Optimal Flash Loan Fee Function with Respect to Leverage Strategies

Chenmin Wang
The University of Aizu
Aizuwakamatsu, Japan
d8211101@u-aizu.ac.jp

Peng Li
The University of Aizu
Aizuwakamatsu, Japan
pengli@u-aizu.ac.jp

Yulong Zeng
YeeZTech
Beijing, China
freeof123@qq.com

Xuepeng Fan
YeeZTech
Beijing, China
xuepeng.fan@yeez.tech

ABSTRACT

We investigate two decentralized methods for leveraging assets: Firstly, investors recurrently commit their target assets as collateral to secure loans, subsequently reinvesting the borrowed funds in the same assets. Secondly, investors pledge their assets once but are required to promptly borrow from a lender and repay the borrowed amount. This model is exemplified by recent Ethereum investment strategies, where investors must weigh the trade-off between gas fees associated with multiple pledging processes and fees charged by the lender, known as the Flash Loan project. Our comprehensive analysis encompasses game theory dynamics, determining optimal strategies for self-interested investors and deriving a unique non-linear optimal fee structure for Flash Loans. This structure remains incentive-compatible, guarding against Sybil attacks and other deviations. Empirical results, under varying environmental parameters, consistently demonstrate the superior revenue performance of our optimal fee structure compared to the commonly used linear fee model within the Flash Loan project.

KEYWORDS

Leverage; Flash Loan; DeFi; Fee Function

ACM Reference Format:

Chenmin Wang, Peng Li, Yulong Zeng, and Xuepeng Fan. 2024. Optimal Flash Loan Fee Function with Respect to Leverage Strategies. In *Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), Auckland, New Zealand, May 6 – 10, 2024*, IFAAMAS, 9 pages.

1 INTRODUCTION

1.1 Motivation and Our Contributions

In the financial field, venture capitalists often use leverage trading to multiply their capital by entering positions larger than their own capital through borrowing funds. The provider of leverage trading, such as a securities exchange, charges a fee known as financing fees as the cost of providing the leverage trading service. In recent years, the rise of decentralized finance (DeFi) [21, 35, 42] has also facilitated leveraged trading through Flash Loan [16, 33, 40], which involves borrowing a capital amount and requiring repayment within a single transaction [38]. Similarly, these Flash Loan projects (FP) that offer leveraged trading also charge financing fees.

Typically, traditional finance providers charge financing fees that are linearly related to the amount of investment funds contributed by investors [28–30]. Likewise, DeFi projects also apply linear financing fees [6, 9] in proportion to the investment amount. For instance, AAVE charges 0.09%, while Uniswap imposes a fee of 0.3%. But using a linear function to charge financing fees is not always optimal for maximizing the project owner's profit [12, 15]. Specifically, Chernenk et al. [15] provide evidence that different lending techniques are employed for various types of borrowers in the commercial loan market. Berg et al. [12] identify the primary objectives behind fees and introduce a novel metric, known as total-cost-of-borrowing, which encompasses the fees imposed by lenders.

On the other hand, in contrast to traditional finance, fee charging in DeFi should also consider situations where investors engage leveraged trading without involving Flash Loan projects due to its decentralized nature. Investors can multiply their capital by utilizing various lending protocols offered by DeFi, including AAVE [4], MakerDAO [1], Compound [2], and more. However, this implementation method incurs operational costs, such as the repetitive invocation of smart contracts, resulting in gas fees [23]. Therefore, investors face a trade-off between the gas fees associated with repeated invocation smart contracts and the financing fees imposed by Flash Loan projects. Rational investors will consistently opt for the approach with lower costs. Flash Loan projects must establish appropriate financing fees to optimize their profits and incentivize rational investors to prefer their leveraged trading services over alternative methods.

In this paper, we present an optimal Flash Loan fee function designed to maximize the profits of Flash Loan project owners while incentivizing self-interested investors. We begin by formalizing two approaches to leverage in DeFi. Using this formalization, we analyze the feasible area for each method and propose a fee function that is optimal for a specific capital value. Furthermore, we demonstrate that this fee function remains optimal across all possible capital values. The induced game, which determines the optimal strategy for self-interested investors, and the corresponding Flash Loan

Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), N. Alechina, V. Dignum, M. Dastani, J.S. Sichman (eds.), May 6 – 10, 2024, Auckland, New Zealand. © 2024 International Foundation for Autonomous Agents and Multiagent Systems (www.ifaamas.org).

fee function for project owners, is commonly referred to as the Stackelberg equilibrium [37].

The main contributions of this paper are summarized as follows.

- We calculate the optimal fee function commitment of Flash Loan projects, taking into account self-interested investors.
- We analysis and reveal a unique global optimal solution that optimizes Flash Loan projects' revenue for investors with any initial asset. This solution is different from the commonly used linear function and is resistant to Sybil attacks [17].
- We conduct an experiment to demonstrate the superior performance of our solution compared to the currently used fee functions of well-known projects.

1.2 Related Works

A collection of literature has explored fee-charging strategies in traditional finance. For instance, [30] investigates the optimal transaction fees for intermediaries in thin markets, where each seller possesses a unique item and faces only a few buyers in each round. On the other hand, [27] analyzes the fee setting mechanism for a seller, buyer, and intermediary in a multi-round game. Additionally, [14] studies fees for stock exchanges and demonstrates that discrete pricing fragments the market and disperses fees. Meanwhile, [22] examines the optimal fee strategy for online sale platforms and proposes that a linear fee function with respect to the reserve price or the final trading price is nearly optimal. Moreover, [24] provides five pieces of advice on fees for investment management. However, to the best of our knowledge, no study has specifically focused on leverage strategies in fee setting.

The concept of investing with leverage in the DeFi ecosystem arose when the AAVE community proposed integrating stETH as collateral in September 2021 [11, 19]. After the proposal was officially launched in February 2022, there was extensive discussion on the specific implementation involving Flash Loan [26], which several DeFi projects on Ethereum mainnet later realized [8, 20]. It's worth noting that our strategy differs from the extensively researched MEV (Maximal Extractable Value) [25, 31, 32, 41], where the latter employs Flash Loan for one-shot arbitrage while the former doesn't necessarily lead to immediate profit but rather a leveraged investment portfolio.

