SoK: DeFi Lending and Yield Aggregation Protocol Taxonomy, Empirical Measurements, and Security Challenges

Arad Kotzer, Tom Azoulay, Yoad Abels, Aviv Yaish and Ori Rottenstreich

***Abstract*—Decentralized Finance (DeFi) lending protocols implement programmable credit markets without intermediaries. This paper systematizes the DeFi lending ecosystem, spanning collateralized lending (including over- and under- collateralized designs, and zero-liquidation loans), uncollateralized primitives (e.g., flashloans), and yield aggregation protocols which allocate capital across underlying lending platforms. Beyond a taxonomy of mechanisms and comparing protocols, we provide empirical on-chain measurements of lending activity and user behavior, using Compound V2 and AAVE V2 as case studies, and connect empirical observations to protocol design choices (e.g., interest-rate models and liquidation incentives). We then characterize vulnerabilities that arise due to notable designs, focusing on interest-rate setting mechanisms and time-measurement approaches. Finally, we outline open questions at the intersection of mechanism design, empirical measurement and security for future research.**

***Index Terms*—Blockchain, Decentralized Finance (DeFi), Lending, Yield Aggregation.**

I. Introduction

The Decentralized Finance (DeFi) ecosystem had an estimated market size of more than 75 billion USD in 2024 [1], and comprises various financial services that run as blockchain applications [2], [3]. Typical DeFi platforms include decentralized exchanges (DEXs) such as Uniswap [4], that allow swapping one token for another (e.g., Ethereum and USDC, a "stablecoin" designed to maintain a peg with the US Dollar), lending platforms like Compound [5], which allow lending and borrowing funds, and yield aggregators that manage and invest user funds automatically. While these may sound similar to age-old financial institutions, the pseudonymous nature of popular blockchains and the difficulty in incorporating off-chain information in on-chain operations imply that experience from "traditional" systems may not apply to blockchain equivalents [6], [7], [8]. For example, consider one crucial question:

> *How can a blockchain lending platform ensure pseudonymous borrowers repay their debt in full?*

Two popular types of blockchain loans attempt to answer this question: (1) *Overcollateralized loans* which require borrowers to provide assets exceeding in value than the ones received in return. (2) *Flashloans* that are granted for the span of a single atomic operation only if the borrower proves the debt can be repaid in full by the end of the operation.

Despite the popularity of these primitives and related ones in the DeFi ecosystem, the SoK literature covering them is incomplete: (1) Notable SoKs adopt a single methodology, for example, the elegant formal modeling of collateralized lending platforms performed by Bartoletti *et al.* [9] does not provide empirical data. (2) Previous multi-method SoKs focus on specific types of platforms but do not systematize the lending ecosystem at large, e.g., Xu and Vadgama [10] consider yield aggregators in particular, and Gogol *et al.* [1] highlight the lack of work on undercollateralized lending platforms such as TrueFi. (3) SoKs that cover attacks involving the lending ecosystem tend to discuss manipulations that use loans as a means to execute attacks on other protocols (e.g., Automated Market Makers (AMMs) and oracle attacks [11]), without covering manipulations that target lending platforms and the protocols they rely on (e.g., interest-rate arbitrage [12], and utilization manipulations [13], [14]). (4) A recent SoK on AMM impermanent loss which does not focus on lending [15]. A summary of the related literature is given in Table I.

Contributions. In this work, we fill the aforementioned gaps. Our main contributions can be summarized as follows:

- **Lending ecosystem.** We systematically examine the ecosystem at large, including (1) collateralized lending pools, (2) flashloan providers, and (3) yield aggregators, and illustrate their relationship with one another.
- **Collateralized lending.** We cover the spectrum of collateralized lending platforms, including those providing over- and under-collateralized loans, and zero liquidation loans. We go over related empirical data, and highlight design considerations faced by platforms.
- **Vulnerabilities.** We discuss various ways in which actors could manipulate the ecosystem to their advantage, including attacks on core lending mechanisms, and also vulnerabilities that arise due to the ecosystem's reliance on specific blockchain consensus mechanisms.
- **Open questions.** We identify important open questions not fully addressed by the state-of-the-art. In particular, we shed light on the possibility of modifying existing attacks and extending them to target new mechanisms.

Paper organization. We organize the paper bottom-up from theoretic mechanisms, to empirical market behavior, and finishing with security challenges. We begin by fixing terminology and actors (in Section II), so that protocol designs

Arad Kotzer, Tom Azoulay, Yoad Abels and Ori Rottenstreich are with the Technion. Aviv Yaish is with Yale University, IC3, and Complexity Science Hub, Vienna. (Emails: aradk@campus.technion.ac.il, tomazoulay@campus.technion.ac.il, yoad.abels@campus.technion.ac.il, or@technion.ac.il, a@yai.sh)

Table I
A SUMMARY OF THE RELATED LITERATURE, COVERING SEVERAL REPRESENTATIVE SOKS AND SURVEYS.

Work	Scope	Methodology	Key Contributions	Gaps
Bartoletti *et al.* [9]	Collateralized Lending	Formal Modeling	Formalization of desired properties and proofs they hold	Lacks empirical measurements, does not cover yield aggregators
Xu & Vadgama [10]	Yield Aggregators	Survey & Taxonomy	A literature review and a characterization of major platforms	Treats underlying lending protocols as "black boxes"
Xu *et al.* [11]	AMMs	Survey & Taxonomy	A literature review and a characterization of major platforms	Does not study overcollateralized lending protocols, lacks empirical measurements
Zhou *et al.* [16]	DeFi Attacks	Incident Analysis	Quantification of attack losses and frequency, highlighting gaps in academic literature	Surveys general exploits (e.g., reentrancy attacks), lacks details on lending-focused manipulations (e.g., on interest-rate mechanisms)
Gogol *et al.* [1]	DeFi Ecosystem	Taxonomy	Classification of protocols into 3 categories, analysis of user risk exposure	Lacks empirical measurements, points to undercollateralized lending as a future challenge
Kotzer *et al.* [15]	AMMs	Survey & Taxonomy	A literature review and a characterization of impermanent loss	Does not study lending protocols

can be expressed in a common model. Then, we develop a taxonomy of lending primitives (in Section III), and map specific primitives and their compositions to notable protocols (in Section IV). We proceed by covering design considerations that platforms face and how these impact economic outcomes (in Section V). Following this mapping of the design space, we present empirical measurements that quantify how these mechanisms are used in practice (in Section VI). Moving upwards, we study yield aggregators (in Section VII), which compose several underlying lending platforms and automate interactions with them. Finally, we systematize manipulations that apply to studied designs (in Section VIII), present open questions driven by our taxonomy and empirical evidence (in Section IX), and conclude (in Section X).

II. System Model

To formalize the discussion of the decentralized lending ecosystem, we now provide a system model.

Blockchain: A blockchain is a decentralized ledger, structured as an immutable chain of blocks. Blocks are lists of transactions and ledger updates that are bundled together. Starting from the first block, the *genesis block*, each block includes the output of a cryptographic hash function computed over the content of the previous block, making it impossible to alter a block without changing all subsequent blocks. Blocks are appended to the chain and become available for read-only access, and typically cannot be deleted or modified.

Miner: Blocks are created by entities called miners. A miner has full control on which transactions to include in its block. Some blockchains call entities with the same or similar roles by other names, such as validators, proposers and builders. For simplicity, we only use the term "miner".

Smart contract: A program which is specified in code and deployed to the blockchain. A user can create a contract, invoke a contract's functions and even transfer money to a contract by sending transactions.

Transaction execution and fee: A transaction's creator pays a fee for its execution and inclusion in a block [17], which is proportional to the transaction's computational complexity as measured in a unit called gas. A transaction can be designed to revert operations it performed if specific conditions are met. A transaction pays a fee even if its actions are reverted [18].

Lending protocol: A platform comprising one or more smart contracts allowing users to take loans or deposit liquidity.

Stablecoin: A token that aims to have its value pegged to another asset. For example, the USDC token strives to maintain a one-to-one exchange rate with the USD. Throughout this work, we use the USD values of tokens (stablecoins or not) to serve as a common point of reference.

Loan: A loan is an amount of money borrowed and has to be paid back, usually together with an additional amount of money called interest.

Borrower: An entity receiving a loan in return for interest.

Liquidity provider: An entity providing liquidity to the protocol, typically in exchange for rewards, e.g., interest. Often, they are also called lenders.

Collateral: In collateral-based loans, a collateral is a guarantee provided by a borrower, which is returned to the borrower upon repaying the loan and any associated fees (e.g., interest).

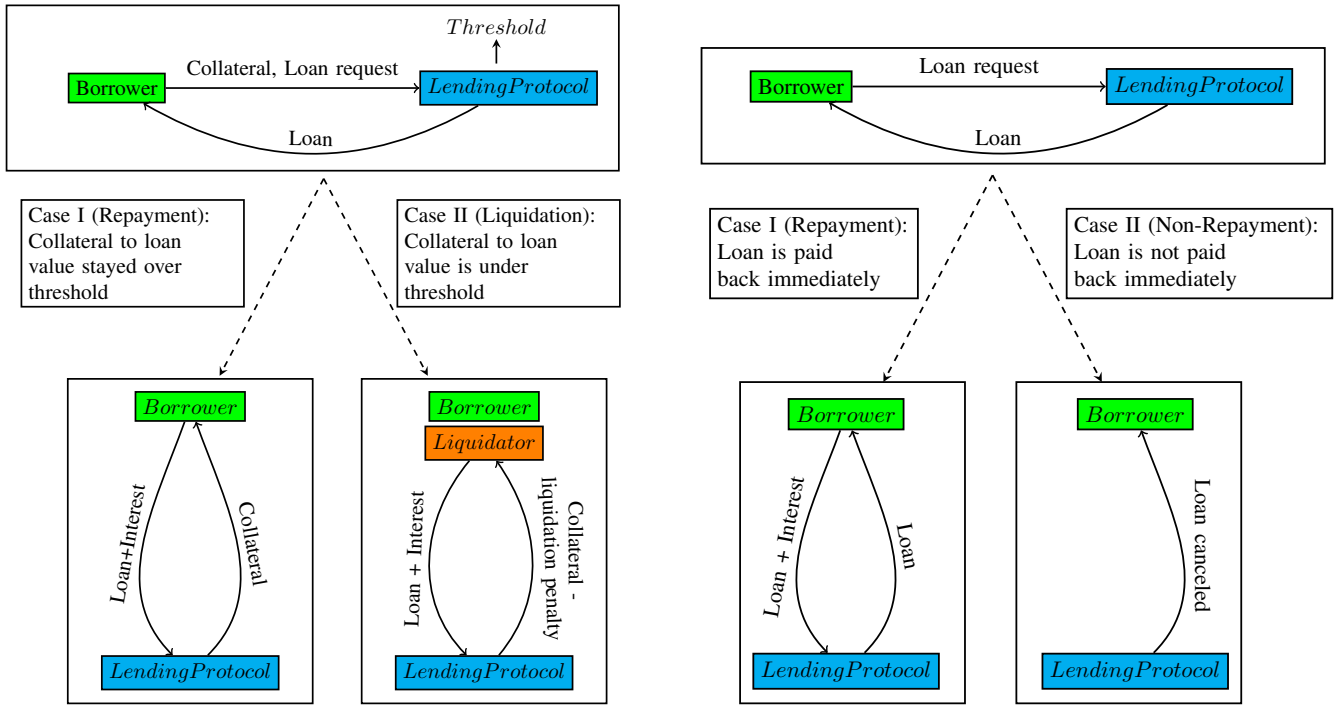
Liquidator: Collateralized loan protocols may protect liquidity providers from bad debt by selling a position's collateral if its value falls relative to the borrowed asset. Then, liquidators can purchase part of the collateral in exchange for the corresponding borrowed asset, possibly at a discount.

