PHBS WORKING PAPER SERIES

On the Fragility of DeFi Lending

Jonathan Chiu
Bank of Canada

Emre Ozdenoren
London Business School

Kathy Yuan
International Monetary Fund
The London School of Economics and Political Science

Shengxing Zhang
Peking University
The London School of Economics and Political Science

November 2022

Working Paper 20221102

Abstract

We develop a dynamic model of DeFi (decentralized finance) lending incorporating the following key features: 1) borrowing and lending are decentralized and anonymous where terms are set by smart contracts; 2) lending is collateralized on the market value of crypto assets where haircuts on the assets are determined rigidly by the smart contract; 3) lenders supply assets to a liquidity pool. The key friction in the model is asymmetric information between borrowers and lenders. We identify a price-liquidity feedback loop in DeFi lending: the market outcome in any given period depends on agents' expectations about lending activities in future periods, higher future price expectation leading to more lending and higher price today. When haircuts are rigid, this feedback loop leads to multiple self-fulfilling equilibria and DeFi lending and asset prices can co-move according to nonfundamental market sentiment. Flexible updates of smart contract terms can improve efficiency and restore equilibrium uniqueness.

Keywords: Decentralized finance, Smart contracts, Dynamic price feedback, Financial fragility, Adverse selection
JEL Classification: G10, G01

Peking University HSBC Business School
University Town, Nanshan District
Shenzhen 518055, China

On the Fragility of DeFi Lending

Jonathan Chiu — Bank of Canada
Emre Ozdenoren — LBS, CEPR
Kathy Yuan — IMF, LSE, FMG, CEPR
Shengxing Zhang* — PHBS, LSE, CEPR

November 2022

Abstract

We develop a dynamic model of DeFi (decentralized finance) lending incorporating the following key features: 1) borrowing and lending are decentralized and anonymous where terms are set by smart contracts; 2) lending is collateralized on the market value of crypto assets where haircuts on the assets are determined rigidly by the smart contract; 3) lenders supply assets to a liquidity pool. The key friction in the model is asymmetric information between borrowers and lenders. We identify a price-liquidity feedback loop in DeFi lending: the market outcome in any given period depends on agents' expectations about lending activities in future periods, higher future price expectation leading to more lending and higher price today. When haircuts are rigid, this feedback loop leads to multiple self-fulfilling equilibria and DeFi lending and asset prices can co-move according to non-fundamental market sentiment. Flexible updates of smart contract terms can improve efficiency and restore equilibrium uniqueness.

Keywords: Decentralized finance; Smart Contracts, Dynamic Price Feedback; Financial Fragility; Adverse Selection

JEL classification: G10, G01

*Chiu (jchiu@bankofcanada.ca), Ozdenoren (eozdenoren@london.edu), Yuan (k.yuan@lse.ac.uk), and Zhang (oo7zsx@gmail.com). Yuan has worked on the revision of the paper during her visit at IMF. We thank our discussants Felix Irresberger, Quentin Vandeweyer and Ganesh Viswanath-Natraj for valuable suggestions, as well as many conference participants for their comments. We thank Hanna Yu for her research assistance. The views expressed in this paper are solely those of the authors and may differ from official Bank of Canada or IMF views.

1 Introduction

Decentralized finance (DeFi) is an umbrella term for a variety of financial service protocols and applications (e.g., decentralized exchanges, lending platforms, asset management) on blockchain. They are anonymous permissionless financial arrangements that aim to replace traditional intermediaries by running smart contracts – immutable, deterministic computer programs – on a blockchain. Thus, they are different from traditional financial arrangements that rely on intermediaries run by third parties. By automating the execution of contracts, DeFi protocols have potential to avoid incentive problems associated with human discretion (e.g., fraud, censorship, racial and cultural bias), expand access to financial services and complement the traditional financial sector. The growth of decentralized finance has been substantial since the "DeFi Summer" in 2020. According to data aggregator DeFiLlama, the total value locked (TVL) of DeFi has reached 230 billion U.S. dollars as of April 2022, up from less than one billion two years ago. As DeFi grows in scale and scope and becomes more connected to the real economy, its vulnerabilities might undermine both crypto and formal financial sector stability (Aramonte, Huang, and Schrimpf (2021)).

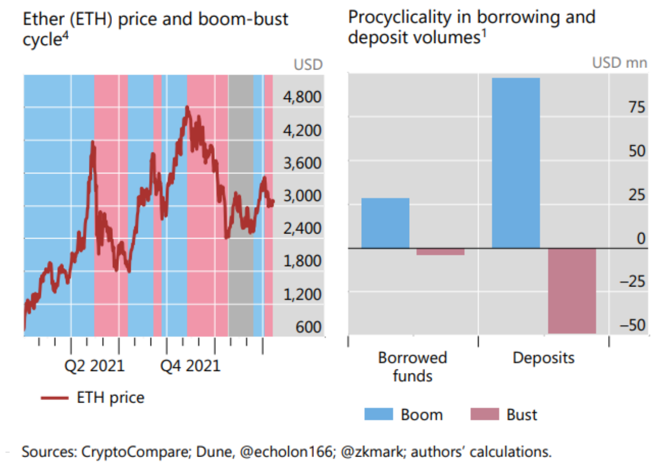
While policy makers and regulators have raised concerns about the financial stability implications of DeFi (FSB 2022; IOSCO 2022)[1], formal economic analysis on this issue is still very limited. In this paper, we examine DeFi lending protocols – an important component of the DeFi eco-system, and the sources and implications of their instability. For example, DeFi lending is much more volatile relative to traditional lending.[2] In addition, Aramonte et al. (2022) argue that DeFi lending generates "procyclicality" – the comovement between crypto prices and lending activities, as shown in Figure 1. We develop a dynamic adverse selection model to capture these key features of DeFi lending, explore its inherent fragility and its relationship to crypto asset price dynamics.

In Figure 2 we show a stylized structure of lending protocols. Anonymous lenders deposit their crypto assets (e.g., stablecoins denoted as $) via a lending smart contract to the lending pool of the corresponding crypto asset. Anonymous borrowers can borrow the crypto asset from its lending pool by pledging *any* crypto collateral accepted by the protocol via a borrowing smart contract. The collateral composition of a lending pool is unobservable, indicating that borrowers are better informed about the collateral quality than the lenders. Collateral assets are valued based on price feeds provided by an

[1] URLs of reports: https://g20.org/wp-content/uploads/2022/02/FSB-Report-on-Assessment-of-Risks-to-Financial-Stability-from-Crypto-assets_.pdf and https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf

[2] For instance, the coefficients of variation for the total values of Aave v2 loans and deposits are respectively 73 and 65 in 2021. The corresponding statistics for the US demand deposits and C&I loans are respectively 10.4 and 2.7.

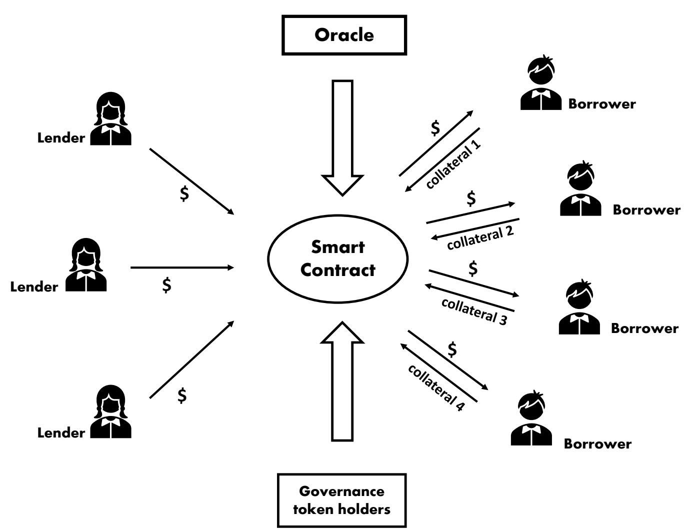
Figure 1: Crypto price boom-bust cycle and pro-cyclicality in DeFi lending



Source: Aramonte et al. (2022)

oracle which can be either on-chain or off-chain. Since crypto assets are volatile, overcollateralized is a key feature of DeFi borrowing. The rules for setting key parameters (e.g., interest rates and haircuts) are pre-programmed in the smart contracts. The protocol is governed by holders of governance tokens in a decentralized fashion. DeFi lending is typically short-term since all lending and borrowing can be terminated at any minute.

Figure 2: Stylized Structure of a DeFi Lending Protocol



DeFi differs from traditional centralized finance (TradFi) in several unique aspects. In TradFi, borrowers can be identified and standard assets are available as collateral. Furthermore, loan contracts can be flexible, with loan officers modifying terms according to the latest hard and soft information. These features help improve loan quality and enforce loan repayments in TradFi, but are not applicable to DeFi lending which is based on a public blockchain. In the DeFi environment, agents are anonymous, credit checks or other borrower-specific evaluations are not feasible. Some intertemporal and/or non-linear features of a loan contract cannot be implemented. For instance, reputational schemes become less effective (individuals can always walk away from a contract without future consequences). If loan size is used to screen borrower types, users may find it optimal to submit multiple transactions from different addresses. In addition, only tokenized assets can be pledged as a collateral. So far, these assets tend to have a very high price volatility and often are bundled into an opaque asset pool. Since a smart contract is used to replace human judgment, all terms (e.g., loan rate formulas, haircuts) need to be pre-programmed and can only be contingent on a small set of quantifiable real-time information. Moreover, contract terms cannot be contingent on soft information. As a result, DeFi lending typically involves a linear, non-recourse debt contract, featuring over-collateralization on a pool of crypto assets as the only risk control. While borrowers can choose to pledge any acceptable collateral assets, lenders cannot control or easily monitor the composition of the underlying collateral pool, implying that DeFi lending is subject to information asymmetry between borrowers and lenders.[3] Last but not least, there are so far no meaningful regulation and oversight of DeFi lending.

Motivated by these empirical observations, we develop a dynamic model of DeFi lending protocol that has the following ingredients. Borrowing is decentralized, over-collateralized, backed by various risky crypto assets, and the rule for haircuts is pre-specified. In addition, borrowers in each market are better informed about the value of the collateral asset. We uncover a price-liquidity feedback effect as the crypto market outcome in any given period depends on agents' expectations about crypto market conditions in future periods. Higher expectation about future crypto asset prices improves DeFi lending and supports higher crypto prices today, leading to multiple self-fulfilling equilibria which give rise to the fragility of DeFi lending. There exist "sentiment" equilibria in which sunspots generate fluctuations in crypto asset prices and DeFi lending volume. Assets of lower average quality are used more as collaterals during periods of negative sentiments. In addition, rigid smart contracts make crypto asset prices and

[3] Borrowers can also have an information advantage relative to the lending protocol when the smart contract relies on an inaccurate price oracle. In the Appendix, we discuss some exploit incidents during the Terra collapse in May 2022 and other price exploits due to inflated on-chain collateral prices.

DeFi lending sensitive to fundamental shocks.

Our work is the first economic paper to develop a dynamic, equilibrium model for studying decentralized lending protocols such as Aave and Compound. While there is a young and growing literature on decentralized finance, there is limited work on DeFi lending platforms. Most existing DeFi papers study decentralized exchanges to understand how automated market makers (e.g., Uniswap) function differently from a traditional exchange (e.g., see Aoyagi and Itoy (2021), Capponi and Jia (2021), Lehar and Parlour (2021), Park (2021)). There are also papers investigating the structure of decentralized stablecoins such as Dai issued by the MakerDAO (e.g., d'Avernas, Bourany, and Vandeweyer (2021), Li and Mayer (2021), Kozhan and Viswanath-Natraj (2021)). Lehar and Parlour (2022) study empirically the impact of collateral liquidations on asset prices. For a general overview of DeFi architecture and applications, see Harvey et al. (2021) and Schar (2021). Chiu, Kahn, and Koeppl (2022) study the value propositions and limitations of DeFi. Vulnerabilities that make DeFi lending protocols fragile (e.g., price oracle exploits by borrowers) are studied in the recent computer science literature. These computer science papers focus mainly on the efficiency of design features of these protocols (e.g, see Gudgeon et al. (2020), Perez et al. (2021), Qin et al. (2020), Qin et al. (2021)).

Our model is related to existing theoretical works on collateralized borrowing in a general equilibrium setting such as Geanakoplos (1997), Geanakoplos and Zame (2002), Geanakoplos (2003), and Fostel and Geanakoplos (2012). Building on Ozdenoren, Yuan, and Zhang (2021), our model captures some essential institutional feature of DeFi lending to study the joint determination of lending activities and collateral asset prices, which help us understand how information frictions and smart contract rigidity contribute to the vulnerabilities of crypto prices and DeFi lending.

This paper is organized as follows. In Section 2, we provide a brief description of features and frictions of lending protocol using Aave as an example to motivate the model assumptions. We describe the model setup in Section 3 and derive the equilibrium lending market in Section 4. In Section 5, we establish the inherent fragility of DeFi lending and discuss how flexible contract design can improve stability and efficiency. Section 6 concludes. In the Online Appendix, we report some evidence to support the case that our model can be useful for understanding the relationship between DeFi lending, crypto prices and market sentiment.

2 Lending Protocols: Features and Frictions

To motivate our model setup, we now describe some key features and frictions of DeFi protocols based on Aave, the largest DeFi lending protocol.

Key players. The Aave eco-system consists of different players. Depositors can deposit a crypto asset into the corresponding pool of the Aave protocol and collect interest over time. Borrowers can borrow these funds from the pool by pledging any acceptable crypto assets as collateral to back the borrow position. A borrower repays the loan in the same asset borrowed. There is no fixed time period to pay back the loan. Partial or full repayments can be made anytime. As long as the position is safe, the loan can continue for an undefined period. However, as time passes, the accrued interest of an unrepaid loan will grow, which might result in the deposited assets becoming more likely to be liquidated. In the eco-system, there are also AAVE token holders. Like "shareholders", they act as residual claimants and vote when necessary to modify the protocol. The daily operations are governed by smart contracts stored on a blockchain that run when predetermined conditions are met.

Loan rate and liquidation threshold. The loan and the deposit rates are set based on the current supply and demand in the pool according to formulas specified in the smart contracts. In particular, as the utilization rate of the deposits in a pool goes up (i.e., a larger fraction of deposits are borrowed), both rates will rise in a deterministic fashion. The Loan to Value (LTV) ratio defines the maximum amount that can be borrowed with a specific collateral. For example, at LTV = .75, for every 1 ETH worth of collateral, borrowers will be able to borrow 0.75 ETH worth of funds. The protocol also defines a liquidation threshold, called the health factor. When the health factor is below 1, a loan is considered undercollateralized and can be liquidated by collateral liquidators. The collateral assets are valued based on price feed provided by Chainlink's decentralized oracles.

Risky collateral. Aave currently accepts over 20 different crypto assets as collateral including WETH, WBTC, USDC and UNI. Most non-stablecoin collateral assets have very volatile market value. As shown in table 3 in the Appendix, the prices of stablecoins such as USDC and DAI (top panel), are not so volatile and they are typically loaned out by lenders. Other crypto assets, which are used as collaterals to back the borrowings, are extremely volatile relative to collateral assets commonly used in traditional finance (bottom panel). For example, ETH, which accounts for about 50% of use non-stablecoin deposits in Aave, has a daily volatility of 5.69%. The maximum daily price drop was over 26% during the sample period. The most volatile one is CRV, the governance token for the decentralized exchange and automated market maker protocol Curve DAO. For CRV the maximum price change within a day was over 40%. For risk management purposes, Aave has imposed very high haircuts on these crypto assets. For example, the haircuts for YFI and SNX are respectively 60% and 85%.[4]

Collateral pool. Loans are backed by a pool of collateral assets. While the borrower can pledge any one of the acceptable assets as a collateral, the lenders cannot control or easily monitor the quality of the underlying collateral pool. As a result, DeFi lending is subject to asymmetric information: borrowers can freely modify the underlying collateral mix without notifying the lenders. Naturally, borrowers and lenders have asymmetric incentives to spend effort acquiring information about the collateral pledged (e.g., monitor new information, conduct data analytics).

Pre-specified loan terms. Aave lending pools follow pre-specified rules to set loan rates and haircuts. As a smart contract is isolated from the outside world, it cannot be contingent on all available real-time information. While asset prices are periodically queried from an oracle (Chainlink), the loan terms do not depend on other soft information (e.g., regulatory changes, projections, statements of future plans, rumors, market commentary) as they cannot be readily quantified and fed into the contract.