2 BACKGROUND

2.1 Preliminary

In traditional finance, leverage is a fundamental tool that allows investors to increase their potential returns by investing multiples of their principal. While it is commonly believed that leverage can only be achieved through centralized contracts provided by banks or exchanges [18, 36], there is a more accessible way to implement it without their assistance. Suppose Alice is bullish on gold and wishes to make a leveraged investment. To achieve this, she requires only two things: a gold market to purchase gold and a pawnshop that allows her to pledge her gold as collateral and borrow funds.

For example, suppose Alice has \$100 and wants to invest in gold with leverage. She spends all her money buying gold in the market, then pledges her gold (worth \$100) at a pawnshop to borrow some money. Typically, there is a discount of, say, 50%, so she can borrow a maximum of \$50. She returns to the gold market and uses the borrowed \$50 to buy more gold, then repeats the process. After repeating this process sufficiently, Alice will have almost $100 + 50 + 25 + \ldots = 200$ dollars worth of gold, serving as collateral in the pawnshop, with a total debt of $50 + 25 + \ldots = 100$ dollars. This allows her to establish almost double leverage without the need for any centralized leverage contracts.

However, Alice may be reluctant to follow this process as it is laborious and costly to repeatedly commute between the gold market and the pawnshop. Therefore, she devises another process: borrowing \$100 from a lender, she spends all \$200 (including her principal) to buy gold. Then, she goes to the pawnshop, pledges all \$200 worth of gold, and borrows \$100. Finally, she repays the \$100 to the lender. This allows Alice to implement exact double leverage without any repeated operations, and since she repays the debt almost instantly, she usually does not need to pay too much interest to the lender. As investors like Alice become more popular, lenders may seek to take advantage by implementing a fee function for these short-term loans.

This example abstracts a series of realistic situations, including money multiplier, second mortgage, and refinancing. A second mortgage is a type of mortgage that is subordinate to the primary (first) mortgage on a property. Refinancing involves replacing an existing mortgage with a new one, typically to secure better terms, such as a lower interest rate or different loan duration. One of the most concrete scenarios is a common situation on Ethereum [13] that features two key elements:

- The cost of each invest-pledge-borrow process is a constant.
- The fee charged by the lender is a function to the loan amount.

2.2 Leverage Strategies in Ethereum

In Ethereum's ecosystem, implementing traditional leverage is challenging due to the limitations of decentralization and the delivery risk stemming from anonymity. Currently, high-quality decentralized exchanges (DEXes) like Uniswap and Curve do not offer leverage products, and although a few small DEXes have introduced the idea, liquidity and availability are limited. Recently, DeFi projects have proposed strategies that involve multiple projects, which allow for decentralized leverage implementation as we have shown above, and have attracted significant attention. To be specific, suppose Alice wants to exchange her original asset, such as ETH, to a target asset, such as stETH, with leverage. The following smart contracts [3, 5, 7] are involved:

- AAVE [5] serves as the pawnshop, allowing users to pledge stETH and borrow ETH with a specified ratio known as Loan-to-Value (LTV).
- Lido [3] functions as the gold market, enabling users to exchange ETH for stETH.
- Balancer [7] serves as the lender or FP, lending ETH to the user and requiring prompt repayment.

Alice can leverage her investment in two ways: 1) She can repeat the process of exchanging ETH to stETH via Lido, pledging stETH, and borrowing ETH via AAVE. 2) She can loan ETH from Balancer, execute the process in 1) only once, and then repay the borrowed ETH to Balancer.

When deciding between the two strategies, Alice must consider the trade-offs involved. In the first strategy, Alice must bear the cost of each pledge-borrow-exchange process, known as the gas fee [23]. This cost is similar to the travel expense from the gold market to the pawnshop and is independent of the amount involved in the process. Repeated processes will stop being rational for investors if the marginal utility is less than the cost, which will also prevent maximizing leverage. On the other hand, in the second strategy, the FP usually charges a fee, which is an additional cost that users must repay. This fee directly reduces Alice's utility. As a self-interested investor, Alice will always choose the strategy that maximizes her utility.

3 MODEL

For the rest of this paper, all values are evaluated in ETH, and we will not explicitly state "value in ETH".

We define the following notations throughout this paper:

- x denotes the amount of ETH held by the investor, which is the original asset.
- m represents the LTV of the (ETH, stETH) pair in AAVE, where $m < 1$. This means that if an investor pledges x worth of stETH, they can borrow up to mx worth of ETH.
- A and B are constants, where $A > 1$ is the common valuation of one stETH. Note that the actual value of stETH may increase over time if it is an interest-earning asset, but we use A to represent its long-term value. Similarly, the owned ETH debt to AAVE is also increasing over time, and $B > 1$ is used to denote the common evaluation of one ETH debt.
- α represents the gas fee for one pledge-borrow-exchange process. This refers to the process where an investor pledges some stETH to AAVE, borrows some ETH, and then exchanges the borrowed ETH to stETH via Lido. The gas fee is independent of all amounts involved in the process, but may fluctuate unpredictably. For simplicity, we take α to be the average cost of the above process.

Next, we will introduce the two strategies mentioned earlier in detail: Multiple Leverage Deposit (MLD) and Full Leverage Deposit (FLD).

3.1 Multiple Leverage Deposit

As demonstrated in the introduction, when disregarding the Flash Loan strategy, a rational investor always adheres to the following rules:

- (MLD1) When an investor holds ETH, she will exchange it for stETH, as the latter's value can be increased by a factor of A.
- (MLD2) An investor will follow the pledge-borrow-exchange process if the cost of the process is less than its marginal utility. This can be expressed as

$$(A - B)t \geq \alpha,$$

where t represents the maximum amount of ETH that the investor can borrow.

By following the rules mentioned above, an investor's utility can be calculated as the difference between the total collateral and total debts, both of which can be expressed as the sum of a geometric series, and then subtracting the costs. The formal formula is presented in the following definition.

Definition 3.1. An investor is considered MLD if she satisfies rules MLD1 and MLD2. Additionally, the utility of an MLD investor with an initial asset of x is given by:

$$U_{MLD} = A(x + mx + m^2x + \ldots + m^kx) - B(mx + m^2x + \ldots + m^kx) - k\alpha,$$

where $k = \lfloor \log_m \frac{\alpha}{(A-B)x} \rfloor$

The MLD investor stops at the k-th pledge-borrow-exchange process when the marginal utility is less than the cost, which can be expressed as $(A - B)m^{k+1}x < \alpha$.

