BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2026
http://excel.fit.vutbr.cz

Security Analysis and Improvement of DeFi Protocols

Adam Šmehýl*

Abstract

While the Decentralized Finance (DeFi) industry continues to see growing adoption, most capital remains concentrated in a select few financial protocols. This not only concentrates adversarial attention but also limits capital efficiency, resulting in billions of dollars sitting idle or earning below 5% APY. Reallocation of idle capital from overprovisioned reserves in pool-based lending protocols can generate additional yield. Automated adjustments to concentrated liquidity positions can help prevent them from falling outside a defined price range. Analytical modeling of the proposed idle-capital reallocation indicates substantial improvements in supplier yield. Automated liquidity repositioning allows yield to be earned over extended periods without manual intervention. This work shows that current DeFi protocols can be further improved in terms of capital efficiency and presents pathways to achieve this.

*xsmehy00@vut.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

As DeFi is connected to real-world finance, DeFi protocols and their users are lucrative targets for exploiters and scammers. This often leads users to default to protocols with a strong security track record, even at the expense of absolute yield gains. This concentrates capital in long-standing protocols that tend to prioritize stability over innovation and therefore do not always utilize capital as efficiently as they could at this scale. As a result, capital worth billions remains partly idle or earns only limited returns.

Asset lending is a prominent DeFi application, with users often preferring pool-based models that use utilization-based interest-rate curves to automatically adjust borrowing rates in response to changes in supply and demand. As utilization rises, borrowing rates increase to improve yields and discourage further borrowing, and vice versa. However, these curves also greatly overprovision capital reserves to preserve sufficient liquidity for further borrowing or supplier withdrawals, leaving a sizable amount of capital idle and earning nothing. This work explores how that idle capital can be utilized.

In token trading, most short-term activity occurs within a relatively narrow price range, so reserving a sizable amount of liquidity for larger price movements is generally inefficient. That's why it's much more capital-efficient to provide trading liquidity over a defined price range. However, once the price moves outside that range, the position becomes stale. The idea is to automatically move the range to prevent that.

This work presents two improvement ideas aimed at increasing capital efficiency in DeFi protocols, one focused on pool-based lending and the other on concentrated liquidity provision.

2. Idle Capital Allocation

In pool-based lending, not all supplied capital is actively earning the borrowing rate at a given time. This creates room for an extension that reallocates the inactive capital into an external yield source without changing the protocol's baseline lending model.

Figure 1 illustrates this with an example of a lending pool utilized at 65%, in which 65% of the managed capital is lent to borrowers, while 35% remains idle. This creates an opportunity to reallocate the idle share into a liquid external strategy, as shown in **Figure 2**.

2.1 Yield Effect

The possible yield improvement from this capital reallocation is quite pronounced. **Figure 3** shows three distinct but related rate functions. While the Borrow Rate often follows a linear model, any interest collected by the pool is shared pro rata across all supplied capital, which makes any idle capital more impactful on the effective Baseline Supply Yield Rate. The Combined

Yield Rate then shows the potential supplier yield if idle capital were reallocated to an external strategy with, for example, a commonly achievable 5% APY.

2.2 Extension-Based Architecture

The attractive aspect of the improvement idea is that it can be implemented as an extension to existing protocols without disrupting their current logic or behavior. The capital reallocation logic can be implemented as a standalone module, as illustrated in **Figure 4**. The only required change to the protocol's core implementation would be the addition of pathways to delegate idle capital to the extension and withdraw it when needed, while the extension itself would manage deployment to and retrieval from the external strategy.

The reallocation strategy is also easily adaptable. To update it, developers would modify the logic and redeploy the extension contract, after which the core protocol admin or a governance-driven time-lock contract would update the extension's deployment address.

2.3 Expected Supplier APY Increase

Table 1 shows a model of possible absolute increases in supplier APY, expressed in annualized percentage points, across various pool utilization levels and external-strategy yield assumptions.

The improvement is more pronounced at lower utilization levels, where a larger share of the capital is typically idle. As more capital can then be reallocated to a strategy yielding more than the protocol's native borrowing return, the resulting gains are larger.

The listed values represent additional supplier yield on top of the baseline lending yield, rather than the total resulting APY. For reference, a typical scenario is that the pool's utilization ranges from 30% to 70%.

3. Automated Liquidity Position Range Migration

For higher capital efficiency, trading liquidity is usually provided within a user-defined narrow price range, where it is available in full. Because crypto asset prices are often volatile, the price can easily move outside that range, causing the position to become inactive.

This is even more pronounced for yield-bearing tokens that exhibit a persistent appreciation against the underlying asset, as the tokenized capital generates yields. Because their prices are relatively stable, these tokens attract significant liquidity, which must be deployed in narrower ranges to maintain an attractive return.

Figure 5 shows a price-ratio chart of the wstETH/ETH pair together with two examples of concentrated liquidity ranges. The orange range represents a typical static position, while the blue range illustrates a hypothetical automatically adjusting position aligned with an annualized upward drift of three percentage points.

3.1 Range Migration Mechanism

While the design of the underlying AMM protocol shapes how liquidity is handled internally, this improvement can still be implemented at a higher level as a series of adjacent narrow liquidity positions. As **Figure 6** shows, the range would be migrated by removing liquidity from the trailing position, swapping the withdrawn assets as needed, and resupplying them into a new position on the advancing side of the price direction.

3.2 Evaluation Context

Although the primary issue with concentrated liquidity positions is that they become inactive when activity moves outside the defined price range, this cannot be resolved simply by widening the range. **Figure 7** shows this through three examples of range width, including a scenario in which the baseline range width earns 5% APY. It should be noted that this is a very optimistic scenario, as it does not account for outside liquidity concentrated around the current price, which would further reduce the utilization of the examined position. As the range widens, a smaller share of the position's liquidity remains available around the current price.

The figure also illustrates the effect of inactivity over time. For example, the share of time spent in range at 11:1 could represent a position that was 22 hours in range and has now been out of range for 2 hours. The longer the position remains inactive, the lower its average realized APY becomes.

Figure 8 illustrates a prototype for how automated range migration could improve the capital efficiency of a concentrated liquidity position. Given a stable directional price drift and a properly set up automated position, the position would stay in range, remaining only subject to minor execution fees. For comparison, the other scenarios project manual rebalancing by the user. While some power users can automate management of their liquidity, most providers rely on manual adjustments. The Alert-assisted rebalance reflects a prompt user who rebalances upon receiving a notification, while the Daily manual rebalance reflects a position that shifts out of range overnight until it is corrected in the morning.

Together, the two proposals show that current DeFi protocols still leave room for meaningful capital-efficiency improvements, although their realized effect depends on protocol design, market conditions, and implementation details.