Yield aggregator: A platform which automates the process of supplying liquidity to DeFi platforms, often with the goal of maximizing the ex-ante return (yield).

III. Types of Loans

DeFi lending has emerged in recent years with the appearance of decentralized lending protocols, such as AAVE, Compound, Cream Finance, and MakerDAO [1]. [19], [20], [21]. While some DeFi platforms rely on a "permissioned" process to accept new customers and assess their credit risk, e.g., using Know-Your-Customer (KYC) checks [22], leading lending platforms are permissionless and do not require users to identify themselves using government-issued documents. Instead, platforms mitigate lending risks using alternative measures, which we now cover (see Table II for a summary).

[1]While the front-end interface was originally named the MakerDAO CDP Portal and has since been rebranded to Oasis.app and then to Summer.fi, the underlying protocol has always been the Maker Protocol, governed by MakerDAO. We use the name 'MakerDAO' to refer to this protocol.



(a) Overcollateralized loan

(b) Flashloan

Figure 1. Overcollateralized loans (Section III-A) and flashloans (Section III-B), depicted above, form the majority of lending activity.

Table II
NOTABLE CHARACTERISTICS OF THE MAJOR TYPES OF LOANS COVERED IN THIS WORK.

Characteristic	**Collateral-based Loans**			**Flashloans**
	Overcollateralized	**Undercollateralized**	**Zero Liquidation**	
Typical use-cases	Speculation, hedging	Financing	Speculation, hedging	Arbitrage, liquidations
Duration	Indefinite	Fixed	Fixed	Immediate
Loan funding	More than loan value	Less than loan value	More than loan value	None
Interest rate for borrowers	Dynamic	Fixed when taking loan	Fixed when taking loan	Fixed before taking loan
Interest rate for lenders	Dynamic	Dynamic	Set by lenders	Commission-based
Leverage obtained	Less than capital	More than capital	Less than capital	All the funds available

A. *Collateral-based Loans*

Overview. A collateral-based loan allows long lending durations and is typically financed by interest paid by the borrower to lenders. The interest owed is commonly based on the duration of the loan and market conditions [12], with interest rate curves possibly fixed in advance [20], adjusted as needed by the platform [23], or set on-the-fly by smart contracts [24]. As with traditional loans [25], collateral is used as a security in case a borrower does not return the loan [26], [27]. To protect lenders from borrowers unwilling or unable to repay their loans, platforms put up bad debt for liquidation [28].

In addition to the regular risk inherent in the ability of borrowers to return loans, DeFi lending has another source of risk, namely, the volatility of the cryptocurrencies that are used in the lending process [29]. Thus, the loan-to-collateral ratio of a given debt position can fluctuate wildly when a cryptocurrency is borrowed or used as collateral. This additional risk is mitigated by requiring debt positions to be over-collateralized: the collateral provided by a borrower has to be worth more than the loan that it covers. To avoid under-collateralization, lending protocols often define minimal liquidation thresholds (with typical values of 120-300%) for various cryptocurrencies. When the collateral-to-loan ratio falls below the threshold, the loan is liquidated and the collateral is sold at a discount. This eliminates the need to return the loan and causes a loss for the borrower since the collateral is worth more than the value of the loan. To reduce the chances of liquidation, borrowers can provide collateral of even higher ratios, or can top-up loans that get close to liquidation [14]. Unfortunately, both options imply low accessibility and high entrance barriers for potential borrowers, who either have to provide a large amount of capital up-front, or have to continuously monitor their positions.

Use cases. A collateral-based loan is used to obtain liquidity while speculating on an asset. A borrower holding a cryptocurrency such as ETH and speculating that its value

will increase can put the cryptocurrency as collateral. The borrower then takes a loan to have liquidity to perform other actions and later pays back the loan and is given the collateral back. The borrower enjoys the liquidity without selling the cryptocurrency used as collateral.

Illustration. A collateral-based loan works in the following way. For each type of collateral (a particular cryptocurrency), the protocol defines a liquidation threshold that serves as a lower bound for the ratio between the collateral value and the loan value. A potential borrower first supplies some collateral to the protocol for the right to take loans. The borrower can then ask for a loan up to a certain value based on the liquidation threshold that is defined by the cryptocurrency of the collateral. If a loan is taken, the collateral is locked until the loan, including interest, is repaid. As long as the lower bound is satisfied, the exact value of the ratio between the collateral value and the loan value is due to the borrower's choice. If the value of the collateral drops and the ratio of collateral to loan goes below the threshold, the collateral is liquidated by the protocol, thereby ending the loan of the borrower. Heimbach and Huang [30] find the average collateral to loan ratio is 1.644 and the median is 1.431, when considering all the loans taken between the 1st of January, 2021 to the 31st of March, 2023 from Compound V2, and both V1 and V2 of AAVE (combined, these held 80% of all value locked in lending platforms). These ratios are higher than the platform-imposed limits, suggesting that on average, users are conservative when taking loans, trying to avoid the risk of liquidation by providing high collateral.

Providing collateral worth more than the loan is required for several reasons. First, it motivates borrowers to return loans to avoid financial losses. Second, it deals with the risk of high volatility in the value of the collateral. For several reasons, such as network congestion or liquidity, there can be a delay (as for every transaction) between the decision about the need for liquidation and the completion of the liquidation process by the protocol, where Qin *et al.* [28] find that liquidations by the MakerDAO platforms have an expected duration of 2 hours with a standard deviation of 6.4 hours. During this time, the value of the collateral may drop even further. To sum up, a collateral-based loan ends in a combination of two outcomes:

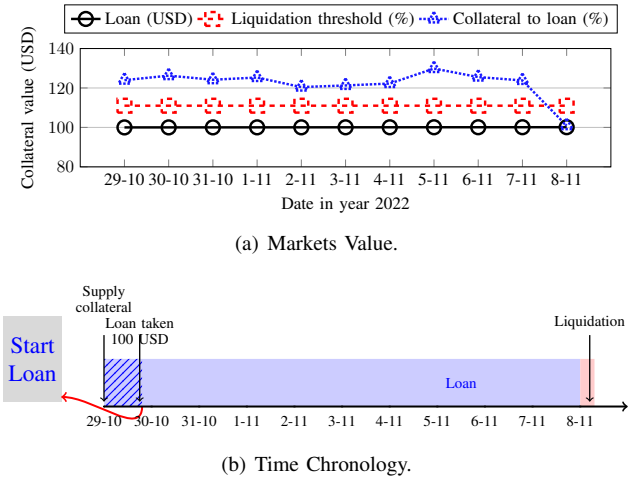
Case I (Repayment): The borrower repays the loan fully with interest and receives the corresponding collateral back.

Case II (Liquidation): A debt position is put up for liquidation when the collateral-to-loan ratio falls under the threshold upon the occurrence of any of the following scenarios:

- The collateral's value decreases
- The loaned asset appreciates in value
- Interest compounds over time, increasing the loan value

If a position is put for liquidation, entities called liquidators can repay the bad debt. In return, the liquidator receives the collateral of the borrower.

A combination of the above scenarios is also possible. Moreover, actors may choose to only partially liquidate a position [13], and liquidation opportunities may not always be seized by actors if, for example, the entailed costs (e.g., the required fees) outweigh the expected profits. In some cases, platforms can even opt to cover bad debt themselves when market forces are slow to do so [13], [31].



(a) Markets Value.

(b) Time Chronology.

Figure 2. An example of a real-world liquidation event.

We illustrate the process in Fig. 1(a) with the two potential cases of repayment (left) and liquidation (right). We highlight the involved entities in different colors: the lending protocol (light blue), the borrower (green) and the liquidator (orange).

Example. To provide real-world grounding, in Fig. 2 we go over an actual loan that was taken by a borrower[2] on October 29, 2022, and which was liquidated on November 8 of the same year as its collateral-to-loan ratio fell below 111.011%, the platform's threshold. Fig. 2(a) shows the daily values of the loan (in USD, in black), the liquidation threshold (in %, in red) and the collateral to loan ratio (in %, in blue). Fig. 2(b) presents the events over the same time period. First, a collateral is supplied on 29-10. A loan of 100 USD is taken on 30-10 such that collateral is worth more than 120% the value of the loan. On 8-11, the collateral value decreases below the liquidation threshold, resulting in liquidation shortly after.

Interest-rate. An important component in the design of a lending platform is its interest rate, paid by its borrowers and to its liquidity providers. The platform often benefits from differences between the rates of these two main players and from additional fees. Lending platforms typically define two types of interest rates:

(i) Borrow rate: the interest borrowers pay to the platform;

(ii) Supply rate: the interest rate paid by a platform to those providing liquidity to the protocol.

We denote these two rates by i_b and i_s, respectively. Inherently, supply rates are lower than borrow rates to allow financial gains of the platform. A major factor in the borrow and supply rates is the utilization - the ratio of borrowed funds among all available funds in the platform. We denote the utilization by U, which has values in $[0, 1]$. While there are protocols with rates that are fixed over time, most models are influenced by the utilization. Upon low utilization, interest rates are lowered to attract borrowers. Upon high utilization, a high interest rate incentivizes borrowers to reimburse, discour-

[2]Address: 0x3087E2A2081C189B40a6938eAA6973FF0FDE9a0F.

ages borrowers from borrowing more funds and encourages supplying liquidity to the protocol.