One could argue that the actual gas fee might differ from $k\alpha$ due to the specific contract used. However, in reality, α is significantly smaller compared to x. Therefore, we make the straightforward assumption that k is much larger than any constant, including α, $1/m$, $1/(1 - m)$, any fixed gas fee consumption when executing smart contracts, and any constant appearing in any utility formula. Based on this assumption, we can simplify the expression by letting $\alpha = (A - B)m^{k+1}x$, since the difference caused is at most α, which can be ignored.

With this assumption, we can rewrite the utility of a MLD investor as

$$\begin{aligned} U_{MLD} &= \frac{Ax(1 - m^{k+1})}{1 - m} - \frac{Bxm - Bxm^{k+1}}{1 - m} - k\alpha \\ &= \frac{x(A - Bm)}{1 - m} - \alpha(k + \frac{1}{1 - m}). \end{aligned}$$

The above value can be denoted by $U_{MLD}(x)$ since it is a function of x.

U_{MLD} serves as the lower bound for the utility of any FLD investor, which we will introduce in the next subsection.

3.2 Full Leverage Deposit

As previously mentioned, a FLD investor effectively utilizes the Flash Loan by borrowing ETH from it and immediately repaying the loan. To be self-interested, she chooses the optimal amount of borrowed ETH, denoted by y, to maximize her utility. However, if the resulting utility is less than U_{MLD}, the investor would instead choose the MLD strategy, thus the FP would earn nothing from the transaction. To prevent this, we impose a constraint that the utility of a FLD investor, denoted by U_{FLD}, must not be less than U_{MLD}.

It is worth noting that while the curve $U_{MLD}(x)$ provides a straightforward lower bound for the investor's utility, and therefore maximizes the FP's revenue to some extent, it is not guaranteed that there is a fee function, which takes the loan amount rather than the principal x as its argument, can produce this curve.

Definition 3.2. A rational investor with an initial asset of x is considered to be a FLD investor if she follows the below process:

- Loan y^* ETH from the Flash Loan project;
- Exchange $x + y^*$ ETH to stETH via Lido;
- Pledge $x + y^*$ (value) stETH into AAVE and borrow $f(y^*)$ ETH from AAVE;
- Repay $f(y^*)$ to the Flash Loan project,

where y^* is the solution to the following optimization problem:

$$\begin{aligned} y^* &= \arg\max\{A(x+y) - B(f(y))\} \qquad (1)\\ s.t.\ A(x+y) - B(f(y)) &\geq U_{MLD}(x)\\ f(y) &\leq m(x+y) \end{aligned}$$

The FLD investor's utility can be expressed as:

$$U_{FLD}(x) = A(x+y^*) - B(f(y^*))$$

The first constraint ensures that the FLD investor does not deviate to the MLD strategy. The second constraint ensures that the borrowed ETH is limited to no more than the LTV rate, which is m, times the total collateral.

It's worth noting that it's suboptimal for the user to have any remaining ETH after implementing the FLD strategy. This is because the user can convert the remaining ETH into stETH and deposit the entire amount into AAVE. This not only preserves the user's profits but also expands their strategic options. Therefore, we should exclusively focus on the scenario in which the user has no ETH on hand, effectively utilizing the borrowed ETH to repay the debt.

Building on the FLD strategy as the optimal choice for self-interested investors, the next challenge is to identify the optimal function $f(\cdot)$ that maximizes the Flash Loan project's revenue from FLD investors.

3.3 Optimal Fee Function

Given an FLD investor's initial asset x, the objective of the FP is to solve the following optimization problem:

$$\begin{aligned} REV(x) &= \max f(y^*) - y^* \qquad (2)\\ y^* &= \arg\max\{A(x+y) - B(f(y))\}\\ s.t.\ A(x+y) - B(f(y)) &\geq U_{MLD}(x)\\ f(y) &\leq m(x+y) \end{aligned}$$

It should be noted that finding an optimal function $f(\cdot)$ for a specific variable x does not guarantee that $f(\cdot)$ will optimize all values of x. The objective is to find a solution that optimizes the above objective for all possible values of x, which is referred to as the global optimal solution.

4 OVERVIEW

We propose a fee function that is optimal with respect to a specific value of x, the investor's initial asset. We then proceed to demonstrate that this fee function is also globally optimal for all possible values of x.

Let $f(\cdot)$ be the fee function to be determined. We define a corresponding curve $h(\cdot)$ as follows:

$$h(y) = Ay - Bf(y) \qquad (3)$$

for all y in $f(\cdot)$'s domain. Note that it matches the objective of problem (1) with the constant term Ax subtracted.

Theorem 4.1. *The optimal curve for $h(\cdot)$ that maximizes FP's revenue is given by:*

$$y = \frac{mx}{1-m} - \frac{\alpha k}{A-Bm} - \frac{\alpha}{(1-m)(A-Bm)},$$
$$h = \frac{(A-B)mx}{1-m} - \alpha(k + \frac{1}{1-m}),$$

where y is the argument and h is the corresponding function value. Note that k is also a function of x.

We refer to the curve in Theorem 4.1 as the **revenue optimal (RO) curve**, which is a parametric equation with respect to x.

5 ANALYSIS

To facilitate understanding, we will first consider two extreme cases and ignore the MLD constraint:

- $f(y) = y$
  In this case, the FP does not charge additional fee and earns nothing, like Balancer. The FLD investor always wants to maximize the loan amount y^* since $U_{FLD} = Ax + (A-B)y^*$. Therefore, the optimal value for y is $y = \frac{mx}{1-m}$ due to the second constraint in problem (1), which results in leverage with a multiple of $1/(1-m)$. This corresponds to the example given in the introduction with $m = 0.5$, where loaning \$100 is optimal.
- $f(y) = Ay/B$
  In this case, the objective function in problem (1) becomes Ax, which means that the investor's choice of loan amount is irrelevant to her utility. In particular, the investor may choose $y = 0$, which does not use the Flash Loan. The FP earns nothing either.

The two extreme cases discussed correspond to $h(y) = (A-B)y$ and $h(y) = 0$, which represent the trivial upper bound and lower bound respectively for $h(y)$.

Suppose that the fee function $f(\cdot)$ is given, which means that the corresponding curve $h(\cdot)$ is given. Now, based on (1) and (3), the problem of the investor can be expressed as follows:

$$\begin{aligned} &\max h(y) \qquad (4)\\ s.t.\ &h(y) \geq U_{MLD}(x) - Ax\\ &h(y) \geq -Bmx + (A-Bm)y \end{aligned}$$

Suppose y^* is the optimal solution for the above problem, the objective of the FP is to maximize the following based on (2) and (3):

$$B \cdot REV(x) = -h(y^*) + (A-B)y^*$$

We first analyze the solution of problem 4. When taking x as constant and $y, h(y)$ as two variables. We create a coordinate system with $y, h(y)$ as coordinates. It is a linear programming problem *at the first step*, where we ignore the constraint that the point $(y, h(y))$ must lie on the given curve $h(\cdot)$.