Decentralized governance. Like many other DeFi protocols, Aave has released the governance to the user community by setting up a decentralized autonomous organization or DAO. Holders of the AAVE token can vote on matters such as adjustments of interest rate functions, addition or removal of assets, and modification of risk parameters such as margin requirements. To implement such changes to the protocol, token holders need to make proposals, discuss with the community, and obtain enough support in a vote. This process helps protect the system against censorship and collusion. However, decentralized governance by a large group of token holders is both time and resource costly. Hence it is not possible to update the protocol or the smart contract terms very frequently. As a result, relative to a centralized organization, a DeFi protocol may be slower to make necessary adjustments to respond to certain unexpected external changes (e.g., changes in market sentiments) in a timely manner. This problem is well documented. For instance, a risk assessment report of Aave in April 2021 pointed out that "As market conditions change, the optimal parameters and suggestions will need to dynamically shift as well. Our results suggest that monitoring and adjustment of protocol parameters is crucial for reducing risk to lenders and slashing in the safety module." [5] In practice, Since the setup of Aave v2 in late 2020 until May 2022, the risk parameters have been updated only 13 times (see Table 2 in

[4]More recently, Aave has started to accept real world asset (RWA) as collateral, allowing businesses to finance their tokenized real estate bridge loans, trade receivables, cargo & freight forwarding invoices, branded inventory financing, and revenue based financing (https://medium.com/centrifuge/rwa-market-the-aave-market-for-real-world-assets-goes-live-48976b984dde). Aave also plans to accept non-fungible tokens (NFTs) as collateral (https://twitter.com/StaniKulechov/status/1400638828264710144). Being non-standardized, NFTs are likely to be subject to even high informational frictions. Popular DeFi lending platforms for NFTs include NFTfi, Arcade, and Nexo.

[5]Source: https://gauntlet.network/reports/aave

the Appendix for some of the key changes). All were conducted after Aave DAO elected Gauntlet, a centralized entity, to provide dynamic risk parameters recommendations.

These features of Aave are common among the DeFi lending protocols, highlight three key frictions in the DeFi lending. First, there is lack of commitment from DeFi borrowers and hence the borrowings have to be (over-)collateralized. Second, There is potentially information asymmetry between DeFi borrowers and lenders because lenders cannot control collateral mix in the collateral pool. Third, DeFi contracts are rigid and based on quantifiable information on blockchain.

3 The Model Setup

The economy is set in discrete time and lasts forever.[6] There are many infinitely-lived borrowers with identical preferences. There is a fixed set of crypto assets. Each borrower can hold at most one unit. There are also potential lenders who live for a single period and are replaced every period. The lending protocol intermediates DeFi lending via a smart contract. All agents can consume/produce a numeraire good at the end of each period with a constant per unit utility/cost.

Gains from Trade A borrower needs funding that can be provided by lenders. There are gains from trade as the value per-unit of funding to a borrower is $z > 1$, while the per-unit cost of providing funding by lenders is normalized to one. In the DeFi setting, borrowers are anonymous and cannot commit to paying their debt. To overcome the commitment problem, loans must be backed by collateral. DeFi lending relies on a smart contract to implement a collateralized loan. The DeFi intermediary determines the terms of the smart contract. Collateral is locked into the smart contract and released to the borrower if and only if a repayment is received.[7]

In DeFi lending protocals such as Aave, borrowers predominantly borrow stablecoins such as USDT and USDC using risky collaterals such as ETH, BTC, YFI, YNX. They use stablecoins to fund various transactions due to their status of medium of exchange and unit of account in DeFi. We can interpret z as the value accrued to the borrowers when using the stablecoins borrowed from the lenders for purchasing assets or converting them into fiat.[8]

[6] In reality, interest payment on the borrowing in the lending protocols is continuously compounded and can be terminated at any time. Therefore, we can interpret that each time period in our model is relatively short.

[7] Chiu, Kahn, and Koeppl (2022) study how a smart contract helps mitigate commitment problems in decentralized lending.

[8] It is straight-forward to introduce governance tokens issued by the intermediary. Governance token holders then provide insurance to lenders by acting as residual claimants. Given risk neutrality, the equilibrium outcome remains the

Crypto Asset's Properties and Information Environment We assume that all crypto assets are ex-ante identical and pay random dividend $\widetilde{\delta}$ at each period and survive to the next period with probability $\widetilde{s}$. The dividend δ captures both pecuniary payoff that the asset generates (e.g., staking returns to the holder), and other private benefits that accrue from holding the crypto asset (e.g., governance right). At the beginning of a period, each asset receives an iid quality shock that determines its current and future period payoffs. Specifically, with probability $1-\lambda$, the quality of an asset is high (H) and probability λ it is low (L). The distribution of $(\widetilde{\delta}, \widetilde{s})$ is F_Q if asset quality is $Q \in \{H, L\}$. We assume F_H first-order stochastically dominates F_L and denote expectation with respect to F_Q with $\mathbb{E}_Q$.

To simplify the analysis we make further assumptions on the distributions. We assume that a high-quality asset pays dividend $\delta > 0$ at the end of the period and survives to the next period with probability $s = 1$. A low-quality asset does not pay any dividends today ($\delta = 0$) and it survives to the next period with probability $s \in [0, 1]$ which is drawn from a distribution F before the end of the period. Here, $1 - s$ captures whether the quality shock has persistent effects on the dividend flow of the crypto asset.

We assume that the crypto asset pays positive dividend in some states. The main role of this assumption is to eliminate non-monetary equilibrium. In our model the asset has collateral service and can have positive price even if it does not pay any dividend. However, there can also be an equilibrium where the asset is worthless because current lenders believe future lenders will not accept the asset the asset as collateral. Positive dividend eliminates the latter equilibrium. As we show later, in our model multiple monetary equilibria emerge when there is asymmetric information about the asset payoff (which includes the asset's dividend and price). Existence of multiplicity does not necessarily require asymmetric information about the dividend. Asymmetric information could be about survival probability of the asset, or dividend, or both which is the case we present here.[9]

At the beginning of each period, the borrower of a crypto asset privately learns the asset's quality (i.e., whether it is high or low). After observing the quality shock, the borrower decides whether and how much to borrow from the platform. The borrower then receives the private return from the loan (which is z times the loan size), and observes the realization of $(\widetilde{\delta}, \widetilde{s})$. Given the information, the borrower decides whether to repay the loan or default. The asset's quality and the state $(\widetilde{\delta}, \widetilde{s})$ are both publicly revealed at the end of each period. In the next period, some low-type assets do not survive and are replaced by new ones that are ex-ante identical. In the main model, we assume that borrowers receive

same.

[9]Our results do not depend on the asymmetric information on the common value component of the dividends. In the Appendix, we explore an alternative setup where there is asymmetric information concerning borrowers' private valuation. The main results hold.

private information every period. In the Appendix, we consider the more general case where private information arrives only infrequently with probability χ, which can capture the degree of information imperfection.

Asset Price At the end of each period, agents meet in a centralized market to trade the assets by transferring the numeraire good. At this point, the private information is revealed publicly. The end-of-period ex-dividend price of a crypto asset that will survive to the next period is denoted as ϕ_t. The pre-dividend price is thus $\Phi_t = \delta + \phi_t$ for a good asset and $s\phi_t$ for a bad asset with survival probability s. In the centralized market, each borrower can acquire at most one unit of crypto asset to the next period.[10]

Smart Contract As discussed in the introduction, DeFi lending is anonymous and collateralized via a smart contract. The smart contract is a debt contract that specifies, at each time t, the haircut and interest rate (h, R_t) set by the lending protocol. The haircut defines the debt limit per unit of collateral according to:

$$D_t \equiv \Phi_t(1 - h) \tag{1}$$

where $\Phi_t = \delta + \phi_t$.

In reality, the floating loan interest rate in the smart contract is a function of the utilization ratio i.e. the ratio of demand and supply for funding, and the collateral specific haircut is infrequently updated. To capture the economic impact of these features, we assume in our main model that the smart contract specifies a flexible market clearing interest rate and a fixed haircut. We investigate the flexible haircut case in an extension.

DeFi Lending & Borrowers In each period, if the borrower borrows ℓ_t units of funding, the face value of the debt is $R_t\ell_t$. After observing the asset quality, the borrower raises funding from a DeFi protocol by executing the lending contract. Given (R_t, D_t), a type $Q = H, L$ borrower chooses how much collateral a_t to pledge and how much loan ℓ_t to borrow from the pool:

$$\max_{a_t, \ell_t} z\ell_t - \mathbb{E}_Q \min\{\ell_t R_t, a_t(\widetilde{\delta} + \widetilde{s}\phi_t)\}$$

subject to a collateral constraint

$$\ell_t R_t \leq a_t D_t$$

[10] The dynamic structure of the model is based on Lagos and Wright (2005).

where D_t is the debt limit pinned down by (1). By borrowing ℓ_t and pledging a_t, the borrower obtains $z\ell_t$ from the loan but needs to either repay $\ell_t R_t$ or lose the collateral value $a_t(\widetilde{\delta} + \widetilde{s}\phi_t)$. The collateral value discounted by the haircut needs to be sufficiently high to cover the loan repayment. Note that, without loss of generality, we can assume that the collateral constraint is binding: $\ell_t R_t = a_t D_t$.[11] So the solution for the borrowing decision is given by

$$a_{it} \in \arg\max_{a_t \in [0,1]} a_t[zD_t/R_t - \mathbb{E}_Q \min\{D_t, \widetilde{\delta} + \widetilde{s}\phi_t\}]. \tag{2}$$

Hence, it is optimal to set $a_t \in \{0, 1\}$. When the term inside the square bracket is positive, the borrower pledges $a_t = 1$ to borrow $\ell_t = D_t/R_t$ and promises to repay D_t. Default happens whenever $D_t > \widetilde{\delta} + \widetilde{s}\phi_t$. When the term inside the square bracket is non-positive, the borrower does not borrow: $a_t = \ell_t = 0$. Since $\mathbb{E}_H \min\{D_t, \delta + \phi_t\} = D_t \geq \mathbb{E}_L \min\{D_t, \widetilde{s}\phi_t\}$, we have $a_{Lt} \geq a_{Ht}$ and $\ell_{Lt} \geq \ell_{Ht}$. That is, the low-type borrowers have higher incentives to borrow than the high-type. When both types borrow, we have a *pooling* outcome. When only the low-type borrows, we have a *separating* outcome.

DeFi Lending & Lenders The intermediary has no initial funding. It obtains funding q_t from the lenders to finance loans to borrowers. When the loan matures, the intermediary passes the cash flows – either the repayment of the borrowers or the resale value of the collateral (in case of a default) – to the lenders, after collecting an intermediation fee (discussed below). Note that the borrower's borrowing decision, $a_{i,t}$ where $i \in \{L, H\}$, is quality dependent, meaning that lenders face adverse selection in DeFi lending. Since lenders are not able to distinguish between low and high quality borrowers at the time of lending, the choice of funding size q_t does not depend on the underlying asset quality. Of course, in equilibrium, lenders take into account the expected quality of the collateral mix backing the loan.

We assume that lending market is competitive. That is, given $\{a_{i,t}\}_{i \in \{L,H\}}$, D_t, and ϕ_t, funding supply q_t satisfies the following zero profit condition:

$$q_t = \frac{1}{1+f}\left\{\frac{1}{a_{L,t}\lambda + a_{H,t}(1-\lambda)}\left[a_{L,t}\lambda\mathbb{E}_L \min\{D_t, \widetilde{s}\phi_t\} + a_{H,t}(1-\lambda)\min\{D_t, \delta + \phi_t\}\right]\right\} \tag{3}$$

where $f < z - 1$ is a fixed fee charged by the intermediary per unit of loan.[12]

When $a_{L,t} = a_{H,t} = 1$ (both types are borrowing) or when $a_{L,t} = 1$, $a_{H,t} = 0$ and the realized type is L,the funding supply is fully utilized and the funding market clears. In the separating case, if the

[11]To see this, suppose (ℓ^*, a^*) is optimal and $\ell^* R < a^* D$. Since the objective function is (weakly) decreasing in a, lowering a (weakly) increases the objective. The increase is strict if $as_L\phi < \ell R$ for some $s_L \in [\underline{s}, \bar{s}]$.

[12]When the loan matures the intermediary takes qf either from the repayment or from the resale value of the collateral. The remaining amount goes to the lender. The assumption of $f < z - 1$ ensures that the net gain from loans is positive.

realized type is H then there is no demand for funding. In this case, we assume the intermediary returns the funding supply to the lenders without charging a fee.

The intermediary's payoff is given by

$$f[\lambda a_{L,t} + (1-\lambda)\, a_{H,t}]q_t. \tag{4}$$

In section 5.5, we consider the case where the intermediary flexibly chooses the haircut. In that case, the intermediary chooses h_t to maximize (4) taking $(a_{i,t})_{i\in\{L,H\}}$ and ϕ_t as given.

Determination of the Crypto Asset Price The price of a crypto asset at the end of period t, $\phi_{t,}$, is given by:

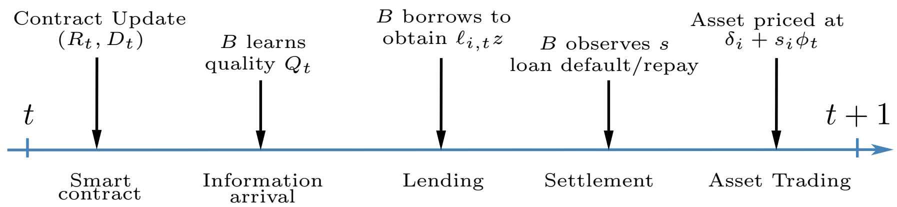
$$\phi_t = \beta \underbrace{\{\lambda\,(\mathbb{E}_L\widetilde{s})\,\phi_{t+1} + (1-\lambda)\,(\delta+\phi_{t+1})\}}_{\text{Fundamental Value}} \tag{5}$$
$$+\beta\underbrace{\left\{\begin{array}{c}\lambda\,(a_{L,t+1}\mathbb{E}_L\,(zD_{t+1}/R_{t+1} - \min\{D_{t+1}, \widetilde{s}\phi_{t+1})\})) \\ +\,(1-\lambda)\,a_{H,t+1}\,(zD_{t+1}/R_{t+1} - \min\{D_{t+1}, \delta+\phi_{t+1}\})\end{array}\right\}}_{\text{Collateral Value}}$$

where β is the discount factor such that $0 < \beta < 1/z$. The continuation value of the asset, is simply the sum of two terms: the fundamental value of the asset which is the discounted value of future dividend and asset resale price, and the collateral value. Importantly, the collateral value of the asset depends on endogenous variables, $(a_{i,t+1})_{i\in\{L,H\}}$, D_{t+1}, R_{t+1} and ϕ_{t+1}, which in turn depend on the extent of asymmetric information in future DeFi lending markets.

Timing The time-line is summarized in Figure (3). In the beginning of each period, the smart contract specifies the debt limit D_t (or equivalently the haircut h) and the loan interest rate. Next, borrower receives private information about the quality of the asset and decides whether to borrow by pledging collateral to the smart contract and lenders supply funding subject to zero profit condition. After this stage, the borrower's type is revealed, and the borrower either repays the loan or defaults and loses the collateral. If the asset survives then its price is determined, consumption takes place and the borrower works to acquire assets for the next period.

Equilibrium Definition Given haircut h and fee f, an equilibrium consists of asset prices $\{\phi_{t,}\}_{t=0}^{\infty}$, debt thresholds $\{D_t\}_{t=0}^{\infty}$, loan rates $\{R_t\}_{t=0}^{\infty}$, funding size $\{q_t\}_{t=0}^{\infty}$ and collateral quantities $\{a_{Lt}, a_{Ht}\}_{t=0}^{\infty}$ such that

Figure 3: Timeline



1. borrowers' loan decisions are optimal (condition 2),
2. lenders earn zero profit (condition 3),
3. funding supply equals funding demand, i.e. $q_t = D_t/R_t$, and
4. the asset pricing equation is satisfied (condition 5).

4 Equilibrium in Lending Market

We begin the analysis by describing the equilibrium in the DeFi lending market for a given asset price ϕ.[13] To study the borrowers' decision, we first define the degree of *information insensitivity* as the ratio of the expected value of the debt contract for types L and H, i.e., $\zeta(\phi; h) = \mathbb{E}_L \min\{D, \widetilde{s}\phi\}/D \in (0,1]$ where $D = (\delta + \phi)(1-h)$. As this ratio increases, the expected values of the debt under the low versus high types become closer, and the adverse selection problem becomes less severe.

There are two cases depending on whether the high-type borrowers are active. In the pooling case, condition (3) implies that the equilibrium funding supplied by lenders is

$$q^P = \frac{1}{1+f}[\lambda \mathbb{E}_L \min\{D, \widetilde{s}\phi\} + (1-\lambda)D].$$

Interest rate is pinned down by $q^P = D/R^P$, that is,

$$R^P = \frac{D(1+f)}{\lambda \mathbb{E}_L [\min\{D, \widetilde{s}\phi\}] + (1-\lambda)D}.$$

In the separating case, the funding from lenders is given by

$$q^S = \frac{1}{1+f}\mathbb{E}_L \min\{D, \widetilde{s}\phi\}.$$

[13] In this section we drop the time subscript t from all the variables to ease the notation.

and the interest rate pinned down by $q^S = D/R^S$, that is,

$$R^S = \frac{D(1+f)}{\mathbb{E}_L \left[\min\{D, \widetilde{s}\phi\}\right]}.$$

Define $\overline{\zeta} \equiv 1 - \frac{z-1-f}{z\lambda}$. The next proposition characterizes the equilibrium in the DeFi lending market for a given asset price ϕ.

