BANK OF CANADA
BANQUE DU CANADA

**Staff Working Paper/Document de travail du personnel—2023-14**

Last updated: February 22, 2023

# On the Fragility of DeFi Lending

by Jonathan Chiu,[1] Emre Ozdenoren,[2] Kathy Yuan[3] and Shengxing Zhang[4]

[1]Banking and Payments Department
Bank of Canada
jchiu@bankofcanada.ca

[2]LBS, CEPR
eozdenoren@london.edu

[3]LSE, FMG, CEPR
k.yuan@lse.ac.uk

[4]PHBS, LSE, CEPR
oo7zsx@gmail.com



**DOI:** https://doi.org/10.34989/swp-2023-14 | **ISSN** 1701-9397

# Acknowledgements

Yuan worked on the revision of the paper during her visit at the IMF. We thank our discussants Felix Irresberger, Quentin Vandeweyer and Ganesh Viswanath-Natraj for valuable suggestions, and we thank 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.

# Abstract

We develop a dynamic model of decentralized finance (DeFi) lending that incorporates two/these key features: 1) borrowing and lending are decentralized, anonymous, overcollateralized and backed by the market value of crypto assets where contract terms are pre-specified and rigid; and 2) information friction exists between borrowers and lenders. We identify a price-liquidity feedback: the market outcome in any given period depends on agents' expectations about lending activities in future periods, with higher price expectations leading to more lending and higher prices in that period. Given the rigidity inherent to smart contracts, this feedback leads to multiple self-fulfilling equilibria where DeFi lending and asset prices move with market sentiment. We show that flexible updates of smart contracts can restore equilibrium uniqueness. This finding highlights the difficulty of achieving stability and efficiency in a decentralized environment without a liquidity backstop.

*Topics: Digital currencies and fintech; Financial stability*
*JEL codes: G10, G01*



# Résumé

Nous élaborons un modèle dynamique du crédit octroyé par l'entremise de la finance décentralisée qui intègre ces principales caractéristiques : 1) les emprunts et les prêts sont décentralisés, sont anonymes, font l'objet d'unsurnantissement et sont garantis par la valeur marchande des cryptoactifs dans le cadre d'un contrat dont les modalités sont préétablies et rigides; 2) il y a une asymétrie d'information entre les emprunteurs et les prêteurs. Nous constatons un effet de rétroaction entre les prix et la liquidité : l'évolution du marché durant une période donnée dépend des attentes des agents à l'égard des activités de prêt dans l'avenir, et des attentes de prix plus élevées entraînent une augmentation des prêts et des prix au cours de cette période. Compte tenu de la rigidité des contrats intelligents, cet effet de rétroaction mène à de multiples situations d'équilibre autoréalisateur dans lesquelles le crédit par la finance décentralisée et les prix des actifs s'alignent sur l'humeur du marché. Nous montrons que des révisions souples de contrats intelligents peuvent rétablir l'unicité de l'équilibre. Cette constatation fait ressortir la difficulté d'atteindre la stabilité et l'efficience dans un environnement décentralisé qui n'offre pas de facilité de liquidité.

*Sujets : Monnaies numériques et technologies financières; Stabilité financière*
*Codes JEL : G10, G01*

# 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) that operate on blockchain technology. They are anonymous permission-less financial arrangements implemented via smart contracts—immutable, deterministic computer programs—on a blockchain that have been designed to replace traditional financial intermediaries (TradFi).

Among the many promises DeFi offers, two stand out. First, DeFi protocols have the potential to democratize the provision of and also expand access to financial services, especially for individuals who are under-served by TradFi, improving social welfare. Second, by automating contract execution, DeFi could resolve incentive problems associated with human discretion (e.g., fraud, censorship, racial and cultural bias) and, hence, complement TradFi.[1]

The growth of decentralized finance has been substantial since the "DeFi Summer" of 2020. According to data aggregator DeFiLlama, the total value locked (TVL) of DeFi had risen to 230 billion U.S. dollars as of April 2022, up from less than one billion two years prior to that time. As DeFi grows in scale and scope and becomes more extensively connected to the real economy, its vulnerabilities might undermine financial-sector stability (Aramonte, Huang, and Schrimpf (2021)). As a result, policymakers and regulators have raised concerns about the implications of DeFi for financial stability (FSB 2022; IOSCO 2022).[2] Yet formal economic analysis of this issue remains 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 than traditional lending.[3] In addition, Aramonte et al. (2022) argue that DeFi lending generates "pro-cyclicality," the co-movement between crypto prices and lending activities. We develop a dynamic model to capture key features of DeFi lending and explore its inherent fragility and its relationship to crypto asset-price dynamics.

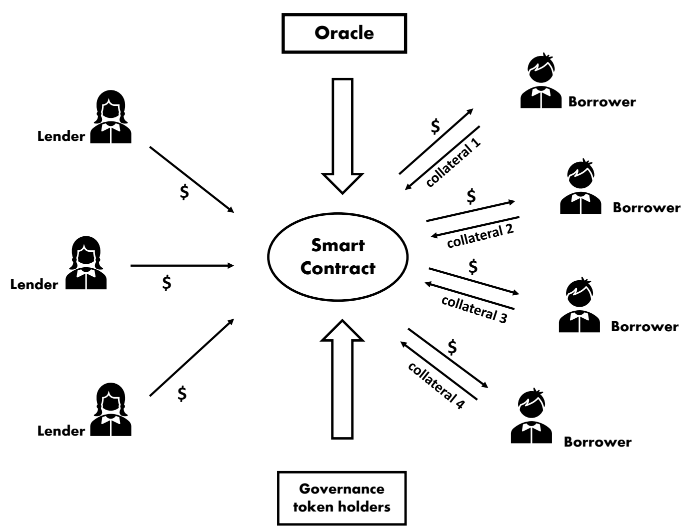
[1]The collapse of the cryptocurrency exchange FTX, an unregulated centralized blockchain trading firm, has further pushed investors away from centralized blockchain platforms towards self-custodial DeFi platforms. For example, it has been reported that Uniswap, one of the largest decentralized exchanges, registered a significant spike in trading volume on November 11, 2022, the day FTX filed for bankruptcy. The subsequent increase in its trading volume has been much higher than similar increases on many centralized exchanges (https://cointelegraph.com/news/after-ftx-defi-can-go-mainstream-if-it-overcomes-its-flaws).