The optimization problem's solution is depicted in Figure 1, and it can be broken down into the following steps:

- The feasible area of problem (4) is the shadow area enclosed by the horizontal line $h(y) = U_{MLD}(x) - Ax$ and the line $h(y) = -Bmx + (A-Bm)y$.
- Then, given the feasible area, which point will the investor choose? Note that the point must also land on the curve $h(\cdot)$.

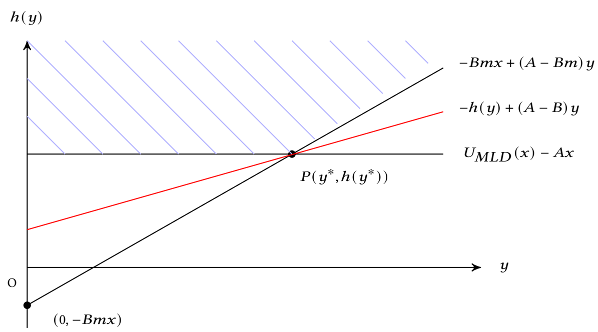


Figure 1: Optimization Problem for $h(y)$.

If the curve $h(\cdot)$ intersects with the shadow area, the solution of problem (4) is the intersection point with the maximum ordinate, among all intersection points.

- Base on the investor's strategy, we can further analyze the optimal $h(\cdot)$ which the FP will choose. Since the objective is $B \cdot REV(x) - h(y^*) + (A-B)y^*$ (y^* is the investor's choice), which is **inversely** proportional to the height of the red line, the line passes through the point $(y^*, h(y^*))$ with slope $A-B$. So, it is the FP's preference to let the red line as low as possible.

Note that the slope of the red line is less than the slope of the line $h(y) = -Bmx + (A-Bm)y$. The point P, which is the intersection of the horizontal line $h(y) = U_{MLD}(x) - Ax$ and the line $h(y) = -Bmx + (A-Bm)y$, plays a crucial role in maximizing $REV(x)$. It is not hard to see that the red line that passes through the point P gives the minimum height among all the points in the shadow area. If the curve $h(\cdot)$ intersects the shadow area only at point P, then $REV(x)$ is maximized. Otherwise, it is the investor's preference to choose a point in the shadow area higher than P, which leads a higher height of the red line and makes $REV(x)$ sub-optimal. Thus, we have the following lemma:

Lemma 5.1. *Given x, if the curve $h(\cdot)$ intersects the area enclosed by the horizontal line $h(y) = U_{MLD}(x) - Ax$ and the line $h(y) = -Bmx + (A-Bm)y$ only at their intersection, then the FP's revenue is maximized at the intersection.*

While constructing a curve that satisfies Lemma 5.1 is simple, our aim is to find a global solution. We can observe that as x changes, the locus of point P gives a curve. It is straight forward to consider the feasibility and optimality of taking this curve as $h(\cdot)$. Remarkably, this is a viable option.

As described in Theorem 4.1, this curve is the revenue optimal (RO) curve. This means that for a given value of x, the corresponding intersection point $(y, h(y))$ described in Lemma 5.1 is obtained by plugging x into the RO curve equation. The calculation process of the RO curve is omitted here.

In order to show the feasibility of the RO curve, we need to prove that y is an increasing function of x.

Lemma 5.2. *The function*

$$y = \frac{mx}{1-m} - \frac{\alpha k}{A-Bm} - \frac{\alpha}{(1-m)(A-Bm)}$$

is increasing with x.

Proof.
$$\frac{dy}{dx} = \frac{m}{1-m} - \frac{\alpha}{A-Bm} \cdot \frac{dk}{dx}$$
Also note that
$$dk/dx = -\frac{1}{x \ln m},$$
we have
$$\frac{dy}{dx} > 0 \Leftrightarrow x > -\frac{\alpha(1-m)}{m(A-Bm)\ln m}.$$
It is trivial to show that y is increasing with x based on the assumption that x is greater than any constant. □

We then show that the RO curve is increasing. Firstly, we can show that the function $U_{MLD}(x) - Ax$ is increasing with x when x is large. This is because the deviation of this function from x is given by $(A-B)m/(1-m) + 1/(x \ln m)$, which is positive for large x. [1]

Combining with Lemma 5.2, it is straightforward to see that the RO curve is increasing. As x increases, the line $h(y) = -Bmx + (A-Bm)y$ shifts to the right, and the line $h(y) = U_{MLD}(x) - Ax$ moves up. Thus the ordinate of point P increases.

We then demonstrate that for any x, the RO curve intersects the shadow area in Figure 1 only at one point. We already know of the intersection point P, but in order to prove that there is no other intersection, we prove that the derivative of any point on the RO curve is less than $A-Bm$, which is the slope of the line $h(y) = -Bmx + (A-Bm)y$. Therefore, the RO curve always grows slower than the line, and they will never intersect.

We can prove the following lemma which is stronger than what is required:

Lemma 5.3. *The deviation of the revenue optimal curve is less than $A-B$ at any point.*

Proof. We have
$$\frac{dy}{dx} = \frac{m}{1-m} - \frac{\alpha}{A-Bm} \cdot \frac{dk}{dx},$$
$$\frac{dh}{dx} = \frac{(A-B)m}{1-m} - \alpha \cdot \frac{dk}{dx},$$
and $\frac{dh}{dy} = \frac{dh}{dx} / \frac{dy}{dx}$.

To prove it is less than $A-B$:
$$\frac{dh}{dy} < A-B \Leftrightarrow -\frac{\alpha(A-B)}{A-Bm} \cdot \frac{dk}{dx} > -\alpha \cdot \frac{dk}{dx}$$
It obvious holds since $\frac{dk}{dx} > 0$ and $m < 1$. Thus the lemma is proved. □

The revenue optimal curve, described in Figure 2, has the line $h(y) = (A-B)y$ as its asymptote.