Proposition 1. *Given asset price ϕ, if the degree of information insensitivity $\zeta(\phi; h) > \overline{\zeta}$, then borrowers' equilibrium funding obtained from DeFi lending is $q = q^P$, interest rate is $R = R^P$ and collateral choices for H type borrower and L type borrower are $a_L = a_H = 1$. If the degree of information insensitivity $\zeta(\phi; h) < \overline{\zeta}$, then borrowers' equilibrium funding from DeFi lending is $q = q^S$, interest rate is $R = R^S$, and collateral choices for H type borrower and L type borrower are $a_L = 1$ and $a_H = 0$. The former condition, for a pooling equilibrium, is easier to satisfy when asset price ϕ, haircut h or productivity from borrowers' private investment z is higher.*

Proposition 1 implies that, given asset price ϕ, there is a unique equilibrium in DeFi lending. It is a pooling (separating) outcome when the debt contract is sufficiently informationally insensitive (sensitive). In particular, when the degree of information insensitivity $\zeta(\phi; h)$ is above the threshold ζ, the adverse selection problem is not too severe and both types borrow. In this case, the loan size is the pooling quantity $q = q^P$. When the degree of information insensitivity is below the threshold, the adverse selection problem is severe and only the low type borrows. In this case, the loan size is the separating amount $q = q^S$. Furthermore, the loan rate in a pooling equilibrium is lower than that in a separating equilibrium.

Note $\zeta(\phi; h) = \mathbb{E}_L \min\{1, \frac{\widetilde{s}\phi}{(\delta+\phi)(1-h)}\}$. As a result, the debt contract becomes informationally less sensitive for a high ϕ and for a high h. The above proposition also indicates that in addition to the parameter λ that characterizes type heterogeneity, the net gains from trade, $z/(1+f)$, is also an important determinant of adverse selection: a lower $z/(1+f)$ leads to a higher $\overline{\zeta}$. In particular, even if there is very little asymmetric information about the quality of the debt contract (i.e., when $\zeta(\phi; h)$ is slightly below 1), as $z/(1+f)$ approaches 1 (so that $\overline{\zeta}$ is close 1), the DeFi lending will be in a separating equilibrium. In other words, when net gains from trade is low, even a slight amount of asymmetric information results in adverse selection problem.

5 Multiple Equilibria in Dynamic DeFi Lending

The analysis in the previous section takes the asset price as given. In this section, we characterize the stationary equilibrium where asset prices are endogenously determined. We demonstrate that DeFi lending is fragile in the sense that it exhibits dynamic multiplicity in prices. Specifically, we show that there might be multiple equilibria in the DeFi lending market justified by different crypto asset prices. The multiple asset prices are in turn justified by the different equilibria in DeFi lending. Since we are focusing on stationary equilibria, we drop the time subscripts.

5.1 Characterization of Stationary Equilibria

5.1.1 Pooling equilibrium

In a stationary pooling equilibrium, all borrowers borrow ($a_L = a_H = 1$). This equilibrium exists when there is an asset price ϕ^P satisfying the equation

$$\phi^P = \beta\left[(z-1-f)q^P\right] + \beta(1-\lambda)\delta + \beta(\lambda\mathbb{E}_L\widetilde{s} + (1-\lambda))\phi^P. \tag{6}$$

The loan size is given by

$$q^P = \frac{1}{1+f}\left(\lambda\mathbb{E}_L\left[\min\{D^P, \widetilde{s}\phi^P\}\right] + (1-\lambda)D^P\right),$$

where $D^P = \left(\delta + \phi^P\right)(1-h)$. In addition, it has to satisfy the high-type borrowers' incentive constraint to pool:

$$\zeta\left(\phi^P; h\right) = \mathbb{E}_L \min\{1, \frac{\widetilde{s}\phi^P}{(\delta+\phi^P)(1-h)}\} \geq \overline{\zeta}. \tag{7}$$

5.1.2 Separating Equilibrium

In a separating equilibrium, only the low-type borrowers borrow (i.e., $a_H = 0$, $a_L = 1$). This equilibrium exists when there is an asset price ϕ^S satisfying the equation

$$\phi^S = \beta\left(\lambda(z-1-f)q^S + (1-\lambda)\delta + (\lambda\mathbb{E}_L\widetilde{s} + (1-\lambda))\phi^S\right). \tag{8}$$

The loan size is given by

$$\frac{D^S}{R} = q^S = \frac{1}{1+f}\mathbb{E}_L\left[\min\{D^S, \widetilde{s}\phi^S\}\right],$$

where $D^S = \left(\delta + \phi^S\right)(1-h)$. In addition, pooling violates the high-type's incentive constraint:

$$\zeta\left(\phi^P; h\right) < \overline{\zeta}. \tag{9}$$

5.2 Existence and Uniqueness

We first focus on the asset pricing equations (6) and (8).

Lemma 1. *Equation (6) has a unique solution ϕ^P and equation (8) has a unique solution ϕ^S. Also, $\phi^P \geq \phi^S$.*

Lemma 1 implies that there exists at most one pooling and one separating stationary equilibrium. If they co-exist, the price in the pooling equilibrium is higher than that in the separating equilibrium. It is also easy to show that both prices are higher than the fundamental price of the asset in autarky, $\underline{\phi} = \frac{\beta(1-\lambda)\delta}{1-\beta(\lambda\mathbb{E}(s_L)+(1-\lambda))}$. This means that the introduction of DeFi lending raises the equilibrium asset price above its fundamental level. Lemma 1 implies that $\zeta(\phi^P; h) \geq \zeta(\phi^S; h)$. Hence, we have the following proposition.

Proposition 2. *There always exists at least one stationary equilibrium:*

- *it is a unique pooling equilibrium when $\overline{\zeta} < \zeta(\phi^S; h)$,*
- *it is a unique separating equilibrium when $\overline{\zeta} > \zeta(\phi^P; h)$,*
- *a pooling equilibrium and a separating equilibrium coexist when $\overline{\zeta} \in [\zeta(\phi^S; h), \zeta(\phi^P; h)]$.*

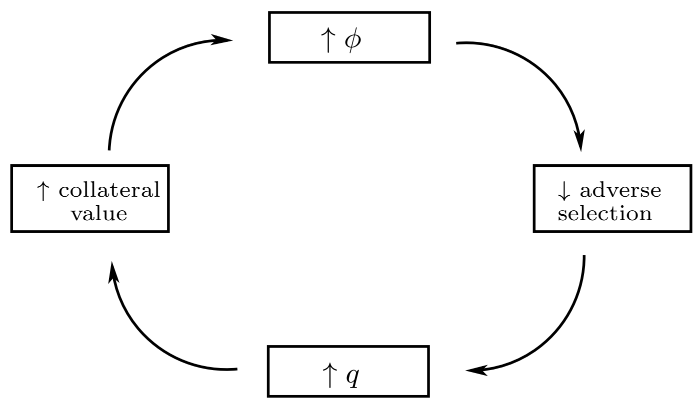
In the next section, we examine the conditions under which the multiplicity arises.

5.3 Haircut and Multiplicity

In Proposition 2, multiplicity arises due to a dynamic price feedback effect described in Figure 4. When the collateral asset price is high, the degree of information insensitivity of the debt contract, $\zeta(\phi^P; h)$, is above the threshold $\overline{\zeta}$. Hence, the adverse selection problem is mild and the high-type borrowers are willing to pool with the low type. In turn, if agents anticipate a pooling equilibrium in future periods, the expected liquidity value of the asset in the next period is large, hence the asset price today is high. Conversely, when the asset price is low, the degree of information insensitivity of the debt contract, $\zeta(\phi^S; h)$, is below the threshold $\overline{\zeta}$. Therefore, the adverse selection problem is severe and the high type retains the asset and chooses not to borrow. In turn, if agents anticipate a separating equilibrium in future periods, the liquidity value of the asset is limited thus the asset price today is low. As a result, the asset prices are self-fulfilling in this economy.

The haircut is a key parameter controlling the degree of information sensitivity. Setting a lower haircut makes the debt contract informationally more sensitive, magnifying the adverse selection problem.

Figure 4: Dynamic Feedback Loop



Defining two thresholds

$$\kappa_P \equiv \frac{\zeta}{\beta z[(1-\lambda)+\zeta\lambda]}$$
$$\kappa_S \equiv \frac{\zeta}{\beta[(1-\lambda)+\zeta\lambda z]} < \kappa_P,$$

we have the following result.

Proposition 3. *Suppose the expected survival probability of the crypto asset satisfies* $\mathbb{E}_L \widetilde{s} \in (\kappa_P, \kappa_S)$. There exists a threshold for haircut such that when the haircut h is below this threshold, there are multiple equilibria.

5.3.1 An Illustrative Example

We now use an example to illustrate the effects of h on the equilibrium outcome. The full analysis is given in the Appendix. Suppose $\widetilde{s}$ is drawn from a two-point distribution such that $s = 1$ with probability π, and $s = 0$ with probability $1 - \pi$. Consider the separating equilibrium. When $s = 0$, a low-type borrower always defaults. When $s = 1$, the low-type defaults if $D^S = \left(\delta + \phi^S\right)(1-h) > \phi^S$ and repays if $D^S \leq \phi^S$. We can rewrite this condition to show that there exists a threshold level $\underline{h}^S$such that when $s = 1$, the low-type defaults if $h < \underline{h}^S$ and repays if $h \geq \underline{h}^S$. In the former case, the low type always defaults so the face value of the loan and consequently the loan size do not depend on the haircut. In the latter case, the low type repays the loan in the good state (i.e., $s = 1$), hence the loan size depends on the face value of the debt. Since the face value of debt declines as the haircut increases, the loan size decreases in h.

We define $\zeta^S(h) \equiv \zeta(\phi^S(h); h)$. That is, we obtain $\zeta^S(h)$ by substituting the price ϕ^S as a function of haircut given fixed values for all other exogenous variables. We define $\zeta^P(h)$ similarly. Using (9), a separating equilibrium exists if $\zeta^S(h) \leq \overline{\zeta}$. The threshold $\zeta^S(h)$ is strictly increasing in h for $h < \underline{h}^S$. The reason is that the high type never defaults, so the expected value of the contract under the high type declines as h increases. The low type, on the other, always defaults and the expected value of the contract under the low type is independent of h. Hence, the information sensitivity of the contract decreases as h increases and it becomes harder to support a separating equilibrium. For $h \geq \underline{h}^S$, $\zeta^S(h) = \pi$ and a separating equilibrium exists whenever $\pi < \overline{\zeta}$. That is, once the haircut is large enough, increasing it further does not affect the information sensitivity of the contract. The reason is that, in this case, the high type always pays the face value and the low type pays the face value only in the good state. As the haircut increases, the face value decreases but the value of the contract declines at the same rate for both types so its information sensitivity remains constant.

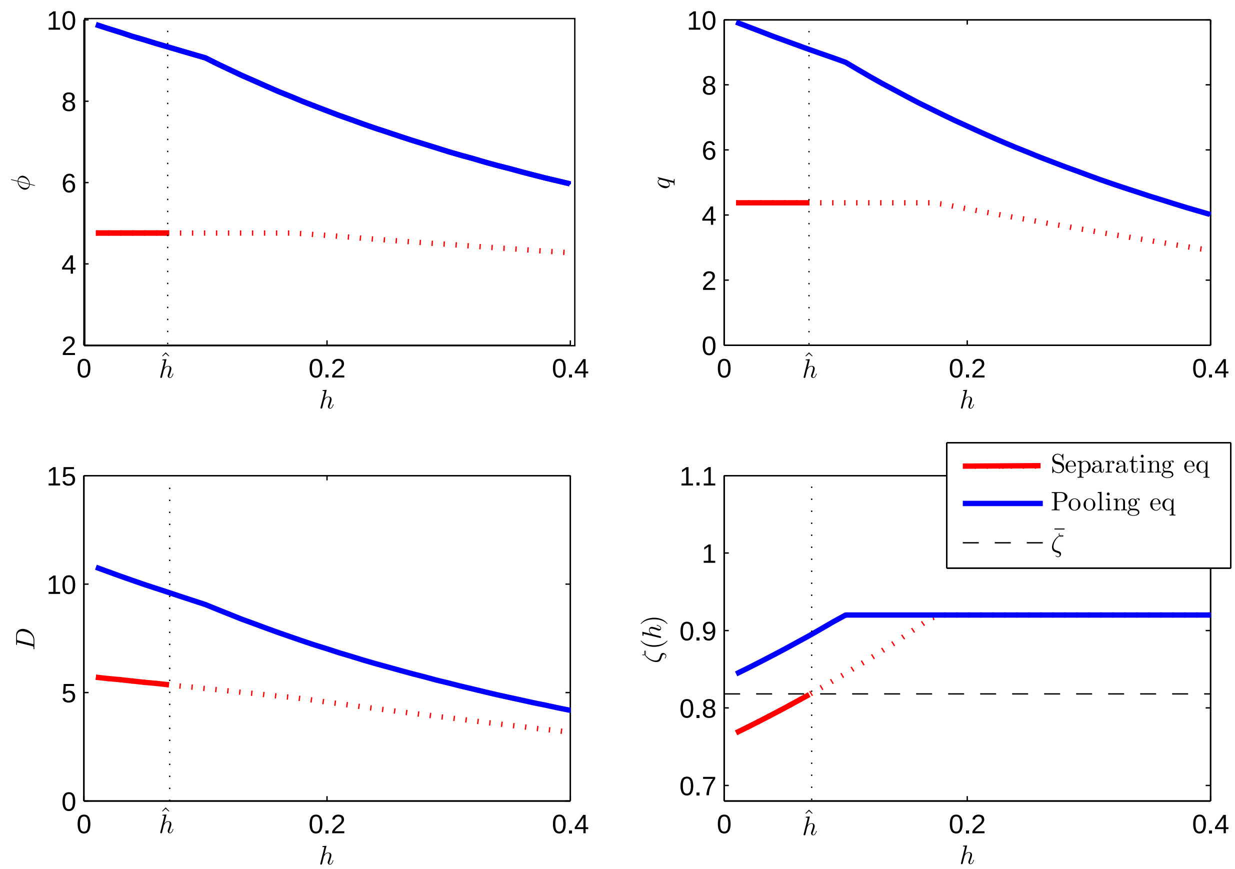
We analyze the pooling equilibrium similarly, and find a threshold $\underline{h}^P < \underline{h}^S$ such that when $s = 1$, the low-type defaults if $h < \underline{h}^P$ and repays if $h \geq \underline{h}^P$. A pooling equilibrium exists if $\zeta^P(h) \geq \overline{\zeta}$. The threshold $\zeta^P(h)$ is strictly increasing in h and $\zeta^P(h) > \zeta^S(h)$ for $h < \underline{h}^P$. For $h \geq \underline{h}^P$, $\zeta^P(h) = \pi$ and a pooling equilibrium exists whenever $\pi > \overline{\zeta}$.

Putting these facts together we see that whenever $h < \underline{h}^S$, we have $\zeta^S(h) < \zeta^P(h)$. Hence when $\overline{\zeta}$ is in this range the two equilibria coexist. When the haircut exceeds $\underline{h}^S$, there can only be a unique equilibrium depending on whether $\overline{\zeta}$ is above or below π.

Figure 5 plots the effects of h on the asset price, the loan size, the debt limit and the degree of information insensitivity of the contract. The red and blue curves indicate respectively the separating and pooling equilibria, assuming their existence. The parameter values used are $z = 1.1$, $\lambda = 0.5$, $\beta = 0.9$, $\delta = 1$, $\pi = 0.92$, $f = 0$, which satisfy the condition $\mathbb{E}_L \widetilde{s} \in (\kappa_P, \kappa_S)$ in Proposition 3. The bottom right plot compares the degrees of information insensitivity to the threshold $\overline{\zeta}$ which is captured by the horizontal dash line. When h is close to zero, the dash line appears above the red curve and below the blue curve, confirming the multiplicity result in Proposition 3. The other three plots also confirm the earlier result that the asset price, loan size and debt limit are higher in a pooling equilibrium. In this example, multiplicity can be ruled out and pooling can be supported by setting $h > \hat{h} = 7.1\%$ where $\overline{\zeta} = \zeta^S(\hat{h})$. [14]

[14]When $h > \hat{h}$,separating equilibrium cannot be sustained and hence in Fgure 5 red lines depicting separating equibriums become red dotted lines in this region.

Figure 5: Effects of Haircut h



5.4 Sentiment Equilibrium

In the middle region where multiple self-fulfilling equilibria coexist, it is possible to construct *sentiment equilibria* where agents' expectations depend on non-fundamental sunspot states (Asriyan, Fuchs, and Green (2017)). Suppose that there are K sentiment states indexed from 1 to K. We let $\sigma_{kk'}$ be the Markov transition probability from sentiment state k to k'.