[2]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

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

In Figure 1 we present a stylized display of the structure of lending protocols. Anonymous lenders deposit their crypto assets (e.g., stablecoins denoted as $) via a lending smart contract to the lending pool associated with 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 not readily observable, implying that borrowers are better informed about collateral quality than lenders are. Collateral assets are valued based on price feeds provided by an oracle, which can be either on-chain or off-chain. Since crypto assets are volatile, overcollateralization is a key feature of DeFi borrowing. The rules for setting key parameters (e.g., interest rates and haircuts) are pre-programmed in smart contracts. The protocol is governed in a decentralized fashion by holders of governance tokens. DeFi lending is typically short term because all lending and borrowing can be terminated at any minute.

Figure 1: Stylized Structure of a DeFi Lending Protocol




DeFi lending differs from TradFi lending in four unique respects. The first key difference involves anonymity: TradFi borrowers are typically identified while DeFi agents are anonymous in crypto space, where credit checks and other borrower-specific evaluations are not feasible. The second difference concerns the collateral asset. In TradFi, standard assets are available as collateral. In DeFi, however, only tokenized assets can be pledged as collateral, and such assets tend to exhibit very high price volatilities. Moreover, these risky assets are often bundled into an opaque asset pool so that, while DeFi borrowers can choose to pledge any acceptable collateral assets, lenders can neither control nor easily monitor the composition of the underlying collateral pool. As a result, DeFi lending is subject to information asymmetry between borrowers and lenders.[4] The third difference is related to loan contracts. TradFi loan contracts can be quite flexible, with loan officers modifying terms according to the latest hard and soft information. These features help to improve loan quality and enforce loan repayments in TradFi but are not applicable to DeFi lending, which is based on a public blockchain.[5] In DeFi, a smart contract is used to replace human judgment, and 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 data. As a result, DeFi lending typically involves linear, non-recourse debt contracts that feature over-collateralization as the only risk control. Furthermore, the decentralized nature of DeFi implies that even a slight modification of a contract can involve a lengthy decision process among governance token holders. Consequently, smart contract terms are modified only occasionally.[6] The fourth difference concerns regulation. There are so far no meaningful regulatory or oversight controls on DeFi lending, while TradFi is heavily regulated.

Motivated by these observations, we develop a dynamic model of DeFi lending with the following features. Borrowing is decentralized, over-collateralized, backed by the market value of various crypto assets, and governed by a linear borrowing contract, while the terms of the borrowing contract (such as the rule for haircuts) are pre-specified and rigid. Moreover, borrowers are better informed about the fundamental values of the crypto collateral assets than lenders.[7]

[4]Borrowers can also have an information advantage relative to the lending protocol when a smart contract relies on an inaccurate price oracle. The price feed of an oracle involves a trade-off between latency and accuracy. For example, the reference implementation to Uniswap's oracle averages prices over a 24-hour window, meaning that short-lived shocks to the price are largely ignored and even a large and sustained shock (e.g., 20% for an hour) will move the oracle price by less than 1%. When the price falls because of falling fundamentals, the oracle price will lag the asset's "true" price significantly. Because crypto is a volatile asset class, with frequent intraday spikes and drops, informed borrowers can take out large loans backed by a crypto asset with a suddenly inflated price from a delayed oracle and default on loan obligations, leaving the lending protocol with a collateral whose value is far below the face value of the loan.

[5]Some intertemporal and/or non-linear features of loan contracts 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 separate addresses.

[6]To amend or upgrade smart contracts, proxy contracts and implementation contracts are deployed to swap old contracts for new smart ones. DeFi protocols are, however, typically controlled using on-chain governance, where token holders vote to modify certain parameters of the smart contracts, resulting in only occasional risk-parameter changes. We find that, for example, the AAVE protocol was subject to only 13 risk-parameter changes in its first two years of operation. There are calls for technology developments to make decentralized governance semi-automatic and data-driven. So far, however, choosing these parameters has been a manual process (see Xu (2022)).

[7]In fact, this information friction need not reflect the quality of the asset. In the appendix, we show that an alternative

In our model, borrowers would like to borrow funds (e.g., stablecoins) from lenders through a lending platform using their crypto asset holdings as collateral. There is asymmetric information regarding the asset's quality between borrowers and lenders. Borrowers who are privately informed that their crypto assets are low quality have stronger incentives to borrow than those who are privately informed that their crypto assets are high quality. Lenders cannot control the collateral mix directly, so this information friction results in the classic lemons problem (Akerlof (1970)) and can severely reduce gains from trade by driving out high-quality borrowers. The DeFi platform imposes a haircut on the crypto asset, which reduces the loan's information sensitivity and mitigates the adverse-selection problem.

Interestingly, the lemons problem gives rise to a feedback effect between price and liquidity: the price of collateral assets affects the borrowing volume which, in turn, affects the equilibrium collateral price. In particular, this feedback is dynamic: the crypto market outcome in any given period depends on agents' expectations of crypto market conditions in future periods. Higher expectations regarding future crypto asset prices improve DeFi lending and support higher crypto prices in the present, leading to multiple self-fulfilling equilibria that make DeFi lending fragile. 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 extensively as collateral during periods when negative sentiment runs high. In addition, crypto asset prices and DeFi loans are more sensitive to fundamental shocks and more volatile.

We then show that the rigidity of a smart contract (e.g., specifying a constant haircut) plays an important role in driving the above mentioned outcomes. Under a flexible smart contract where the haircut can be updated nonlinearly in response to changes in market prices and the information environment, it is possible to support a unique equilibrium with high and stable lending volume and asset prices. Such contracts are, however, costly and difficult to implement in a decentralized environment, pinpointing the inherent fragility of DeFi lending protocols. To improve stability, it is necessary to give up a certain degree of decentralization in DeFi. For example, some platforms need to re-introduce human actors to provide real-time risk management—an arrangement that would force the decentralized protocol to rely on a trusted third party. While decentralization in participation and governance is fundamental to DeFi's exciting prospects for democratizing finance, our finding highlights the fact that decentralization also imposes limitations on DeFi's efficiency, complexity, and flexibility.