There are various variants of the rates. The rates can change dynamically over time (e.g., based on the updated utilization) or be fixed based on the rates at the time the loan was taken or liquidity was provided. The dependency of the borrow rate and supply rate can also have multiple forms: They can have a fixed ratio between their values or alternatively a ratio that is also a function of the utilization U. We detail later in Section IV some particular interest rate functions for major platforms. We overview here some of their general forms [20]. Often, there is a factor U between the borrow rate and the lower supply rate such that $i_s(U) = i_b(U) \cdot U$. Some models employ an additional multiplying factor of $(1-\lambda)$ where λ is a reserve factor such that $i_s(U) = i_b(U) \cdot U \cdot (1-\lambda)$. The factor U allows the lending platform to enjoy the difference between the borrow and the lower supply rate. Such a ratio makes it relatively more attractive to supply liquidity in times of high utilization. The value $(1-\lambda)$ can be seen as a conservative mechanism to increase the profit of the lending platform by enhancing the difference between the interest rates, even when the utilization is high.

1) Linear curve: Borrow rate $i_b(U) = \alpha + \beta \cdot U$. Here, α, β are some tunable parameters for a base rate and utility multiplier, respectively.
2) Kinked curve: This curve is piecewise linear and has a steeper slope after some predefined optimal utilization value U^*. The borrow rate has the form

$$i_b(U) = \alpha + \begin{cases} \beta \cdot U & U < U^* \\ \beta \cdot U^* + \gamma \cdot (U - U^*) & U \geq U^* \end{cases}$$

   Here, γ indicates the increase in the slope value.
3) Non-linear curve: This curve is relatively generic and can have multiple forms such as with borrow rate of

$$i_b(U) = \alpha \cdot U + \beta \cdot U^b + \gamma \cdot U^c$$

   where b, c can have values of tens, such as 32 and 64.

B. Flashloans

Overview. A flashloan is a type of loan that is taken and returned within a single transaction without collateral [32], [33]. We provide an illustration of the process in Fig. 1(b). The debt is protected by the atomicity enforced by smart contracts: If the loan is not repaid with interest within the block, the whole transaction with a flashloan is canceled.

Flashloans enjoy three key advantages [34]:

- No collateral: The borrower is not required to provide collateral for taking a loan.
- No default risk: The lender has no concern of potential default of the loan due to the atomicity and the return of the loan within the same block.
- High loan values: Flashloans allow for taking loans of higher values based on liquidity available that can be utilized for the time of a single block.

Use cases. Flashloans are popular for obtaining very large amounts of capital without collateral. They can be used to take advantage of arbitrage across different DEXs [35], [36], to execute liquidations [13], or for attacks and manipulations that require large amounts of capital [16]. Flash loans are also useful for collateral swaps in which borrowers switch the collateral backing a loan in a lending platform by an alternative collateral of a different cryptocurrency [37].

Illustration. In a flashloan, a potential borrower asks for a loan on a protocol allowing flashloans. The platform approves the loan as long as it has enough funds for such a loan. The borrower then adds additional actions to the transaction and sends all the actions he wants to take bundled in one blockchain transaction or a short sequence of transactions. The protocol checks whether the loan has been repaid with interest by the borrower within the same block. All transactions pertaining to the same block have the same timestamp, and therefore are considered to have happened simultaneously. If this is the case, the protocol receives the loan value with its interest. If not, the protocol reverts the transaction and the loan is canceled. This allows the protocol to return to the state before the loan. Flashloans have proved applicable but were also used in attacks that involve attackers with low funds [34].

In its common form, a flashloan is taken and repaid in the same cryptocurrency. Uniswap V2 [38] allows for some flexibility with the participation of a decentralized exchange with a liquidity pool that allows the exchange of two cryptocurrencies. By the common Automated Market Maker (AMM) model, such a pool holds a pair of cryptocurrencies and follows the constant product formula:

$$x \cdot y = k,$$

where x is the quantity of the first cryptocurrency in the pool and y is the quantity of the second cryptocurrency. The formula determines the dynamic exchange rate of the two cryptocurrencies based on their current quantity. Uniswap V2 allows the loan to be returned by an alternative cryptocurrency that constitutes a pool with the original cryptocurrency in which the loan was taken. In such a case, the repayment should include also a swap fee.

Interest rate. Flashloans are taken for the span of a single transaction, i.e., such a loan is "atomic" and can be thought of as being taken for an infinitesimal duration. Due to this, flashloans do not rely on time-based interest rates; instead, platforms charge borrowers fees as a function of the amount taken. In particular, AAVE V2 charges 0.07%, AAVE V3 charges 0.05% [39], and the rate in Uniswap V2 is 0.3% [40].

C. Zero Liquidation Loans

The so-called zero liquidation loans are proposed by Sardon [43]. Such loans are given for a fixed loan duration, and, as in a collateral-based loan, potential borrowers need to provide collateral. Given some collateral, a borrower is then able to take a loan of a value that equals some portion of the collateral value. The loan is only terminated at the end of the set term and cannot be liquidated beforehand, hence the name. Termination proceeds in one of two ways: the loan is either repaid fully with interest, or the collateral is forfeited. Since the value of the collateral may decrease,

Table III
MAJOR LENDING PLATFORMS DETAILS AS OF JANUARY 2025 [41]. "TOTAL VALUE LOCKED (TVL)", "CURRENTLY BORROWED FUNDS" ARE IN USD. PROTOCOLS WERE SELECTED TO COVER THE MAIN LENDING DESIGNS DISCUSSED IN SECTION IV, WHILE PRIORITIZING ECONOMICALLY SIGNIFICANT ONES. WE NOTE THAT WHILE DYDX DISABLED NEW LENDING POSITIONS ON NOV '21, THE PLATFORM IS STILL OPERATIONAL AND SUPPORTS OTHER OPERATIONS [42]. "–" DENOTES CHARACTERISTICS WHICH ARE IRRELEVANT (E.G., LIQUIDATION THRESHOLDS FOR FLASHLOAN PLATFORMS).

Characteristic	AAVE	Compound	MakerDAO	dYdX (lending)	Uniswap	Maple	TrueFi
Activity period	Nov '17 -	Sep '18 -	Dec '17 -	Jul '17 - Nov '21	Nov '18 -	May '21 -	Nov '20 -
Total value locked (TVL)	$5.58B	$1.85B	$6.24B	$0	$6B	$490.62M	$14M
Number of forks	65	143	3	1	809	0	0
TVL of forks	$5.45B	$2.87B	$0.5B	$0	$4.5B	$0	$0
Loan types	Over-collateralized, Flashloans	Over-collateralized	Over-collateralized, Flashloans	Over-collateralized, Flashloans	Flashloans	Over-collateralized	Under-collateralized
Tokens supported	34	17	1	3	100	6	4
Notable supported tokens	ETH, DAI, USDC, USDT	ETH, DAI, USDC, USDT, WBTC	DAI	ETH, DAI, USDC	ETH, DAI, USDC, USDT, WBTC	ETH, USDC, WBTC	USDC, USDT
Typical liquidation thresholds	114-250%	117-167%	150%	115%	–	Time-based	Time-based
Borrowed funds	$2.75B	$0.753B	$4.7B	$0	–	$225.35M	$15.01M

in order to ensure security, both the collateral-to-loan value and the interest rate are high in zero liquidation loans. One platform offering this type of loan is MYSO [44]. Among the drawbacks of such a protocol are very high interest rates and the potential loss in case of a price drop of the collateral. In such a case, the protocol ends with a collateral value lower than the loan value, implying a loss to the lending platform. Zero liquidation loans can be attractive for borrowers due to eliminating the uncertainty in the potential risk of liquidation. A borrower does not have to closely track the value of the collateral, and has certainty as to the loan repayment amount. From the platform's perspective, the fixed loan term, larger collateral, and higher interest rates reduce risk. Moreover, based on the estimation of price volatility and the correlation among cryptocurrencies, the platform can limit the collateral to be in particular cryptocurrencies and request high initial collateral-to-loan values.

IV. DEFI LENDING PLATFORMS

Having defined the core lending primitives, we now examine how major platforms instantiate and combine them. Decentralized lending platforms offer various services. A small number of them cover the majority of the total value of the provided liquidity and borrowed funds. Almost all of these platforms support collateralized loans, and three of them also support flashloans. Table III details the main characteristics of the lending platforms covered in this section. Table III is not intended as an exhaustive list of all live lending protocols, but rather to present notable designs, whether due to economic significance (e.g., when considering January 2025 TVL for protocols deployed on Ethereum, the two leading lending platforms were AAVE and MakerDAO, Uniswap was the top decentralized exchange, and, when considering the combined TVL of all forks, Uniswap and Compound V2 rank first and second) or to cover distinct designs (e.g., dYdX featured non-linear interest rates, while Maple and TrueFi supported under-collateralized loans for institutions).

AAVE. AAVE is a decentralized platform that deployed three versions of its platform (AAVE V1, V2, and V3) on eight different blockchains. It supports both collateral-based loans and flashloans. For collateral-based loans, AAVE uses kinked interest rate curves (see Section III-A).

AAVE accrues interest according to the time since a debt position was created. The platform measures elapsed time using the blockchain's per-block timestamps. Interest accrual is "lazy" and performed when a user performs any action that reads or modifies its balance [45]. AAVE *tokenizes* lending positions by representing them using a derivative "aToken" for each supported token (e.g., AAVE's USDC derivative is called aUSDC) [46]. Thus, when a user deposits some amount of a specific token to an AAVE pool, the platform mints an equal amount of the corresponding aToken, which can be exchanged at any time for an equal amount of the original token.

Lastly, AAVE monitors a position's solvency using a so-called "health score" for each borrower on the platform. When a health score is below 1, the position can be liquidated.

Compound. Compound deployed three versions of its platform (Compound V1, V2 and V3) across three different blockchains. It employs the kinked model for the interest rate (as defined in Section III-A). To illustrate, the curve of blue squares in Fig. 3 and Eq. (1) depicts the interest-rate curve currently used by Compound's ETH pool [47]. Diving into the technical details, the pool employs an optimal utilization value of $U^* = 0.9$, a base rate equal to $\alpha = 3.17 \cdot 10^{-10}$, a "low" slope of $\beta = 4.91 \cdot 10^{-10}$ when utilization is below U^*, and a "high" slope equal to $\gamma = 3.99 \cdot 10^{-8}$. The resulting interest rate function is thus:

$$i_b(U) = 3.17 \cdot 10^{-10} + \begin{cases} 4.91 \cdot 10^{-10} \cdot U & U < 0.9 \\ (4.42 + 399(U - 0.9)) \cdot 10^{-10} & U \geq 0.9 \end{cases} \quad (1)$$

As discussed in Chaudhary *et al.* [48], in selecting the interest rate model, Compound makes a distinction based on the level of risk of cryptocurrencies. An example can be six principal cryptocurrencies offered in the Compound

protocol in February 2020: The Stablecoins USDC, Tether and DAI and other cryptocurrencies ETH, ZRX and WBTC. While the average slope for stablecoins was 0.07-0.1, for the risky cryptocurrencies, the slope had an average value of 0.3. Accordingly, upon the utilization increases by 1%, for stablecoins the interest rates increase by 7 to 10 basis points, and by 30 basis points for the risky cryptocurrencies.

