Speculative Multipliers on DeFi: Quantifying On-Chain Leverage Risks

Zhipeng Wang(✉), Kaihua Qin, Duc Vu Minh, and Arthur Gervais

Imperial College London, London, UK
{zhipeng.wang20,kaihua.qin,duc.vu-minh20,a.gervais}@imperial.ac.uk

Abstract. Blockchains and DeFi have consistently shown to attract financial speculators. One avenue to increase the potential upside (and risks) of financial speculation is leverage trading, in which a trader borrows assets to participate in the financial market. While well-known over-collateralized loans, such as MakerDAO, only enable leverage multipliers of 1.67×, new under-collateralized lending platforms, such as Alpha Homora (AH), unlock leverage multipliers of up to 8× and attracted over 1.2B USD of locked value at the time of writing.

In this paper, we are the first to formalize a model for under-collateralized DeFi lending platforms. We analytically exposit and empirically evaluate the three main risks of a leverage-engaging borrower: *(i)* impermanent loss (IL) inherent to Automated Market Makers (AMMs), *(ii)* arbitrage loss in AMMs, and *(iii)* collateral liquidation. Based on our analytical and empirical results of AH over a timeframe of 9 months, we find that a borrower may mitigate the IL through a high leverage multiplier (e.g., more than 4×) and a margin trading before supplying borrowed assets into AMMs. We interestingly find that the arbitrage and liquidation losses are proportional to the leverage multiplier. In addition, we find that 72.35% of the leverage taking borrowers suffer from a negative APY, when ignoring the governance token incentivization in AH. Finally, when assuming a maximum ±10% move among two stablecoins, we pave the way for more extreme on-chain leverage multipliers of up to 91.9× by providing appropriate system settings.

1 Introduction

Over 44% of the total locked DeFi value is dedicated to lending and borrowing services. Financial debt has therefore manifested its importance within the decentralized financial ecosystem. The very first DeFi debt protocols focused on so-called *over-collateralized loans*—wherein a borrower must collateralize more financial value than the lent debt amounts to [4,15,16]. Common over-collateralized loan systems require the collateral value not to decline below 150% of the total debt value. While over-collateralized loans grant the borrower a wide degree of flexibility in using the borrowed' assets, they remain capital-inefficient

I. Eyal and J. Garay (Eds.): FC 2022, LNCS 13411, pp. 38–56, 2022.
https://doi.org/10.1007/978-3-031-18283-9_3

and limit the borrowers leverage multipliers below 2×[1]—that is the multiplier by which traders can increase their financial up- or downside of a loan.

In *under-collateralized loans*, however, speculate-afine traders can gamble with leverage multipliers beyond 2×, which we subsequently refer to as leverage trading. While the borrowed assets remain under the tight control of immutable on-chain smart contracts, existing on-chain leverage platform, such as Alpha Homora [1] grants the borrowers the ability to speculate with a leverage of up to 8×. To the best of our knowledge, this is the first work to explore the practices and possibilities of secure under-collateralized on-chain leverage. We formalize an on-chain leverage model, measure existing lending practices and assess the risks quantitatively as we summarize in our contributions:

On-chain Leverage Model: To the best of our knowledge, we are the first to provide a model for on-chain lending platforms with a leverage factor beyond 2×. We formalize the generic users and components to encompass future leverage designs. We show that with reasonable system settings, an on-chain lending system can achieve a leverage multiplier of up to 91.9×.

On-chain Leverage Analytics: Over a timeframe of 9 months, we analyze on-chain data analytics of Alpha Homora (AH), with 1.2B `USD` of locked value, the largest on-chain leverage platform in DeFi. We find that lenders consistently benefit from a positive APY, while 72.35% of the leverage taking borrowers suffer from a negative APY, when ignoring the governance token incentivization in AH.

Leverage Risk Quantification: We identify three risks causing borrower losses: *(1)* impermanent loss (IL) inherent to Automated Market Makers, *(2)* asset arbitrage, and *(3)* collateral liquidation. We find that out of the 10,430 positions analyzed over 9 months for leverage trading in AH, 1,139 suffer from IL, 149 are susceptible to asset arbitrage and 270 suffered from collateral liquidation. We find that a borrower may mitigate the risk of IL by simultaneously (1) employing a high leverage multiplier (e.g., more than 4×) and (2) performing a margin trade to swap the borrowed assets to collateralized tokens before supplying assets into AMMs.

2 Background

In the following, we provide essential notions of DeFi to further understand the novelties presented in this paper.

2.1 DeFi

Decentralized Finance, also known as DeFi, is a financial ecosystem which runs autonomously on smart-contracts-enabled blockchains and has grown to a total locked value (TVL) of over 100B `USD` at the time of writing. Many DeFi protocols are inspired by traditional centralized finance (CeFi) systems, such as

[1] For instance, 1.67×, in the case of MakerDAO, where the collateral value shall not decline below 150% of the debt value.

lending and borrowing platforms, asset exchanges, derivatives, and margin trading systems. However, compared to CeFi, DeFi offers distinct features to its users, such as complete transparency and non-custodial asset control. DeFi also enables novel financial primitives that do not exist in traditional CeFi, such as flash loans [27]. Flash loans enable borrowers with nearly zero upfront collateral to borrow instantly billions of USD. Such financial enablers grant arbitrageur traders significant power through the atomic execution of arbitrage transactions across the many composable DeFi markets. For a more thorough background on DeFi, we refer the interested reader to the related works [24,28].

2.2 Price Oracles

While DeFi is being built, the decentralized finance paradigm remains deeply connected to CeFi. Because blockchains are isolated databases, and cannot access off-chain data, DeFi gathers external data from third-party services, commonly referred to as oracles. Price oracles allow feeding e.g. stock or other asset price information to smart contracts and can therefore act as a bridge between DeFi and the external world [17]. Oracles can be classified as centralized and decentralized oracles based on the number of external sources. Two major decentralized DeFi oracle providers are Chainlink [8] and the Band Protocol [23].

2.3 Automated Market Maker

The prevalent price-finding and order matching mechanism in centralized exchanges (CEXs) is the limit order-book model (LOB), which matches buyers' bids to sellers' ask prices [24]. In decentralized exchanges (DEXs) [29,31], the Automated Market Maker (AMM) evolved to replace LOB due to its suitability for low-throughput blockchains [36]. An AMM consists of a liquidity pool which receives and emits financial assets through the control of a pre-defined algorithm, in its simplest form a constant product formula. A pool is funded by liquidity providers (LP), who receive LP tokens matching the accounting share of their pool ownership. Liquidity takers (LT) request a trade with the pool by providing one asset X plus a transaction fee [9] while receiving another asset Y in return. The transaction fees are paid to the LPs, proportionally to the LP pool shares.

Impermanent Loss. Liquidity providers have the choice of either depositing their assets to a liquidity pool, or holding the assets in their wallets. If the accumulative value of the tokens in a liquidity pool drops below the hypothetical value of simply holding the assets in a wallet, there exists an impermanent loss (IL), also known as divergence loss. From the moment of an LP deposit, the accumulative asset value decline may occur, when the tokens in a liquidity pool diverge in price from each other [6,9]. If the token values revert to the price ratio at the time of the LP deposit, the IL is reverted. An IL is therefore only *realized*, when an LP exits a liquidity pool in a state where there exists an IL.

Arbitrage. Arbitrage is the process of profiting by selling/buying assets among multiple markets, leveraging price differences. Arbitrage increases the DeFi market efficiency and is typically considered benign. Previous works [10,34,36] have shown that DeFi arbitrage bots monitor blockchain state changes and execute arbitrages among AMMs to make profits.

2.4 Financial Leverage

Leverage is the practice of taking on debt, i.e., to borrow assets for a subsequent financial operation [5]. One such operation is to perform a momentary exchange of assets, which is commonly referred to as margin trading. Another operation would be to take the lent assets and provide these towards a financial instrument, such as a DeFi liquidity pool, as we investigate within this work.