Our study is the first economics paper to develop a dynamic equilibrium model for studying decen-

information friction, unobservable private valuation, leads to the same price-liquidity feedback effects and multiple equilibria in the outcomes.

tralized lending protocols such as Aave and Compound. While there is a new and growing body of literature on decentralized finance, there is limited work on DeFi lending platforms. Most 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 MakerDAO (e.g., d'Avernas, Bourany, and Vandeweyer (2021), Li and Mayer (2021), Kozhan and Viswanath-Natraj (2021)). Lehar and Parlour (2022) empirically study 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) have been studied in recent computer science literature. These computer science papers focus mainly on the efficiency of the 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 theoretical work 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 features of DeFi lending to facilitate our study of the joint determination of lending activities and collateral asset prices, which helps 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 the features of and frictions that affect lending protocols 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.

## 2 Lending Protocols: Features and Frictions

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

**Key players.** The Aave eco-system consists of several types of participants. Depositors can deposit a crypto asset into the corresponding pool of the Aave protocol and collect interest over time. Borrowers can borrow funds from the pool by pledging any acceptable crypto assets as collateral to back the borrowing position. A borrower repays the loan in the same borrowed asset. There is no fixed time period within which to pay back the loan. Partial or full repayments can be made at any time. As long as the position is safe, the loan can continue for an undefined period. As time passes, though, the accrued interest on an unpaid loan will grow, which might make it more likely that the deposited assets are liquidated by liquidators. This eco-system also includes AAVE token holders. Like shareholders, token holders 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 runs when predetermined conditions are met.

**Loan rate and liquidation threshold.** Loan and deposit rates are set based on 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 rises (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 specific collateral. For example, at LTV = .75, for every 1 ETH of collateral, borrowers can borrow 0.75 ETHs' 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 feeds provided by Chainlink's decentralized oracles.

**Risky collateral.** Aave currently accepts more than 20 distinct crypto assets as collateral, including WETH, WBTC, USDC, and UNI. The market value of most non-stablecoin collateral assets is highly volatile. The prices of stablecoins such as USDC and DAI (top panel) are not particularly volatile and they are typically loaned out by lenders. Other crypto assets, which are used as collateral to back borrowings, are extremely volatile compared with collateral assets commonly used in TradFi (bottom panel). For example, ETH, which accounts for about 50% of non-stablecoin deposits in Aave, exhibits daily volatility of 5.69%. The maximum daily price drop was over 26% during the sample period. The most volatile asset is CRV, the governance token for the decentralized exchange and automated market-maker protocol Curve DAO. The maximum CRV 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 60% and 85%, respectively.[8]

[8] More recently, Aave has begun accepting tokenized real-world assets (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). As non-standardized assets, NFTs are likely to be subject to even more severe informational frictions. Popular DeFi lending platforms for NFTs include NFTfi, Arcade, and Nexo.

**Collateral pool.** Loans are backed by a pool of collateral assets. While the borrower can pledge any one of the acceptable assets as collateral, 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 lenders. Naturally, borrowers and lenders have asymmetric incentives to expend effort acquiring information about pledged collateral (e.g., monitoring new information, conducting 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 a contract.

**Decentralized governance.** Like many other DeFi protocols, Aave has deferred governance to the user community by setting up a decentralized autonomous organization (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 protocol changes, token holders need to make proposals, discuss them with the community, and obtain enough support in a vote. This process helps protect the system against censorship and collusion. Decentralized governance by a large group of token holders is, however, costly in both time and resources. Hence, it is not possible to update the protocol or the smart contract terms very frequently. As a result, when compared with a centralized organization, a DeFi protocol may be slower to make necessary adjustments in response to certain unexpected external changes (e.g., changes in market sentiment) in a timely manner. This problem is well documented. For instance, a risk-assessment report issued by 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."[9] In practice, between the setup of Aave v2 in late 2020 and May 2022, the risk parameters have been updated only 13 times. All updates were conducted after Aave DAO elected Gauntlet, a centralized entity, to provide dynamic risk-parameter recommendations.

These features of Aave are common among the DeFi lending protocols, highlighting three key frictions that affect DeFi lending. First, there is a lack of commitment from DeFi borrowers and, hence, the borrowings have to be (over-)collateralized. Second, information asymmetry between DeFi borrowers

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

and lenders can occur because lenders cannot control the collateral mix in the collateral pool. Third, DeFi contracts are rigid and based on quantifiable information stored on the blockchain.

# 3 The Model Setup

The economy is set in discrete time and lasts forever.[10] There are many infinitely lived borrowers with identical preferences. There is a fixed set of crypto assets. Every 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 smart contracts. All agents can consume/produce a numeraire good at the end of each period with a constant per-unit utility/cost.

***Gains from Trade and the Lending Platform*** A borrower needs funding that can be provided by lenders. There are gains from trade as the value per unit of funding for 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 smart contracts to implement collateralized loans. The DeFi intermediary determines the terms of a smart contract. Collateral is locked into the smart contract and released to the borrower if and only if repayment is received.[11]

In DeFi lending protocols such as Aave, borrowers borrow predominantly stablecoins such as USDT and USDC, using risky crypto assets as collateral (e.g., ETH, BTC, YFI, YNX). As stablecoins are regarded as a medium of exchange and a unit of account in DeFi, they are used to fund various transactions or to increase leverage in crypto investment. We interpret $z$ as the value accrued to borrowers when using stablecoins borrowed from lenders for speculative or productive purposes.[12]

***Crypto Asset Properties and the Information Environment*** We assume that all crypto assets are, ex ante, identical and pay random dividends, $\widetilde{\delta}$, in each period and survive to the next period with random probability, $\widetilde{s}$.[13] The dividend $\delta$ captures both the pecuniary payoff that the asset generates

[10] In reality, interest payments on the borrowing in the lending protocols are compounded continuously and can be terminated at any time. Therefore, time periods in our model are relatively brief.

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

[12] It is straightforward to introduce governance tokens issued by the intermediary—the lending platform. Governance token holders then provide insurance to lenders by acting as residual claimants. Given risk neutrality, the equilibrium outcome remains the same.

[13] We use ˜ to denote random variables.

(e.g., staking returns to the holder) and other private benefits that accrue from holding the crypto asset (e.g., governance rights). 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 with probability $\lambda$ it is low ($L$). The distribution of $(\widetilde{\delta}, \widetilde{s})$ is $F_Q$ if asset quality is $Q \in \{H, L\}$. We assume that $F_H$ first-order stochastically dominates $F_L$ and denote expectation with respect to $F_Q$ by $\mathbb{E}_Q$.

To simplify the analysis, we make further assumptions regarding 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 in the present ($\delta = 0$) and survives to the next period with probability $s \in [0, 1]$. The survival probability of the low-quality asset, $s$, 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 from the crypto asset.