Compound calculates accrued interest by measuring elapsed time according to the number of blocks created, under the assumption of a fixed inter-block time interval. Wrapping-up our overview of Compound's technicalities, we note that it allows positions with a low collateral-to-loan ratio to be liquidated by liquidators.

MakerDAO. MakerDAO facilitates borrowing using collateralized debt positions, or CDPs, in short. To borrow funds, a user can create a CDP by providing collateral, against which the platform creates (mints) new DAI tokens that are given to the user. As of 2023, the platform is deployed on the Ethereum and Optimism networks and has outstanding borrow positions with a value of 1.5 billion USD, backed by collateral worth 4.4 billion USD. The platform enables both collateral-based loans and flashloans. To allow flashloans, the platform supports a special action called flash. The user is able to generate DAI without collateral but must return it with an interest rate in the same transaction. This platform uses the term "stability fee" to refer to its interest rate. MakerDAO uses the stability fee to maintain a dollar peg. Therefore, if DAI is worth less than one USD then stability fees increase to refrain from generating more DAI. If the situation is reversed, the stability fee will go down. Unlike the common scenario among platforms, the stability fee is not predetermined by a known function of the utility, but is rather subject to update on a weekly basis. Liquidation is performed in an auction approach in which keepers offer a bid on the collateral.

dYdX. The dYdX platform deployed two versions of its decentralized overcollateralized lending protocol (dYdX V1, V2) on the Ethereum blockchain. The platform disabled collateral-based borrowing functions in 2022 due to low utilization of funds that led to unprofitable results. Similar to previous platforms, interest in this platform is based on utilization. The platform's interest rate curves follow the non-linear model introduced in Section III-A. While the platform does not allow new lending positions anymore, some of the previous values it used to set the interest rate are still available [49]. When using the parameters $\alpha = 70 \cdot 2^{-10}, \beta = 10 \cdot 2^{-10}, \gamma = 20 \cdot 2^{-10}$ and $b = 32, c = 64$, we obtain the following interest-rate curve:

$$i_b(U) = (70 \cdot U + 10 \cdot U^{32} + 20 \cdot U^{64}) \cdot 2^{-10} \qquad (2)$$

The resulting curve is illustrated in orange circles in Fig. 3, and as a comparison with the curve of Compound V2 (blue squares) shows, it can be seen as a smoothed approximation of a kinked curve.

Uniswap. Uniswap is a decentralized cryptocurrency exchange (DEX) that operates on the Ethereum blockchain, established in 2018. As was detailed in Section III-B, Uniswap relies on a model named Automated Market Maker (AMM) with the use of liquidity pools to enable trading. Each pool is a collection of

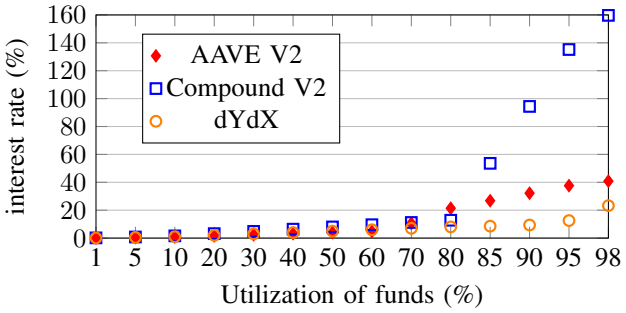


Figure 3. The interest rate as a function of utilization in various platforms.

a pair of cryptocurrencies with an exchange rate determined by their amounts in the pool. Uniswap allows liquidity providers to provide liquidity to pools and enjoy, in return, revenues from their fees. Uniswap supports flashloans. In addition, it also supports flashswaps, which, unlike flashloans, the repayment of a loan is done in a possibly different cryptocurrency than in which the loan was taken, assuming the availability of a pool connecting the two cryptocurrencies. Similarly to flashloans, this is done atomically in a single transaction, without collateral and is often used to take advantage of arbitrage opportunities. Uniswap charges a fee of 0.3% on the borrowed amount, in each of its versions V2 and V3.

Maple. The Maple Finance platform launched in 2021 [50], initially supporting both over- and under-collateralized loans for institutional borrowers. As of 2023, the platform has turned its focus to over-collateralized loans [51]. Maple performs KYC checks on new users. Such processes can include the collection of documents for identification, accreditation checks and the disclosure of financial information to estimate potential risk. Maple operates two major pools that support different major cryptocurrencies: 1. The "Blue Chip" secured pool, where lenders deposit USDC and can provide BTC or SOL tokens as collateral. 2. The "High Yield" secured pool, which accepts a wider range of assets and may have higher interest rates for lenders. In July 2024, Maple Finance launched another service named Syrup that aims to make lending services accessible to individuals. Syrup is permissionless and does not require KYC. To deal with temporary low interest rates, Maple supports open term loans, which can be ongoing but with the ability of the platform to force a borrower to repay a loan within 14-30 days so the loan can be reissued later at better conditions for the platform. This allows Maple to support loans with fixed interest rates that are known in advance and not affected by changes in the platform's utilization.

TrueFi. TrueFi is a decentralized lending platform that connects lenders, borrowers such as small businesses, and portfolio managers via smart contracts governed by the TRU token. The platform facilitates under-loans, allowing borrowers to access capital without providing collateral, and lenders to earn returns on their investments. Staking TRU on the protocol enables stakers to govern the protocol by voting on-chain with regard to loan requests and the approval of new borrowers. While voting is based on risk assessment, such staking also invokes risk, as in the event of a default in one of the

DAO pools, a certain percentage of the staked TRU will be liquidated and transferred to the central lending pool. TrueFi interest rates are influenced by utilization, with an upper bound set by the borrower. Lenders earn a dynamic rate based on the pool utilization and interest rate curve configuration. Since its launch in November 2020, TrueFi has originated more than 1.7 billion USD in loans to more than 30 borrowers.

V. Design Considerations

In this section, we study the various design considerations of lending platforms. We refer to financial aspects, the engagement of important entities, and necessities such as security.

A. Liquidity Providers

A platform's functionality hinges on the availability of funds, enabling borrowing and other activities. The lending platforms are funded by investors which are called liquidity providers, and all the invested money is concentrated in a singular place: the liquidity pool. To incentivize the liquidity providers to provide the necessary funds, they are rewarded with a share of the platform's profits. Borrowers, in turn, contribute to these profits by paying interest.

The platform's interest rates are set according to the utilization rate of its liquidity pools. Platforms aim to keep it above a certain level to make reasonable profits but below a certain level to not endanger the protocol in case of defaults. As presented for borrowers, the higher the utilization of the platform the higher the rewards which attract liquidity. Rewards for fidelity are also distributed to provide an additional reward of use. If utilization is too low, the reverse happens. The rewards are very low so liquidity providers will provide fewer funds, reducing the utilization.

B. Interest Rate Model and Borrowers

Interest rates in DeFi lending platforms have two main forms. The interest rate can be fixed at different periods, like in MakerDAO, or dynamically change based on the utilization, and the ratio of borrowed funds among all available funds in the platform. The lower the utilization, the lower the interest rate to attract borrowers. Upon high utilization, a high interest rate incentives borrowers to reimburse and prevents borrowers from borrowing more funds. AAVE and Compound have a slope of interest, which is dependent on utilization. They divide the slope into two domains one below optimal utilization and one above what is named the optimal utilization rate. Yearly borrow interest rates are per-assets based, varying between 0.5-12% in most cases. Fig. 3 shows the slope for ETH in three platforms: Compound V2 with blue squares, dYdX with orange circles and AAVE V2 in red diamonds. Optimal utilization is different on the platforms as Compound takes a more aggressive approach which causes very high interest rates when that threshold is passed.

C. Liquidation Processes

Liquidation is not an automatic process. It is based on a financial incentive. For each asset, a liquidation threshold is set. When the collateral-to-loan value is under the threshold the assets of the collateral are eligible for liquidation by anyone who is willing to repay the loan (including interest). In exchange, the liquidator receives a part of the collateral. The remaining share of the collateral, often called the liquidation penalty, is kept by the protocol. As liquidation thresholds have values larger than one, the collateral's value is greater than the loan's value, allowing the remainder to be divided between the liquidator and the protocol. The threshold typically aims to reflect the price stability of an asset. Generally, the higher an asset's price stability, the lower the threshold, as collateral can be sold without expecting a significant loss in value.

To liquidate a loan there exist two alternative processes.

First come, first served. By this process, the first liquidator to submit an account for liquidation will obtain it. Therefore, opportunities are taken very rapidly by bots that optimize the transaction and work in concert with miners to get their transactions included and obtain the liquidation. Some liquidators do not even own enough funds and rely on flashloans to make a profit, repaying it with their profits.

Auction. In an auction mechanism to liquidate an account, an auction is opened. The auction is closed when the time limit is reached, or no new bid is submitted for a long period. This approach leads to a slower liquidation process but a more rewarding one for the protocol because the liquidator who repays the loan while receiving the minimal part of the collateral wins the auction.

Qin *et al.* [28] looked into the different liquidation processes. Some of their findings include showing that liquidation deeply favors the liquidator to the borrower's detriment. Liquidation is an essential process for the health of a platform. If liquidation is not performed, the value of the collateral may drop further and end up being lower than the debt. This results in what is called bad debt of type I. A bad debt of type II relates to another effect. The excess of the collateral compared to the loan that the liquidator receives is his gain. This gain is sometimes lower than the transaction fee of the liquidation; therefore, the liquidator will not cover the debt because it is not profitable. Since transaction fees are dynamic, this type of bad debt can become profitable again. An additional parameter to consider is the amount of the discount offered to liquidators on the collateral. The trade-off is between how fast the loan can be liquidated to avoid bad debt versus the amount of money the protocol keeps as a liquidation penalty. Missed opportunities in liquidation and also borrowing are investigated by Yaish *et al.* [13], indicating that liquidators can compete to improve on sub-optimal transactions.

VI. Empirical Overview of Compound V2 and AAVE V2

After describing the theoretical design space, we quantify how these mechanisms behave in real deployments using real-world data. We review data from *The Graph* [52] - a decentralized protocol for indexing and querying blockchain data across a large number of networks. We focus on two protocols: Compound V2 and AAVE V2, both implemented over Ethereum, based on the indexed subgraphs in The Graph.