In the presence of sentiments we modify the model as follows. Let ϕ^k be the price of the asset, R^k be the loan rate, and $D^k = \left(\delta + \phi^k\right)(1 - h)$ be the debt limit in sentiment state k. Quantities of collateral a_L^k, a_H^k chosen by each type must be optimal given the price and rate at each sentiment state k. The loan size chosen by the lender in sentiment state k is given by:

$$q^k = \lambda E_L \left[\min\{D^k, s\phi^k\}\right] + (1-\lambda)D^k$$

The price of crypto asset in sentiment state k is given by:

$$\phi^k = \beta\{\sum_{k'=1}^{K} \sigma_{kk'}\{\lambda \int_{\underline{s}}^{\bar{s}} s_L \phi^{k'} dF(s_L) + (1-\lambda)\left(\delta + \phi^{k'}\right)$$
$$+ \lambda \left(a_L^{k'} \int_{\underline{s}}^{\bar{s}} \left(zD^{k'}/R^{k'} - \min\{D^{k'}, s_L\phi^{k'})\}\right) dF(s_L)\right) + (1-\lambda)\, a_H^{k'} \left(zD^{k'}/R^{k'} - D^{k'}\right)\}.$$

We want to construct a *non-trivial sentiment equilibrium* such that the economy supports a pooling outcome in states $k = 1, ..., \bar{k}$ and a separating outcome in states $k = \bar{k}+1, ..., K$. By continuity, one can obtain the following result.

Proposition 4. *Suppose $\mathbb{E}(s) \in (\kappa_P, \kappa_S)$ and haircut is not too big. Then for σ_{kk} large enough, there exists a non-trivial sentiment equilibrium.*

To demonstrate non-trivial sentiment equilibrium and examine equilibrium properties, we provide the following two numerical examples. In both examples we assume $\widetilde{s}$ is drawn from a two-point distribution such that $s = 1$ with probability π, and $s = 0$ with probability $1-\pi$.

Example 1. Suppose $K = 3$ and $\bar{k} = 1$. The economy stays in the same state with probability σ and moves to the next state with probability $1-\sigma$ where the next state from 1 is 2, from 2 is 3 and from 3 is 1. We can interpret the three states as follows:

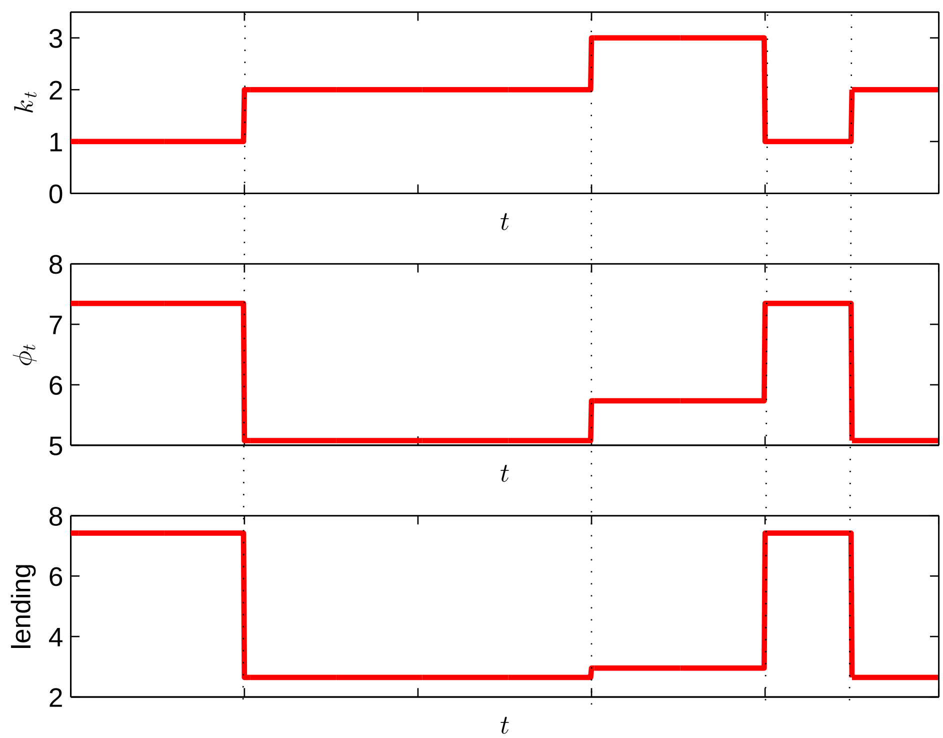
- $k = 1$: Boom state
  - $a_L^1 = a_H^1 = 1$, $q^1 = \lambda\pi \min\{(\delta + \phi^1)(1-h), \phi^1\} + (1-\lambda)(\delta + \phi^1)(1-h)$
- $k = 2$: Crash state
  - $a_L^2 = 1, a_H^2 = 0$, $q^2 = \pi \min\{(\delta + \phi^2)(1-h), \phi^2\}$
- $k = 3$: Recovery state
  - $a_L^3 = 1, a_H^3 = 0$, $q^3 = \pi \min\{(\delta + \phi^3)(1-h), \phi^3\}$

The asset prices are then given by

$$\begin{aligned}\phi^k =&\beta\sigma_{k1}\left[(z-1)q^1 + (1-\lambda)\delta + (\lambda\pi + (1-\lambda))\phi^1\right]\\ &+\beta\sigma_{k2}\left[\lambda(z-1)q^2 + (1-\lambda)\delta + (\lambda\pi + (1-\lambda))\phi^2\right]\\ &+\beta\sigma_{k3}\left[\lambda(z-1)q^3 + (1-\lambda)\delta + (\lambda\pi + (1-\lambda))\phi^3\right]\end{aligned}$$

Figure 6 below plots the effects of sentiment states on asset prices and total lending. When $\sigma = 0.95$, the sentiment state is sufficiently persistent so that the above sentiment equilibrium exists. As shown, the sentiment dynamics drive the endogenous asset price cycle: The asset price declines when the economy enters the crash state, jumps up when the economy moves from the crash state to the recovery state, and jumps up further when the economy returns to the boom state. Note that the total lending, $\left(\lambda a_L^k + (1-\lambda) a_H^k\right) q^k$ is "pro-cyclical" in the sense that it is positively correlated with the asset price.

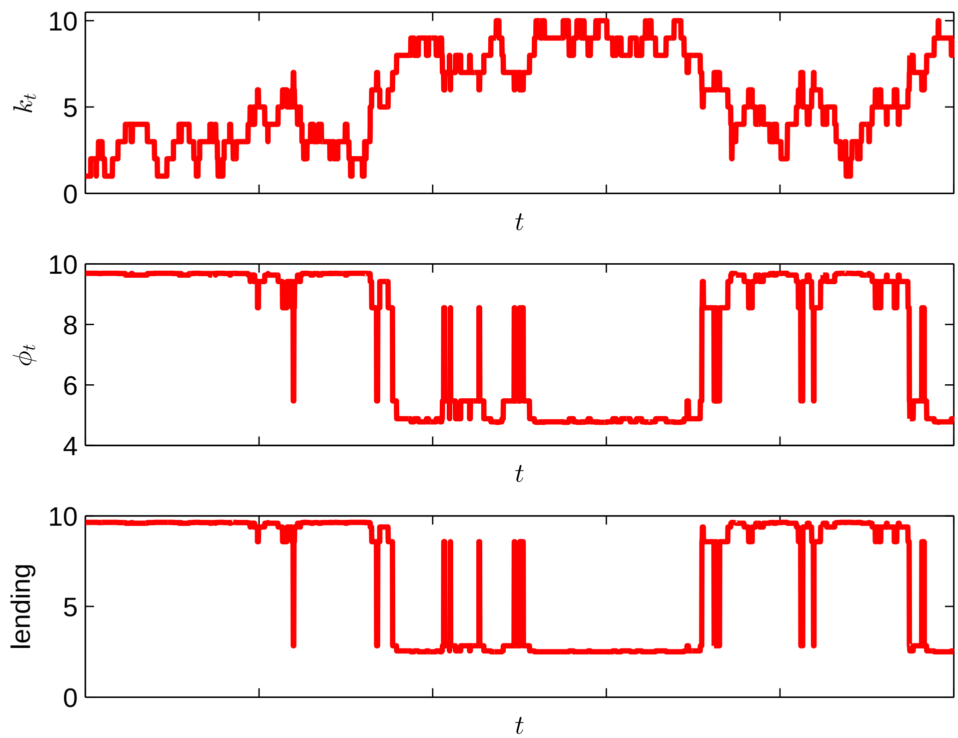
Figure 6: Sentiment Equilibrium Example 1



Next, we show a similar pro-cyclical pattern of lending and asset prices in an example where there are more (than three) states and a state moves to an up or a down state with an equal probability. In this example, equilibrium lending and asset prices are more volatile.

Example 2. Let $K = 10$. If the economy is in state k in a given period, in the next period sentiment stays the same with probability σ. From states $k \in \{2, \ldots, K-1\}$ economy moves to state $k-1$ with probability $(1-\sigma)/2$ and to state $k+1$ with probability $(1-\sigma)/2$. From state 1 economy moves to state 2 with probability $1-\sigma$. From state K economy moves to state $K-1$ with probability $1-\sigma$. Figure 7 plots a simulation for 5000 periods when $\sigma = 0.95$ and $\bar{k} = 6$.

Figure 7: Sentiment Equilibrium Example 2



5.5 Uniqueness under Flexible Design of Debt limit

We have shown that DeFi lending subject to a rigid haircut can lead to multiplicity when the debt contract is too informationally sensitive. We now show that a flexible contract design supports a unique equilibrium and generates higher social surplus from lending compared to the case with a rigid haircut.

Under flexible design, the smart contract is no longer subject to the constraint (1). Instead, in each period, the contract designer can choose any feasible debt contract, $y(D, \widetilde{\delta} + \widetilde{s}\phi_t) = \min(D, \widetilde{\delta} + \widetilde{s}\phi_t)$ for $0 \leq D \leq \delta + \phi_t$. Let $\widehat{z}$ denote the marginal value of obtaining funding from lenders deducting the intermediation fee f to the intermediary,

$$\widehat{z} = \frac{z}{1+f}.$$

Recall from (4) that intermediary maximizes the expected loan size times the intermediation fee:

$$f[\lambda + (1-\lambda)\, a_{H,t}]q_t\left(y(D, \widetilde{\delta} + \widetilde{s}\phi_t)\right)$$

The loan size is:

$$q_t\left(y(D, \widetilde{\delta} + \widetilde{s}\phi_t)\right) = \frac{1}{1+f}\frac{[\lambda \mathbb{E}_L + a_{H,t}\,(1-\lambda)\,\mathbb{E}_H]\, y(D, \widetilde{\delta} + \widetilde{s}\phi_t)}{\lambda + a_{H,t}\,(1-\lambda)} \tag{10}$$

where

$$a_{H,t} = \begin{cases} 1 & \text{if } \widehat{z}\,[\lambda \mathbb{E}_L + (1-\lambda)\mathbb{E}_H]\, y(D, \widetilde{\delta} + \widetilde{s}\phi_t) \geq \mathbb{E}_H y(D, \widetilde{\delta} + \widetilde{s}\phi_t) \\ 0 & \text{otherwise} \end{cases}. \tag{11}$$

Equivalently the intermediary maximizes

$$[\lambda \mathbb{E}_L + a_{H,t}\,(1-\lambda)\,\mathbb{E}_H]\, y(D, \widetilde{\delta} + \widetilde{s}\phi_t) \tag{12}$$

subject to (11).In words, the intermediary takes the price ϕ_t as given and sets the debt threshold D to maximize the expected loan size taking into account the impact if the contract on the funding that the lenders are willing to supply under the separating and the pooling cases. The value of the asset to the borrower is:

$$\begin{aligned} V_t = \max_{0 \leq D \leq \delta + \phi_t} \lambda &\left[\widehat{z}q_t\left(y(D, \widetilde{\delta} + \widetilde{s}\phi_t)\right) - \mathbb{E}_L y(D, \widetilde{\delta} + \widetilde{s}\phi_t) + \mathbb{E}_L\left(\widetilde{\delta} + \widetilde{s}\phi_t\right)\right] \\ &+ (1-\lambda)\left[a_{H,t}\left\{\widehat{z}q_t\left(y(D, \widetilde{\delta} + \widetilde{s}\phi_t)\right) - \mathbb{E}_H y(D, \widetilde{\delta} + \widetilde{s}\phi_t)\right\} + \mathbb{E}_H\left(\widetilde{\delta} + \widetilde{s}\phi_t\right)\right] \end{aligned} \tag{13}$$

Given the optimal design, the asset price at the end of the previous period equals

$$\phi_{t-1} = \beta V_t. \tag{14}$$

An equilibrium under flexible design of smart contracts is D, V_t, and ϕ_t such that (i) D maximizes 12 taking ϕ_t as given and, (ii) V_t, and ϕ_t satisfy (13) and (14).

We also make the same simplifying assumptions on the distribution of $\left(\widetilde{\delta}, \widetilde{s}\right)$ that we make in the rigid haircut case. That is, we assume

$$\mathbb{E}_H y(D, \widetilde{\delta} + \widetilde{s}\phi_t) = y(D, \delta + \phi_t);$$

and

$$\mathbb{E}_L y(D, \widetilde{\delta} + \widetilde{s}\phi_t) = \int_{\underline{s}}^{\bar{s}} y(D, s_L\phi_t) dF\left(s_L\right).$$

The following proposition compares the outcomes under flexible contract design with those under a DeFi lending contract subject to the rigid haircut rule (1).

Proposition 5. *Under flexible optimal debt limit,*

(i) there exists a unique stationary equilibrium.

(ii) given any end-of-period price ϕ_t, the asset price in the previous period and the lending volume are higher than those under the rigid DeFi contract,

(iii) the stationary equilibrium Pareto dominates the one under DeFi.

The proposition shows that the equilibrium under flexible contract design is unique and generates more social surplus. For example, when ϕ_t is high (which makes the debt contract informationally less sensitive), the designer can increase D_t to raise the surplus from lending, inducing a higher lending volume. In contrast, when ϕ_t is low (which makes the contract informationally more sensitive), the designer may choose to lower D_t to maintain a pooling outcome to induce a higher lending volume.[15] This flexibility in adjusting D_t implies that, given any end-of-period price ϕ_t, the price of asset in the previous period and the loan size are weakly greater than those under the rigid DeFi contract. Therefore, the steady state price and loan size are also weakly greater than those under DeFi. The borrower is better off under flexible contract design while lenders are not worse off. The stationary equilibrium therefore Pareto dominates the one under DeFi.

The above result suggests that the rigid haircut rule (1) imposed by the DeFi smart contract generates financial instability in the form of multiple equilibria, and potential sentiment driven equilibria (e.g. Asriyan, Fuchs, and Green (2017)), and lowers welfare. Can a DeFi smart contract be pre-programmed to replicate the flexible contract design? This can be challenging in practice. First, flexible contract cannot be implemented using simple linear hair-cut rules that are typically en-coded in DeFi contracts. Second, the optimal debt threshold depends on information that may not be readily available on-chain (e.g., z, λ). Alternatively, the lending protocol can replace the algorithm by a human risk manager who can adjust risk parameters in real time according to the latest information. Relying fully on a trusted third party, however, can be controversial for a DeFi protocol. Our results highlight the difficulty in achieving stability and efficiency in a decentralized environment subject to informational frictions.

5.5.1 A Simple Example

In the example with a two-point distribution, the optimal flexible debt limit depends on parameter values. As shown in the Appendix, when $\pi < \zeta$, the pooling equilibrium does not exist. It is thus

[15] Notice that, depending on parameter values, the designer may also choose to raise D_t to induce a separating equilibrium.

optimal for the intermediary to set $D_t^S = \phi_t$ to support a separating equilibrium. When $\pi \geq \zeta$, the pooling equilibrium exists and dominates the separating one. The intermediary's optimal choice is to set

$$D_t^P = \min\left\{\frac{\pi\phi_t}{\zeta}, \delta + \phi_t\right\}.$$

Therefore, when the debt limit is flexible, there exists a unique stationary equilibrium. The implied haircut is not a fixed number but a non-linear function:

$$h_t = \begin{cases} 0 & \text{, if } \pi < \zeta, \\ \max\left\{1 - \frac{\pi\phi_t}{\zeta(\delta+\phi_t)}, 0\right\} & \text{, if } \pi \geq \zeta. \end{cases}$$

6 Conclusion

In this paper, we study the sources of vulnerability in DeFi lending related to a few fundamental features of DeFi lending (collateral with uncertain quality, oracle problem, and rigid contract terms). We demonstrate the inherent instability of DeFi lending due to a price-liquidity feedback exacerbated by informational frictions, leading to self-fulfilling sentiment driven cycles. Stability requires flexible and state-contingent smart contracts. To achieve that, the smart contract may take a complex form and require a reliable oracle to feed real-time hard and soft information from the off-chain world. Alternatively, DeFi lending may need to re-introduce human intervention to provide real-time risk management – an arrangement that forces the decentralized protocol to rely on a trusted third party. Our finding highlights DeFi protocols' difficulty to achieve efficiency and stability while maintaining a high degree of decentralization.