We assume that the crypto asset pays positive dividends in some states. The main role of this assumption is to eliminate a non-monetary equilibrium. In our model the asset has collateral service and can have a positive price even if it pays no dividend. There can, however, be an equilibrium where the asset is worthless because current lenders believe future lenders will not accept the asset as collateral. A 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's payoff (which includes the asset's dividend and price) and its survival probability.[14][15]

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 assets that are, ex ante, identical. In the main model, we assume that borrowers receive private information in every period. In the Appendix, we consider the more general case where

[14] Although we demonstrate the existence of multiple equilibria in a setting with asymmetric information about both components, the result would go through as long as there is asymmetric information about either one of these components.

[15] Our results do not depend on asymmetric information about the common value component of the dividends. In Appendix A.6, we explore an alternative setup where there is asymmetric information concerning borrowers' private valuations. The main results hold. In Appendix A.7, we show that our setup can also be extended to time-varying information frictions.

private information arrives only infrequently with probability $\chi$, which captures 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 $\phi_t$. 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 the crypto asset that is held into the next period.[16]

***Smart Contracts*** As discussed in the introduction, DeFi lending is anonymous and collateralized via smart contracts. A 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, that is, the ratio of demand and supply for funding, and the collateral-specific haircut is updated infrequently. 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 $\ell_t$ 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 the amount of collateral $a_t$ to pledge and the size of the loan $\ell_t$ to take 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 collateral constraint

$$\ell_t R_t \leq a_t D_t,$$

where $D_t$ is the debt limit pinned down by (1). By borrowing $\ell_t$ 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

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

value discounted by the haircut needs to be sufficiently high to cover the loan repayment. Note that, without loss of generality, we assume that the collateral constraint is binding: $\ell_t R_t = a_t D_t$.[17] 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 occurs whenever $D_t > \widetilde{\delta} + \widetilde{s}\phi_t$. When the term inside the square bracket is non-positive, the borrower does not borrow: $a_t = \ell_t = 0$. Because $\mathbb{E}_H \min\{D_t, \delta + \phi_t\} = D_t \geq \mathbb{E}_L \min\{D_t, \widetilde{s}\phi_t\}$, we have $a_{Lt} \geq a_{Ht}$ and $\ell_{Lt} \geq \ell_{Ht}$, that is, low-type borrowers have stronger incentives to borrow than high-type borrowers. When both types borrow, we have a *pooling* outcome. When only low-type borrowers borrow, we have a *separating* outcome.

***DeFi Lending and Lenders*** The intermediary has no initial funding. It obtains funding $q_t$ from lenders to finance loans to borrowers. When a loan matures, the intermediary passes the cash flows—either a borrower's repayment 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. Inasmuch as lenders are unable 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 account for the expected quality of the collateral mix that backs the loan.

We assume that the lending market is competitive, that is, given $\{a_{i,t}\}_{i\in\{L,H\}}$, $D_t$, and $\phi_t$, 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.[18]

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

[17]To see this, suppose $(\ell^*, a^*)$ is optimal and $\ell^* R < a^* D$. Because the objective function is (weakly) decreasing in $a$, lowering $a$ (weakly) increases the objective. The increase is strict if $as\phi < \ell R$ for some realization of $s$.

[18]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 the loan is positive.

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 $\phi_t$ 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

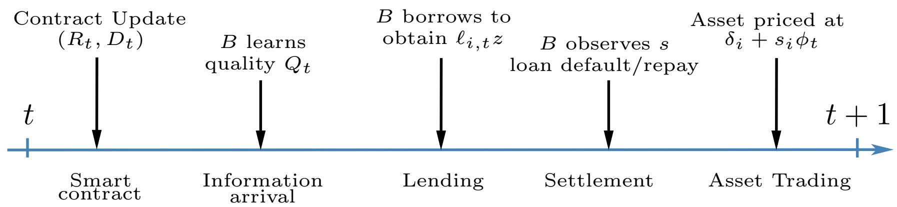
$$\begin{aligned} \phi_t = \beta & \underbrace{\{\lambda\left(\mathbb{E}_L \widetilde{s}\right)\phi_{t+1} + (1-\lambda)\left(\delta + \phi_{t+1}\right)\}}_{\text{Fundamental Value}} \\ +\beta & \underbrace{\left\{ \begin{array}{c} \lambda\left(a_{L,t+1}\mathbb{E}_L\left(zD_{t+1}/R_{t+1} - \min\{D_{t+1},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

where $\beta$ 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 the 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 $\phi_{t+1}$, which in turn depend on the extent of asymmetric information in future DeFi lending markets.

***Timing*** The time line is summarized in Figure (2). At 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, the borrower receives private information about the quality of the asset and decides whether to borrow from the lending platform by pledging collateral to the smart contract. Lenders supply funding subject to the 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 occurs, and the borrower works to acquire assets for the next period.

Note that on this time line the lending platform is exposed to information friction, the asset market is frictionless, and we assume that they do not open simultaneously, which reflects the natural timing of the information-revelation process. In reality, a privately informed borrower can choose to offload the underlying asset to a lending platform by borrowing a stablecoin loan against it or conducting an outright sale in an exchange (i.e., an asset market). Theoretically, however, it may not be optimal for a borrower to conduct an outright sale to raise money when there is adverse selection related to asset quality. The

Figure 2: Time Line




adverse-selection problem is more severe in an asset exchange because the borrower is selling an equity contract but less so in a lending platform because the borrower is selling a debt contract.[19] Empirically, other technical frictions occur when selling crypto assets on decentralized and centralized exchanges on blockchains. Transferring crypto assets to an off-chain centralized exchange is often subject to a long time lag before the assets can be traded, while transactions on an on-chain decentralized exchange are often subject to market illiquidity and price slippage. Therefore, for expositional clarity and without loss of generality, we assume that the asset market with frictions does not open simultaneously with the lending platform.

***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

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

# 4 Equilibrium in the Lending Market

We begin the analysis by describing the equilibrium in the DeFi lending market for a given asset price $\phi$.[20] To study the borrowers' decision, we first define the degree of *information insensitivity* as the

[19]Ozdenoren, Yuan, and Zhang (2021) have shown the optimal security for privately informed borrowers to sell in a similar setting consists of a debt contract (which both high- and low-quality borrowers sell) and a residual equity contract (which only low-quality borrowers sell).