Leverage, in general, can amplify trader profits, as well as losses. Aggressive traders are known to be willing to undertake such risks in pursuit of higher returns [30]. The degree of amplification is determined by the leverage multiplier, which is defined as the ratio of the total assets to the equity (or cash) that a trader holds. The leverage multiplier can be freely adjusted by the trader, i.e., by providing or removing ad hoc collateral from the leverage position. A multiplier of 1× means that the total assets that the trader has access to are equivalent to the trader's equity, i.e., the trader does not borrow any assets. A leverage factor beyond 1× is achieved as soon as the trader can borrow assets to perform a subsequent financial operation. Centralized cryptocurrency trading platforms have readily introduced leverage trading, e.g., Prime XBT [33], OkEX [19], BitMEX [7], and Poloniex [22], offering leverage multipliers *from* 2.5× *to* 100× [20].

2.5 Leverage in DeFi

Because of the lack of Know-Your-Customer (KYC) verifications and the blockchain's pseudonymity, DeFi users cannot safely resort to credit to exert leverage. Therefore, DeFi borrowing is usually fully collateralized or over-collateralized and (with 29B `USD` of total locked value) widely applied in several lending platforms such as MakerDAO [16], Compound [15] and Aave [4]. MakerDAO for instance, allows traders to open collateralized debt positions by providing various cryptocurrencies as a then locked security deposit. In exchange for locking these assets, the trader can then mint a stablecoin DAI, which can be freely used, as long as the collateral value does not decline below a certain threshold. Specifically, MakerDAO requires that the collateral value does not decline below 150% of the granted debt position. As such, MakerDAO enables maximum leverage of $2.5/1.5 \approx 1.67\times$, while in this work we investigate protocols that enable higher leverage multipliers. If the collateral value declines below 150% in MakerDAO, the debt position becomes liquidatable as we elaborate further in the following.

2.6 Liquidations

If the value of debt collateral in a lending system declines below a custom threshold, then the debt position may be opened for liquidation. The Health Factor

(HF) is a common metric to measure the health of a debt position, whereas an HF smaller than 1 indicates that a debt position is liquidatable [25]. A liquidation is then an event in which a liquidator repays outstanding debts of a position and, in return, receives a portion of the collateral of the position as a reward. Liquidations in DeFi are widely practiced, and related works have quantified that over the years 2020 and 2021, liquidators realized a financial profit of over 800M USD while performing liquidations [25].

3 On-Chain Leverage System

We proceed to outline the actors and components of on-chain leverage systems as shown in Fig. 1.

Lending Pool. A lending pool is a multi-asset management pool that allows capital-providing entities to earn interest on their capital as well as capital-taking entities to trade with a multiple of the capital they hold. Essentially, three actors interact with a lending pool: **Lenders**, **Borrowers** as well as **Liquidators**.

Lender. Lenders supply assets (e.g., ETH, USDT) to the lending pool to earn from the lending interest rate. The lending interest rate is paid by the borrowing interest rate that leveraged yield farmers contribute for borrowing assets.

Borrower. Borrowers supply assets as collateral to the lending pool to then open leveraged positions, while paying borrowing interests. To avoid liquidations, borrowers can provide additional collateral or partially repay their position. In addition, borrowers can supply the borrowed assets to liquidity providing pools to earn trading fees, or stake LP tokens to liquidity mining pools to earn profits.

Liquidator. Leveraged positions are subject to liquidation when the debt becomes unhealthy [25]. A liquidator can repay the debt and benefit from a liquidation spread.

Price Oracle. The lending pool obtains the asset prices of various cryptocurrencies through external price oracles, which can then inform the smart contract whether a position is liquidatable.

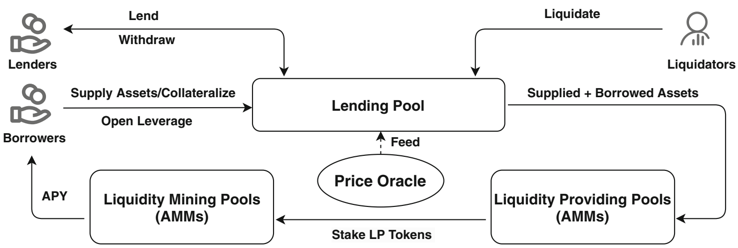

Fig. 1. High-level system diagram of on-chain leverage platforms. The solid arrows (→) represent the movement of cryptocurrencies, and the dash arrows (⇢) represent the transmission of data.

Table 1. Notation summary

Notations	Definitions	Notations	Definitions
$\mathcal{LV}$	leverage platform	$\texttt{Coll}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{C}})$	amount of collateral cryptocurrency
$\mathbf{P}_{\mathsf{id}} = (\texttt{C}, \texttt{B})$	debt position	$\texttt{Borr}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{B}})$	amount of borrowing cryptocurrency
$x\,\texttt{X}$	x amount of cryptocurrency $\texttt{X}$	$p_t^{\texttt{B}\to\texttt{C}}$	price of $\texttt{B}$ in the unit $\texttt{C}$ at time t
$\mathsf{DebtRatio}_t(\mathbf{P}_{\mathsf{id}})$	debt ratio	$(\texttt{B}, \texttt{C})$	how much credit a position gains when collaterizing 1 $\texttt{C}$ and borrowing 1 $\texttt{B}$
$\mathsf{LM}_t(\mathbf{P}_{\mathsf{id}})$	leverage multiplier	m	the initial leverage multiplier when opening a position
$\mathsf{Loss}^{\mathsf{IL}}$	impermanent loss	$\mathsf{Return}_{\mathsf{cp}}^{\mathsf{IL,Mg}}$	the return from impermanent loss and margin trading
$\mathsf{Loss}^{\mathsf{AR}}$	arbitrage loss	$\mathsf{Return}_{\mathsf{cp}}^{\mathsf{Mg}}$	the return from margin trading without impermanent loss
$\mathsf{Loss}^{\mathsf{LQ}}$	liquidation loss	LS	liquidation spread, which determines the rewards for a liquidator after repaying the debt

3.1 Formal Leverage Model

In the following, we formalize the leverage model.We also provide a table to summarize the notations used in this paper (cf. Table 1).

We denote an on-chain leverage platform as $\mathcal{LV} = \langle \mathbb{C}, \mathbb{B}, \mathbb{P}, \mathbb{F} \rangle$, where $\mathbb{C}$ denotes the set of collateral cryptocurrencies; $\mathbb{B}$ denotes the set of debt cryptocurrencies available for borrowing; $\mathbb{P}$ denotes the set of debt positions. A position is denoted as $\mathbf{P} = (\texttt{C}, \texttt{B})$, where $\texttt{C} \in \mathbb{C}$ is a collateral cryptocurrency and $\texttt{B} \in \mathbb{B}$ is a debt cryptocurrency. $\mathbb{F}$ denotes the set of farming cryptocurrencies that borrowers can receive after providing their borrowing cryptocurrencies into farming pools. In practice, borrowers can *(1)* supply their borrowing cryptocurrencies to liquidity providing pools to earn trading fees, and *(2)* stake LP tokens to liquidity mining pools to earn profits. For simplicity, in our model, we regard steps *(1)* and *(2)* as block box and only consider borrowers' final returns.

Each debt position $\mathbf{P} = (\texttt{C}, \texttt{B})$ has a unique id, denoted as $\mathbf{P}_{\mathsf{id}}$. We define $\texttt{Coll}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{C}})$ and $\texttt{Borr}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{B}})$ as the amount of collateral and borrowing cryptocurrencies of a position $\mathbf{P}_{\mathsf{id}}$ respectively in $\mathcal{LV}$ at time t (in practice, time t is measured in block timestamp). In a leverage platform, the prices of cryptocurrencies are available through a price oracle (cf. Sect. 2.2). We denote x amount of cryptocurrency $\texttt{X}$ with $x\ \texttt{X}$. We denote $p_t^{\texttt{B}\to\texttt{C}}$ as the price of $\texttt{B}$ in the unit $\texttt{C}$ at time t, i.e., $1\ \texttt{B} = p_t^{\texttt{B}\to\texttt{C}}\ \texttt{C}$.