References

Aoyagi, J. and Y. Itoy (2021). *Coexisting Exchange Platforms: Limit Order Books and Automated Market Makers.* URL: `https://ssrn.com/abstract=3808755`.

Aramonte, Sirio, Wenqian Huang, and Andreas Schrimpf (2021). "DeFi Risks and the Decentralisation Illusion". *BIS Quarterly Review.*

Aramonte, Sirio et al. (2022). "DeFi lending: intermediation without information?" *BIS Bulletin.*

Asriyan, Vladimir, William Fuchs, and Brett Green (2017). "Liquidity sentiments". *Working paper.*

Capponi, A. and R. Jia (2021). *Decentralized Stablecoins and Collateral Risk.* URL: `arXiv:2103.08842`.

Chiu, J., C. Kahn, and T. Koeppl (2022). *Grasping De(centralized) Fi(nance) through the Lens of Economic Theory*. URL: https://ssrn.com/abstract=4221027.

d'Avernas, A., T. Bourany, and Q. Vandeweyer (2021). *Are Stablecoins Stable?* URL: https://www.banque-france.fr/sites/default/files/media/2021/06/10/gdre_bounary.pdf.

Fostel, Ana and John Geanakoplos (2012). "Tranching, CDS, and asset prices: how financial innovation can cause bubbles and crashes". *American Economic Journal: Macroeconomics* 4.1, pp. 190–225. DOI: 10.1257/mac.4.1.190.

Geanakoplos, John (1997). "Promises, promises". *The economy as an evolving complex system II* 1997, pp. 285–320.

— (2003). "Liquidity, default, and crashes endogenous contracts in general". In: *Advances in economics and econometrics: theory and applications: eighth World Congress*. Vol. 170.

Geanakoplos, John and William Zame (2002). *Collateral and the enforcement of intertemporal contracts*. Yale University working paper.

Gudgeon, Lewis et al. (2020). "DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency". In: *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. AFT '20. New York, NY, USA: Association for Computing Machinery, 92?112. ISBN: 9781450381390. DOI: 10.1145/3419614.3423254. URL: https://doi.org/10.1145/3419614.3423254.

Harvey, C.R. et al. (2021). *DeFi and the Future of Finance*. Wiley. ISBN: 9781119836018. URL: https://books.google.co.uk/books?id=CGM4EAAAQBAJ.

Kozhan, R. and G.F. Viswanath-Natraj (2021). *Decentralized Stablecoins and Collateral Risk*. WBS Finance Group Research Paper.

Lagos, Ricardo and Randall Wright (2005). "A unified framework for monetary theory and policy analysis". *Journal of Political Economy* 113.3, pp. 463–484.

Lehar, Alfred and Christine A. Parlour (2021). *Decentralized exchanges*. University of Calgary and University of California, Berkeley.

— (2022). *Systemic Fragility in Decentralized Markets*. University of Calgary and University of California, Berkeley.

Li, Ye and Simon Mayer (2021). *Money creation in decentralized finance: A dynamic model of stablecoin and crypto shadow banking*. CESifo Working Paper No. 9260.

Ozdenoren, Emre, Kathy Yuan, and Shengxing Zhang (2021). *Dynamic Asset-Backed Security Design*. London School of Economics.

Park, Andrea (2021). *The Conceptual Flaws of Constant Product Automated Market Making*. University of Toronto.

Perez, Daniel et al. (2021). "Liquidations: DeFi on a Knife-Edge". In: *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1?5, 2021, Revised Selected Papers, Part II*. Berlin, Heidelberg: Springer-Verlag, 457?476. ISBN: 978-3-662-64330-3. DOI: 10.1007/978-3-662-64331-0_24. URL: https://doi.org/10.1007/978-3-662-64331-0_24.

Qin, Kaihua et al. (2020). *Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit*. DOI: 10.48550/ARXIV.2003.03810. URL: https://arxiv.org/abs/2003.03810.

Qin, Kaihua et al. (2021). "An empirical study of DeFi liquidations". In: *Proceedings of the 21st ACM Internet Measurement Conference*. ACM. DOI: 10.1145/3487552.3487811. URL: https://doi.org/10.1145%2F3487552.3487811.

Schar, Fabian (2021). "Decentralized finance: On blockchain-and smart contract-based financial markets.n". *FRB of St. Louis Review*.

A Appendix

A.1 Proof of Proposition 1

Condition (2) implies that, in a pooling equilibrium, the high-type borrower is willing to borrow if and only if

$$zq^P \geq \mathbb{E}\min\{D, \delta + \phi\},$$

which is equivalent to

$$\mathbb{E}y_L(s_L, \phi)/\mathbb{E}y_H(\phi) \geq \zeta.$$

If $\mathbb{E}y_L(s_L, \phi)/\mathbb{E}y_H(\phi) > \zeta$ then it is optimal for the intermediary to set $R = R^P$. To see this, note that at this rate lenders provide loan q^P and, by assumption, the high type borrower indeed chooses to borrow. This is clearly optimal because setting a higher rate lowers total lending and at a lower rate lenders do not break even. If $\mathbb{E}y_L(s_L, \phi)/\mathbb{E}y_H(\phi) < \zeta$ then the intermediary's problem is solved by setting $R = R^S$. In this case, if the intermediary lowers the rate sufficiently below R^P then the high type would borrow. However, at that rate lenders would make negative profit.

Since $\mathbb{E}y_L(s_L, \phi)/\mathbb{E}y_H(\phi) = \mathbb{E}\min\{1, \frac{s_L\phi}{(\delta+\phi)(1-h)}\}$, a higher ϕ or h make the condition for the pooling outcome easier to satisfy.

A.2 Proof of Proposition 2

First, we define functions

$$\hat{q}^S(\phi) = \frac{1}{1+f}\mathbb{E}\left[\min\{(1-h)(\phi+\delta), s_L\phi\}\right],$$
$$\hat{q}^P(\phi) = \frac{1}{1+f}\mathbb{E}\left[\lambda\min\{(1-h)(\phi+\delta), s_L\phi\} + (1-\lambda)(1-h)(\phi+\delta)\right].$$

Note that their difference is

$$\begin{aligned}&\hat{q}^P(\phi) - \hat{q}^S(\phi)\\ =&\frac{1-\lambda}{1+f}[(1-\lambda)(1-h)(\phi+\delta) - \mathbb{E}\min\{(1-\lambda)(1-h)(\phi+\delta), s_L\phi\}]\\ \geq&0,\end{aligned}$$

and $0 < \hat{q}^{S\prime}(\phi) < \hat{q}^{P\prime}(\phi) < 1$. Similarly, we define functions

$$\hat{\phi}^P(\phi) = \beta\left[(z-1-f)\hat{q}^P(\phi)\right] + \beta(1-\lambda)\delta + \beta(\lambda\mathbb{E}(s_L) + (1-\lambda))\phi,$$

$$\hat{\phi}^S(\phi) = \beta\lambda(z-1-f)\hat{q}^S(\phi) + \beta(1-\lambda)\delta + \beta(\lambda\mathbb{E}(s_L) + (1-\lambda))\phi,$$

which have the following properties:

$$\begin{aligned}&\hat{\phi}^P(0) = \beta(1-\lambda)\delta + \beta\frac{(z-1-f)(1-\lambda)(1-h)\delta}{1+f} > \beta(1-\lambda)\delta = \hat{\phi}^S(0),\\ &\hat{\phi}^{P\prime}(\phi) > \hat{\phi}^{S\prime}(\phi) > 0,\\ &\hat{\phi}^{P\prime}(\phi) = \beta\left[(z-1-f)\hat{q}^{P\prime}(\phi)\right] + \beta(\lambda\mathbb{E}(s_L) + (1-\lambda)) < 1,\\ &\hat{\phi}^{S\prime}(\phi) = \beta\lambda(z-1-f)\hat{q}^{S\prime}(\phi) + \beta(\lambda\mathbb{E}(s_L) + (1-\lambda)) < 1,\end{aligned}$$

and the difference between the two functions is

$$\begin{aligned}&\hat{\phi}^P(\phi) - \hat{\phi}^S(\phi)\\ =&\beta(1-\lambda)(z-1-f)\hat{q}^P(\phi) + \beta\lambda(z-1-f)(\hat{q}^P(\phi) - \hat{q}^S(\phi)) > 0.\end{aligned}$$

The above properties imply that both functions have a unique fixed point and that $\phi^P > \phi^S$.

A.3 Proof of Proposition 3

Separating equilibrium

Consider first a separating equilibrium where a borrower chooses $a_L = 1$ and $a_H = 0$:

Debt limit:

$$D^S = \left(\delta + \phi^S\right)(1 - h)$$

Loan size:

$$\ell_L = q^S = \mathbb{E}\left[\min\{D^S, s\phi^S\}\right]$$

Asset price:

$$\phi^S = \beta\left(\lambda\left[zq^S - \mathbb{E}\min\{D^S, s\phi^S\}\right] + (1-\lambda)\delta + (\lambda\mathbb{E}(s) + (1-\lambda))\phi^S\right)$$

Existence of separating equilibrium:

$$\frac{E_L y}{E_H y} = \frac{\mathbb{E}\min\{D^S, s\phi^S\}}{(\delta + \phi^S)(1-h)} < \zeta$$

We now look at the limiting case as $h \to 0$:

Debt limit:

$$D^S = \left(\delta + \phi^S\right)$$

Loan size:

$$q^S = \mathbb{E}(s)\phi^S$$

Asset price:

$$\phi^S = \frac{\beta(1-\lambda)\delta}{1 - \beta[\lambda z\mathbb{E}(s) + (1-\lambda)]}$$

Existence of separating equilibrium:

$$\frac{E_L y}{E_H y} = \frac{\mathbb{E}\min\{D^S, s\phi^S\}}{(\delta + \phi^S)(1-h)} = \frac{\mathbb{E}(s)\phi^S}{(\delta + \phi^S)} < \zeta$$

Hence, a separating equilibrium exists when

$$\mathbb{E}(s) < \frac{\zeta}{\beta[(1-\lambda) + \zeta\lambda z]} \equiv \kappa_S.$$

Pooling equilibrium

We now consider a pooling equilibrium where $a_L = 1$ and $a_H = 1$:

Debt limit:

$$D^P = \left(\delta + \phi^P\right)(1 - h)$$

Loan size:

$$\ell_L = \ell_H = q^P = \lambda \mathbb{E}\left[\min\{D^P, s\phi^P\}\right] + (1-\lambda)D^P$$

Asset price:

$$\phi^P = \beta\left[zq^P - \lambda\mathbb{E}\min\{D^P, s\phi^P\} - (1-\lambda)D^P\right]$$
$$+ \beta(1-\lambda)\delta + \beta(\lambda\mathbb{E}(s) + (1-\lambda))\phi^P$$

Existence of pooling equilibrium:

$$\frac{E_L y}{E_H y} = \frac{\mathbb{E}\min\{D^P, s\phi^P\}}{(\delta + \phi^P)\,(1-h)} > \zeta$$

As $h \to 0$, we have

Debt limit:

$$D^P = \left(\delta + \phi^P\right)$$

Loan size:

$$\ell_L = \ell_H = q^P = \lambda\mathbb{E}(s)\phi^P + (1-\lambda)(\delta + \phi^P)$$

Asset price:

$$\phi^P = \frac{\beta z(1-\lambda)\delta}{1 - \beta z[\lambda\mathbb{E}(s) + (1-\lambda)]}$$

Existence of pooling equilibrium:

$$\frac{E_L y}{E_H y} = \frac{\mathbb{E}\min\{D^S, s\phi^S\}}{(\delta + \phi^S)\,(1-h)} = \frac{\mathbb{E}(s)\phi^P}{(\delta + \phi^P)} > \zeta$$

Hence a pooling equilibrium exists when

$$\mathbb{E}(s) > \frac{\zeta}{\beta z[(1-\lambda) + \zeta\lambda]} \equiv \kappa_P < \kappa_S$$

Therefore, when $\mathbb{E}(s) \in (\kappa_P, \kappa_S)$, there are multiple equilibria in the neighborhood of $h = 0$.

A.4 Two-point Distribution Example

A.4.1 Separating Equilibrium

Suppose $s_L = 1$ w.p. π, and $s_L = 0$ w.p. $1-\pi$.

In a separating equilibrium:

Debt limit:

$$D^S = \left(\delta + \phi^S\right)(1-h)$$

Loan size:

$$\ell_L = q^S = \mathbb{E}\left[\min\{D^S, s\phi^S\}\right] = \pi \min\{D^S, \phi^S\}$$

There are two cases.

Case (i) $D^S > \phi^S$

This is true when

$$\delta\frac{1-h}{h} > \phi^S.$$

We then have

$$q^S = \pi\phi^S,$$
$$\phi^S = \frac{\beta(1-\lambda)\delta}{1-\beta[\lambda z\pi + (1-\lambda)]}.$$

The existence of separating equilibrium requires

$$\zeta^S(h) = \frac{\pi\phi^S}{(\delta+\phi^S)(1-h)} < \zeta.$$

We define a threshold

$$\underline{h}^S \equiv \frac{\delta}{\phi^S+\delta} = \frac{1-\beta[\lambda z\pi + (1-\lambda)]}{1-\beta\lambda z\pi}.$$

When the haircut is lower than the threshold $\underline{h}$, the low type borrowers default even when $s_L = 1$. In this case, the loan size is equal to the expected value of the asset, $\pi\phi^S$, which does not depend on the haircut. Hence, the asset price is also independent of h. An increase in h, however, makes it harder to support a separating equilibrium as the contract becomes less information sensitive.

Case (ii) $D^S < \phi^S$

This is true when

$$\delta\frac{1-h}{h} < \phi^S.$$

We then have

$$q^S = \pi(\delta + \phi^S)(1-h)$$
$$\phi^S = \frac{\beta(\lambda(z-1)\pi(1-h) + (1-\lambda))\delta}{1-\beta[\lambda(z-1)\pi(1-h) + (1-\lambda) + \lambda\pi]}.$$

The existence of separating equilibrium requires

$$\zeta^S(h) = \pi < \zeta.$$

When the haircut is higher than the threshold $\underline{h}$, the low type pays back the loan to retain the collateral when $s_L = 1$. In this case, the loan size is equal to the πD. Hence, the asset price is decreasing in h. A separating equilibrium exists whenever $\pi < \zeta$ as h does not affect the information sensitivity of the contract.

A.4.2 Pooling Equilibrium

In a pooling equilibrium:

Debt limit:

$$D^P = \left(\delta + \phi^P\right)(1-h)$$

Loan size:

$$q^P = \lambda \mathbb{E}\left[\min\{D^P, s\phi^P\}\right] + (1-\lambda)D^P = \lambda\pi\min\{D^P, \phi^P\} + (1-\lambda)D^P$$

There are two cases.

Case (i) $D^P > \phi^P$

This is true when

$$\delta\frac{1-h}{h} > \phi^P.$$

We then have

$$q^P = \lambda\pi\phi^P + (1-\lambda)D^P$$
$$\phi^P = \frac{\beta(1-\lambda)\delta[(z-1)(1-h)+1]}{1-\beta[\lambda(z-1)\pi + (z-1)(1-\lambda)(1-h) + \lambda\pi + 1 - \lambda]}$$

The existence of separating equilibrium requires

$$\zeta^P(h) = \frac{\pi\phi^P}{\left(\delta + \phi^P\right)(1-h)} > \zeta.$$

We can again define a threshold

$$\underline{h}^P \equiv \frac{1-\beta[\lambda(z-1)\pi+(z-1)(1-\lambda)+\lambda\pi+1-\lambda]}{1-z\beta\lambda\pi-\beta(z-1)(1-\lambda)} < \underline{h}^S$$

such that this case holds when $h < \underline{h}^P$.

Case (ii) $D^P < \phi^P$

This is true when

$$\delta\frac{1-h}{h} < \phi^P.$$

We then have

$$\begin{aligned} q^P &= \lambda\pi D^P + (1-\lambda)D^P \\ \phi^P &= \beta\delta\frac{(z-1)(\lambda\pi+1-\lambda)(1-h)+(1-\lambda)}{1-\beta[(z-1)(\lambda\pi+1-\lambda)(1-h)+\lambda\pi+1-\lambda]} \end{aligned}$$

The existence of pooling equilibrium requires

$$\zeta^P(h) = \pi > \zeta.$$

A.5 Proof of Uniqueness Under a Flexible Smart Contract

Denote the debt contract $y(D,\widetilde{\delta}+\widetilde{s}\phi) = \min(D,\widetilde{\delta}+\widetilde{s}\phi)$. We prove the result for the main model where

$$\mathbb{E}_H y(D,\widetilde{\delta}+\widetilde{s}\phi) = y(D,\delta+\phi);$$

and

$$\mathbb{E}_L y(D,\widetilde{\delta}+\widetilde{s}\phi) = \int_{\underline{s}}^{\bar{s}} y(D,s\phi)dF(s).$$

The arguments, however, generalize to the more general case with some modifications.