Proof of Theorem 4.1. Based on Lemma 5.2, we know that the revenue optimal curve is a feasible and increasing function. Moreover, by Lemma 5.3, we know that for all x, it satisfies the condition of Lemma 5.1. Thus, according to Lemma 5.1, the revenue optimal curve is globally optimal. □

[1] The RO curve may potentially be decreasing when x is small, but this does not impact any of the results in this paper, given the assumption about the range of x.

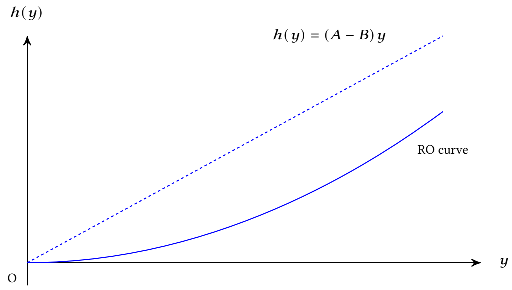


Figure 2: Revenue Optimal Curve.

5.1 Incentive Compatibility

Next, we demonstrate that the revenue optimal curve is incentive compatible by examining possible deviations from investors and proving that they cannot increase utility.

Given that the Sybil attack [17, 39, 43] is the most prevalent and distinctive form of attack in blockchain mechanisms, the ability to resist such an attack stands as the paramount attribute of on-chain mechanisms. Additionally, the four deviation scenarios we consider encompass the majority of conceivable attacks, including various strategy combinations, and showcase a broad anti-attack effectiveness in practical implementation. Finally, while other potential attacks do exist, they can typically be categorized as one of these four attack types. Due to space constraints, providing a detailed description of each is impractical.

(**Deviation 1**) Instead of loaning y from FP, an investor loans separate amounts of y_1 and y_2 (implying multiple identities) such that $y_1 + y_2 = y$, with the expectation of a lower total fee.

In order for the optimal fee function to be resistant to Sybil attacks, it must satisfy the condition $f(y_1 + y_2) < f(y_1) + f(y_2)$. This is equivalent to the condition that the revenue optimal curve, $h(y_1 + y_2) > h(y_1) + h(y_2)$. We provide the following lemma:

Lemma 5.4. *For any $y_1, y_2 > 0$, the revenue optimal curve $h(\cdot)$ satisfies $h(y_1 + y_2) > h(y_1) + h(y_2)$.*

Proof. Define $y_3 = y_1 + y_2$. Using the parametric function in Theorem 4.1, let $x_i, i = 1, 2, 3$ be the parameters w.r.t. y_i, so

$$y_i = \frac{mx_i}{1-m} - \frac{\alpha k_i}{A-Bm} - \frac{\alpha}{(1-m)(A-Bm)}$$

$$h_i = \frac{(A-B)mx_i}{1-m} - \alpha(k_i + \frac{1}{1-m}), i = 1, 2, 3,$$

where k_i satisfies $\alpha = (A-B)m^{k_i+1}x_i$.

$y_3 = y_1 + y_2$ gives

$$\frac{m(x_1+x_2-x_3)}{1-m} - \frac{\alpha(k_1+k_2-k_3)}{A-Bm} - \frac{\alpha}{(1-m)(A-Bm)} = 0,$$

and $h(y_1 + y_2) > h(y_1) + h(y_2)$ is equivalent to

$$\frac{(A-B)m(x_1+x_2-x_3)}{1-m} - \alpha(k_1+k_2-k_3) - \frac{\alpha}{1-m} < 0$$

By combining the above two formulas and canceling terms of k_i, we only need to prove

$$(\frac{(A-B)m}{1-m} - \frac{(A-Bm)m}{1-m})(x_1+x_2-x_3) < 0,$$

which is equivalent to prove $x_1 + x_2 > x_3$.

We have shown that the function $y(x)$ is monotonically increasing, so

$$x_1 + x_2 > x_3 \Leftrightarrow y(x_1+x_2) > y(x_3) \Leftrightarrow y(x_1+x_2) > y(x_1) + y(x_2),$$

which is equivalent to prove

$$k_4 - k_1 - k_2 < \frac{1}{1-m},$$

where k_4 satisfies $\alpha = (A-B)m^{k_4+1}(x_1+x_2)$. The relation of k_i gives

$$(\frac{1}{m})^{k_1} + (\frac{1}{m})^{k_2} = (\frac{1}{m})^{k_4}. \tag{5}$$

Without loss of generality, we can assume that $k_1 < k_2 < k_4$. Next, we can fix k_1 and determine the value of $k_4 - k_2$ that maximizes it.

Equation (5) gives

$$(\frac{1}{m})^{k_2}((\frac{1}{m})^{k_4-k_2} - 1) = (\frac{1}{m})^{k_1}.$$

It can be shown that $k_4 - k_2$ is a decreasing function of k_2. Therefore, $k_4 - k_2$ is maximized when $k_2 = k_1$. We only need to prove this particular case.

(5) now becomes $2(\frac{1}{m})^{k_1} = (\frac{1}{m})^{k_4}$, and what we need to prove is $k_4 - 2k_1 < \frac{1}{1-m}$

After taking the logarithm, the condition becomes $\log_{\frac{1}{m}} 2 + k_1 = k_4$. Cancelling k_4, we need to prove

$$k_1 > \log_{\frac{1}{m}} 2 - \frac{1}{1-m}$$

Actually, it can be shown that the right side is negative, as demonstrated in the following lemma. Thus, the lemma is proven. □

Lemma 5.5. *For any $0 < m < 1$, $\log_{\frac{1}{m}} 2 - \frac{1}{1-m} < 0$*

Proof. Let $t = \frac{1}{m} > 1$, the inequality becomes

$$\log_t 2 < \frac{t}{t-1}.$$

Since $t > 1$, it is equivalent to

$$2 < t^{\frac{t}{t-1}}.$$

If $t \geq 2$, it obviously holds since $\frac{t}{t-1} > 1$.

If $t < 2$, then

$$t^{\frac{t}{t-1}} = (1+t-1)^{\frac{1}{t-1}} \cdot t > (1+t-1)^{\frac{1}{t-1}} > 2$$

The last inequality follows from the fact that the function $(1+x)^{\frac{1}{x}}$ is decreasing. Hence, the lemma is proven. □

The lemma we just proved implies that our mechanism is resistant against another type of Sybil attack.

(**Deviation 2**) The investor divides her initial asset x into two parts, x_1 and x_2, and runs FLD separately on each part.