$\mathcal{LV}$ maintains the state of every position $\mathbf{P}_{\mathsf{id}} \in \mathbb{P}$, and the state is quantified by the debt ratio $\mathsf{DebtRatio}_t(\mathbf{P}_{\mathsf{id}}) = \frac{\texttt{Borr}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{B}})}{\texttt{Coll}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{C}})} \cdot (\texttt{B}, \texttt{C}) \cdot p_t^{\texttt{B}\to\texttt{C}} \cdot 100\%$, where $(\texttt{B}, \texttt{C})$ is a fixed parameter set by the platform $\mathcal{LV}$, which determines how much credit $\mathbf{P}_{\mathsf{id}}$ receives when collaterizing 1 $\texttt{C}$ and borrowing 1 $\texttt{B}$. When $\mathsf{DebtRatio}_t(\mathbf{P}_{\mathsf{id}})$ exceeds 100% due to, for example, the fluctuations of price $p_t^{\texttt{B}\to\texttt{C}}$, $\mathbf{P}_{\mathsf{id}}$ becomes available for liquidations.

A position $\mathbf{P}_{\mathsf{id}}$ is over-collateralized, if $\texttt{Coll}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{C}}) > \texttt{Borr}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{B}}) \cdot p_t^{\texttt{B}\to\texttt{C}}$, and under-collateralized otherwise. Debt positions in a leverage platform $\mathcal{LV}$ are typically under-collateralized. We finally define the leverage multiplier to measure to what degree borrowers can expand their assets in a position $\mathbf{P}_{\mathsf{id}}$, i.e., $\mathsf{LM}_t(\mathbf{P}_{\mathsf{id}}) = \frac{\texttt{Borr}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{B}}) \cdot p_t^{\texttt{B}\to\texttt{C}} + \texttt{Coll}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{C}})}{\texttt{Coll}_t(\mathbf{P}_{\mathsf{id}}^{\texttt{C}})}$.

3.2 AMM Model

AMM exchanges are to date the most prevalent markets where leverage borrowers deposit borrowed assets to realize revenue through the collection of trading fees. Hence, the borrowers' returns and risks are fundamentally influenced by the underlying AMM mechanisms. To ease our subsequent analysis, we proceed to outline an AMM (cf. Sect. 2.3) model. We assume the existence of an AMM **A** allowing the exchange between a pair of cryptocurrencies X and Y. x_t and y_t denote the amount of X and Y respectively supplied in **A** at time t. x_t and y_t satisfy a conservation function $f(x_t, y_t, \boldsymbol{k}) = 0$, where $\boldsymbol{k}$ is invariant over time. The spot price of X with respect to Y in **A** at time t is defined as $p_t = \frac{\partial f}{\partial y_t} / \frac{\partial f}{\partial x_t}$. We assume that at time t, a trader swaps δx X to δy Y. Following the conservation function, δx and δy should satisfy $f(x_t, y_t, \boldsymbol{k}) = 0$ and $f(x_t + \delta x, y_t - \delta y, \boldsymbol{k}) = 0$.

Liquidity providers (LPs) provide liquidity to **A** by depositing asset X and Y. Due to the price movement between X and Y, x_t and y_t may change over time. Hence, the amount of X and Y that a LP is allowed to redeem varies with respect to p_t, denoted by $g_t^{\mathtt{X}}(p_t)$ and $g_t^{\mathtt{Y}}(p_t)$.

Constant Product AMMs. For a constant product AMM **A**, the conservation function is $f(x_t, y_t, k) = x_t \cdot y_t - k = 0$, which stipulates that the product of x_t and y_t remains constant after an asset exchange and generally defines the AMM's bonding curve. The spot price in **A** is derived with $p_t = \frac{y_t}{x_t}$.

Exchange. When a trader purchases Y from **A** with δx X, we can derive the output amount of Y with $\delta y = y_t - \frac{x_t \cdot y_t}{x_t + \delta x}$. Note that the realized exchange rate $\frac{\delta y}{\delta x}$ is lower than the spot price p_t, as the executed price depends on the trade volume along the AMM bonding curve. We refer to the difference between the expected price (i.e., the spot price) and the actual exchange rate as slippage [36].

Liquidity Supply. Liquidity providers supply X and Y to a pool **A** while typically not changing the pool's spot price. The ratio between the supplied X and Y in a single deposit at time t therefore follows $\frac{\Delta y}{\Delta x} = \frac{y_t}{x_t}$.

4 Analytical Evaluation

While leverage is a speculative tool to increase the borrowers' profit, this upside increases the potential monetary risks as we outline in the following. The primary risks we identify are *(i)* impermanent loss, *(ii)* arbitrage and *(iii)* liquidation.

4.1 Impermanent Loss Risk

As widely understood, the impermanent loss (IL) [6,9] is caused by diverging asset prices within a liquidity pool (cf. Sect. 2.3). In the following, we investigate the financial risks created through the IL. Notably, we find that the return from margin trading through leverage may positively outweigh IL (cf. Fig. 3).

Generic Formulas for IL. We assume that at time t_0, the price $p_{t_0}^{\mathtt{B} \rightarrow \mathtt{C}}$ in an AMM **A** is p_0, i.e., $1\,\mathtt{B} = p_0\,\mathtt{C}$. A borrower supplies $g_{t_0}^{\mathtt{C}}(p_0)\,\mathtt{C} + g_{t_0}^{\mathtt{B}}(p_0)\,\mathtt{B}$ to **A**.

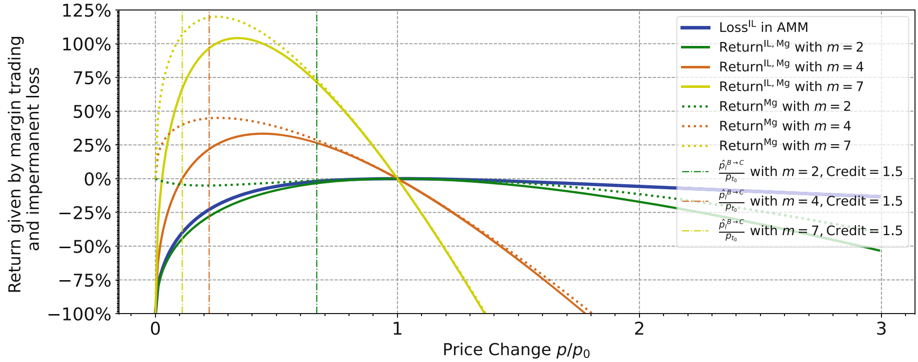

Fig. 2. Resulting return from impermanent loss in constant product AMMs and margin trading in on-chain leverage systems such as Alpha Homora. We find that the return from margin trading through leverage may positively outweigh the impermanent loss if the leverage multiplier is sufficiently high. For example, at a leverage of 7×, we find that upon a price change of 0.64, the return given by margin trading is 94.43%, while the impermanent loss amounts to −2.44%.

We further assume that, at time $t_0 + \Delta$, the price changes to p and the borrower removes all supplied tokens from **A**. Due to the price movement, the assets that the borrower is allowed to redeem become $g^{\mathsf{C}}_{t_0+\Delta}(p)\,\mathtt{C}$ and $g^{\mathsf{B}}_{t_0+\Delta}(p)\,\mathtt{B}$. We can then derive the borrower's impermanent loss in **A** with Eq. 1.

$$\mathsf{Loss}^{\mathsf{IL}} = \frac{g^{\mathsf{C}}_{t_0+\Delta}(p)\cdot 1 + g^{\mathsf{B}}_{t_0+\Delta}(p)\cdot p}{g^{\mathsf{C}}_{t_0}(p_0)\cdot 1 + g^{\mathsf{B}}_{t_0}(p_0)\cdot p} - 1 \tag{1}$$

IL in Constant Product AMMs. We assume that at time t_0, a borrower collateralizes $c\,\mathtt{C}$ in the leverage platform $\mathcal{LV}$, sets the leverage multiplier as m to borrow $g^{\mathsf{C}}_{t_0}(p_0)\,\mathtt{C} + g^{\mathsf{B}}_{t_0}(p_0)\,\mathtt{B}$, and then provides the assets to a constant product AMM **A**. Because **A** typically requires to receive a specific proportion of supplied assets for returning LP tokens, $g^{\mathsf{C}}_{t_0}(p_0)$ and $g^{\mathsf{B}}_{t_0}(p_0)$ need to satisfy $\frac{g^{\mathsf{C}}_{t_0}(p_0)}{g^{\mathsf{B}}_{t_0}(p_0)} = p_0$. We can then derive that $g^{\mathsf{C}}_{t_0}(mc, p_0) = \frac{mc}{2}$ and $g^{\mathsf{B}}_{t_0}(mc, p_0) = \frac{mc}{2p_0}$.