[20]In this section, for ease of notation, we drop the time subscript $t$ from all the variables.

ratio of the expected value of the debt contract for type $L$ to the expected value of the debt contract for type $H$, that is, $\zeta(\phi;h) = \mathbb{E}_L \min\{D, \widetilde{s}\phi\}/D \in (0,1]$, where $D = (\delta + \phi)(1-h)$. As this ratio increases, the expected values of the debt under the low- and high-type borrowers 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

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

The 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

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

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

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

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 $\phi$.

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

Proposition 1 implies that, given asset price $\phi$, there is a unique equilibrium in DeFi lending. This equilibrium is pooling (separating) when the debt contract is sufficiently informationally insensitive (sensitive). In particular, when the degree of information insensitivity $\zeta(\phi;h)$ is above the threshold $\zeta$, the adverse-selection problem is not particularly severe and both types of borrowers 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 borrower 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 that $\zeta(\phi; h) = \mathbb{E}_L \min\{1, \frac{\widetilde{s}\phi}{(\delta+\phi)(1-h)}\}$. As a result, the debt contract becomes informationally less sensitive for a high $\phi$ and a high $h$. The above proposition also indicates that, in addition to the parameter $\lambda$ that characterizes type heterogeneity, the net gains from trade, $z/(1+f)$, are 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 to 1), the DeFi lending will be in a separating equilibrium. In other words, when net gains from trade are low, even a slight degree of information asymmetry results in an adverse-selection problem.

# 5 Multiple Equilibria in Dynamic DeFi Lending

The analysis presented 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 varying crypto asset prices. The multiple asset prices are, in turn, justified by the multiple equilibria in DeFi lending. Inasmuch as we focus 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 $\phi^P$ that satisfies 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, the high-type borrower's incentive constraint to pool with the low-type borrower must hold:

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

#### 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 $\phi^S$ that satisfies 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 borrower's incentive constraint:

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

### 5.2 Existence and Uniqueness

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

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

Lemma 1 implies that there exists at most one pooling and one separating stationary equilibrium. If these equilbria 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:*

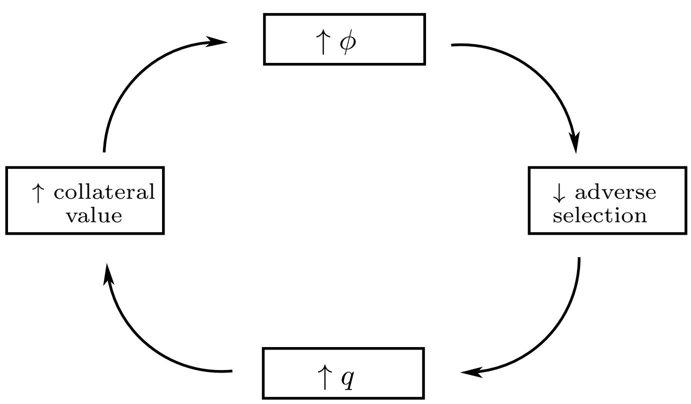
- *it is a unique pooling equilibrium when $\overline{\zeta} < \zeta(\phi^S; h)$,*
- *it is a unique separating equilibrium when $\overline{\zeta} > \zeta(\phi^P; h)$,*
- *a pooling equilibrium and a separating equilibrium coexist when $\overline{\zeta} \in [\zeta(\phi^S; h), \zeta(\phi^P; h)]$.*

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

### 5.3 Haircuts and Multiplicity

In Proposition 2, multiplicity arises as a result of a dynamic price-feedback effect, described in Figure 3. 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 borrowers. In turn, if agents anticipate a pooling equilibrium in future periods, the expected liquidity value of the asset in the next period is high and, hence, the asset price in the present 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 borrower retains the asset and chooses not to borrow. In turn, if agents anticipate separating equilibria in future periods, the liquidity value of the asset is limited and thus the present asset price is low. As a result, the asset prices in this economy are self-fulfilling.

Figure 3: Dynamic Feedback Loop




The haircut is a key parameter that controls the degree of information sensitivity. Setting a lower haircut makes the debt contract informationally more sensitive, magnifying the adverse-selection problem. 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 that the expected survival probability of the crypto asset satisfies $\mathbb{E}_L\widetilde{s} \in (\kappa_P, \kappa_S)$. There exists a threshold for the haircut such that when $h$ is below this threshold, there are* *multiple equilibria.*

### 5.3.1 Example: Two-Point Distribution

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 $\pi$ 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 borrower 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 borrower defaults if $h < \underline{h}^S$ and repays if $h \geq \underline{h}^S$. In the former case, the low-type borrower always defaults so neither the face value of the loan nor, consequently, the loan size depends on the haircut. In the latter case, the low-type borrower repays the loan in the good state (i.e., $s = 1$); hence, the loan size depends on the face value of the debt. The face value of debt declines as the haircut increases, so 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 $\phi^S$ as a function of the 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 $h < \underline{h}^S$ because the high-type borrower never defaults, so the expected value of the contract with the high-type borrower declines as $h$ increases. The low-type borrower, on the other hand, always defaults, and the expected value of the contract with the low-type borrower 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 because, in this case, the high-type borrower always pays the face value and the low-type borrower 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 of borrowers 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 borrower 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 $\underline{h}^S$, only a unique equilibrium can exist, depending on whether $\overline{\zeta}$ is above or below $\pi$.

In Figure 4 we plot 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 the separating and pooling equilibria, respectively, assuming their existence. The parameter values used are $z = 1.1$, $\lambda = 0.5$, $\beta = 0.9$, $\delta = 1$, $\pi = 0.92$, and $f = 0$, which satisfy the condition $\mathbb{E}_L \widetilde{s} \in (\kappa_P, \kappa_S)$ in Proposition 3. In the bottom right plot we compare the degrees of information insensitivity to the threshold $\overline{\zeta}$, which is captured by the dashed horizontal line. When $h$ is close to zero, the dashed line appears above the red curve and below the blue curve, confirming the multiplicity result specified in Proposition 3. The other three plots also confirm the earlier result that the asset price, loan size, and debt limit are all 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 $\overline{\zeta} = \zeta^S(\hat{h})$.[21]

### 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 through $K$. 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 $\phi^k$ be the price of the asset, $R^k$ the loan rate, and $D^k = \left(\delta + \phi^k\right)(1-h)$ the debt limit in sentiment state $k$. Quantities of collateral $a_L^k, a_H^k$ chosen by each borrower type must be optimal given the asset price and loan rate at each sentiment state $k$. The loan size chosen by the lender in sentiment state $k$ is given by