Denote $D^* \leq \delta+\phi$ the maximum face value so that the incentive constraint of the high type borrower is satisfied

$$\widehat{z}\left[\lambda\mathbb{E}_L y(D,\widetilde{\delta}+\widetilde{s}\phi)+(1-\lambda)\mathbb{E}_H y(D,\widetilde{\delta}+\widetilde{s}\phi)\right] \geq \mathbb{E}_H y(D,\widetilde{\delta}+\widetilde{s}\phi)$$

in which case there is a pooling equilibrium.

In the baseline model, the intermediary takes haircut as given and maximizes revenue from trading securities. Maximizing revenue is the same as maximizing trade volume of the deposit contract because the fee per volume is taken as given.

When the intermediary designs the smart deposit contract flexbly, the intermediary still aims to maximize the expected trading volume. Specifically, the intermediary chooses D, or equivalently haircut, to maximize expected trade volume $[\lambda \mathbb{E}_L + a_{H,t}(1-\lambda)\mathbb{E}_H]\min(D, \widetilde{\delta} + \widetilde{s}\phi)$ taking ϕ as given. Note that the intermediary's payoff is increasing in D as long as the equilibrium does not switch from pooling to separating. Hence, if the intermediary chooses a contract that leads to a pooling outcome, then $D = D^*$, and if the intermediary chooses a contract that leads to a separating outcome, then $D = \delta + \phi$.

Next we look at the two cases:

Pooling case:

If $D^* < \phi$, we can denote $s^* = D^*/\phi$. In this case, all terms in the incentive constraint for the high type are proportional to the asset price ϕ, which drops out of the constraint. So, the high type's incentive constraint is satisfied iff

$$\widehat{z}\,[\lambda \mathbb{E}_L \min(s^*, s) + (1-\lambda)s^*] \geq s^*$$

Let $\mathcal{F}(\hat{s}) \equiv \widehat{z}\,[\lambda \mathbb{E}_L \min(\hat{s}, s) + (1-\lambda)\hat{s}] - \hat{s}$ and note the high type's incentive constraint is satisfied iff $\mathcal{F}(\hat{s}) \geq 0$. $\mathcal{F}(\hat{s})$ has the following properties:

$$\mathcal{F}(0) \geq 0$$
$$\mathcal{F}'(0) = \widehat{z} - 1 > 0$$
$$\mathcal{F}''(\hat{s}) = -\widehat{z}\lambda f(\hat{s}) < 0$$

So $\mathcal{F}(\hat{s})$ is concave and strictly positive when $\hat{s}$ is close to 0. Suppose the information friction is severe enough so that $\mathcal{F}(1) = \widehat{z}(\lambda \mathbb{E}_L s + (1-\lambda)) - 1 < 0$, or equivalently $\mathbb{E}_L s < \frac{1-(1-\lambda)\widehat{z}}{\lambda \widehat{z}} = 1 + \frac{1}{\lambda \widehat{z}} - \frac{1}{\lambda} < 1$. In this case, there exists a unique threshold $0 < s^* < 1$ such that $\mathcal{F}(s^*) = 0$. Since the asset price ϕ drops out, threshold s^* does not depend on ϕ.

Taking next period asset price ϕ as given, the asset price in the current period under pooling equilibrium is

$$\phi^P(\phi) = \beta\left[(\widehat{z}-1)\left(\lambda \mathbb{E}_L \min(s^*, s) + (1-\lambda)\, s^*\right)\phi + \lambda \phi \mathbb{E}_L s + (1-\lambda)(\delta + \phi)\right] \tag{A.1}$$

which has the following property

$$\frac{\partial \phi^P(\phi)}{\partial \phi} = \beta\left[(\widehat{z}-1)\left(\lambda \mathbb{E}_L \min(s^*, s) + (1-\lambda)\, s^*\right) + \lambda \mathbb{E}_L s + (1-\lambda)\right] < 1$$
$$\phi^P(0) = \beta(1-\lambda)\delta.$$

So, $\phi^P(\phi)$ is a straight line with slope $\frac{\partial \phi^P(\phi)}{\partial \phi}$ and intercept $\phi^P(0) = \beta(1-\lambda)\delta$. Hence there is a unique steady state price satisfying $\phi^P(\phi) = \phi$.

Suppose information friction is not so severe so that $\mathcal{F}(1) > 0$, or equivalently, $1 > \mathbb{E}_L s > 1 + \frac{1}{\lambda \widehat{z}} - \frac{1}{\lambda}$. In this case, the face value of the debt is $D^* \geq \phi$. Let $d^*(\phi) = D^* - \phi$. There are two possibilities: either high type's incentive constraint is binding and there is $d^*(\phi) \leq \delta$ that satisfies:

$$\widehat{z}\left[\lambda \phi \mathbb{E}_L s + (1-\lambda)(d^*(\phi) + \phi)\right] = d^*(\phi) + \phi$$

or the high-type's incentive constraint is slack for all D. In the former case

$$d^*(\phi) = \frac{\widehat{z}\left[\lambda \mathbb{E}_L s + (1-\lambda)\right] - 1}{1 - \widehat{z}(1-\lambda)} \phi.$$

In the latter case $d^*(\phi) = \delta$. If $\frac{\widehat{z}[\lambda \mathbb{E}_L s + (1-\lambda)] - 1}{1 - \widehat{z}(1-\lambda)} \phi < \delta$,

$$\phi^P(\phi) = \beta \left[\frac{\lambda \widehat{z}}{1 - \widehat{z}(1-\lambda)} \lambda \mathbb{E}_L s \phi + (1-\lambda)(\delta + \phi) \right] \tag{A.2}$$

$$\phi^P(0) = \beta(1-\lambda)\delta$$

$$\frac{\partial \phi^P(\phi)}{\partial \phi} = \beta \left(\frac{\lambda \widehat{z}}{1 - \widehat{z}(1-\lambda)} \lambda \mathbb{E}_L s + 1 - \lambda \right)$$

$\phi^P(\phi)$ is a straight line with slope $\frac{\partial \phi^P(\phi)}{\partial \phi}$ and intercept $\phi^P(0)$.

If $\frac{\widehat{z}[\lambda \mathbb{E}_L s + (1-\lambda)]}{1 - \widehat{z}(1-\lambda)} \phi > \delta$,

$$\begin{aligned}\phi^P(\phi) &= \beta \widehat{z}\left[\lambda \mathbb{E}_L s \phi + (1-\lambda)(\delta + \phi)\right] \\ &= \beta \widehat{z}\left[(1-\lambda)\delta + (\lambda \mathbb{E}_L s + 1 - \lambda)\phi\right]\end{aligned}$$

$$\phi^P(0) = \beta \widehat{z}(1-\lambda)\delta$$

$$\frac{\partial \phi^P(\phi)}{\partial \phi} = \beta \widehat{z}(\lambda \mathbb{E}_L s + 1 - \lambda) < 1$$

By comparing the slopes of $\phi^P(\phi)$ when $\frac{\widehat{z}[\lambda \mathbb{E}_L s + (1-\lambda)]}{1 - \widehat{z}(1-\lambda)} \phi$ is below and above δ, we can see that $\phi^P(\phi)$ is concave with slope less than 1 when $\frac{\widehat{z}[\lambda \mathbb{E}_L s + (1-\lambda)]}{1 - \widehat{z}(1-\lambda)} \phi > \delta$.

Note that when $D^* \geq \phi$ in a pooling equilibrium or $\mathbb{E}_L s > 1 + \frac{1}{\lambda \widehat{z}} - \frac{1}{\lambda}$, the value of a pooling contract is always greater than that of a separating contract. This is because the intermediary designs the contract optimally to maximize the expected trade volume. The expected value of a loan to a low type is the same in a separating equilibrium and a pooling equilibrium when $D^* \geq \phi$. So the intermediary strictly prefers designing a pooling contract as the revenue from the pooling contract strictly dominates that of a separating contract.

Hence when $\mathbb{E}_L s > 1 + \frac{1}{\lambda \widehat{z}} - \frac{1}{\lambda}$, we can focus on the pooling equilibrium. From the analysis above, $\phi^P(\phi)$ is concave with slope less than 1 when $\frac{\widehat{z}[\lambda \mathbb{E}_L s + (1-\lambda)]}{1 - \widehat{z}(1-\lambda)} \phi > \delta$. Hence, in this part of the parameter space there exists a unique equilibrium where the loan is traded in a pooling equilibrium.

Separating case:

As argued above, when analyzing the optimal contract in a separating equilibrium, we can focus on the parameter space where

$$E_L s < 1 + \frac{1}{\lambda \widehat{z}} - \frac{1}{\lambda}. \tag{A.3}$$

If the optimal contract supports a separating equilibrium, the intermediary would set $D = \delta + \phi$ to maximize the loan size to the low type. In the special parametrization of the model, any face value between ϕ and $\delta + \phi$ generates the same revenue from borrowing because a low quality asset does not pay any dividend. More generally, low quality assets could pay positive dividend. So the maximum face value $D = \delta + \phi$ is a more robust form of debt design in the separating case.

Given the face value $D = \delta + \phi$, the incentive constraint for the high type not to borrow is

$$\delta + \phi \geq \widehat{z}\mathbb{E}_L s\phi \tag{A.4}$$

Note that condition (A.3) implies that

$$\widehat{z}\mathbb{E}_L s < 1 + (\widehat{z} - 1)\,(1 - \frac{1}{\lambda}) < 1.$$

The condition for the existence of a separating equilibrium,(A.4), always holds.

In a separating equilibrium, the asset price is

$$\phi^S(\phi) = \beta\left[(\widehat{z} - 1)\lambda\mathbb{E}_L s\phi + \lambda\mathbb{E}_L s\phi + (1 - \lambda)(\delta + \phi)\right] \tag{A.5}$$

which has the following property

$$\phi^S(0) = \beta(1 - \lambda)\delta$$
$$\frac{\partial\phi^S(\phi)}{\partial\phi} = \beta\left(\widehat{z}\lambda\mathbb{E}_L s + 1 - \lambda\right)$$

So in this case, $\phi^S(\phi)$ is a straight line with slope $\frac{\partial\phi^S(\phi)}{\partial\phi}$ and intercept $\phi^S(0) = \beta(1 - \lambda)\delta$.

Then, when the intermediary designs the contract optimally to maximize the expected trade volume, the asset price taking the next-period price ϕ as given is

$$\phi'(\phi) = \max\{\phi^P(\phi), \phi^S(\phi)\}$$

where $\phi^P(\phi)$ satisfies (A.1) and $\phi^S(\phi)$ satisfies (A.5). Notice that $\phi^S(\phi)$ and $\phi^P(\phi)$ are two straight lines that have a common positive intercept $\phi^S(0) = \phi^P(0) = \beta(1 - \lambda)\delta$. So the intermediary chooses the pooling contract if and only if

$$\phi\left(1 - \beta\left[(\widehat{z} - 1)\left(\lambda\mathbb{E}_L \min(s^*, s) + (1 - \lambda)\, s^*\right) + \lambda\mathbb{E}_L s + (1 - \lambda)\right]\right) = \beta\,(1 - \lambda)\,\delta$$

$$\phi\left(1-\beta\left[(\widehat{z}-1)\lambda\mathbb{E}_L s+\lambda\mathbb{E}_L s+(1-\lambda)\right]\right)=\beta\left(1-\lambda\right)\delta$$

$$\lambda\mathbb{E}_L y(D,\widetilde{\delta}+\widetilde{s}\phi^S)$$

$$\left[\lambda\mathbb{E}_L+(1-\lambda)\,\mathbb{E}_H\right]y(D,\widetilde{\delta}+\widetilde{s}\phi^P)$$

$$\lambda\int_{\underline{s}}^{\bar{s}}\min(D,s\phi^S)dF\left(s\right)$$

$$\left[\lambda\mathbb{E}_L\min(s^*,s)+(1-\lambda)\,s^*\right]\phi^P\geq\phi^S\lambda\mathbb{E}_L s$$

$$\frac{\left[\lambda\mathbb{E}_L\min(s^*,s)+(1-\lambda)\,s^*\right]}{1-\beta\left[(\widehat{z}-1)\left(\lambda\mathbb{E}_L\min(s^*,s)+(1-\lambda)\,s^*\right)+\lambda\mathbb{E}_L s+(1-\lambda)\right]}\geq\frac{\lambda\mathbb{E}_L s}{1-\beta\left[(\widehat{z}-1)\lambda\mathbb{E}_L s+\lambda\mathbb{E}_L s+(1-\lambda)\right]}$$

$$\frac{x}{1-\beta(\widehat{z}-1)x-\beta y}$$

$$1-\beta\left(\lambda\mathbb{E}_L s+(1-\lambda)\right)>0$$

the slope of $\phi^P(\phi)$ exceeds that of $\phi^S(\phi)$, or

$$\lambda\mathbb{E}_L\min(s^*,s)+(1-\lambda)\,s^*-\lambda\mathbb{E}_L s>0. \tag{A.6}$$

In either case, the equilibrium is unique.

To summarize the equilibrium characterization, when $\mathbb{E}_L s<1+\frac{1}{\lambda\widehat{z}}-\frac{1}{\lambda}$, the equilibrium contract is a pooling one with face value $D=s^*\phi<\phi$ with s^* being the unique solution to

$$\widehat{z}\left[\lambda\mathbb{E}_L\min(s^*,s)+(1-\lambda)s^*\right]=s^*$$

when condition (A.6) holds. Otherwise, the equilibrium contract is a separating one with face value $D=\delta+\phi$.

When $\mathbb{E}_L s>1+\frac{1}{\lambda\widehat{z}}-\frac{1}{\lambda}$, the equilibrium contract is a pooling one with face value $D=d^*+\phi$ where

$$d^*=\min\left\{\delta,\frac{\widehat{z}\left[\lambda E_L s+(1-\lambda)\right]-1}{1-\widehat{z}(1-\lambda)}\phi\right\}.$$

A.6 Optimal Flexible Debt Limit (Two-point Distribution Example)

Suppose the intermediary can set D_t as a function of ϕ_t to maximize

$$f[\lambda\ell_{Lt}+(1-\lambda)\ell_{Ht}]$$

Separating equilibrium

In a separating equilibrium, $\ell_{Ht}=0$ and

$$\ell_{Lt}=\pi\min\{D^S,\phi_t\}$$

So the optimal debt limit is

$$D^S = \phi_t.$$

Given this debt policy, the loan size is $q_t = \pi\phi_t$ and the asset price in the previous period is given by

$$\begin{aligned}\phi^S_{t-1} &= \beta\left(\lambda(z-1)\pi\phi_t + (1-\lambda)\delta + (\lambda\pi + (1-\lambda))\phi_t\right)\\ &= \beta[\lambda(z-1)\pi + (\lambda\pi + (1-\lambda))]\phi_t + \beta(1-\lambda)\delta\end{aligned}$$

The function $\phi^S_{t-1}(\phi_t)$ is linear with an intercept $\phi^S_{t-1}(0) = \beta(1-\lambda)$ and slope

$$\phi^{S\prime}_{t-1}(\phi_t) = \beta[\lambda(z-1)\pi + (\lambda\pi + (1-\lambda))] < 1$$

implying a unique fixed point

$$\phi^S = \frac{\beta(1-\lambda)\delta}{1-\beta[\lambda(z-1)\pi + (\lambda\pi + (1-\lambda))]}.$$

Pooling equilibrium

In a pooling equilibrium,

$$\ell_L = \ell_H = q^P = \lambda\mathbb{E}\left[\min\{D^P, s\phi_t\}\right] + (1-\lambda)D^P$$

the optimal debt limit is the maximum value that satisfies

$$\frac{\mathbb{E}\min\{D^P, s\phi_t\}}{\min\{D^P, \delta+\phi_t\}} = \frac{\pi\min\{D^P, \phi_t\}}{\min\{D^P, \delta+\phi_t\}} > \zeta$$

For $D^P < \delta + \phi_t$:

The solution solves

$$\pi\min\{1, \frac{\phi_t}{D^P}\} = \zeta.$$

Note that there is a solution exists only when $\pi \geq \zeta$. When $\pi \geq \zeta$, the optimal debt limit is given by

$$D^P = \frac{\pi\phi_t}{\zeta}.$$

The condition $D^P < \delta + \phi_t$ is violated when

$$D^P = \frac{\pi\phi_t}{\zeta} \geq \delta + \phi_t.$$

This happens when

$$\phi_t \geq \frac{\zeta\delta}{\pi-\zeta}.$$

In that case, the optimal debt limit is $D^P = \delta + \phi_t$.