We further assume that the percentage of the total liquidity that the borrower owns in **A** is invariant over time. Then at time $t_0 + \Delta$, the borrower can redeem $g^{\mathsf{C}}_{t_0+\Delta}(mc, p)\,\mathtt{C} = \frac{mc}{2\sqrt{p_0}}\sqrt{p}\,\mathtt{C}$ and $g^{\mathsf{B}}_{t_0+\Delta}(mc, p)\,\mathtt{B} = \frac{mc}{2\sqrt{p \cdot p_0}}\,\mathtt{B}$. Then according to Eq. 1, the borrower's impermanent loss in **A** is $\mathsf{Loss}^{\mathsf{IL}}_{\mathsf{cp}} = \frac{2\sqrt{\frac{p}{p_0}}}{1+\frac{p}{p_0}} - 1$.

Speculation Through Margin Trading. If we only consider the impermanent loss in **A**, the borrower will always suffer from $\mathsf{Loss}^{\mathsf{IL}}$. However, a borrower can choose to mitigate the IL though a margin trading as follows: *(1)* the borrower collateralizes $c\,\mathtt{C}$, and sets the leverage multiplier as $m (m > 2)$ to borrow $\frac{(m-1)c}{p_0}\,\mathtt{B}$; *(2)* the borrower then swaps $(\frac{m}{2} - 1)\frac{c}{p_0}\,\mathtt{B}$ to $(\frac{m}{2} - 1)c\,\mathtt{C}$ and supplies $\frac{mc}{2}\,\mathtt{C} + \frac{mc}{2p_0}\,\mathtt{B}$ into **A**; *(3)* the borrower removes all assets in **A** and repays the

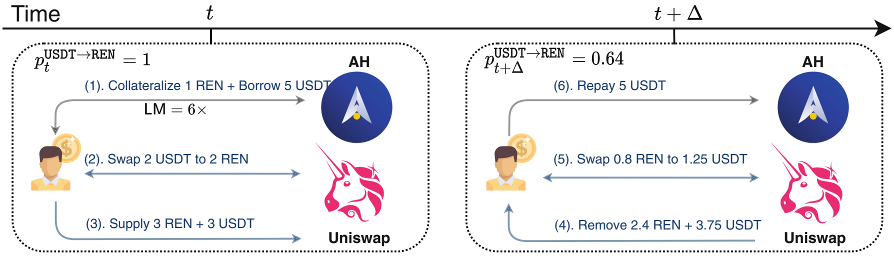

Fig. 3. Example of positive return from margin trading and IL: We assume that, at time t, the price between two tokens USDT and REN is $p_t^{\text{USDT}\rightarrow\text{REN}} = 1$ in Uniswap [31], which is a constant product AMM exchange. A borrower, namely Bob, *(1)* collateralizes 1 REN in AH and sets a 6× leverage multiplier to borrow 5 USDT. *(2)* Bob then swaps 2 USDT to 2 REN, and *(3)* supplies 3 USDT and 3 REN to Uniswap. If at time $t + \Delta$, the price $p_{t+\Delta}^{\text{USDT}\rightarrow\text{REN}}$ becomes 0.64, Bob then holds 2.4 REN and 3.75 USDT in Uniswap. Bob suffers from an IL of $\frac{3.75\times0.64+2.4}{3\times0.64+3} - 1 = -2.44\%$. *(4)* Finally, Bob removes all assets from Uniswap and *(5)* swaps 0.8 REN to 1.25 USDT (now Bob has $1.25+3.75 = 5$ USDT), and *(6)* repays the debt with 5 USDT. Bob's final return is $2.4 - 0.8 - 1 = 0.6$ REN, a profit realized through leverage and margin trading.

debt at time $t + \Delta$. We can then derive the borrower's resulting return from impermanent loss and margin trading with Eq. 2.

$$\mathsf{Return}_{\mathsf{cp}}^{\mathsf{IL,Mg}} = \frac{\frac{mc}{2\sqrt{p_0}}\sqrt{p}\cdot 1 + \frac{mc}{2\sqrt{p\cdot p_0}}\cdot p - \frac{(m-1)c}{p_0}\cdot p}{c} - 1 = m(\sqrt{\frac{p}{p_0}} - \frac{p}{p_0}) + \frac{p}{p_0} - 1 \tag{2}$$

We notice that, because the borrower performs a margin trade to swap the borrowed token B (i.e., *shorts* the debt B) to the collateralizing token C (i.e., *longs* the collateral C) before supplying assets into **A**, the decline of p may help the borrower to increase the financial return. We can further derive the return from margin trading without IL: $\mathsf{Return}_{\mathsf{cp}}^{\mathsf{Mg}} = \mathsf{Return}_{\mathsf{cp}}^{\mathsf{IL,Mg}} - \mathsf{Loss}_{\mathsf{cp}}^{\mathsf{IL}} = m(\sqrt{\frac{p}{p_0}} - \frac{p}{p_0}) + \frac{p}{p_0} - \frac{2\sqrt{\frac{p}{p_0}}}{1+\frac{p}{p_0}}$. This return may outweigh the impermanent loss $\mathsf{Loss}_{\mathsf{cp}}^{\mathsf{IL}}$, when the leverage m satisfies $m > \frac{1-\frac{p}{p_0}}{\sqrt{\frac{p}{p_0}} - \frac{p}{p_0}}$.

In Fig. 2, we set the leverage of a position to be 2×, 4× and 7×. We then visualize the return $\mathsf{Return}_{\mathsf{cp}}^{\mathsf{IL,Mg}}$ of such position by capturing a hypothetical price change $\frac{p}{p_0}$ in the range of 0 to 3. Under a leverage setting of 4 or 7, we observe that the borrower may receive a positive return, if $\frac{1}{9} < \frac{p}{p_0} < 1$. We provide an example to show our results in practice (cf. Fig. 3).

4.2 Arbitrage Risk

A liquidity pool typically requires receiving a specific proportion of supplied assets before returning the accounting LP tokens. The LP therefore may need to exchange parts of its assets prior to providing the liquidity. Because liquidity provisions may involve significant liquidity amounts, the prior swap of assets may cause a slippage which can be exploited by DeFi arbitrageurs [10,34,36].

Although arbitrage is regarded as benign for the whole DeFi ecosystem (cf. Sect. 2.3), borrowers on a leverage platform can suffer from a loss when swapping their assets in AMMs, which may generate profitable opportunities for arbitrageurs. In the following, we formalize the financial risks originating through arbitrage loss.

Generic Formulas for Arbitrage Loss. We assume that there are two constant product AMMs $\mathbf{A}_1$ and $\mathbf{A}_2$ allowing exchanges between cryptocurrencies $\mathtt{B}$ and $\mathtt{C}$. At time t, $\mathbf{A}_1$ and $\mathbf{A}_2$ have the same spot price $p_t^{\mathtt{B}\to\mathtt{C}} = p_t(x_t, y_t)$. A borrower swaps $\delta x\,\mathtt{C}$ to $\delta y\,\mathtt{B}$ in $\mathbf{A}_1$. We can then derive that the new spot price $p_{t+\delta}^{\mathtt{B}\to\mathtt{C}}$ in $\mathbf{A}_1$ is $p_{t+\delta}^{\mathtt{B}\to\mathtt{C}} = p_{t+\delta}(x_t + \delta x, y_t - \delta y + \delta y)$.