We focus on these two platforms as examples of major platforms which support over-collateralized loans (see the TVL value in Table III).

Note that it is difficult to identify whether a user makes use of two account addresses. Accordingly, in the analysis, we use the term address while potentially one user might hold more than a single address.

A. Source of Data and Transaction Types

We collect each protocol's transactions across various contracts. In The Graph's data model, each subgraph exposes two event streams and state snapshots. Event entities are an indexed log of protocol actions where each record represents an on-chain action with its timestamp, asset and size. The per-address histograms come from grouping borrow events by borrower. The token pie charts come from grouping borrow events (loans) and deposit events (collateral) by asset, by number of transactions. We use the different events to build a profile for an address with its transaction list.

We made this analysis' code available in [53]. We pulled data via GraphQL POST requests to The Graph Gateway endpoint, iterating month-by-month over the time window and paging through each entity list in deterministic order. For both event roots (e.g., borrows, deposits, repays, withdraws, liquidates, and flashloans where available) and snapshot roots (e.g., marketDailySnapshots, financialsDailySnapshots, usageMetricsDailySnapshots), the collector queries are parameterized with a per-month timestamp filter and pagination on the entity id, ordered ascending by id. Each request fetches up to first=1000 rows (one page) at a time. Rows are flattened into a stable CSV header and appended to a per-month CSV part; at the end, the monthly parts are concatenated into a single file per platform and root for downstream analysis.

The analyzed events are the following:

Borrow: whenever an address borrows an asset. The field named "account borrows" contains the total amount currently borrowed (including interest) for the asset.

Repay (Reimbursement): This event mentions the amount paid and the leftover debt of the account (0 in case of full repayment). The payment can be made by any account, not necessarily the address that borrowed the asset.

Deposit (Collateral Supply): Providing coins to the platform in one of the accepted assets to allow lending at a later time.

Withdraw (Collateral): This event represents removing of supplied assets that were supplied as collateral from the protocol. This is not possible if the coins in the base asset serve as collateral for an open borrow.

LiquidateBorrow (Liquidation): The borrower's loan is paid back by another address (i.e. liquidator). This liquidator can then claim the borrower's collateral.

The data covers the time period until January 2024. For Compound V2, the data spans block numbers 7710833 (Tue May 07 2019 01:41:22 GMT) and 19129417 (Wed Jan 31 2024 22:24:47 GMT), roughly 57 months. For AAVE V2, the data spans block numbers 11363052 (Mon Nov 30 2020 23:11:40 GMT) and 19129823 (Wed Jan 31 2024 23:46:47 GMT), roughly 38 months.

Table IV
COMPOUND V2 - DISTRIBUTION OF LENDING EVENTS.

Lending event type	Number	Value (in Billion USD)
Borrow	219739	101
Repay (Reimbursements)	189566	96.4
Deposit (Collateral Supply)	948257	304.9
Withdraw	504540	305
LiquidateBorrow (Liquidation)	18407	1.1

Table V
AAVE V2 - DISTRIBUTION OF LENDING EVENTS

Lending event type	Number	Value (in Billion USD)
Borrow	252590	95.6
Repay (Reimbursements)	21197	4.23
Deposit	471800	380.5
Withdraw	358165	371.3
LiquidateBorrow (Liquidation)	28972	1.2

B. Lending Protocol Statistics

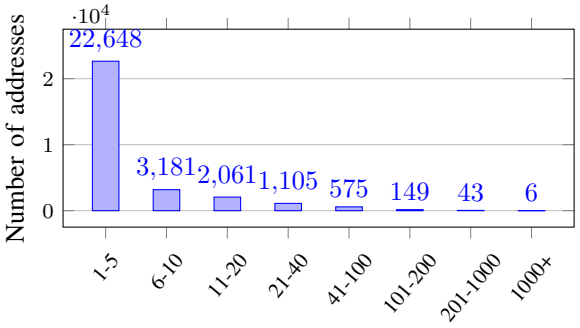
We present statistics from each of the platforms and highlight some of their similar and different properties. Note that a liquidation event does not refer to particular loans but to a borrower with its aggregated total updated debt.

Compound V2. In that platform, we observe a total of 29768 borrowers. Among them, 4656 (15.64%) were liquidated at least once. The number of liquidations is 18407 with 2923 borrowers being liquidated more than once. Table IV presents the transaction types and their importance in the model. The most common event is supply of collateral.

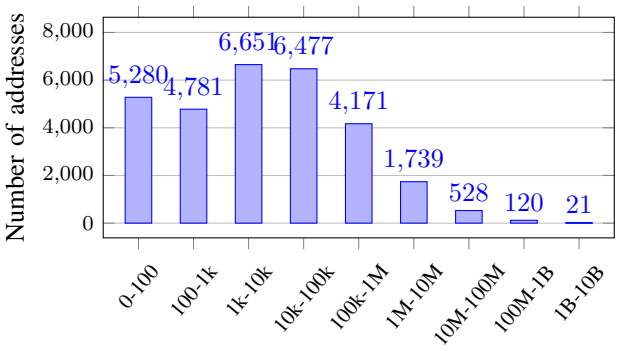
Similarly, Fig. 4(a) and Fig. 4(b) represent the distribution of the number of transactions each address performed and the value loaned by an address. Most accounts have a relatively small total number of transactions and borrow a low amount of funds. Over the analyzed time period, the average collateral to debt ratio (i.e., the total collateral value deposited versus the total value loaned) is 348.5%.

There is a difference in the distribution of types of cryptocurrencies in which collaterals are provided and in which loans are taken. Fig. 4(c) shows the cryptocurrencies in which loans are taken. Similarly, Fig. 4(d) shows those cryptocurrencies in which collateral was provided. While in both the two most common cryptocurrencies were USDC and DAI, their portion changes and we also observe major changes in the ratio of USDT and ETH among the two scenarios.

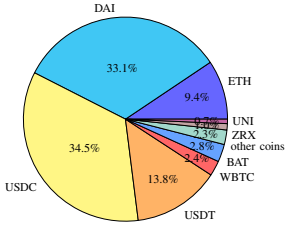
AAVE V2. We observe 53514 borrowers for this platform. Among them, 6042 borrowers (11.29%) were liquidated once or more and 4299 borrowers were liquidated at least two times. The average collateral to debt ratio was similar but slightly lower as 333.3%. Table V shows the distribution of events in the platform, indicating the popularity of the supply collateral event also here. One potential reason for the relatively low number of repay events in AAVE V2 is the gradual launch of AAVE V3 during 2022 and 2023. Fig. 5(a)-Fig. 5(d) present the distribution of the number of loans and aggregated values of loans per address as well as the distribution of tokens in loans and collateral.



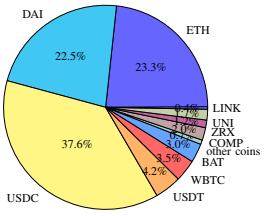
(a) Number of loans per address.



(b) Aggregated values of loans per address.

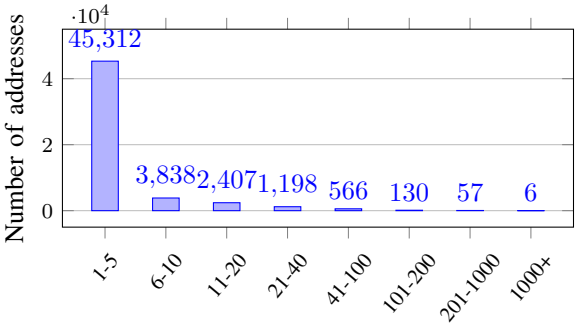


(c) Token distribution in loans transactions requests.

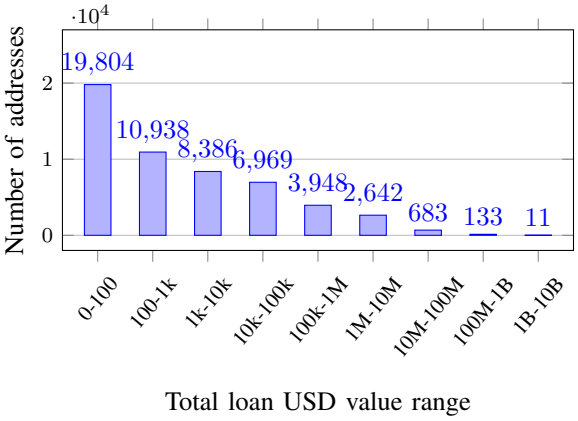


(d) Token distribution in collateral transactions.

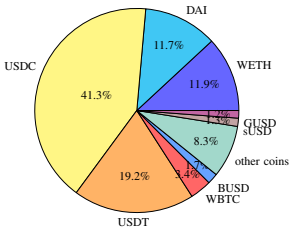
Figure 4. Compound V2 data analysis - Distribution of the number of transactions and total values of loans per address.



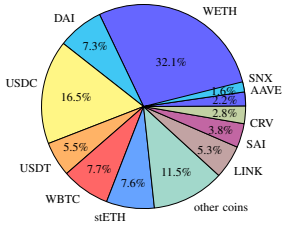
(a) Number of loans per address



(b) Aggregated values of loans per address



(c) Token distribution in loans transactions requests



(d) Token distribution in collateral transactions

Figure 5. AAVE V2 data analysis - Distribution of the number of transactions and total values of loans per address.

High-level comparison. There are many angles by which such a simple analysis can show similarity and dissimilarity among the two platforms.

- Overall, for most event types, the total value in USD has the same order of magnitude in both platforms. An exception is AAVE V2 repayment value, which is low.
- In both platforms, a high portion of borrowers perform 1-5 loans with a corresponding ratio of 76.1% in Compound V2 and a higher ratio of 84.7% in AAVE V2. In both, there are roughly 200 borrowers with 100 loans or more.
- The total loans value in USD per borrower has a different distribution on the two platforms. In Compound V2, 22.3% of them have a value between 1k-10k USD, and 17.7% have at most 100 USD. In AAVE V2, only 15.6% have 1k-10k USD and those with 0-100 USD are frequent with a ratio of 37%. This aligns with the typically lower number of loans per borrower in AAVE V2.
- Stable coins like USDC, USDT and DAI are common in both platforms as the cryptocurrency in loans with variable popularity. In both platforms, ETH (or its form as WETH) is more than twice as common when used as collateral than as a loan.
- Another point refers to the distribution of the time between pairs of events performed by the same address. This is summarized in Table VI with units shown in either days (D), hours (H) or minutes (M). We compare the time between deposit and borrow as well as between borrow and repay among addresses participating in two such events in that order in the recorded time period. In both platforms, the values between deposit and borrow are typically lower than between borrow and repay. Intu-

Table VI
STATISTICS OF TIME DIFFERENCE BETWEEN EVENTS IN COMPOUND V2 AND AAVE V2. VALUES APPEAR IN UNITS OF DAYS (D) OR HOURS (H) OR MINUTES (M).