The proof is straightforward. Let y_1 and y_2 be the loan amounts corresponding to x_1 and x_2, respectively. The investor pays a total fee of $f(y_1) + f(y_2)$ for these loans. We can compare this to the intermediate operation, in which the investor loans $y_1 + y_2$ together and pays $f(y_1 + y_2)$. This is feasible since $h(y_1 + y_2) \geq h(y_1) + h(y_2) \geq -Bm(x_1 + x_2) + (A - Bm)(y_1 + y_2)$ and increases utility since $f(y_1 + y_2) < f(y_1) + f(y_2)$ and the deposited amount is the same. From Lemma 5.1, we know that the intermediate operation is suboptimal compared to FLD with initial $x_1 + x_2$.

The following deviation is immediately implied by this.

(**Deviation 3**) The investor splits her initial asset x into two parts, x_1 and x_2. She then runs FLD with x_1 and MLD with x_2.

As the utility from the MLD part is no more than the utility from the FLD part, the proof can be reduced to Deviation 2.

(**Deviation 4**) The investor runs MLD for one (which implies several) step and then runs FLD for borrowed ETH.

The investor exchanges all of their ETH to stETH, pledges it into AAVE, and borrows mx ETH. Then, she uses the borrowed ETH as her initial asset and runs FLD. Therefore, the total utility is $Ax - Bmx + U_{FLD}(mx) + \alpha$. Since $U_{FLD}(x) = U_{MLD}(x)$, the total utility can also be expressed as $Ax - Bmx + U_{MLD}(mx) + \alpha = U_{MLD}(x) = U_{FLD}(x)$, which is no better than FLD.

5.2 Linear Fee Function

In practice, many FPs prefer to use a linear fee function (with zero bias) due to its simplicity for implementation. In this subsection, we will investigate how to select an optimal linear fee function, which can be represented as $f(y) = ty$, where t is a parameter.

From Lemma 5.1, we know that for a specific x, a necessary condition for optimality is that $h(y)$ passes point P, which implies that the solution in Theorem 4.1 is unique. Based on this, we can state the following theorem:

Theorem 5.6. *There is no linear fee function that is globally optimal.*

In order to be second-best, we aim to find a linear fee function that satisfies the constraints for some x, where investors will choose FLD over MLD and the FP can generate positive revenue. We note that the range of y has a maximum value of y_{max}, which corresponds to the total amount of ETH that the FP owns. We choose the linear function $h(y)$ to be the line that passes through $(0, 0)$ to $(y_{max}, h^*(y_{max}))$, where h^* is the revenue optimal curve. We then prove that this linear function is FLD-feasible for all $y < y_{max}$, meaning that the linear function intersects the shadow area in Figure 1, but the intersection points may not be unique. To prove this, we need to show that the revenue optimal curve is convex, as illustrated in Figure 3.

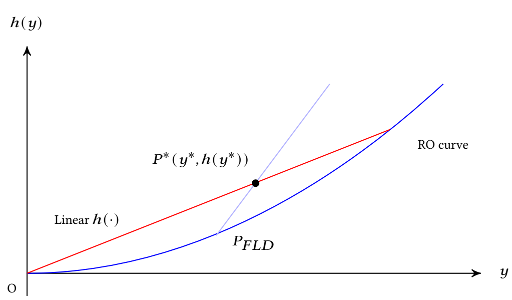


Figure 3: Linear Fee Function. P_{FLD} denotes the intersection point on the revenue-optimal curve $h(y)$ determined by x, which corresponds to point P in Figure 1. $P^*(y^*, h(y^*))$ denotes the optimal FLD-feasible choice of the investor.

Lemma 5.7. *The revenue optimal curve is convex.*

Proof. Recall that in the proof of Lemma 5.3:

$$\frac{dy}{dx} = \frac{m}{1-m} - \frac{\alpha}{A - Bm} \cdot \frac{dk}{dx},$$
$$\frac{dh}{dx} = \frac{(A-B)m}{1-m} - \alpha \cdot \frac{dk}{dx}.$$

Note that $\frac{dk}{dx} = -\frac{1}{x \ln m}$, so $\frac{d(dk/dx)}{dx} < 0$.

We also have

$$\frac{d(dh/dy)}{d(dk/dx)} < 0 \Leftrightarrow \frac{(A-B)m\alpha}{(1-m)(A-Bm)} < \frac{\alpha m}{1-m}$$

holds, so $\frac{d(dh/dy)}{dx} > 0$, which also means $\frac{d(dh/dy)}{dy} > 0$ since $\frac{dy}{dx} > 0$.

The lemma is proved. □

Choosing a linear fee function entails a trade-off for the FP: a lower slope results in higher average revenue but also imposes a smaller threshold y_{max}, which is the maximum value supported by the fee function, beyond which the revenue is zero.

6 EXPERIMENTS

6.1 Statistics of FLD Market

We analyzed Ethereum transactions related to wETH (equivalent to ETH) Flash Loan in 2022 from March 1st (block 14,297,758), when AAVE integrated stETH as collateral, to July 1st (block 15,053,226), for Balancer Vault Contract and AAVE Lending Pool V2 Contract. Figure 4 presents a comparison between the total number of Flash Loan transactions and FLD-related transactions, as well as their total volume.

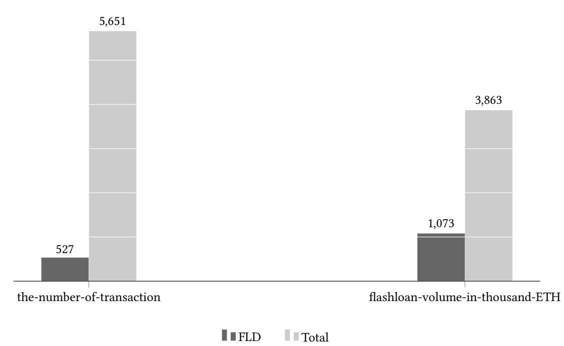
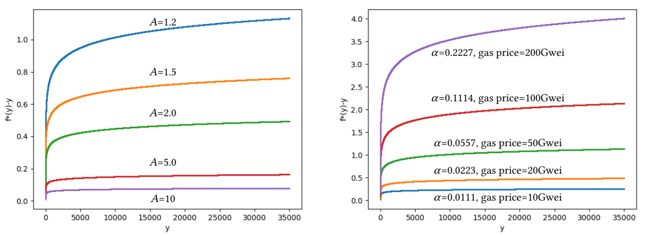


Figure 4: Comparison of FLD and Total in Flash Loan Transactions and Borrowing Volume in ETH.