We assume that the spot price in $\mathbf{A}_2$ does not change from time t to $t+\delta$. If $p_{t+\delta}^{\mathtt{B}\to\mathtt{C}} < p_t^{\mathtt{B}\to\mathtt{C}}$, an arbitrageur can undertake the following actions to make profits: *(1)* The arbitrageur first swaps $\delta y_2\,\mathtt{B}$ to $\delta y_2 \cdot p_t^{\mathtt{B}\to\mathtt{C}}\,\mathtt{C}$ in $\mathbf{A}_2$; *(2)* The arbitrageur then swaps $\delta y_2 \cdot p_t^{\mathtt{B}\to\mathtt{C}}\,\mathtt{C}$ to $\frac{\delta y_2 \cdot p_t^{\mathtt{B}\to\mathtt{C}}}{p_{t+\delta}^{\mathtt{B}\to\mathtt{C}}}\,\mathtt{B}$ in $\mathbf{A}_1$. We can then derive the arbitrageur's final profits is $\mathsf{Loss}^{\mathsf{AR}} = \delta y_2 \cdot \left(\frac{p_t^{\mathtt{B}\to\mathtt{C}}}{p_{t+\delta}^{\mathtt{B}\to\mathtt{C}}} - 1\right)\mathtt{B}$, which also equals to the loss of the borrower who supplies $\delta x\,\mathtt{C}$ to $\mathbf{A}_1$.

Arbitrage Risk in Constant Product AMMs. If $\mathbf{A}_1$ and $\mathbf{A}_2$ are both constant product AMMs, then $p_t^{\mathtt{B}\to\mathtt{C}} = \frac{y_t}{x_t}$. If the borrower performs a margin trading, then $\delta x = (\frac{m}{2} - 1)c$, and $p_{t+\delta}^{\mathtt{B}\to\mathtt{C}} = \frac{y_t - \delta y + \delta y}{x_t + \delta x} = \frac{y_t}{x_t + \delta x}$. We can derive the arbitrage loss as $\mathsf{Loss}_{\mathsf{cp}}^{\mathsf{AR}} = \delta y_2 \cdot \left(\frac{x_t + \delta x}{x_t} - 1\right)\mathtt{B} = \frac{(\frac{m}{2}-1)c\cdot\delta y_2}{x_t}\,\mathtt{B}$.

We find that the arbitrage loss $\mathsf{Loss}_{\mathsf{cp}}^{\mathsf{AR}}$ is proportional to δx, the amount of $\mathtt{C}$ supplied by the borrower, and δy_2, the amount of $\mathtt{B}$ swapped by the arbitrageur. Hence, to reduce the arbitrage loss $\mathsf{Loss}_{\mathsf{cp}}^{\mathsf{AR}}$, the borrower can simply supply assets to the liquidity pool through multiple (temporally distributed) transactions by dividing the entire volume into smaller chunks suffering from less slippage. Note that generating several transactions will involve additional blockchain fees.

4.3 Liquidation Risk

As discussed in Sect. 3, a position is liquidatable when the debt becomes unhealthy, i.e., $\mathsf{DebtRatio}_{t+\Delta}(\mathbf{P}_{\mathsf{id}}) > 100\%$, due to a price change of $p_t^{\mathtt{B}\to\mathtt{C}}$. In the following, we explore what price changes may cause liquidations and associated financial risks in leverage systems.

We denote the leverage multiplier at time t as m. To capture how the price affects a position's health, we compute the liquidation threshold price $\hat{p_l}^{\mathtt{B}\to\mathtt{C}}$ at which the position is eligible for liquidation (cf. Eq. 3).

$$\mathsf{DebtRatio}_{t+\Delta}(\mathbf{P}_{\mathsf{id}}) \leq 1 \Longleftrightarrow \frac{\hat{p_l}^{\mathtt{B}\to\mathtt{C}}}{p_{t_0}} \leq \frac{1}{(\mathtt{B},\mathtt{C}) \cdot (m-1)} \tag{3}$$

In Fig. 2, we choose $(\mathtt{B},\mathtt{C}) = 1.5$ and show the liquidation thresholds of $\hat{p_l}^{\mathtt{B}\to\mathtt{C}}$ given a leverage 2×, 4× and 7×. We find that the threshold $\hat{p_l}^{\mathtt{B}\to\mathtt{C}}$ is inversely proportional to the chosen leverage. Moreover, the threshold $\hat{p_l}^{\mathtt{B}\to\mathtt{C}}$ is unrelated to the resulting return from impermanent loss and margin trading, i.e., even if the return is positive under a leverage 4× or 7×, the position can still be liquidatable when $\frac{p_t^{\mathtt{B}\to\mathtt{C}}}{p_{t_0}} > \frac{1}{9}$.

In addition, according to Sect. 2.6, the financial loss from a liquidation for a position $\mathbf{P}_{\mathsf{id}}$ at time t can be derived as $\mathsf{Loss}^{\mathsf{LQ}} = \frac{\mathtt{Borr}_t(\mathbf{P}^{\mathtt{B}}_{\mathsf{id}})\cdot \mathtt{LS}\cdot c_l \cdot p_t^{\mathtt{B}\to\mathtt{C}}}{\mathtt{Coll}_t(\mathbf{P}^{\mathtt{C}}_{\mathsf{id}})} = (m-1)\cdot \mathtt{LS}\cdot c_l \cdot \frac{p_t^{\mathtt{B}\to\mathtt{C}}}{p_{t_0}}$, where $\mathtt{LS} \in (0,1]$ is a parameter for the liquidation spread set by the leverage platform $\mathcal{LV}$, with which a liquidator can receive profits by repaying the debt[2]; $c_l \in (0,1]$ is a parameter that the liquidator chooses to determine what percentage of the debt shall be repaid.

4.4 Maximum Reasonable On-Chain Leverage

In the following, we investigate how to achieve a larger maximum on-chain leverage multiplier, by changing the system parameters of a DeFi leverage platform. Note that the maximum leverage multiplier discussed in this section is limited to the liquidation risk.

We consider two conditions regarding liquidations: *(1)* To avoid an instant liquidation when opening a position, the debt ratio should be less than 1 after setting the initial leverage, i.e., $\mathsf{DebtRatio}_t(\mathbf{P}_{\mathsf{id}}) \leq 1$ (cf. Eq. 3); *(2)* To incentivize liquidators, a position should have sufficient collateral to repay for a liquidation, i.e., $\mathsf{Loss}^{\mathsf{LQ}} \leq 1$ (cf. Sect. 4.3). By combining the two conditions, we derive the maximum leverage multiplier $m_{\max}$ in Eq. 4.

$$m_{\max} = \frac{1}{\max(\mathtt{LS}, (\mathtt{B},\mathtt{C})) \cdot \max(\frac{p_t}{p_{t_0}})} + 1 \tag{4}$$

We notice that three parameters play herein an important role: *(1)* $(\mathtt{B},\mathtt{C})$, a parameter determining the credit that a position gains when collaterizing 1 C and borrowing 1 B (cf. Sect. 3.1). *(2)* LS, the liquidation spread on the system (cf. Sect. 4.3). *(3)* $\frac{p_t}{p_{t_0}}$, the price change with respect to the initial price when opening a position, which varies over time. Both $(\mathtt{B},\mathtt{C})$ and LS are configurable system parameters, while $\frac{p_t}{p_{t_0}}$ indicates the price volatility.