	Compound V2		AAVE V2	
	deposit → borrow	borrow → repay	deposit → borrow	borrow → repay
Mean	23.36 D	47.45 D	9.95 D	68.80 D
Std	86.32 D	111.03 D	53.49 D	120.95 D
10%	1.28 M	6.53 M	0.95 M	12.41 H
Median	21.84 M	7.01 D	7.06 M	22.89 D
90%	44.00 D	132.65 D	4.25 D	172.22 D

itively, deposit events have the goal to allow borrowing while the loan itself can be taken out for a meaningful time. Likewise, the median values for the first time difference are in the scale of minutes and for the second time difference are in the scale of days. Interestingly, the time difference between deposit and borrow is typically shorter in AAVE V2 than in Compound V2; Values are lower in Compound V2 compared to AAVE V2 for the time difference between borrow and repay. While typically values are at a similar scale, for the second time difference, in Compound V2 we observe several very low values bringing the 10% to be in the scale of minutes while its scale is in hours for AAVE V2.

VII. YIELD AGGREGATORS

In this paper we distinguish between *protocol types* and *user strategies*. DeFi *lending protocols* implement borrowing and lending primitives. They are typically governed by interest-rate models, and, when collateralized, liquidation mechanisms. *Yield farming* focuses on deploying capital into DeFi protocols (including lending and DEX liquidity pools) to earn interest, fees and other rewards. *Yield aggregators* automate such strategies by allocating funds across underlying venues via vaults that rebalance and compound returns. While the mechanics of yield aggregators and lending protocols differ, the two types of platforms are inherently closely tied together due to the fact that aggregation platforms invest in lending protocols.

Yield farming is a notable user strategy in Decentralized Finance of providing liquidity to DeFi protocols in exchange for fee participation rewards or interest [10]. The process of yield farming works as follows: First, the investor (yield farmer) supplies liquidity to a DEX or lending platform by depositing a pair of cryptocurrencies or lending its tokens to a platform. Once farmers provide liquidity, they usually receive receipt tokens (e.g., LP tokens in AMMs or interest-bearing tokens in lending protocols) in return. These tokens represent their share of the liquidity pool and can be redeemed later to withdraw the original assets and any rewards earned. Rewards are gained from transaction fees generated by the platform, and can also include interest or governance tokens. Rewards can vary depending on the amount of liquidity provided and the demand for liquidity on the platform. When farmers want to redeem their funds, they initiate a transaction to redeem receipt tokens and profits back to the original funds.

Yield farming offers higher returns compared to traditional finance, attracting investors seeking to optimize their capital. Additionally, usually, the yields are reinvested to increase the revenue even more, performing as a compounding mechanism. Yield farming was first popularized in 2020 by the leading PLF Compound by introducing its governance token *COMP* [54]. Compound participants get rewarded with newly minted COMP tokens through both lending and borrowing activities, which lead to offsetting some loan costs for borrowers and increasing the return for lenders. This incentive scheme was quickly adopted by other protocols such as Uniswap [4] and Yearn Finance to attract liquidity and participation.

Yield aggregation protocols are designed to simplify and optimize yield farming. Manual yield farming requires hands-on monitoring and actions by actors, who may pay higher than necessary fees when redeeming their assets. On the other hand, yield aggregators automate yield farming strategies and try to reduce transaction fees. Yield aggregators consist of several *vaults*, where each vault represents a liquidity pool that employs automated strategies to optimize returns. Each vault uses different strategies to maximize revenue. Investing in a yield aggregator works as follows: First, the investor chooses a yield aggregator protocol and a vault (or multiple vaults). Then, the investor transfers tokens to the desired vault. The yield of the vault is automatically invested back in the vault, allowing a compound interest. As with traditional yield farming, re-investing the vault's yield required initiating a transaction. Yet, since the vault consists of funds of multiple investors, the transaction fees are split between the investors, reducing the fee of each user.

A. Yield Aggregation Trends

As the DeFi market is relatively new and major changes still occur on a regular basis, we provide an overview of the trends regarding the top yield aggregators in the market. Xu and Reap [10] performed an analysis of the market share information of the top yield aggregators in August 2022. By that time, the total TVL locked in yield aggregators was around 1.5B USD. In January 2025, this number increased to 2.7B USD. Despite the TVL increase, the market is far beyond its peak of 12.85B USD, reached in December 2021.

Table VII presents the top yield aggregators (in TVL) as of January 2025 and the top ten in August 2022 presented in [10]. The data was taken from DefiLlama [3]. Specifically, for the January 2025 snapshot, we used the DeFiLlama *Yield Aggregator Protocols* page (https://defillama.com/protocols/yield-aggregator) and sorted the *Protocol Rankings* table by the TVL column to extract the top ten protocols. The total TVL of yield aggregators (e.g., 2.7B USD in January 2025) was taken from DeFiLlama's *Total Value Locked* metric for the full yield-aggregator category (i.e., across all protocols).

Fig. 6 presents the TVL distribution of the leading yield aggregators in 2022 and 2025. For each year, a protocol's market share is computed as its TVL divided by the total category TVL reported by DeFiLlama at the same snapshot. As of 2025, the foremost aggregator was DeSyn Liquid Strategy, holding

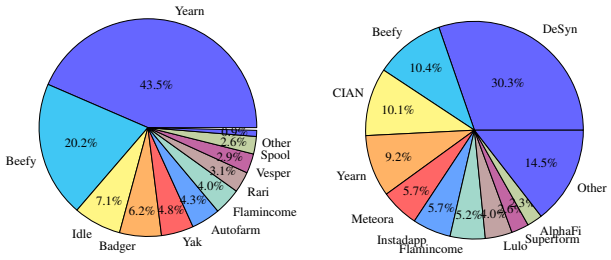
[3]https://defillama.com/

Table VII
THE TOP TEN YIELD AGGREGATORS IN 2022 AND 2025, ACCORDING TO TVL. WHERE NECESSARY, "-" IS USED TO DENOTE THE TVL OF PLATFORMS THAT DID NOT EXIST IN 2022 OR STOPPED OPERATING BY 2025.

Yield Aggregator	TVL Rank		TVL (in Million USD)		Launch Year
	2025	2022	2025	2022	
DeSyn Liquid Strategy	1	–	820	–	2021
Beefy	2	2	281	303	2020
CIAN Yield Layer	3	–	273	–	2022
Yearn Finance	4	1	248	652	2020
Meteora vaults	5	–	156	–	2022
Instadapp Lite	6	–	154	–	2019
Flamincome	7	7	139	60	2020
Lulo	8	–	109	–	2023
Superform	9	–	71	–	2024
AlphaFi Agg	10	–	63	–	2024
Idle Finance	13	3	39	107	2020
Badger DAO	15	4	31	94	2020
Yield Yak	16	5	29	72	2021
Autofarm	22	6	10	65	2021
Rari Capital	29	8	7	47	2020
Vesper Finance	–	9	–	43	2021
Spool	–	10	–	39	2021

Table VIII
THE TOP YIELD AGGREGATOR VAULTS, ACCORDING TO TVL.

Yield Aggregator	Vault Symbol	TVL (in Million USD)	APY (in % per 30D)	Chain
DeSyn Liquid Strategy	dwbtc2	260.7	10	Bitlayer
	dBFBTC	209.2	5	AILayer
	dmbtc2	203.1	15	Mode
CIAN Yield Layer	BTCLST	117	6.52	Ethereum
	stETH	54.5	14.3	Ethereum
	rsETH	46.7	5.89	Ethereum
Yearn Finance	yvWETH	68.7	2.4	Ethereum
	yvDAI	18	5.4	Ethereum
	yvyCRV	16.8	16.4	Ethereum
Beefy	cbETH-ETH	15.2	6	Ethereum
	BIFI	11.6	9.8	Ethereum
	wstETH-rETH-sfrxETH	6.9	2.8	Ethereum



(a) 2022 (b) 2025

Figure 6. The distribution of TVL among yield aggregators in 2022 and 2025.

820M USD, i.e, 30% of the total market TVL. DeSyn's TVL is also three times that of the second in-line, Beefy. In comparison, Yearn Finance was 2022's leading platform, with a TVL of 652M USD, corresponding to more than 43% of the market. Three years later, Yearn constitutes less than 10% of the market, and holds the fourth place with respect to TVL. Only three leading yield aggregators in 2022 remain in the top ten in 2025: Beefy, Yearn Finance, and Flamincome. For instance, Badger DAO ranked third in 2022, was ranked 15th in 2025. Additionally, two leading yield aggregators - Vesper Finance and Spool - who had a total of almost 82M USD, do not appear in the yield-aggregator rankings page in the January 2025 snapshot. Moreover, although the total TVL of yield aggregators increased between 2022 and 2025, the TVL of some of 2022's leading aggregators decreased: The TVL of Yearn Finance, 2022's foremost aggregator, was cut by 62%, decreasing from 652M to 248M. The TVL of Beefy also decreased, reaching 281M in 2025 compared to 303M in 2022. The only aggregator that increased the amount of locked TVL was Flamincome, with 60M in 2022 and 139M in 2025. This indicates that yield aggregators that were not among the top ten in 2022 (e.g., DeSyn and CIAN) have taken over the market since 2022, at the expense of others.

While the snapshot-based comparison does not establish causality, the shift in market share is consistent with several characteristics that may differentiate successful yield aggregators. First, TVL concentration patterns in Table VIII suggest different *vault design choices*: DeSyn and CIAN concentrate a large fraction of TVL in a small number of large vaults, whereas Beefy spreads TVL over many smaller vaults. Second, leading platforms appear to emphasize *strategy automation*

and compounding (reducing the per-user gas cost of frequent rebalancing) and *deployment across multiple networks*, which can broaden the user base. Finally, yield aggregators inherit risks from their underlying venues (DEX pools, lending markets, bridges, and oracles); thus, perceived *risk management* and the robustness of integration choices may also influence user preference over time. These hypotheses suggest that future empirical work could relate TVL dynamics to measurable platform attributes such as chain coverage, vault concentration, strategy complexity, and dependency footprint.