Overall, the optimal debt limit to support a pooling outcome is

$$D^P = \min\left\{\frac{\pi\phi_t}{\zeta}, \delta + \phi_t\right\}.$$

Given this debt policy, the loan size is

$$q_t = \lambda\pi\phi_t + (1-\lambda)\min\left\{\frac{\pi\phi_t}{\zeta}, \delta + \phi_t\right\},$$

and the asset price in the previous period is given by

$$\phi_{t-1}^P = \beta(z-1)\lambda\pi\phi_t + \beta(z-1)(1-\lambda)\min\left\{\frac{\pi\phi_t}{\zeta}, \delta + \phi_t\right\}$$
$$+ \beta(1-\lambda)\delta + \beta(\lambda\pi + (1-\lambda))\phi_t$$

The function $\phi_{t-1}^P(\phi_t)$ is linear with an intercept $\phi_{t-1}^P(0) = \beta(1-\lambda)$ and slope

$$\phi_{t-1}^{P\prime}(\phi_t) = \begin{cases} \phi_{t-1}^{S\prime}(\phi_t) + \beta(z-1)(1-\lambda)\frac{\pi}{\zeta} & , \text{ for } \phi_t < \frac{\zeta\delta}{\pi-\zeta} \\ \phi_{t-1}^{S\prime}(\phi_t) + \beta(z-1)(1-\lambda) < 1 & , \text{ for } \phi_t \geq \frac{\zeta\delta}{\pi-\zeta} \end{cases}$$

implying a unique fixed point.

Optimal debt limit

When $\pi < \zeta$, the pooling equilibrium is not feasible. The optimal debt limit is

$$D_t^S = \phi_t.$$

When $\pi \geq \zeta$, the pooling equilibrium is feasible and dominates the separating equilibrium. The optimal debt limit is

$$D_t^P = \min\left\{\frac{\pi\phi_t}{\zeta}, \delta + \phi_t\right\}.$$

A.7 Private Information Parameter $\chi < 1$

We have considered the case where there is private information in each period. We now introduce a parameter, χ, to control the degree of information imperfection. With probability $1-\chi$, there is no private information in the sense that there are no low-quality assets (denoted by state 0). All the equilibrium conditions remain the same except that the asset prices satisfy

$$\phi_t = \beta\chi\left\{\lambda\left[\int_{\underline{s}}^{\bar{s}}(z\ell_{L,t+1} - \min\{\ell_{L,t+1}R_{t+1}, a_{L,t+1}s_L\phi_{t+1})\} + s_L\phi_{t+1})\,dF(s_L)\right]\right.$$
$$\left. + \chi(1-\lambda)\left[z\ell_{H,t+1} - \min\{\ell_{H,t+1}R_{t+1}, a_{H,t+1}(\delta + \phi_{t+1})\} + \delta + \phi_{t+1}\right]\right\}$$
$$+ \beta(1-\chi)\left[z\ell_{t+1}^0 - \min\{\ell_{t+1}^0 R_{t+1}^0, a_{t+1}^0(\delta + \phi_{t+1})\} + \delta + \phi_{t+1}\right].$$

where $a^0 = 1$, $\ell_t^0 = q_t^0 = \frac{1}{1+f}(\delta + \phi_t)(1-h)$ and $R_t^0 = (\delta + \phi_t)(1-h)/q_t^0$. By continuity, all results hold when χ is sufficiently close to 1.

A.8 An Alternative Setup with Unobservable Private Valuation

We briefly consider an alternative setup where the private information is related to borrowers' private valuation of the asset, instead of the asset's common value. We show that the main results hold.

Suppose with probability $1-\varepsilon$, the state is good ($s = 1$) and the asset pays dividend δ. With probability ε, the state is bad ($s = 0$), it does not pay any dividends. In addition, the borrower has unobservable private valuation. A type $i = H, L$ borrower, if holding an asset, receives a private value $v_i(s)$ before the asset market opens and after the loan is settled. The type i is determined before the loan is made and the information is private. With probability λ, the borrower is of type $i = L$, and the private valuation is $v_L(1) = v$ in the good state and $v_L(0) = 0$ in the bad state. With probability $1-\lambda$, the borrower's type is $i = H$ and the private valuation is $v_H(1) = v_H(0) = v$. After observing the private information, the borrower borrows from the platform. After observing the realization of δ, the borrower decides whether to repay or to default. After the loan is settled, the borrower, if holding the asset, receives the private valuation. At the end of the period, the asset is traded at $\delta+\phi$ in the good state and at ϕ in the bad state.

The debt limit is given by $D = (\delta + \phi)(1-h)$. We assume that $v > \delta$. As a result, all borrowers repay in the good state. Low type borrower defaults in the bad state when $D > \phi$. Our analysis will focus on the case of $D \geq \phi$ as it is suboptimal to set $D < \phi$.

In the separating equilibrium, the loan size is

$$q^S = D^S - \varepsilon(D^S - \phi^S)$$

and the asset price is

$$\phi^S = \beta \frac{\lambda(z-1)(1-h)(1-\varepsilon)\delta + (1-\varepsilon)\delta + (1-\varepsilon\lambda)v}{1-\beta-\beta\lambda(z-1)(1-h(1-\varepsilon))}.$$

The separating equilibrium exists when

$$\frac{(1-\varepsilon)D^S + \varepsilon\phi^S}{D^S} < \zeta.$$

In the pooling equilibrium, the loan size is

$$q^P = D^P + \lambda\varepsilon(\phi^P - D^P)$$

and the asset price is

$$\phi^P = \beta\frac{(z-1)\delta(1-h)(1-\varepsilon\lambda) + \beta(1-\varepsilon)\delta + \beta(1-\varepsilon\lambda)v}{1-\beta-\beta(z-1)(1-h(1-\varepsilon\lambda))}.$$

The pooling equilibrium exists when

$$\frac{(1-\varepsilon)D^P + \varepsilon\phi^P}{D^P} > \zeta.$$

Hence we can reproduce the main multiplicity result.

Proposition 6. *For h not too large, $\phi^P > \phi^S$ and multiplicity exists when*

$$1 - \frac{\varepsilon\delta}{\delta + \phi^P} > \zeta > 1 - \frac{\varepsilon\delta}{\delta + \phi^S}.$$

B More Details about Aave Lending Protocol

According to DeFiLlama, there are 1485 DeFi protocols running on different blockchains (e.g., Ethereum, Terra, BSC, Avalanche, Fantom, Solana) as of April 2022. The TVL of these protocols are 237 billion USD with lending protocols accounting for about 20%. (Figure 8).[16] Table 1 reports some basic statistics about the three main lending protocols: Compound operating on Ethereum, Venus on the BSC and Aave on multiple chains. Operating on multiple blockchains, Aave is the largest among the three in terms of TVL, deposits and borrows, and market capitalization of its governance tokens. Below, we give a brief overview of some key features of the Aave lending protocol. More details can be found in the appendix.

B.1 Tokens

Aave issues two types of tokens: (i) aTokens, issued to lenders so they can collect interest on deposits, and (ii) AAVE tokens, which are the native token of Aave.[17] **aTokens** are interest-bearing tokens that are minted upon deposit and and burned at withdraw. The aTokens' value is pegged to the value of the corresponding deposited asset at a 1:1 ratio, and can be safely stored, transferred or traded. Withdrawals

[16] Collateralized debt position (CDP), e.g., MakerDAO, accounts for 8% of the TVL. Both lending and CDP protocols support collateralized lending. The key difference is that a lending protocol lends out assets deposited by lenders while a CDP lends out assets (e.g., stablecoins) minted by the protocol.

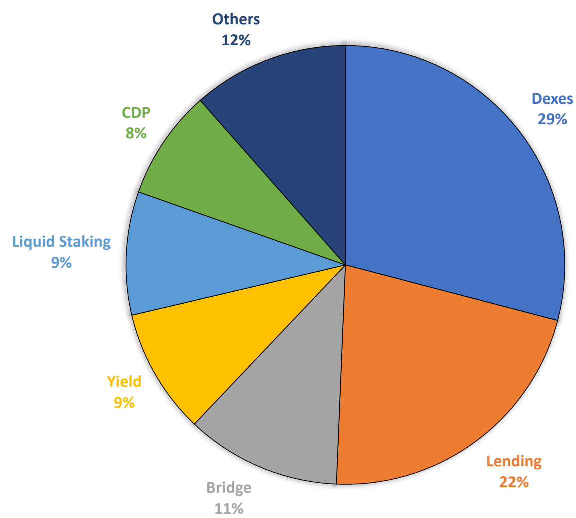
[17] One may interpret aTokens as bank deposits and AAVE tokens as bank equity shares.

Table 1: Major decentralized lending Platforms (April 17, 2022)

	Aave	**Compound**	**Venus**
Total value locked (USD)	13.35 B	6.35 B	1.51 B
Blockchain	Multi	Ethereum	BSC
Total deposits (USD)	15.37 B	9.51 B	1.51 B
Total borrows (USD)	5.93 B	3.21 B	0.82 B
Governance Token	AAVE	COMP	XVS
Market Cap (USD)	2.38 B	0.99 B	0.13 B

Data Source: DefiLlamma; Aavewatch; Compound.finance; Venus.io; Glassnode.

Figure 8: Composition of TVL of all DeFi Protocols on all Chains (April 2022)



Data Source: DefiLlamma.

of the deposited assets burns the aTokens. **AAVE tokens** are used to vote and influence the governance of the protocol. AAVE holders can also lock (known as "staking") the tokens to provide insurance to the protocol/depositors and earn staking rewards and fees from the protocol (more details below).

B.2 Deposits and loans

By depositing a certain amount of an asset into the protocol, a **depositor** mints and receives the same amount of corresponding aTokens. All interest collected by these aTokens are distributed directly to the depositor.

Borrowers can borrow these funds with collateral backing the borrow position. A borrower repays the loan in the same asset borrowed. There is no fixed time period to pay back the loan. Partial or full repayments can be made anytime. As long as the position is safe, the loan can continue for an undefined period. However, as time passes, the accrued interest of an unrepaid loan will grow, which might result in the deposited assets becoming more likely to be liquidated.

Every borrowing position can be opened with a stable or variable rate. The **loan rate** follows the model:

$$Rate = \begin{cases} R_0 + \frac{U}{U_{optimal}} R_{slope1} & \text{, if } U \leq U_{optimal} \\ R_0 + R_{slope1} + \frac{U - U_{optimal}}{1 - U_{optimal}} R_{slope2} & \text{, if } U > U_{optimal} \end{cases}$$

where $U = Total\ Borrows / Total\ Liquidity$ is the share of the liquidity borrowed.[18]

The **variable rate** is the rate based on the current supply and demand in Aave. **Stable rates** act as a fixed rate.[19] The current model parameters for stable and variable interest rates are given in Figure 9. Figure 10 shows Dai's rate schedule as an example.

The **deposit rate** is given by

$$\text{Deposit Rate}_t = U_t(SB_t \times S_t + VB_t \times V_t)(1 - R_t)$$

where SB_t is the share of stable borrows, S_t is average stable rate, VB_t is the share of variable borrows, V_t is average variable rate, R_t is the reserve factor (a fraction of interests allocated to mitigate shortfall events discussed below). The **Loan to Value** (LTV) ratio defines the maximum amount that can be borrowed with a specific collateral. It's expressed in percentage: at $LTV = 75\%$, for every 1 ETH worth of collateral, borrowers will be able to borrow 0.75 ETH worth of the corresponding currency of the loan. The current risk parameters are given in Figure 11.

B.3 Collateral and Liquidation

The **liquidation threshold** (LQ) is the percentage at which a loan is defined as undercollateralized. For example, a LQ of 80% means that if the value rises above 80% of the collateral, the loan is undercollateralised and could be liquidated. The LQ of a borrower's position is the weighted average of those

[18]Total "liquidity" refers to the total deposits of a loanable asset.

[19]The stable rate for new loans varies over time. However, once the stable loan is taken, borrowers will not experience interest rate volatility. There is one caveat though: if the protocol is in dire need of liquidity, then some stable rate loans might undergo a procedure called rebalancing. In particular, it will happen if the average borrow rate is lower than 25% APY and the utilization rate is over 95%.

Figure 9: Current Rate Parameters

		Variable Rate			Stable Rate Rebalance if U > 95% + Average APY < 25%		
	Uoptimal	Base	Slope 1	Slope 2	Average Market Rate	Slope 1	Slope 2
BUSD	80%	0%	4%	100%			
DAI	80%	0%	4%	75%	4%	2%	75%
sUSD	80%	0%	4%	100%			
TUSD	80%	0%	4%	75%	4%	2%	75%
USDC	90%	0%	4%	60%	4%	2%	60%
USDT	90%	0%	4%	60%	4%	2%	60%
AAVE							
BAT	45%	0%	7%	300%	3%	10%	300%
ENJ	45%	0%	7%	300%			
ETH	65%	0%	8%	100%	3%	10%	100%
KNC	65%	0%	8%	300%	3%	10%	300%
LINK	45%	0%	7%	300%	3%	10%	300%
MANA	45%	0%	8%	300%	3%	10%	300%
MKR	45%	0%	7%	300%	3%	10%	300%
REN	45%	0%	7%	300%			
SNX	80%	3%	12%	100%			
UNI	45%	0%	7%	300%			
WBTC	65%	0%	8%	100%	3%	10%	100%
YFI	45%	0%	7%	300%			
ZRX	45%	0%	7%	300%	3%	10%	300%

Table Source: Aave.com

of the collateral assets:

$$LQ = \frac{\sum_i \text{Collateral i in ETH} * LQ_i}{\text{Total Borrows in ETH}}$$

The difference between the LTV and the LQ is a safety cushion for borrowers. The values of assets are based on **price feed** provided by Chainlink's decentralized oracles. The LQ is also called the **health factor** *(Hf)*. When $Hf < 1$, a loan is considered undercollateralized and can be liquidated. When the health factor of a position is below 1, **liquidators** repay part or all of the outstanding borrowed amount on behalf of the borrower, while receiving an equivalent amount of collateral in return plus a liquidation "bonus" (see Figure 11).[20] When the liquidation is completed successfully, the health factor of the

[20]Example: Bob deposits 5 ETH and 4 ETH worth of YFI, and borrows 5 ETH worth of DAI. If Bob's Health Factor drops below 1 his loan will be eligible for liquidation. A liquidator can repay up to 50% of a single borrowed amount = 2.5 ETH worth of DAI. In return, the liquidator can claim a single collateral, as the liquidation bonus is higher for YFI (15%)

Figure 10: Stable vs Variable Rates for Dai

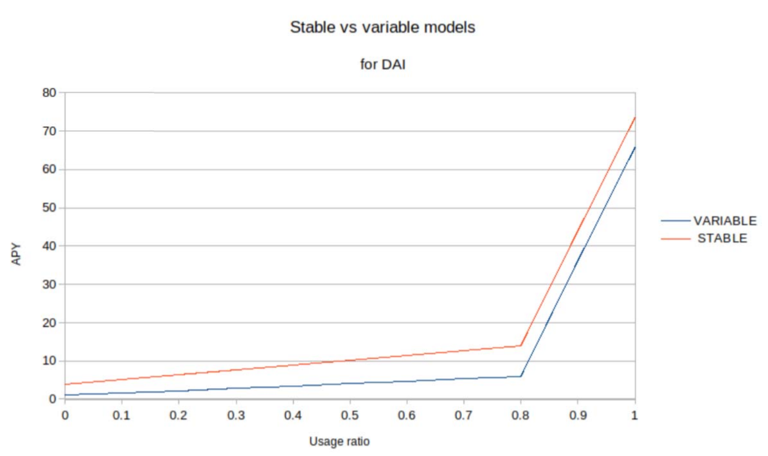


Figure Source: Aave.com

position is increased, bringing the health factor above 1.

B.4 Infrequent Updates on the Risk Parameters in Smart Contracts

Table 2: Historical AAVE V1 Risk Parameter Changes

Date	Asset	LTV	Liquidation threshold	Liquidation Bonus	Comment
10/21/20	MKR	50%	65%	10%	Decreased volatility
10/21/20	TUSD	75%	80%	5%	Following reivew of smart contract
7/22/20	LEND	50%	65%	10%	LEND cannot be borrowed due to migration incoming
7/16/20	LEND	50%	65%	10%	Improved risk parameter
7/16/20	SNX	15%	40%	10%	New Collateral
7/16/20	ENJ	55%	65%	10%	New Asset
7/16/20	REN	50%	65%	10%	New Asset
6/19/20	TUSD	1%	80%	5%	Unaudited update

than ETH (5%) the liquidator chooses to claim YFI. The liquidator claims 2.5 + 0.375 ETH worth of YFI for repaying 2.5 ETH worth of DAI.