Given $(\mathtt{B},\mathtt{C})$, LS and $\max(\frac{p_t}{p_{t_0}})$, we plot the distribution of $m_{\max}$ in Fig. 4. We discuss three cases for choosing $m_{\max}$ for stablecoins:

- **Case 1:** If $\max(\frac{p_t}{p_{t_0}}) = 1.1$, choosing $\max(\mathtt{LS}, (\mathtt{B},\mathtt{C})) = 0.11$, then $m_{\max} = 9.3\times$. In this case, we assume that *the price change* $\frac{p_t}{p_{t_0}}$ *always remains below* 1.1. This is a reasonable assumption for stablecoins in practice. For instance,

[2] For example, in Alpha Homora V2, if a liquidator repays all debt of a position, the liquidator will receive 5% of debts as rewards, i.e., $\mathtt{LS} = 5\%$.

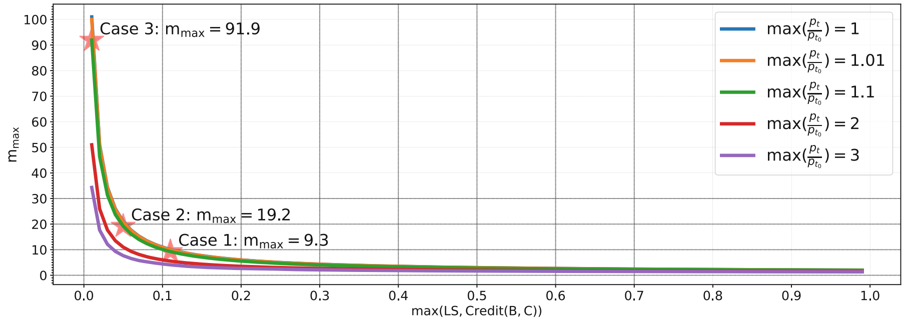

Fig. 4. Distribution of the maximum leverage multiplier $m_{\max}$ over $\max(\texttt{LS}, (\texttt{B}, \texttt{C}))$, when $\max(\frac{p_t}{p_{t_0}})$ is fixed.

the prices of USDT and USDC range between 0.99 USD and 1.01 USD in 2020 [18, 24]. Moreover, the two system parameters $(\texttt{B}, \texttt{C})$ and LS satisfy the following constraints: *(1)* $(\texttt{B}, \texttt{C})$ *is less than* 0.11, which is a practical number adopted on AHv2 [3] when B and C are stablecoins. *(2) The liquidation spread LS on the system is at most* 11%, which is larger than the LS on AHv2 (i.e., 5%).

- **Case 2:** If $\max(\frac{p_t}{p_{t_0}}) = 1.1$, choosing $\max(\texttt{LS}, (\texttt{B}, \texttt{C})) = 0.05$, then $m_{\max} = 19.2\times$. In this case, $(\texttt{B}, \texttt{C})$ is equal to the LS on AHv2.
- **Case 3:** If $\max(\frac{p_t}{p_{t_0}}) = 1.1$, choosing $\max(\texttt{LS}, (\texttt{B}, \texttt{C})) = 0.01$, then $m_{\max} = 91.9\times$. In this case, LS decreases to 1%. However, as $m_{\max}$ increases, liquidators' final rewards do not drop (cf. Sect. 4.3) and they will still be incentivized to liquidate unhealthy positions in practice.

Furthermore, according to Fig. 4, to achieve a large leverage multiplier for non-stablecoins (e.g., cryptocurrencies with a high price volatility $\frac{p_t}{p_{t_0}} > 1.1$), the leverage system needs to choose small $(\texttt{B}, \texttt{C})$ and LS.

5 Empirical Evaluation

This section outlines our empirical evaluation of user behavior and risks in Alpha Homora, the biggest leverage platform to date.

Measurement Setup. We crawl the on-chain events of AH's smart contracts [14] (e.g., `borrow`, `repay` and `liquidate` events) and related blockchain states (e.g., oracle prices, the supply interest rates of a lending pool on a specific block height, etc.) from Ethereum block 11,007,158 (7th October, 2020, the inception of AH) to 13,010,057 (12th August, 2021). We use an Ethereum full archive node, on an AMD Ryzen Threadripper 3990X with 64 cores, 256 GB of RAM, and 2×8 TB NVMe SSD in Raid 0 configuration. Note that we capture both AHv1 [2] and AHv2 [3], while AHv2 debuted at block 11,515,006 (24th December, 2020).

We observe a total of 5,110 `borrow`, 3,616 `repay`, and 122 `liquidate` events in AHv2. In AHv1, we find 14,466 `work` (emitted during borrows and repays) and 148 `kill` (liquidation) events. We normalize the prices of different tokens to `ETH` by calling the smart contract of the platform's on-chain price oracles at the block when an event was triggered. Note that we do not rely on any third-party API or external oracle for our data, and solely use the publicly available on-chain data which eases the reproducibility of our results.

5.1 User Behavior in On-Chain Leverage Platforms

We proceed to empirically analyze the user behavior for borrowers and lenders in Alpha Homora. We identify that 3,800 borrowers opened 10,430 leverage positions in AH (i.e., 7,081 in AHv1 and 3,349 in AHv2). In addition, because lending on AH is basically the same as on other lending protocols [4,12,15], which have been investigated thoroughly in related works [21,25], we focus on AH borrowers in this section and analyze lenders in our full paper [32].

Borrower Leverage Multiplier. In AH, borrowers can collateralize their assets and then open a leverage position by setting the leverage multiplier while borrowing assets from the lending pool. For each leverage position, we crawl the amount of collateralized and borrowed assets from the `transfer` and `borrow` events in AH, at the time when opening the position. Given a position' collateral and debt, we can calculate the leverage multiplier.

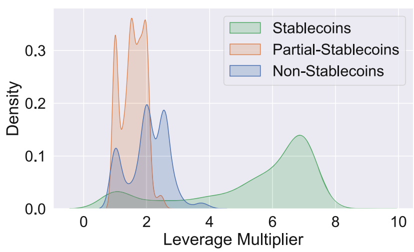

Fig. 5. Distribution of leverage over tokens. Stablecoins attract higher leverage settings. Partial-stablecoin means that borrowers collateralize stable and non-stable coins simultaneously.

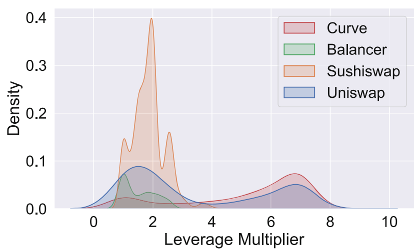

Fig. 6. Platform leverage distribution. The stablecoin platform Curve appears to attract higher leverage settings.

We find that 65% of the 3,349 borrower positions in AHv2 select a leverage multiplier smaller than 3.0, the average leverage multiplier is 3.07×. In AHv1, the maximum and average leverage multiplier of the 7,071 positions are 3× and 2.01×, respectively.

Contrary to AHv1, which only supports borrowing `ETH`, in AHv2, a borrower can collateralize (resp. borrow) 43 (resp. 12) tokens and then provide liquidity to Uniswap, Sushiswap, Curve, and Balancer. We plot the leverages' distribution when borrowers collateralize stable and non-stable coins (cf. Fig. 5) and when borrowers provide liquidity to the four platforms (cf. Fig. 6). We observe that borrowers in AHv2 tend to choose a high leverage multiplier while collateralizing stablecoins or providing liquidity to Curve. This can be explained by the fact that stablecoin pools (which Curve specializes in) are less volatile and hence less likely to experience a liquidation event. We find that stablecoin pools are being used with an average leverage of 5.39×, which is 344.70% higher than the average leverage on non-stablecoin pools.

A borrower can choose to dynamically adjust the leverage of a position, by adding or removing collateral. In Fig. 7 we visualize the distribution of 2,581 closed positions in AHv2 over their adjustment frequency and initial leverage (upon position creation). We find that 348 positions are adjusted more than once and the higher the initial leverage, the less likely this position will be adjusted. Moreover, we observe that 67.92% (i.e., 1,753) of the positions are open for less than two weeks (cf. Fig. 8).