B. Yield Aggregation Revenues

To understand the trends of the main DeFi vaults, Table VIII presents the top three vaults (in TVL) of each of the four leading yield aggregators: DeSyn, Beefy, CIAN and Yearn. For each aggregator, we selected the three vaults with the highest TVL as reported by the corresponding source in a January 2025 snapshot. The data of the yield aggregator was taken from several sources: DeSyn data was taken from their official website [4]. The data of Beefy was taken from DefiLlama [5]. For CIAN, the data was collected using the public API [6], and for Yearn the data was collected using Dune [7], a web-based platform that allows querying public blockchain. TVL and APY values are reported as provided by each source.

DeSyn comprises three main vaults that store more than 80% of the platform's total TVL. Each of these vaults has more than 200M USD locked, and operates on a different network. The APY (annual percentage yield) varies from 5% to 15%, depending on the vault. Beefy, on the other hand, consists of many small vaults and while the total TVL is 281M USD, the largest vault has 15M USD. The APY of the vaults varies from 2.8% to 9.8%. For CIAN and Yearn, most funds are locked on the Ethereum chain alone. In CIAN, for instance, out of 273M USD, less than 15K USD was locked out of the Ethereum chain. The largest vault is of size 117M USD, and the APY varies between 5.89% to 14.3%. Yearn has a large vault (69M) and some smaller ones with less than 20M, all in Ethereum too, APYs ranging from 2.4% to 16.4%.

VIII. Lending Ecosystem Vulnerabilities

A. Inaccurate Time Measurement

The ability to accurately measure time is crucial to correctly accrue interest. However, currently popular blockchain mechanisms may fall short in this regard. Thus, using block timestamps for this purpose is well known to be inaccurate in several major cryptocurrencies, with a formal analysis of this issue given in [55]. On the other hand, measuring elapsed time by assuming some average inter-block time may also be prone to inaccuracies. For example, the mechanism used by Ethereum since its inception and up to September 15, 2022 relied, by design, on a variable block time [12], with the average block rate changing over time [55]. These considerations also affect yield aggregators which compare platforms that measure time differently, as miners can skew comparisons to inaccurately favor a less profitable lending platform over a better one [13]. For a formalization of protocols susceptible to issues due to inaccurate time measurement, see [56].

B. Interest-Rate Manipulations

The aforementioned issues with measuring time in blockchains can be intentionally manipulated by miners for a profit. Thus, the "stretching and squeezing" attack, which was formalized and characterized by Yaish *et al.* [12] allows malicious miners to influence the block rate by strategically turning their mining machines on and off to increase their profit from lending positions. As the authors' analysis shows, the profits from the attack can cover the potential losses from not mining, and, that miners can also avoid such losses by simply mining other cryptocurrencies instead of turning their machines off. While the previous attack requires potentially expensive mining equipment to be executed, Yaish *et al.* [13] formalize utilization-based lending protocols and show that liquidity providers can also manipulate interest-rates by adjusting their supplied liquidity. As they show, platforms do not always quickly recover from sudden liquidity shocks, thus allowing some liquidity providers to increase their absolute profit over relatively long periods of time.

C. Community Engagement and Associated Risks

DeFi platforms have a decentralized organization, often called a DAO, that the platform relies on for making decisions based on the votes of the community members. Decisions can be very broad and include future developments, strategies, and compensations distributed to the programmers, users of the platform, or even the appropriate reactions to market change. A decision is typically represented in code that is to be executed by the platform if adopted by the DAO. Votes are represented by tokens, the higher the number of tokens of an account, the higher the weight of the vote. The community's engagement is twofold. It needs to be informed based on factual criteria and risk-aware. The community also gains from widening prompting for higher quality in smart contracts and faster development through collaboration. Those structures aim to be transparent, democratic and decentralized, though it is not always the case. Although proposals commonly require some form of documentation, voters may not be familiar enough with the corresponding technicalities to fully understand the implications of adopting a given proposal. Moreover, the presence of users with a large amount of tokens or a lack of community involvement implies that the community may fail to pass good proposals, or, conversely, adopt bad ones [57]. This can be an outcome of the popular "airdrop" token issuance strategy, where tokens are given to platform users based on their participation [58], which can result in giving more power to those who have the cheapest participation costs [22]. These are not necessarily the users that are most interested in the platform's well-being, and, frequently are operated by for-profit "farming" operations [59]. A study of attacks on governance protocols is performed by [60].

[4] https://www.desyn.io/#/markets?network=bitlayer
[5] https://defillama.com/protocol/beefy#yields
[6] https://docs.cian.app/getting-started-with-cian/yield-layer/introduction/cian-yield-layer-tech-docs
[7] https://dune.com/zootrop/yearn-vaults

D. Slow-By-Design Governance Process

An example of one decision made by DeFi platform governance mechanisms is setting the value of the lending parameters for various platform tokens. To illustrate, we go over a case study that took place in the Compound V2 platform [61], where a user proposed to modify an asset's collateral factor from 73.0% to 70.0%, meaning that given a collateral in this asset, one can only borrow up to 70% of the collateral's value. Although this change implies that the perceived risk of this asset is higher, this particular process lasted a week before taking effect. This is due to the hard-coded governance process requiring several checks-and-balances to give the community enough time to properly evaluate the proposal. Thus, decentralization gives power to many but can hold back a fast reaction time that is sometimes critical to protect the protocol. A formal study of this issue is provided by [62].

E. Governance Token Issuance

Dotan *et al.* [57] discuss the practice of issuing governance tokens to borrowers and lenders, and show that this can make it profitable to borrow funds, even when considering the interest rate paid. This is explored in more detail by Park and Stinner [63], who focus on a specific strategy which entails depositing and borrowing funds at the same time, thereby allowing one to earn rewards for both types of actions. Empirically, their data indicates that 32% of loaned funds and 18% deposited funds correspond to actors employing strategies in this vein. Dotan *et al.* [57] and Feichtinger *et al.* [60] highlight the possibility of actors swaying votes by obtaining governance tokens via lending platforms, and present a concrete instance of such an attack taking place in 2022 on the Beanstalk lending platform, which resulted in losses of 182M USD.

IX. Open Questions

In this section, we overview challenges and open questions that we identify as promising directions for future work.

A. Proof-of-Stake Timing Attacks

While previous work proposed analyzed attacks on lending pools that operate in so-called Proof-of-Work based blockchains which have a variable inter-block time by design [12], [64], none considered Proof-of-Stake mechanisms that are supposed to have fixed block rates, like the one used by Ethereum since Sep. 15, 2022. While Ethereum's mechanism specifies a block time of exactly 12 seconds, its construction may technically disregard missing blocks, thus allowing for consecutively numbered blocks to have larger time gaps (see the 24 second gap between blocks 21875905 and 21875906), and such occurrences are not rare [65]. Thus, interest-rate manipulations in the vein of the "stretching and squeezing" attack [12], where actors slow down the block rate, are also viable in such mechanisms. We note that this can be combined to increase the profits from the RANDAO manipulations of Alpturer and Weinberg [66], where adversaries intentionally "miss" blocks, as this can increase the number of future blocks that they will create. Given the above, an interesting future direction is to quantify how interest-rate manipulations can increase RANDAO manipulations' profitability.

B. Code Security

Code security is a core component of the lending market. Since smart contracts are the trusted intermediary, they must be audited to prevent potential hackers from accessing the locked funds. This threat is present with 197M USD being stolen from Euler Finance in March 2023. Auditing is becoming standardized in the industry but exploits may still exist prompting borrowers to cluster around popular and established platforms.

Moreover, price crashes are not uncommon which affects the strategies of platforms. An asset that is used as collateral can crash. In this event, the collateral loses value fast and many loans need to be liquidated. The reaction time is crucial to block the asset as collateral and ensure that the protocol does not end with collateral with no value for the loans. An additional challenge faced by the platforms is liquidity. When a loan's collateral value needs to be liquidated liquidity can play a crucial role. If the liquidity of the collateral, given in rewards to a liquidator is low, liquidators may refrain from liquidating the loan. Liquidators generally rapidly exchange the collateral acquired for a more widely used cryptocurrency. Not being able to perform such an exchange weighs on the decision to liquidate. An additional concern for liquidators is the price change caused by a massive exchange. Acquiring a significant market share of a given cryptocurrency means that exchanging all of it might create a price drop. In such a case, the value of the collateral might become lower than the amount repaid by the liquidator making the transaction not profitable. The absence of liquidation creates bad debt for the protocol, a financial loss for the protocol since the collateral's value is less than the loan's value.

C. Financial Risk and Operational Margin

To be profitable and extract value from their activity, platforms face various trade-offs. For instance, when collecting borrowing fees (the platform's revenue) a fraction of it is set aside to serve as the platform's "reserve", which is used to compensate for losses, e.g., due to bad debt or an attack. This fraction is called the *reserve factor*; Intuitively, this is a trade-off between protecting liquidity providers (by choosing a large factor) and maintaining high revenue (by setting a low factor). A relevant study by Castro-Iragorri *et al.* [67] estimates the profitability margin for both Compound and AAVE at 1%. Another trade-off can be found when choosing which tokens to allow using as collateral. Some tokens may be risky, for instance, due to relying on new and not yet well-understood and battle-tested mechanisms, or due to having low liquidity, which implies that the market would have a harder time reacting to sudden shocks [13]. This should motivate a protocol to list only a selected number of coins. On the other hand, listing the most recent tokens allows a protocol to potentially capture and lock in new market segments of borrowers interested in these tokens. To balance between these two considerations, some platforms may choose to gradually introduce new tokens. For example, a platform can first require higher overcollateralization for borrowing newly introduced tokens, and then gradually lower this requirement when the token is more battle-tested. Other options include setting high

reserve factors for borrowing these tokens, and capping the total amount of loans collateralized by them. Furthermore, platforms such as Compound and AAVE even enlist specialized firms to assess the risk of new and existing assets, and to suggest how to set the aforementioned parameters.

D. Revenue-based Financing

A popular approach to loans is extending a loan that is reimbursed by future revenue without the need for collateral. The borrower and the liquidity provider agree that after receiving the loan, a predefined fraction of the borrower's monthly income serves to reimburse the liquidity provider. This requires making sure that income is known to the liquidity provider to recoup the loan. A challenge with this approach is the difficulty in assessing the income of the borrower. A malicious borrower could redirect future funds to a different account. In this way, the loan is never reimbursed since the revenue of the borrower becomes non-existent. Since no collateral is provided, the default comes at a great cost for the liquidity provider. To the best of our knowledge, this technique is not implemented in an existing platform and it can be interesting to examine its potential.