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

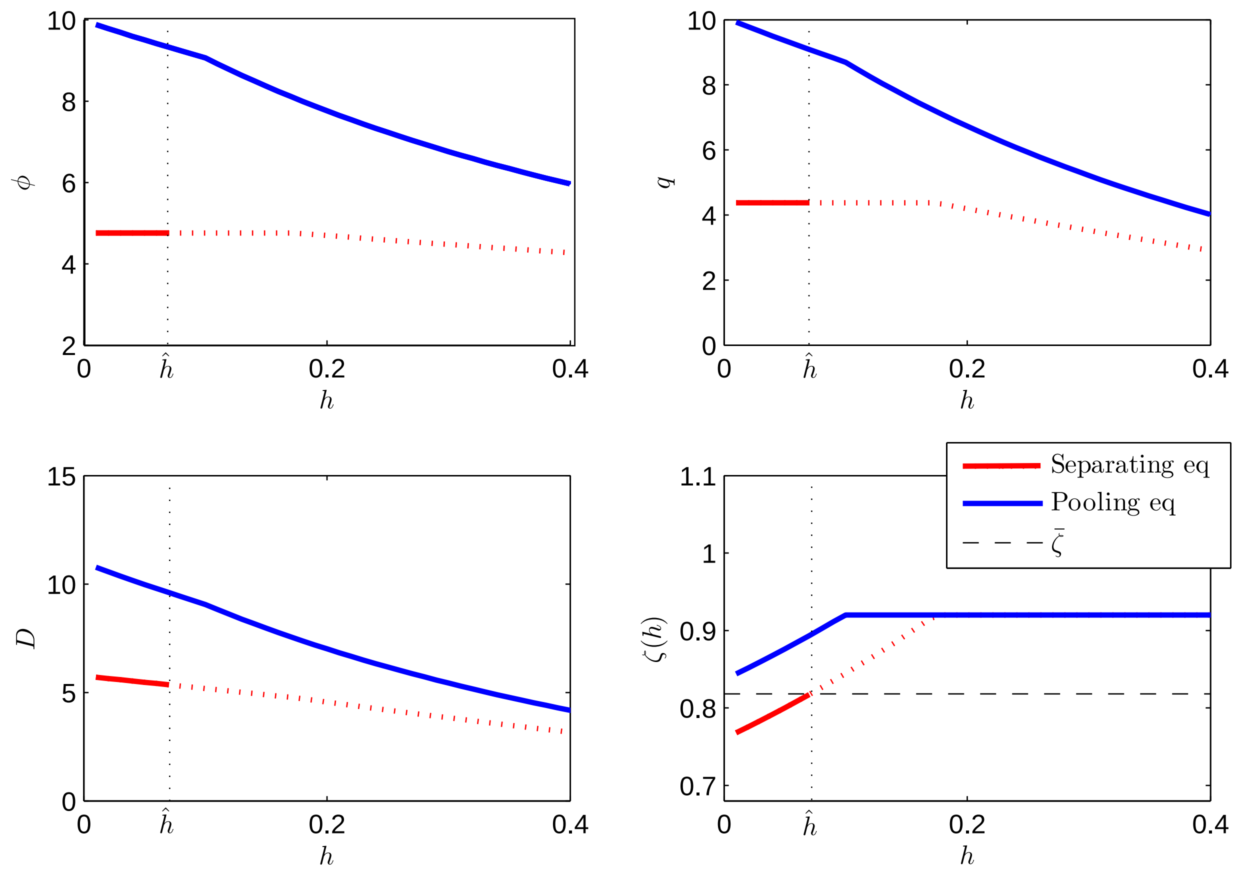
The price of the crypto asset in sentiment state $k$ is given by

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

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, we can

[21]When $h > \hat{h}$, the separating equilibrium cannot be sustained and, hence, in Figure 4 the red lines depicting separating equilibria become red dotted lines in this region.

Figure 4: Effects of Haircut $h$




obtain the following result.

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

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

**Example 1.** Suppose that $K = 3$ and $\bar{k} = 1$. The economy remains in the same state with probability $\sigma$ 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 5 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.

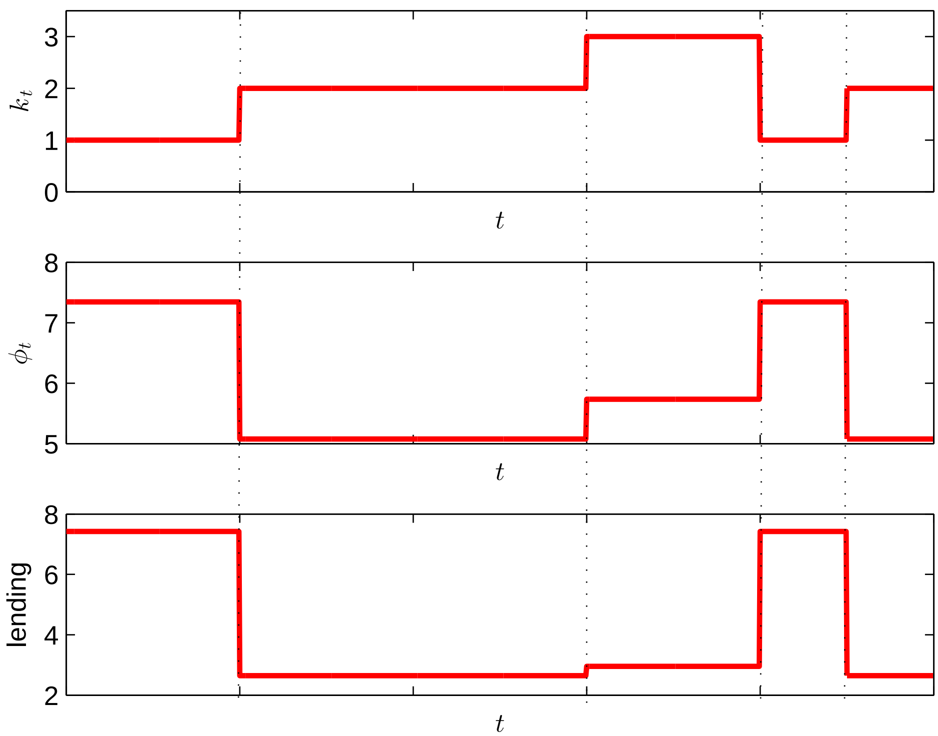
Next, we reveal a similar pro-cyclical pattern of lending and asset prices in an example where there are more (than three) states and a state moves to an up or down state with equal probability. In this example, equilibrium lending and asset prices are more volatile.