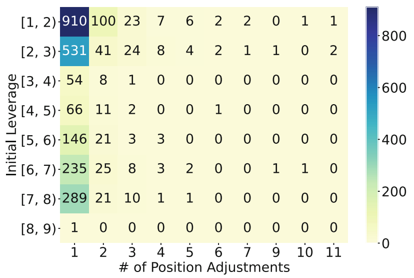

Fig. 7. Debt position distribution over leverage multiplier and adjustment frequency.

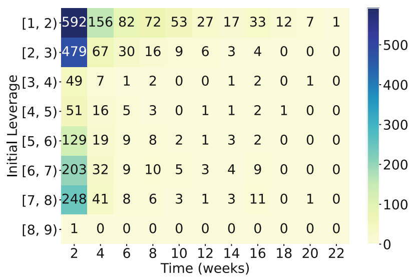

Fig. 8. Debt position distribution over leverage multiplier and duration.

Borrower APY. In the following, we analytically derive the borrower interest rates on closed debt positions with only 1 adjustment, i.e. which went through the entire cycle of opening a position with collateral, without modifying the leverage intermediately, and ultimately closing the debt. By focusing on closed positions we achieve a holistic image of the borrowers' return and behavior over the entire life-cycle of a leveraged debt position.

To calculate the APY of a borrower, we crawl the initial collateral deposit and the collateral return amounts, as well as the position opening and closure timestamps. Given this data, we can infer the financial return or APY of a closed position. Note that we convert all assets to `USD` (cf. Fig. 9) at the position opening and closure moments. Beware that we do ignore the additional potential revenue from Alpha token yield farming, as these are custom temporary protocol participation incentives [32].

Figure 9 visualizes the relationship between the BorrowAPY and the leverage multipliers. The average APY of a maximum of 1-day long positions is −585.70%.

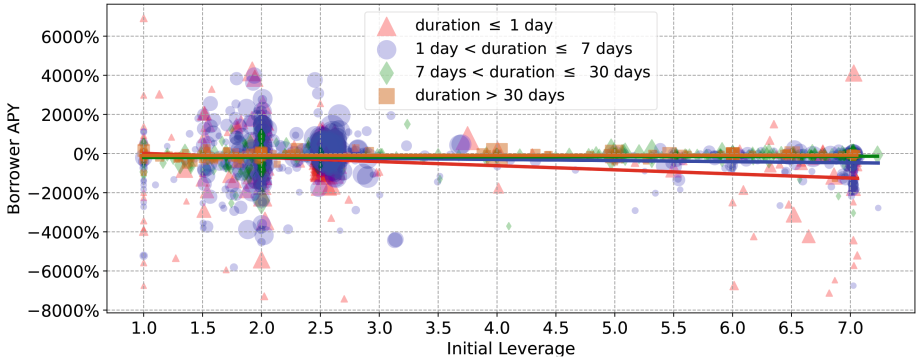

Fig. 9. Distribution of debt positions over BorrowAPY and leverage multipliers. The marker size in the figure is proportional position's collateral value. The linear regression lines are for the APY of the positions with the same duration (i.e., the same color). We find that any leverage setting is prone to negative and positive APY.

From the regression lines, we infer that the longer a position is open (i.e., more than 7 days), the more likely the borrower achieves an APY of 0%. By separating the DeFi platforms to which the borrowers supply borrowed assets, we observe that BorrowAPY varies across platforms [32].

Notably, we find that for 72.35% of the closed positions, the borrowers achieve a negative APY, i.e., lose assets despite leverage. Therefore, we can conclude that, in practice, platform subsidies (i.e., governance token rewards such as Alpha tokens) are an essential incentive mechanism for borrowers using leverage.

5.2 Empirical Analysis of Risks

In the following, we provide an empirical analysis of three risks for borrowers in Alpha Homora, and compare our results with Sect. 4.

Impermanent Loss. We investigate the AH borrowers' IL when supplying assets into constant product AMMs. We find that 1,139 closed positions in AHv2 interact with Sushi- or Uniswap. For each position, we crawl the spot price in the liquidity pool when a borrower deposits and withdraws assets. We observe that all 1,139 positions suffer from impermanent loss, with a price change $\frac{p}{p_0}$ from 0.63 to 1.62. Interestingly, we find that if the borrowers perform a margin trade (cf. Sect. 4.1) before supplying assets into the liquidity, 44.95% (i.e., 512) positions can benefit from a positive return, which compensates IL (cf. Fig. 10).

Arbitrage Loss. We find that borrowers suffer an arbitrage loss in 149 AH positions, when swapping and supplying assets in Uni- or Sushiswap. To further investigate the arbitrage loss, we crawl the cryptocurrency `X`'s amount x_t in the pool, the borrowers' collateral c, and the arbitrageur's swapped assets δy_2. We find that for the positions in AHv2 suffering from arbitrage losses, the average leverage multiplier is $5.25 \pm 1.95\times$, and the average collateral is 2.03 ± 4.21M `USD`,

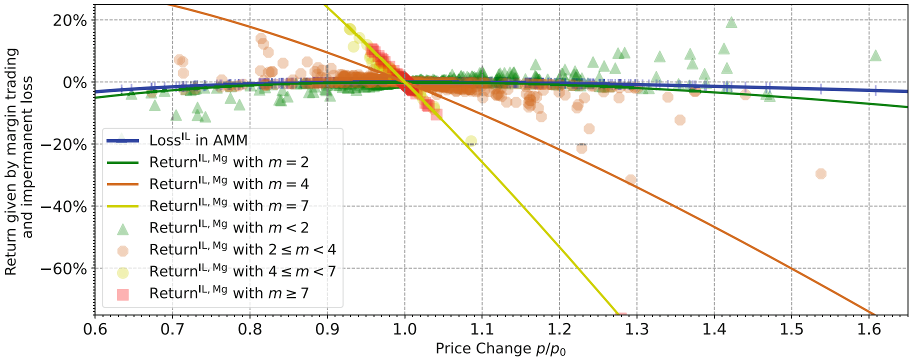

Fig. 10. Distribution of IL for AHv2 positions interacting with Uni- and Sushiswap. The continuous lines show our analytical results, while the points represent the empirical measurements. Note that the difference between our results can be explained by the fact our analytical results assume a constant leverage factor.

which are 61.04% and 21.06% higher than the average leverage multiplier and collateral in AHv2, respectively. Interestingly, we find that the position with id 61 suffered from the most important arbitrage loss, i.e., 81.67% (1.66M USD) of the collateral was lost due to the arbitrage [32].

To show an arbitrageur's expected return, given a borrower's collateral and leverage, we visualize the relationship between $\frac{\text{Loss}^{\text{AR}}_{\text{cp}}}{\delta y_2}$ and $\frac{c}{x_t}$ in Fig. 11. We find that arbitrageurs achieve less profits than our analytical results when the leverage multiplier is large (i.e., $m > 4$). This is probably because the borrowers do not perform a margin trading to swap $(\frac{m}{2} - 1)c\,\texttt{X}$ (cf. Sect. 4.2).

Liquidation Loss. We identify 50 unique liquidators performing 270 liquidations in AH to repay 4,352.52 ETH of debt in total. To show the liquidation loss, we crawl a position's collateral before and after the liquidation. Figure 12 visualizes the relationship between liquidation loss and the initial leverage multiplier. We find that the average leverage for the 122 liquidated positions in AHv2 is 2.01×, and the maximal liquidation loss is 10.63%. We observe that, due to the change of p_t, 73.77% positions suffer from a higher liquidation loss than the analytical results (cf. Sect. 4.3) when $\texttt{LS} = 5\%$, and $c_l = 1$ (i.e., the liquidator repays all the debt).

6 Related Work

In this section, we proceed to discuss existing work related to this paper.

Liquidations in DeFi. A growing body of literature has studied liquidations on borrowing and lending platforms in DeFi. Qin *et al.* [25] measure various risks that liquidation participants are exposed to on four major Ethereum lending pools (i.e., MakerDAO [16], Aave [4], Compound [15], and dYdX [12]), and quantify the instabilities of existing lending protocols. Darlin *et al.* [11] analyze the optimal bidding strategies for auction liquidations.