Figure 11: Current Risk Parameters

	LTV	Liquidation Threshold	Liquidation Bonus	Overall Risks	Reserve Factor
BUSD				B	10%
DAI	75%	80%	5%	B	10%
sUSD				C+	20%
TUSD	75%	80%	5%	B	10%
USDC	80%	85%	5%	B+	10%
USDT				B+	10%
AAVE	50%	65%	10%	C+	
BAT	70%	75%	10%	B+	20%
ENJ	55%	60%	10%	B+	20%
ETH	80%	82.5%	5%	A+	10%
KNC	60%	65%	10%	B+	20%
LINK	70%	75%	10%	B+	20%
MANA	60%	65%	10%	B-	35%
MKR	60%	65%	10%	B-	20%
REN	55%	60%	10%	B	20%
SNX	15%	40%	10%	C+	35%
UNI	60%	65%	10%	B	20%
WBTC	70%	75%	10%	B-	20%
YFI	40%	55%	15%	B-	20%
ZRX	60%	65%	10%	B+	20%

Table Source: Aave.com

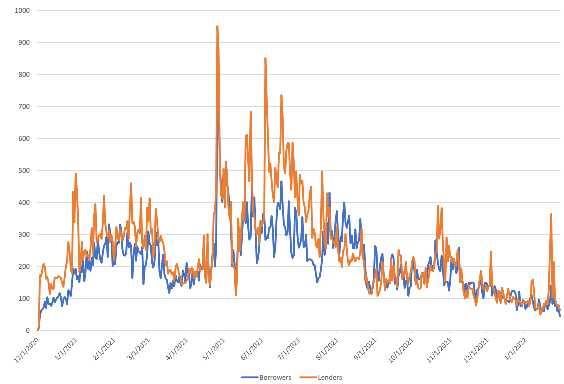
B.5 Shortfall Event

The primary mechanism for securing the Aave Protocol is the incentivization of AAVE holders (stakers) to lock tokens into a Smart Contract-based component called the **Safety Module** (SM). The locked AAVE will be used as a mitigation tool in case of a Shortfall Event (i.e., when there is a deficit). In the instance of a Shortfall Event, part of the locked AAVE are auctioned on the market to be sold against the assets needed to mitigate the occurred deficit. To contribute to the safety of the protocol and receive incentives, AAVE holders will deposit their tokens into the SM. In return, they receive rewards (periodic issuance of AAVE known as Safety Incentives (SI)) and fees generated from the protocol (see reserve factor above).

B.6 Recovery Issuance

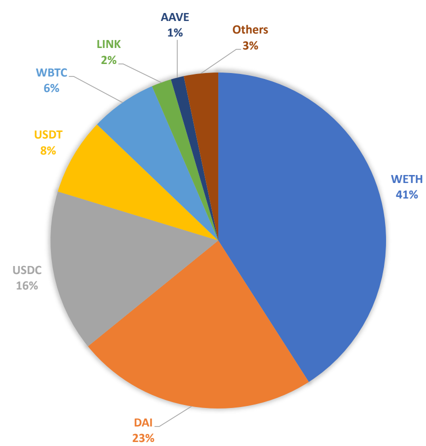
In case the SM is not able to cover all of the deficit incurred, an ad-hoc Recovery Issuance event is triggered where new AAVE is issued and sold in an open auction.

(a) Total Value (USD) Locked in Aave

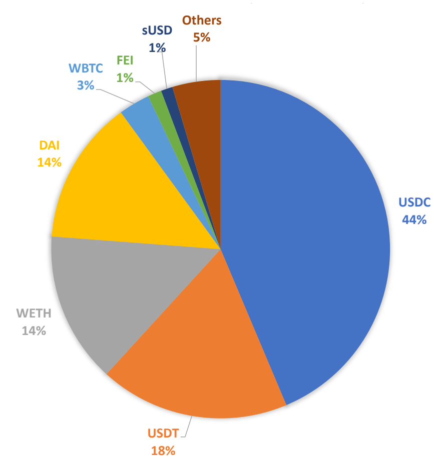


(b) Number of Unique Users per Day

Figure 12: Aave v2 TVL and Users Over time

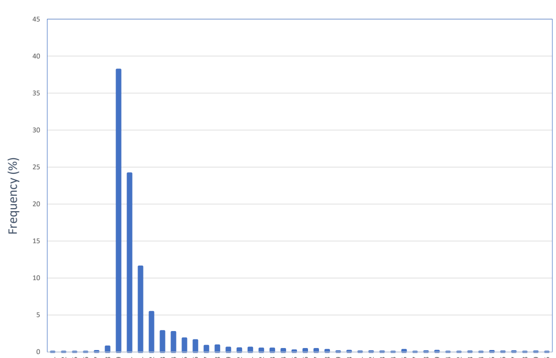


(a) Avg. Deposit Composition (Jan 2021-Jan 2022)

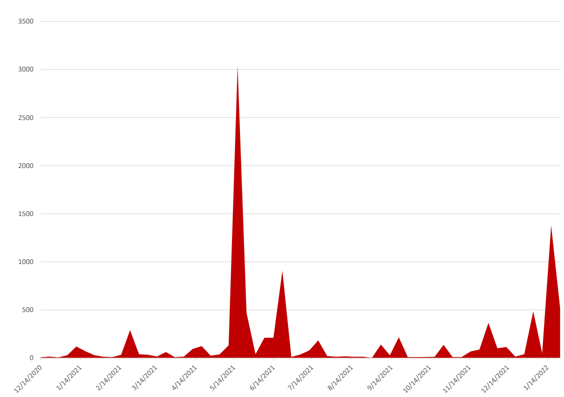


(b) Avg. Loan Composition (Jan 2021-Jan 2022)

Figure 13: Asset Compositions in Aave v2



(a) Health Factor (January 2022)



(b) Number of Liquidtions per Week

Figure 14: Liquidation Risk in Aave v2

B.7 Some Basic Statistics

Figures 12-14 show some basic statistics describing the Aave lending protocol. In April 2022, Aave supports the lending of 31 tokens and the total market size is about 11 billion USD. As shown in Figure 12 (a), the total value locked in Aave has increased substantially from mid 2020 to mid 2021, and has gone through a few ups and downs since then. The numbers of active lenders and borrowers, reported in panel (b), have also fluctuated over time. Figure 13 shows the average compositions of deposits and borrows. Aave does not show explicitly which deposited crypto assets are used as collaterals. These graphs however suggest that stablecoins such as USDC and USDT are borrowed disproportionately relative to their deposits. Stablecoins account for over 75% of loans. At the same time, the frequencies of borrowing assets like ETH and BTC (WETH and WBTC in the figures) are lower than those of depositing them, suggesting that they are mostly used as collaterals. It is also observed that the leverage of these loans is relatively high since the distribution of the health factors is skewed towards the left in Figure 14 (a), with 40% with a health factor below 1.[21] Liquidations happen frequently as a result of the volatile collateral prices and high leverage. Panel (b) shows the time series of collateral liquidations.

[21]In practice, a position with health factor below one may not be liquidated immediately due to the execution costs involved.

C Volatility of Collateral Value

Table 3: The Volatility of Collateral Value (January 2021 - April 2022)

	Daily Volatility	Largest daily increase	Largest daily decrease
Stable Coins			
DAI	0.32%	1.26%	-1.33%
TUSD	0.39%	2.97%	-2.01%
USDC	0.34%	1.94%	-1.57%
Other Coins			
AAVE	7.15%	31.33%	-33.47%
BAT	7.48%	47.60%	-31.05%
BAL	6.62%	22.65%	-31.03%
CRV	8.89%	51.18%	-43.16%
ENJ	8.96%	56.46%	-35.61%
ETH	5.19%	24.53%	-26.30%
KNC	7.19%	30.57%	-31.98%
LINK	6.66%	30.38%	-35.65%
MANA	10.92%	151.66%	-29.79%
MKR	7.10%	51.31%	-24.24%
REN	8.05%	44.84%	-35.82%
SNX	7.36%	25.22%	-36.24%
UNI	7.14%	45.32%	-32.94%
WBTC	4.01%	19.04%	-13.75%
WETH	5.21%	25.96%	-26.12%
XSUSHI	7.65%	33.19%	-29.54%
YFI	6.82%	46.00%	-36.35%
ZRX	7.57%	56.02%	-36.31%
Other Benchmarks			
Stock Market (SPY ETF)	1.00%	2.68%	-3.70%
Treasury (BATS ETF)	0.35%	1.25%	-1.72%
AAA Bond (QLTA ETF)	0.41%	1.11%	-1.33%
Gold (GLD ETF)	0.89%	2.74%	-3.42%

Source: CoinGecko.

D Price Exploits

We discuss some evidence where borrowers pledged inflated collateral assets to obtain loans from lending protocols which later suffered big financial losses due to the bad debt.

As discussed in the Introduction, borrowers can have information advantage relative to the lending protocol when the smart contract relies on an inaccurate price feeds. For example, during the Terra collapse in May 2022, as a result of the extreme volatility in the price of LUNA tokens, the price feed used by DeFi smart contracts for the LUNA token was significantly higher than the actual market value of the token. Attackers exploited the price discrepancy to borrow loans collateralized on inflated LUNA from the Venus Protocol, the biggest lending platform on BSC, leading to a loss of about $11.2 million to the protocol. The protocol later increased the haircut of LUNA from 45% to 100%. Similar exploits have depleted the entire lending pool of Avalanche lending protocol Blizz Finance, which has lost about $8.28 million due to this incident.

Similar price exploits can also happen when price oracles are based on on-chain AMMs that are subject to liquidity problems or price manipulation. At times, token prices on DEX can deviate substantially from those on CEX. There are multiple incidents indicating that borrowers exploit lending protocols by borrowing against over-valued collateral assets. For instance, on May 18, 2021, the Venus Protocol faced a massive collateral liquidation. This incident occurred because a large sum of XVS was collateralized at a high price (possibly after price manipulation causing price to shoot up from $80 to $145 in three hours) to borrow 4,100 BTC and nearly 10,000 ETH from the lending protocol. When the price of XVS dropped four hours later, the loans became undercollateralized, resulting in $200 million in liquidations and more than $100 million in bad debts, with the borrowers profiting from this exploit. In this particular episode, borrowers were able to exploit their information advantage of the overpricing of XVS while lenders were unable to exclude XVS being used as a collateral. Similar exploits happened to Ethereum-based lending protocols Cheese Bank (with $3.3 million loss in November 2020), Vesper Finance (with $3 millions loss in November 2021), and Inverse Finance (with $15.6 million loss in April 2022).

E Some Empirical evidence (for Online Appendix)

Here we report some evidence to support the case that our model can be useful for understanding the relationship between DeFi lending, crypto prices and market sentiment.

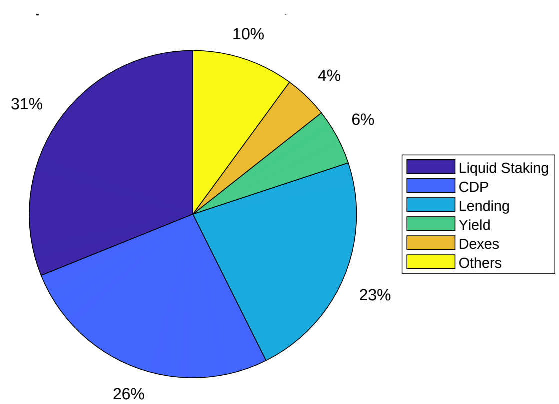
E.1 Effects of DeFi Lending on ETH Price

Our model predicts that DeFi lending should be positively correlated with crypto prices due to the price-liquidity feedback loop. Since the Ethereum blockchain is the main platform for DeFi, we use WETH TVL data from DeFiLlama to test this hypothesis. The sample is from 2018 January to 2022 March. Figure 15 shows that lending accounts for about 23% of DeFi TVL. We run an OLS

$$log(ETHP) = \alpha_0 + \alpha_1 log(LTCP) + \alpha_2 BURN + \alpha_3 DEFI + \alpha_4 LEND,$$

where $ETHP$ is the price of ETH, $LTCP$ is the price of Litecoin (LTC), $BURN$ is the amount of ETH burned since the London Fork as a percentage of ETH supply, $DEFI$ is the fraction of WETH locked into DeFi protocols, and $LEND$ is the fraction of WETH locked into DeFi lending. Since Litecoin has limited use in DeFi, we use its price to capture non-DeFi factors that can influence the price of ETH. As expected, results in Table 2 suggests that the prices of ETH and LTC are highly correlated. Also, unsurprisingly, by removing tokens from the circulating supply, BURN has a positive effect on the ETH price. Finally, after controlling for the general effects of DeFi on the price of ETH, TVL in DeFi lending is still positively correlated with the price of ETH, consistent with the prediction of our model.

Figure 15: Composition of WETH TVL in DeFi (March 2022)



Data Source: DefiLlamma.

E.2 Collateral Composition and Market Sentiment

Our model predicts that good market sentiment can help mitigate adverse selection, improving the quality of the collateral pool. We use the Aave platform data to examine the relationship between collateral

Table 4: **DeFi Lending and Crypto Prices**

	Estimate	Std. Err.	T-Stat	p
Intercept	1.0845	0.07905	13.72	1.6765e-40
Log(LTCP)	1.0545	0.017673	59.665	0
BURN	0.42739	0.027956	15.288	3.1158e-49
DEFI	4.9181	0.92868	5.2957	1.3566e-07
LEND	36.438	2.5999	14.015	4.3029e-42
No. obs. :	1546			
R^2	0.925	Adj. R^2	0.925	

composition and market sentiment. The market sentiment are measured by the "Crypto Fear & Greed Index" (FGI) for Bitcoin and other large cryptocurrencies.[22] The construction of the Index is based on measures of market volatility, market momentum/volume, social media, surveys, token dominance and Google Trends data. The Index is supposed to measure the emotions and sentiments from different sources, with a value of 0 indicating "Extreme Fear" while a value of 100 indicating "Extreme Greed". Since Aave does not provide collateral data, we need to use outstanding deposits of collateralizable tokens as a proxy. Basing on their internal risk assessment, Aave assigns risk ratings to each token ranging from C+ to A+. We use these risk parameters to measure the quality of these assets. Figure 16 shows how the composition changes over time. Note that tokens have different USD prices. Hence, changing prices will affect their (nominal) shares in the pool. To remove the effects of token price changes on the composition, we fix their prices at the median level over the sample period (Jan 2021- April 2022). So the results derived below capture only variations in token quantities and not in their prices.

We study how sentiment is related to the overall quality of the collateral pool proxied by the weighted average of the ratings of all outstanding collateralizable deposits.[23] We run an OLS regressing log(Rating) on a dummy and log(FGI) as follows

$$Log(Rating) = \alpha_0 + \alpha_1 Dummy + \alpha_2 log(FGI)$$

where Dummy=1 for days after April 26 (the date when Aave provided incentives to users who bor-

[22]The Index is developed by the "Alternative.me" website since early 2018 (https://alternative.me/crypto/fear-and-greed-index/).

[23]We convert ratings into numerical values as follows: Rating = 6 for "A", = 5 for "A-", ..., =1 for "C+".

Figure 16: Composition of Collateralizable Asset Mix

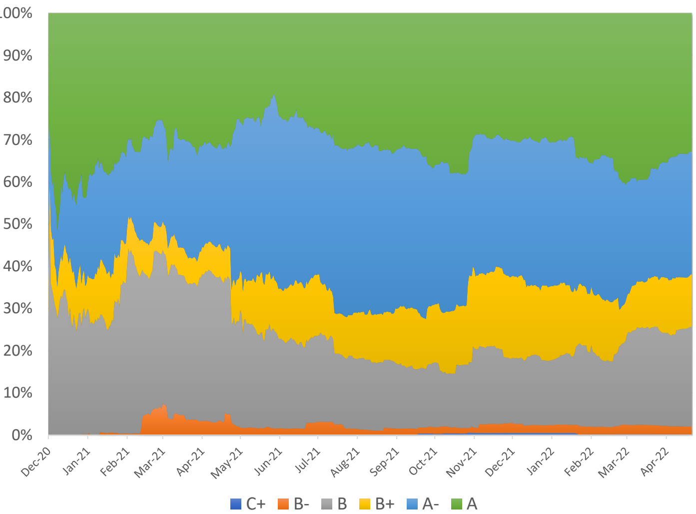


Figure Source: Dune Analytics

row/lend certain tokens). We report the result in Table 4. Both variables are significant, suggesting that the average rating of the collateral mix goes up when the sentiment captured by the FGI is high, as predicted by our model.

Table 5: **Sentiment and Collateral Rating**

	Estimate	Std. Err.	T-Stat	p
Intercept	1.4469	0.010123	142.93	0
Dummy	0.058287	0.0029707	19.62	4.2179e-64
Log(FGI)	0.01467	0.0022778	6.4405	2.7814e-10
No. obs. :	507			
R^2	0.464	Adj. R^2	0.461	

Figure 17: Effects of FG Index on Average Risk Rating

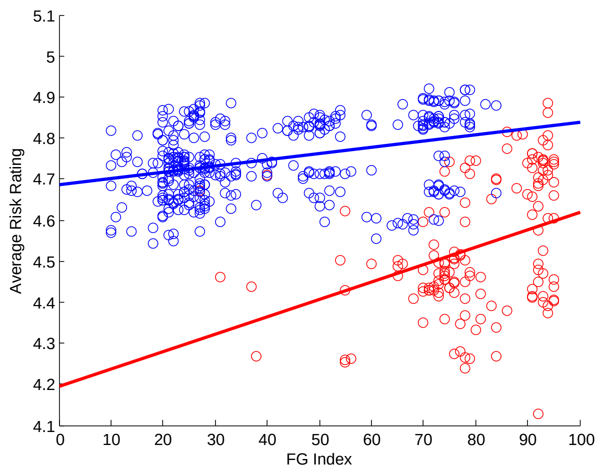


Figure Source: Dune Analytics

Blue (red) markers denote the sample period with (without) incentives