**Example 2.** Let $K = 10$. If the economy is in state $k$ in a given period, in the next period sentiment remains the same with probability $\sigma$. From states $k \in \{2, \ldots, K-1\}$, the economy moves to state $k-1$ with probability $(1-\sigma)/2$ and to state $k+1$ with probability $(1-\sigma)/2$. From state 1, the economy moves to state 2 with probability $1-\sigma$. From state $K$, the economy moves to state $K-1$ with probability $1-\sigma$. Figure 6 plots a simulation for 5,000 periods when $\sigma = 0.95$ and $\bar{k} = 6$.

### 5.5 Uniqueness Under Flexible Design of the Debt Limit

We have shown that when DeFi lending is subject to a rigid haircut, multiplicity occurs if 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 than in the case with a rigid haircut.

Figure 5: Sentiment Equilibrium, Example 1




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

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

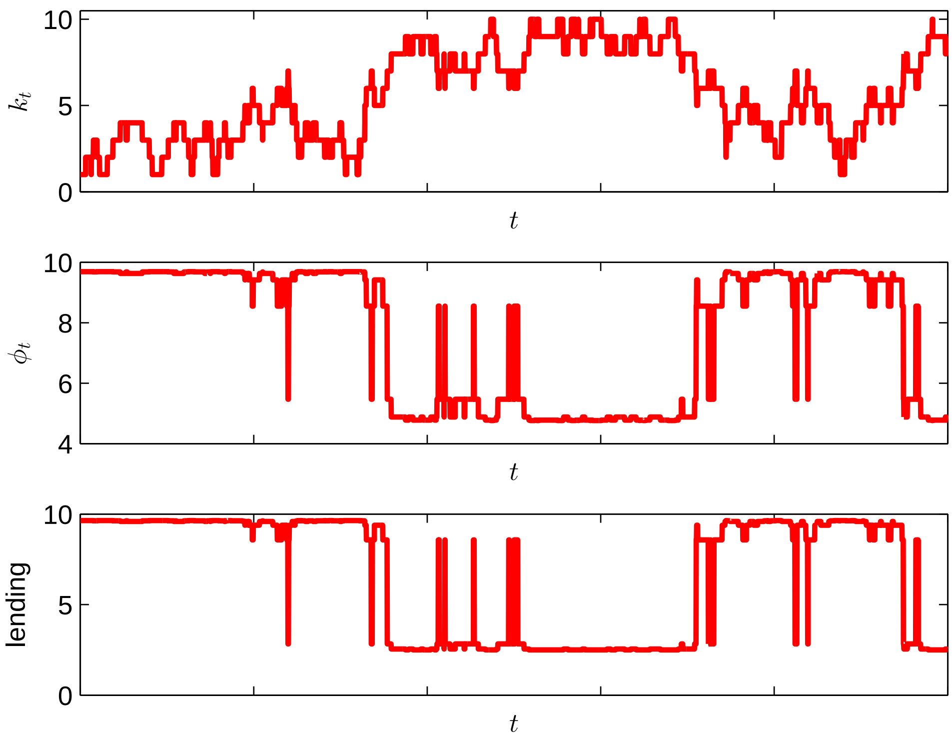
Recall from (4) that the intermediary maximizes the expected loan size times the intermediation fee:

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

The loan size is

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

Figure 6: Sentiment Equilibrium, Example 2




where

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

Equivalently, the intermediary maximizes

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

subject to (11). In other words, the intermediary takes the price $\phi_t$ as given and sets the debt threshold $D$ to maximize the expected loan size, taking into account the impact of the contract on the funding that lenders are willing to supply. The value of the asset to the borrower is

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

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 smart contract design is debt face value $D_t$, the borrower's value for the asset at the beginning of period $t$ $V_t$ and the resale price of the asset at the end of period $t$ $\phi_t$, such that (i) $D_t$ maximizes (12) taking $\phi_t$ as given, and (ii) $V_t$, and $\phi_t$ satisfy (13) and (14).

We also make the same simplifying assumptions regarding the distribution of $\left(\widetilde{\delta}, \widetilde{s}\right)$ that we make in the rigid haircut case, that is, we assume that a high-quality asset pays dividend $\delta > 0$ at the end of the period and survives to the next period with certainty, which implies

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

and the low-type asset pays no dividends and it survives to the next period with probability $s \in [0, 1]$, which is drawn from a distribution $F$, which implies

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

The following proposition describes the optimal debt threshold and the implied haircut as a function of the asset price $\phi_t$.

**Proposition 5.** *If $\mathbb{E}_L s < 1 + \frac{1}{\lambda \widehat{z}} - \frac{1}{\lambda}$, then let $s^*$ be the unique solution to*

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

*In this case, the equilibrium contract is a pooling contract ($a_{H,t} = 1$) with face value $D_t = s^*\phi_t$ when*

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

*Otherwise, the equilibrium contract is a separating contract ($a_{H,t} = 0$) with face value $D_t = \delta + \phi_t$. The implied haircut is*

$$h_t = \begin{cases} 0 & \text{if } \lambda \mathbb{E}_L \min(s^*, s) + (1-\lambda)\, s^* - \lambda \mathbb{E}_L s < 0, \\ 1 - \frac{s^*\phi_t}{\delta + \phi_t} & \text{if } \lambda \mathbb{E}_L \min(s^*, s) + (1-\lambda)\, s^* - \lambda \mathbb{E}_L s \geq 0. \end{cases}$$

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

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

*The implied haircut is*

$$h_t = \max\left\{0, 1 - \frac{\widehat{z}\lambda E_L s}{1-\widehat{z}(1-\lambda)}\frac{\phi_t}{\delta+\phi_t}\right\}.$$

*Moreover, given any end-of-period price $\phi_t$, the asset price in the previous period and the lending volume are higher than those under the rigid DeFi contract.*

Note that the optimal haircut rule is not a fixed number or a simple linear rule but is non-linear in price $\phi_t$. The proposition shows that a flexible contract generates a higher social surplus. For example, when $\phi_t$ is high (which makes the debt contract informationally less sensitive), the intermediary can increase $D_t$ to induce a higher lending volume, which raises the surplus gained from lending. In contrast, when $\phi_t$ is low (which makes the contract informationally more sensitive), the intermediary may choose to lower $D_t$ to maintain a pooling outcome. Depending on the parameter values, the intermediary may also choose to raise $D_t$ to induce a separating equilibrium. This flexibility in adjusting $D_t$ implies that, given any end-of-period price $\phi_t$, the price of the asset in the previous period and the loan size are weakly greater than those under the rigid DeFi contract.