We excluded Flash Loan transactions from other FPs such as Uniswap and Dodo since they were extremely rare. We also excluded meaningless Flash Loan transactions that solely involved wETH. Our findings indicate that FLD-related transactions accounted for over 9.3% of total transactions, highlighting FLD's significant role in Flash Loan applications.

Out of the total FLD transactions, only 68 of them use AAVE Flash Loan, with a maximum volume of only 698.13 ETH. This is mainly because the fee strategy of FLD is dominated by Balancer, which charges zero fees. Furthermore, we will demonstrate that even without the presence of Balancer, the fee strategy of FLD is still suboptimal for rational users.



(a) A**=1.2, 1.5, 2, 5, 10 and** α**=0.0557** **(b)** α**=0.0111, 0.0223, 0.0557, 0.1114, 0.2227 and** A**=1.2**

Figure 5: $f^*(y) - y$ **with different values of** A **and** α**, and fixed values of** B**=1,** m**=0.7.**

6.2 Fee Function for RO Curve

In this experiment, we set $B = 1$ and $m = 0.7$. We denote the fee function corresponding to the RO curve as $f^*(y)$. Figure 5(a) shows the revenue curves for RO with different values of A, while Figure 5(b) shows the revenue curves for different values of α.

6.3 Comparison Between RO and AAVE Curve

Figure 6 illustrates the fee function for RO and AAVE, with $A = 1.2$. In Figure 6, the fee function $f(y) = f^*(y) - y$ intersects with AAVE fee function $f(y) = 1.0009y$ at $y = 872.69$. This means that a rational user would choose the MLD strategy instead of AAVE when $y > 872.69$, which matches the statistics that the maximum volume of FLD transactions using AAVE is only 698.13 ETH. However, for cases where $y < 872.69$, it is still sub-optimal compared to the RO curve.

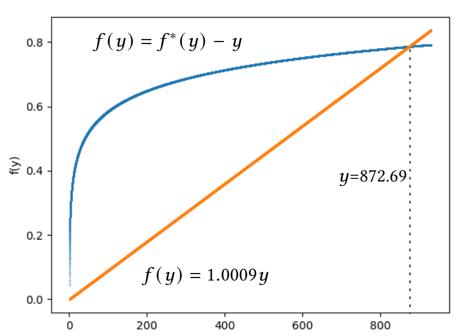
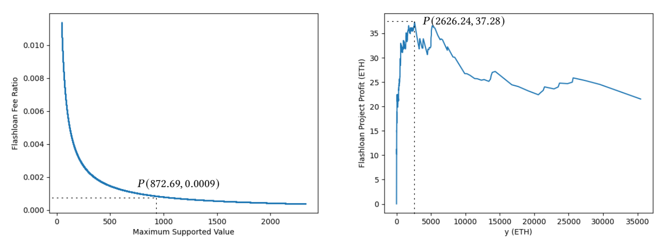


Figure 6: $f(y) = f^*(y) - y$ **interacts with the line** $f(y) = 1.0009y$ **at** y**=872.69.**

It should be noted that as the parameter A increases and α decreases, the maximum supported value, represented by the intersection point at $y = 872.69$, decreases. This implies that it becomes increasingly difficult to attract high-value users to use AAVE Flash Loan. Additionally, with the current average gas price at only 10 Gwei after ETH2.0 merge [10, 34]).

6.4 Advice about Choosing Linear Fee Functions

Referring to the information presented in Figure 6, an FP must make a trade-off between a higher slope of the linear fee function (i.e., a higher fee ratio) and the maximum supported value. A higher slope leads to a lower maximum supported value, which means that the FP becomes less attractive to high-value investors and earns less revenue from them. For instance, if the slope is 1.0009, the maximum supported value is 872.69 ETH. To illustrate this trade-off, Figure 7(a) plots the curve of the maximum supported value against the slope minus 1, which represents the Flash Loan fee ratio.



(a) Maximum supported value for the Flash Loan fee ratio **(b) Flash Loan project profit**

Figure 7: Flash Loan fee ratio and Flash Loan project profit.

We collected data on all 527 FLD transactions and their distribution, with the maximum volume being 35,467.82 ETH. Based on these statistics, we can plot the curve of the maximum supported value against the FP's revenue. For instance, if the FP selects the maximum supported value as 872.69, then the corresponding Flash Loan fee is 0.0009, and the FP earns 0.09% of the transaction volume below 872.69 ETH. The result is presented in Figure 7(b), indicating that it is optimal for the FP to set the maximum supported value to be 2626.24 ETH, where the corresponding Flash Loan fee is 0.034%, and the FP can earn a revenue of 37.3 ETH.

7 CONCLUSION

We analyze two decentralized methods for achieving leverage: Multiple Leverage Deposit (MLD) and Full Leverage Deposit (FLD). By carefully examining the trade-off between gas fees incurred by MLD and the fees charged by FLD, we determine the optimal strategy for self-interested investors and the optimal Flash Loan fee function for the Flash Loan owner with respect to these investors. We prove that there exists a unique optimal fee function that is not linear but is incentive-compatible against Sybil attacks and other possible deviations. Experimental results show that our optimal fee function outperforms the commonly used linear fee function.