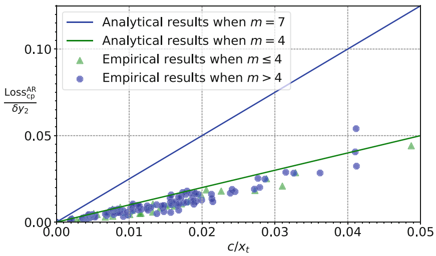

Fig. 11. Distribution of arbitrage loss for 149 debt positions in AH. Arbitrageurs achieve fewer profits than our analytical results when $m > 4$.

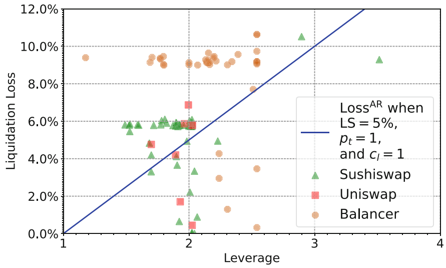

Fig. 12. Distribution of liquidation loss for 122 debt positions in AHv2. We observe that liquidations on Balancer cause higher loss (i.e., 8.51% on average).

Blockchain Extractable Value. Eskandir *et al.* [13] are the first to propose a front-running taxonomy for permissionless blockchains. Daian *et al.* [10] follow up by introducing the concept of Miner Extractable Value (MEV) on blockchains. Zhou *et al.* [36] formalize sandwich attacks on AMM exchanges, which involve front- and back-running victim transactions on DEXs. Qin *et al.* [26] quantify how much value was sourced from blockchain extractable value (BEV), such as sandwich attacks, liquidations, and decentralized exchange arbitrage [35].

7 Conclusion

In this work, we are to the best of our knowledge the first to provide a deep dive into under-collateralized DeFi lending protocols. While under-collateralization reduces the flexibility of the borrowed funds, with up to 8× leverage multipliers, such designs grant speculators more powerful tools to indulge in riskier on-chain trading. We qualitatively and quantitatively analyze the risks caused by impermanent loss, arbitrage, and liquidation. We find that 72.35% of the closed debt positions suffer from a negative APY, when ignoring the rewards of Alpha token in AH. We also find empirical evidence that stablecoin leverage is on average 344.70% higher than non-stable coin leverage. We finally show that with reasonable system settings, an on-chain leverage system can achieve a leverage multiplier of up to 91.9×.

Acknowledgments. We thank the anonymous reviewers and Stephanie Hurder for providing valuable comments and feedback which helped us to strengthen the paper. We are moreover grateful to Nimiq for partially funding this work.

References

1. Alpha homora (2021). https://alphafinancelab.gitbook.io/alpha-finance-lab/alpha-products/alpha-homora
2. Alpha homora v1 (2021). https://homora.alphafinance.io/
3. Alpha homora v2 (2021). https://homora-v2.alphafinance.io/
4. Aave: Aave Protocol (2020). https://github.com/aave/aave-protocol
5. Adrian, T., Shin, H.S.: Liquidity and leverage. J. Financ. Intermed. **19**(3), 418–437 (2010)
6. Aigner, A.A., Dhaliwal, G.: Uniswap: impermanent loss and risk profile of a liquidity provider. arXiv preprint arXiv:2106.14404 (2021)
7. BitMEX: Bitmex (2021). https://www.bitmex.com/
8. Breidenbach, L., et al.: Chainlink 2.0: next steps in the evolution of decentralized oracle networks (2021)
9. Cousaert, S., Xu, J., Matsui, T.: SoK: yield aggregators in DeFi. In: 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1–14. IEEE (2022)
10. Daian, P., et al.: Flash boys 2.0: frontrunning, transaction reordering, and consensus instability in decentralized exchanges. In: IEEE Symposium on Security and Privacy (SP) (2020)
11. Darlin, M., Papadis, N., Tassiulas, L.: Optimal bidding strategy for maker auctions. arXiv preprint arXiv:2009.07086 (2020)
12. dYdX: dYdX (2020). https://dydx.exchange/
13. Eskandari, S., Moosavi, M., Clark, J.: SoK: transparent dishonesty: front-running attacks on blockchain (2019)
14. Alpha Finance: AHV contract addresses (2021). https://immunefi.com/bounty/alphafinance/
15. Compound Finance: Compound finance (2019). https://compound.finance/
16. The Maker Foundation: Makerdao (2019). https://makerdao.com/en/
17. Liu, B., Szalachowski, P., Zhou, J.: A first look into DeFi oracles, pp. 39–48 (2021)
18. Moin, A., Sekniqi, K., Sirer, E.G.: SoK: a classification framework for stablecoin designs. In: Bonneau, J., Heninger, N. (eds.) FC 2020. LNCS, vol. 12059, pp. 174–197. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-51280-4_11
19. OkEX: Okex (2021). https://www.okex.com/
20. Trading Crypto with Leverage & the Top 6 Providers (2019). https://blog.goodaudience.com/trading-crypto-with-leverage-the-top-6-providers-31d4db6d3e00
21. Perez, D., Werner, S.M., Xu, J., Livshits, B.: Liquidations: DeFi on a knife-edge. In: Borisov, N., Diaz, C. (eds.) FC 2021. LNCS, vol. 12675, pp. 457–476. Springer, Heidelberg (2021). https://doi.org/10.1007/978-3-662-64331-0_24
22. Poloniex: Poloniex (2021). https://poloniex.com/
23. Band Protocol: Band protocol (2019). https://bandprotocol.com/
24. Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L., Gervais, A.: CeFi vs. DeFi-comparing centralized to decentralized finance. In: 2021 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE (2021)
25. Qin, K., Zhou, L., Gamito, P., Jovanovic, P., Gervais, A.: An empirical study of DeFi liquidations: incentives, risks, and instabilities. In: Proceedings of the 21st ACM Internet Measurement Conference, pp. 336–350. ACM (2021)
26. Qin, K., Zhou, L., Gervais, A.: Quantifying blockchain extractable value: how dark is the forest? In: 2022 IEEE Symposium on Security and Privacy (SP). IEEE (2022)

27. Qin, K., Zhou, L., Livshits, B., Gervais, A.: Attacking the DeFi ecosystem with flash loans for fun and profit. In: Borisov, N., Diaz, C. (eds.) FC 2021. LNCS, vol. 12674, pp. 3–32. Springer, Heidelberg (2021). https://doi.org/10.1007/978-3-662-64322-8_1
28. Schär, F.: Decentralized finance: on blockchain-and smart contract-based financial markets. Available at SSRN 3571335 (2020)
29. SushiSwap: SushiSwap (2020). https://sushi.com/
30. Thurner, S., Farmer, J.D., Geanakoplos, J.: Leverage causes fat tails and clustered volatility. Quant. Finance **12**(5), 695–707 (2012)
31. Uniswap: Uniswap (2020). https://uniswap.org/
32. Wang, Z., Qin, K., Minh, D.V., Gervais, A.: Speculative multipliers on DeFi: quantifying on-chain leverage risks. Financ. Cryptogr. Data Secur. (2022). https://www.ifca.ai/fc22/preproceedings/71.pdf
33. Prime XBT: Prime XBT (2021). https://primexbt.com/
34. Zhou, L., Qin, K., Cully, A., Livshits, B., Gervais, A.: On the just-in-time discovery of profit-generating transactions in DeFi protocols. In: 2021 IEEE Symposium on Security and Privacy (SP), pp. 919–936 (2021)
35. Zhou, L., Qin, K., Gervais, A.: A2MM: mitigating frontrunning, transaction reordering and consensus instability in decentralized exchanges. arXiv preprint arXiv:2106.07371 (2021)
36. Zhou, L., Qin, K., Torres, C.F., Le, D.V., Gervais, A.: High-frequency trading on decentralized on-chain exchanges. In: 2021 IEEE Symposium on Security and Privacy (SP), pp. 428–445. IEEE (2021)