X. Conclusion and Outlook

In this SoK, we examine DeFi lending mechanisms and yield aggregators. We describe various major loan types with their main characteristics and applications. The DeFi lending ecosystem relies on smart contracts to operate, making it accessible and transparent, both technically (e.g., a platform's operation is governed by publicly available code), and empirically (the public availability of blockchain data allows real-time tracking of market dynamics and patterns). Moreover, the unique features of blockchain networks facilitate the creation of novel mechanisms, such as flashloans, while also allowing for new manipulations that do not apply to traditional systems. We go over several relevant attacks from the literature. Finally, we discuss open questions and directions for future work.

References

[1] K. Gogol, C. Killer, M. Schlosser, T. Bocek, B. Stiller, and C. J. Tessone, "SoK: Decentralized finance (DeFi) - Fundamentals, taxonomy and risks," *CoRR*, vol. abs/2404.11281, 2024.

[2] F. Schär, "Decentralized finance: On blockchain-and smart contract-based financial markets," *FRB of St. Louis Review*, 2021.

[3] A. Kotzer, D. Gandelman, and O. Rottenstreich, "SoK: Applications of sketches and rollups in blockchain networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 3, pp. 3194–3208, 2024.

[4] [Online]. Available: https://app.uniswap.org

[5] [Online]. Available: https://compound.finance/markets

[6] T. J. Rivera, F. Saleh, and Q. Vandeweyer, "Equilibrium in a DeFi Lending Market," 2023.

[7] F. Irresberger, K. John, and F. Saleh, "Chapter 2: Decentralized lending," in *The Elgar Companion to Decentralized Finance, Digital Assets, and Blockchain Technologies*. Edward Elgar Publishing, 2024.

[8] A. Yaish, N. Chemaya, D. Malkhi, and L. W. Cong, "Inequality in the age of pseudonymity," in *AAAI Conference on Artificial Intelligence*, 2026.

[9] M. Bartoletti, J. H. Chiang, and A. Lluch-Lafuente, "SoK: Lending pools in decentralized finance," in *Financial Cryptography and Data Security (FC) International Workshops*, 2021.

[10] J. Xu and Y. Feng, "Reap the harvest on blockchain: A survey of yield farming protocols," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 858–869, 2022.

[11] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "Sok: Decentralized exchanges (DEX) with automated market maker (AMM) protocols," *ACM Comput. Surv.*, vol. 55, no. 11, 2023.

[12] A. Yaish, S. Tochner, and A. Zohar, "Blockchain stretching & squeezing: Manipulating time for your best interest," in *ACM Conference on Economics and Computation*, 2022.

[13] A. Yaish, M. Dotan, K. Qin, A. Zohar, and A. Gervais, "Suboptimality in DeFi," *IACR Cryptol. ePrint Arch.*, p. 892, 2023.

[14] J. Halpern, R. Pass, and A. Saraf, "Fair interest rates are impossible for lending pools: Results from options pricing," *CoRR*, vol. abs/2410.11053, 2024.

[15] A. Kotzer and O. Rottenstreich, "SoK: Impermanent loss, an unavoidable fee or a controlled phenomenon?" in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2026.

[16] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "SoK: Decentralized finance (DeFi) attacks," in *IEEE Symposium on Security and Privacy*, 2023.

[17] Y. Gafni and A. Yaish, "Transaction fee mechanisms robust to welfare-increasing collusion," *Games and Economic Behavior*, 2026.

[18] A. Yaish, K. Qin, L. Zhou, A. Zohar, and A. Gervais, "Speculative denial-of-service attacks in ethereum," in *33rd USENIX Security Symposium*, 2024.

[19] J. Xu and N. Vadgama, "From banks to DeFi: The evolution of the lending market," *CoRR*, vol. abs/2104.00970, 2021.

[20] L. Gudgeon, S. Werner, D. Perez, and W. J. Knottenbelt, "DeFi protocols for loanable funds: Interest rates, liquidity and market efficiency," in *ACM Conference on Advances in Financial Technologies*, 2020.

[21] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized finance (DeFi)," in *ACM Conference on Advances in Financial Technologies (AFT)*, 2022.

[22] H. Hałaburda, B. Livshits, and A. Yaish, "Platform building with fake consumers: On double dippers and airdrop farmers," 2025.

[23] J. Chiu, E. Ozdenoren, K. Yuan, and S. Zhang, "Cryptocurrency as Collateral in DeFi Lending Platforms," 2022.

[24] M. Bastankhah, V. Nadkarni, C. Jin, S. Kulkarni, and P. Viswanath, "Thinking Fast and Slow: Data-Driven Adaptive DeFi Borrow-Lending Protocol," in *Advances in Financial Technologies (AFT)*, 2024.

[25] F. Barbiero, G. Schepens, and J.-D. Sigaux, "Liquidation Value and Loan Pricing," *The Journal of Finance*, vol. 79, no. 1, pp. 95–128, 2024.

[26] T. Azoulay, U. Carl, and O. Rottenstreich, "Allowing blockchain loans with low collateral," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023.

[27] T. Azoulay and O. Rottenstreich, "Accurate credit scoring for blockchain lending with conformalized quantile regression," in *International Conference on Blockchain Computing and Applications (BCCA)*, 2025.

[28] K. Qin, L. Zhou, P. Gamito, P. Jovanovic, and A. Gervais, "An empirical study of DeFi liquidations: Incentives, risks, and instabilities," in *ACM Internet Measurement Conference*, 2021.

[29] A. Yaish and A. Zohar, "Correct cryptocurrency asic pricing: Are miners overpaying?" in *Advances in Financial Technologies (AFT)*, 2023.

[30] L. Heimbach and W. Huang, "DeFi Leverage," May 2023.

[31] L. Heimbach, E. Schertenleib, and R. Wattenhofer, "Short Squeeze in DeFi Lending Market: Decentralization in Jeopardy?" in *Financial Cryptography and Data Security (FC) Workshops*, 2023.

[32] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability," in *IEEE Symposium on Security and Privacy (SP)*, 2020.

[33] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, and K. Ren, "Towards a first step to understand flash loan and its applications in DeFi ecosystem," in *International Workshop on Security in Blockchain and Cloud Computing*, 2021.

[34] K. Qin, L. Zhou, B. Livshits, and A. Gervais, "Attacking the DeFi ecosystem with flash loans for fun and profit," in *International Conference on Financial Cryptography and Data Security*, 2021.

[35] Y. Wang, Y. Chen, H. Wu, L. Zhou, S. Deng, and R. Wattenhofer, "Cyclic arbitrage in decentralized exchanges," in *Companion Proceedings of the Web Conference (WWW)*, 2022.

[36] O. Mazor and O. Rottenstreich, "An empirical study of cross-chain arbitrage in decentralized exchanges," in *International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 2024.

[37] F. Gronde, "Flash loans and decentralized lending protocols: An in-depth analysis," Master's thesis, University of Basel, 2021.

[38] [Online]. Available: https://blog.uniswap.org/uniswap-v2

[39] [Online]. Available: https://aave.com/docs/concepts/flash-loans

[40] [Online]. Available: https://docs.uniswap.org/contracts/v2/guides/smart-contract-integration/using-flash-swaps#single-token
[41] [Online]. Available: https://defillama.com/
[42] [Online]. Available: https://help.dydx.exchange/en/articles/5695617-v1-v2-dydx-solo-protocol-layer-1-wind-down
[43] A. Sardon, "Zero-liquidation loans: A structured product approach to DeFi lending," *arXiv:2110.13533*, 2021.
[44] ——, "Myso v1 core a trust-minimized protocol for zero-liquidation loans," 2022.
[45] [Online]. Available: https://github.com/aave-dao/aave-v3-origin/blob/1dab6e/src/contracts/rewards/RewardsDistributor.sol#L473-L474
[46] [Online]. Available: https://github.com/aave/aave-protocol/blob/4b4545/contracts/tokenization/AToken.sol#L452
[47] [Online]. Available: https://etherscan.io/address/0xA17581A9E3356d9A858b789D68B4d866e593aE94
[48] A. Chaudhary, R. Kozhan, and G. Viswanath-Natraj, "Interest rate rules in decentralized finance: Evidence from Compound," *Open Access Series in Informatics (OASIcs)*, 2023.
[49] [Online]. Available: https://etherscan.io/address/0xaEE83ca85Ad63DFA04993adcd76CB2B3589eCa49
[50] [Online]. Available: https://maple.finance/
[51] A. Gilbert, "Why maple is ditching under-collateralised lending: 'no one's profitable'," 2023. [Online]. Available: https://www.dlnews.com/articles/defi/crypto-lender-maple-ditches-under-collateralised-lending/
[52] [Online]. Available: https://thegraph.com/
[53] Y. Abels, "DeFi Data Pullers — Aave V2 + Compound V2 (Ethereum) via The Graph," https://github.com/yoadhamagniv/the_graph_data_fetching, 2026.
[54] [Online]. Available: https://medium.com/compound-finance/expanding-compound-governance-ce13fcd4fe36
[55] A. Yaish, G. Stern, and A. Zohar, "Uncle maker: (Time)stamping out the competition in ethereum," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2023.
[56] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2016.
[57] M. Dotan, A. Yaish, H.-C. Yin, E. Tsytkin, and A. Zohar, "The vulnerable nature of decentralized governance in DeFi," in *ACM Workshop on Decentralized Finance and Security*, 2023.
[58] C. A. Makridis, M. Fröwis, K. Sridhar, and R. Böhme, "The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens," *Journal of Corporate Finance*, vol. 79, 2023.
[59] J. Messias, A. Yaish, and B. Livshits, "Airdrops: Giving money away is harder than it seems," 2023.
[60] R. Feichtinger, R. Fritsch, L. Heimbach, Y. Vonlanthen, and R. Wattenhofer, "SoK: Attacks on DAOs," in *Advances in Financial Technologies (AFT)*, 2024.
[61] [Online]. Available: https://compound.finance/governance/proposals/133
[62] J. Xu, Y. Feng, D. Perez, and B. Livshits, "Auto.gov: Learning-based governance for decentralized finance (DeFi)," *IEEE Transactions on Services Computing*, vol. 18, no. 3, pp. 1278–1292, 2025.
[63] A. Park and J. Stinner, "Phantom Liquidity in Decentralized Lending," *SSRN*, vol. 10.2139/ssrn.4489732, 2023.
[64] A. Yaish, "Incentives in the ether: Practical cryptocurrency economics & security," in *Companion Proceedings of the ACM on Web Conference*, 2024.
[65] [Online]. Available: https://beaconscan.com/slots-skipped
[66] K. Alpturer and S. M. Weinberg, "Optimal RANDAO Manipulation in Ethereum," in *Conference on Advances in Financial Technologies*, 2024.
[67] C. Castro-Iragorri, J. Ramirez, and S. Velez, "Financial intermediation and risk in decentralized lending protocols," *arXiv:2107.14678*, 2021.