The following proposition shows that flexibility in setting the haircut optimally in response to changes in the asset price leads to a unique stationary equilibrium with a fixed realized equilibrium haircut.

**Proposition 6.** *Under a flexible optimal debt limit there exists a unique stationary equilibrium that Pareto dominates the equilibrium 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 potentially sentiment-driven equilibria (e.g., Asriyan, Fuchs, and Green (2017)) while reducing welfare. Can a DeFi smart contract be pre-programmed to replicate the flexible contract design? This can be challenging to execute in practice. First, a flexible contract cannot be implemented using simple linear haircut rules that are typically encoded in DeFi contracts. Second, the optimal debt threshold depends on information that may not be readily available on the blockchain (e.g., $z, \lambda$). Alternatively, the lending protocol can replace the algorithm with 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 involved in achieving stability and efficiency in a decentralized environment that is subject to informational frictions.

## 6 Conclusion

In this paper, we study sources of fragility in DeFi lending caused by several of its fundamental features. These features are informational frictions, such as asymmetric information about collateral quality, oracle problems, and rigid contract terms. We demonstrate the inherent instability of DeFi lending that results from 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 end, a smart contract may take a complex form. Such a contract also requires a reliable oracle to feed real-time hard and soft information from the off-chain world. Alternatively, DeFi lending could abandon complete decentralization and re-introduce human intervention to provide real-time risk management—an arrangement that would force the protocol to rely on a trusted third party. Our finding highlights a trilemma faced by DeFi protocols: the difficulty involved in achieving simplicity in smart contracts and stability in asset prices while maintaining a high degree of decentralization.

## References


Akerlof, George A (1970). "The Market for" Lemons": Quality Uncertainty and the Market Mechanism". *Quarterly Journal of Economics* 84.3, pp. 488–500.

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*.

Xu, Jiahua (2022). *Auto.gov: Optimal On-chain Governance for DeFi*. Tech. rep. UCL.

# 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 reduces 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 borrower will borrow. At that rate, however, lenders would earn negative profit.

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

## 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 that $s_L = 1$ w.p. $\pi$ 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 a 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 informationally 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 a separating equilibrium requires

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

When the haircut is higher than the threshold $\underline{h}$, the low-type borrower pays back the loan to retain the collateral when $s_L = 1$. In this case, the loan size is equal to the $\pi D$. 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

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

The existence of a 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

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

The existence of a pooling equilibrium requires

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

## A.5 Proof of Uniqueness Under a Flexible Smart Contract

Denote the debt contract as $y(D, \widetilde{\delta} + \widetilde{s}\phi) = \min(D, \widetilde{\delta} + \widetilde{s}\phi)$. 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 modifications.

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

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

in which case there is a pooling equilibrium.

When the intermediary designs the smart deposit contract flexibly, it aims to maximize the expected trading volume. Specifically, the intermediary chooses $D$, or equivalently, a 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 $\phi$ 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 $\hat{s} = D/\phi$. In this case, all terms in the incentive constraint for the high-type borrower are proportional to the asset price $\phi$, which drops out of the constraint. So, the high-type borrower's incentive constraint is satisfied if and only if

$$\widehat{z}\left[\lambda \mathbb{E}_L \min(\hat{s}, s) + (1-\lambda)\hat{s}\right] \geq \hat{s}.$$

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

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

So, $\mathcal{F}(\hat{s})$ is concave and strictly positive when $\hat{s}$ is close to 0. Suppose that 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 $\mathcal{F}(s^*) = 0$. Because the asset price $\phi$ drops out, threshold $s^*$ does not depend on $\phi$.

Taking the next period asset price $\phi$ as given, the asset price in the current period under a 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:

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

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 that satisfies $\phi^P(\phi) = \phi$.

Suppose that information friction is too 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 the high-type borrower's incentive constraint is binding and there is $d^*(\phi) \leq \delta$, which satisfies

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

or the high-type borrower'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 $\frac{\widehat{z}[\lambda \mathbb{E}_L s + (1-\lambda)] - 1}{1 - \widehat{z}(1-\lambda)} \phi < \delta$,

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

Note that

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

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

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

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

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

Note that

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

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

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 $\delta$, we can see that $\phi^P(\phi)$ is concave with a slope of 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 for a low-type borrower 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, we know that $\phi^P(\phi)$ is concave with a slope of 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 borrower. In the special parameterization of the model, any face value between $\phi$ and $\delta + \phi$ generates the same revenue from borrowing because a low-quality asset pays no dividend. More generally, low-quality assets could pay positive dividends. So the maximum face value $D = \delta + \phi$ is a more robust form of debt design in the separating case.

Given face value $D = \delta + \phi$, the incentive constraint for the high-type borrower 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 $\phi^S(0) = \beta(1-\lambda)\delta$.

The intermediary chooses the pooling contract if and only if

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

or

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

where $s^*$ is the unique solution to

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

Plugging in for $\phi^P$ and $\phi^S$, we can rewrite the inequality as

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

which holds if and only if

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

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 $D = s^*\phi < \phi$ 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

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

## A.6 An Alternative Setup with Unobservable Private Valuation

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

Suppose that with probability $1-\varepsilon$, the state is good ($s = 1$) and the asset pays dividend $\delta$. With probability $\varepsilon$, the state is bad ($s = 0$) and the asset pays no 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-$i$ borrower is determined before the loan is made and the information is private. With probability $\lambda$, the borrower is 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 $\delta$, the borrower decides whether to repay or 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 $\phi$ 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. A 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 7.** *For $h$ that is not too large, $\phi^P > \phi^S$ and multiplicity exists when*

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

## 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, $\chi$, 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

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

where $a^0 = 1$, $\ell^0_t = q^0_t = \frac{1}{1+f}(\delta+\phi_t)(1-h)$ and $R^0_t = (\delta+\phi_t)(1-h)/q^0_t$. By continuity, all results hold when $\chi$ is sufficiently close to 1.