trust

Ondo Finance announces strategic partnership with Nonco - Nonco

Ondo and Polygon Labs Announce Strategic Alliance to Help Drive Adoption of Institutional-Grade DeFi Products and Services

Ondo Finance to Move $95M to BlackRock's Tokenized Fund for Instant Settlements for Its T-Bill Token

WISCONSIN
SCHOOL OF BUSINESS
UNIVERSITY OF WISCONSIN–MADISON

DEPARTMENT OF
FINANCE, INVESTMENT
& BANKING

WISCONSIN
SCHOOL OF BUSINESS
UNIVERSITY OF WISCONSIN–MADISON

TOGETHER
FORWARD®