REFERENCES

[1] 2017, Dec. MakerDAO. [Online]. Available: https://makerdao.com/.
[2] 2018, Jun. Compound. [Online]. Available: https://compound.finance/.
[3] 2020, Dec. Lido Contract. [Online]. Available: https://etherscan.io/address/0xae7ab96520DE3A18E5e111B5EaAb095312D7fE84.
[4] 2020, Jan. AAVE. [Online]. Available: https://aave.com.
[5] 2020, Nov. AAVE Lenging Pool V2 Contract. [Online]. Available: https://etherscan.io/address/0x7d2768de32b0b80b7a3454c06bdac94a69ddc7a9.
[6] 2021, Apr. AAVE Flash Loan Fee. [Online]. Available: https://docs.aave.com/developers/v/2.0/guides/flash-loans.
[7] 2021, Apr. Balancer Contract. [Online]. Available: https://etherscan.io/address/0xba12222222228d8ba445958a75a0704d566bf2c8.
[8] 2022, May. EFLeverVault. [Online]. Available: https://etherscan.io/address/0xe39fd820B58f83205Db1D9225f28105971c3D309.
[9] 2023, Jan. Uniswap Flash Loan Fee. [Online]. Available: https://docs.uniswap.org/contracts/v2/guides/smart-contract-integration/using-flash-swaps.
[10] 2023, Mar. The Merge. [Online]. Available: https://ethereum.org/en/upgrades/merge/.
[11] Adria Parcerisas Albés. 2021, Oct. How can Lido users use stETH and why should they do? [Online]. Available: https://medium.datadriveninvestor.com/how-can-lido-users-use-steth-and-why-should-they-b3be8147e056.
[12] Tobias Berg, Anthony Saunders, and Sascha Steffen. 2016. The total cost of corporate borrowing in the loan market: Don't ignore the fees. *The Journal of Finance* 71, 3 (2016), 1357–1392.
[13] Vitalik Buterin et al. 2014. A next-generation smart contract and decentralized application platform. *white paper* 3, 37 (2014), 2–1.
[14] Yong Chao, Chen Yao, and Mao Ye. 2019. Why discrete price fragments US stock exchanges and disperses their fee structures. *The Review of Financial Studies* 32, 3 (2019), 1068–1101.
[15] Sergey Chernenko, Isil Erel, Robert Prilmeier, et al. 2019. *Nonbank lending.* National Bureau of Economic Research.
[16] Xiaolei Ding, Lingwei Zhang, and Shujuan Sun. 2023. Design of" Flash Loan" under Decentralized System. In *Proceedings of the 2nd International Conference on Internet Technology and Educational Informatization, ITEI 2022, December 23-25, 2022, Harbin, China.*
[17] John R Douceur. 2002. The sybil attack. In *Peer-to-Peer Systems: First InternationalWorkshop, IPTPS 2002 Cambridge, MA, USA, March 7–8, 2002 Revised Papers 1.* Springer, 251–260.
[18] Khandokar Istiak and Apostolos Serletis. 2020. Risk, uncertainty, and leverage. *Economic Modelling* 91 (2020), 257–273.
[19] jbeezy. 2021, Sep. ARC: Add support for stETH (Lido). [Online]. Available: https://governance.aave.com/t/arc-add-support-for-steth-lido/5793.
[20] Jeiwan. 2022, Apr. Leveraged ETH staking strategy contract. [Online]. Available: https://github.com/Jeiwan/defi-strategy-eth-staking/tree/main/src.
[21] Johannes Rude Jensen, Victor von Wachter, and Omri Ross. 2021. An introduction to decentralized finance (defi). *Complex Systems Informatics and Modeling Quarterly* 26 (2021), 46–54.
[22] Justin Jia. 2016. Managing the revenue of sales platforms: Insights into service fees. *Production and Operations Management* 25, 6 (2016), 1026–1037.
[23] Joshua. 2022, Dec. Gas and Fees. [Online]. Available: https://ethereum.org/en/developers/do-cs/gas/.
[24] Ronald N Kahn, Matthew H Scanlan, and Laurence B Siegel. 2006. Five myths about fees. *The Journal of Portfolio Management* 32, 3 (2006), 56–64.
[25] Kshitij Kulkarni, Theo Diamandis, and Tarun Chitra. 2022. Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers. *arXiv preprint arXiv:2207.11835* (2022).
[26] Ivan Kuznetsov. 2022, Apr. Evaluating DeFi Strategies Using Foundry. [Online]. Available: https://jeiwan.net/posts/evaluating-defi-strategy-in-foundry/.
[27] Simon Loertscher and Andras Niedermayer. 2008. *Fee setting intermediaries: on real estate agents, stock brokers, and auction houses.* Technical Report. Discussion paper.
[28] Simon Loertscher and Andras Niedermayer. 2012. Assessing the Performance of Simple Contracts Empirically: The Case of Percentage Fees. (2012).
[29] Simon Loertscher and Andras Niedermayer. 2017. *Percentage fees in thin markets: An empirical perspective.* Technical Report. Mimeo.
[30] Simon Loertscher and Andras Niedermayer. 2019. *An optimal pricing theory of transaction fees in thin markets.* Technical Report.
[31] Dahlia Malkhi and Pawel Szalachowski. 2022. Maximal Extractable Value (MEV) Protection on a DAG. *arXiv preprint arXiv:2208.00940* (2022).
[32] Philémon Poux, Primavera De Filippi, and Bruno Deffains. 2022. Maximal Extractable Value and the Blockchain Commons. *Available at SSRN* (2022).
[33] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the defi ecosystem with flash loans for fun and profit. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I.* Springer, 3–32.
[34] Daniel Ramos and Gabriel Zanko. 2021. Ethereum 2.0–A Review of the Causes and Consequences of the Upcoming Update to Ethereum's Mainnet. (2021).
[35] Patrick Schueffel. 2021. DeFi: decentralized finance-an introduction and overview. *Journal of Innovation Management* 9, 3 (2021), I–XI.
[36] Stefano Sgambati. 2019. The art of leverage: A study of bank power, money-making and debt finance. *Review of international political economy* 26, 2 (2019), 287–312.
[37] Marwaan Simaan and Jose B Cruz. 1973. On the Stackelberg strategy in nonzero-sum games. *Journal of Optimization Theory and Applications* 11, 5 (1973), 533–555.
[38] Corwin Smith. 2023, Apr. Transactions. [Online]. Available: https://ethereum.org/en/developers/docs/transactions/.
[39] P Swathi, Chirag Modi, and Dhiren Patel. 2019. Preventing sybil attack in blockchain using distributed behavior monitoring of miners. In *2019 10th international conference on computing, communication and networking technologies (ICCCNT).* IEEE, 1–6.
[40] Dabao Wang, Siwei Wu, Ziling Lin, Lei Wu, Xingliang Yuan, Yajin Zhou, Haoyu Wang, and Kui Ren. 2021. Towards a first step to understand flash loan and its applications in defi ecosystem. In *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing.* 23–28.
[41] Ben Weintraub, Christof Ferreira Torres, Cristina Nita-Rotaru, and Radu State. 2022. A Flash (bot) in the Pan: Measuring Maximal Extractable Value in Private Pools. *arXiv preprint arXiv:2206.04185* (2022).
[42] Dirk A Zetzsche, Douglas W Arner, and Ross P Buckley. 2020. Decentralized finance (defi). *Journal of Financial Regulation* 6 (2020), 172–203.
[43] Shijie Zhang and Jong-Hyouk Lee. 2019. Double-spending with a sybil attack in the bitcoin decentralized network. *IEEE transactions on Industrial Informatics* 15, 10 (2019), 5715–5722.