On the Inherent Fragility of DeFi Lending

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

August 2022

Abstract

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

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

JEL classification: G10, G01

---

*Chiu (jchiu@bankofcanada.ca), Ozdenoren (eozdenoren@london.edu), Yuan (k.yuan@lse.ac.uk), and Zhang (s.zhang31@lse.ac.uk). Yuan has worked on the revision of the paper during her visit at IMF. We thank our discussant Ganesh Viswanath-Natraj for valuable suggestions, as well as many conference participants for their comments. We thank Hanna Yu for her research assistance. The views expressed in this paper are solely those of the authors and may differ from official Bank of Canada or IMF views.

1 Introduction

Decentralized finance (DeFi) is an umbrella term for a variety of financial service protocols and applications (e.g., decentralized exchanges, lending platforms, asset management) on blockchain. These are anonymous permissionless financial arrangements that aim to replace traditional intermediaries by running smart contracts – immutable, deterministic computer programs – on a blockchain. This is different from traditional financial arrangements that rely on intermediaries run by third parties. By automating the execution of contracts, DeFi protocols have potential to avoid incentive problems associated with human discretion (e.g., fraud, censorship, racial and cultural bias), expand the access to financial services and complement the traditional financial sector. The growth of decentralized finance has been substantial since the "DeFi Summer" in 2020. According to data aggregator DeFiLlama, the total value locked (TVL) of DeFi has reached 230 billion U.S. dollars as of April 2022, up from less than one billion two years ago. As DeFi grows in scale and scope and becomes more connected to the real economy, its vulnerabilities might undermine both crypto and formal financial sector stability (Aramonte, Huang, and Schrimpf (2021)). While policy makers and regulators have raised concerns about the financial stability implications of DeFi (FSB 2022; IOSCO 2022)[1], formal economic analysis on this issue is still very limited. In this paper, we examine DeFi lending protocols – an important component of the DeFi eco-system, and the sources and implications of their instability.[2] We develop a dynamic adverse selection model to capture key features of DeFi lending, explore its inherent fragility and its relationship to crypto asset price dynamics.

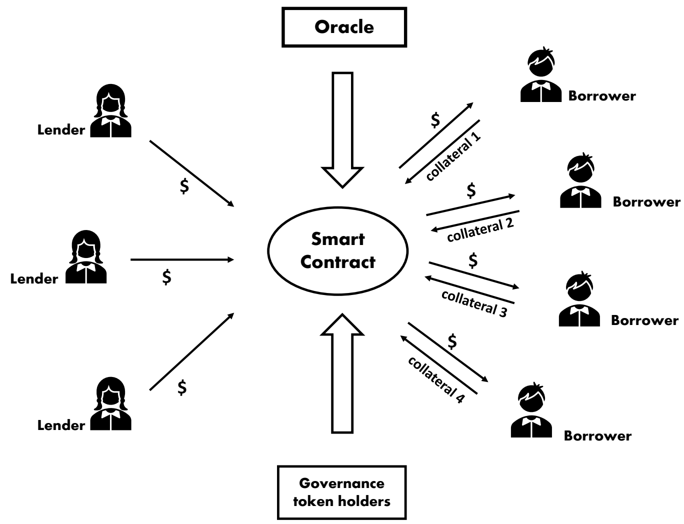
As documented in Section 2, DeFi lending is one of the most popular DeFi services. Figure 1 shows a stylized structure of lending protocols. Anonymous lenders deposit their crypto assets (e.g., stablecoins denoted as $) via a lending smart contract to the lending pool of the corresponding crypto asset. Anonymous borrowers can borrow the crypto asset from its lending pool by pledging *any* collateral accepted by the protocol via a borrowing smart contract. DeFi lending is typically short-term since all lending and borrowing can be terminated at any minute. The rules for setting key parameters (e.g., interest rates and haircuts) are pre-programmed in the smart contracts. Collateral assets are valued based on price feeds provided by an oracle which can be either on-chain or off-chain. The protocol is

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

[2]DeFi lending is much more volatile relative to traditional lending. For example, the coefficients of variation for the total values of Aave v2 loans and deposits are respectively 73 and 65 in 2021. The corresponding statistics for the US demand deposits and C&I loans are respectively 10.4 and 2.7. In addition, Aramonte et al. (2022) argue that DeFi lending generates "procyclicality" – a feature that arise endogenously in our model.

governed by holders of governance tokens in a decentralized fashion.

Figure 1: Stylized Structure of a DeFi Lending Protocol



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

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

Our work is the first economic paper to develop a dynamic, equilibrium model for studying decentralized lending protocols such as Aave and Compound. While there is a young and growing literature on decentralized finance, there are very limited work on DeFi lending platforms. Most existing DeFi papers study decentralized exchanges to understand how automated market makers (e.g., Uniswap) function differently from a traditional exchange (e.g., see Aoyagi and Itoy (2021), Capponi and Jia (2021), Lehar and Parlour (2021), Park (2021). There are also papers investigating the structure of decentralized stablecoins such as Dai issued by the MakerDAO (e.g., d'Avernas, Bourany, and Vandeweyer (2021), Li and Mayer (2021), Kozhan and Viswanath-Natraj (2021)). Lehar and Parlour (2022) study empirically the impact of collateral liquidations on asset prices. For a general overview of DeFi architecture and applications, see Harvey et al. (2021) and Schar (2021).

Our model is related to existing theoretical works on collateralized borrowing in a general equilibrium setting such as Geanakoplos (1997), Geanakoplos and Zame (2002), Geanakoplos (2003), and Fostel and Geanakoplos (2012). Building on Ozdenoren, Yuan, and Zhang (2021), our model captures some essential institutional feature of DeFi lending to study the joint determination of lending activities and collateral

[3]Borrowers can also have an information advantage relative to the lending protocol when the smart contract relies on an inaccurate price oracle. Section 6 discusses some exploit incidents during the Terra collapse in May 2022 and other price exploits due to inflated on-chain collateral prices.

asset prices, which help us understand how information frictions and smart contract rigidity contribute to the vulnerabilities of crypto prices and DeFi lending.

This paper is organized as follows. In Section 2, we provide a brief description of the Aave lending protocol as an example. We then 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 discusses some evidence and Section 7 concludes.

2 A Brief Description of Aave Lending Protocol

According to DeFiLlama, there are 1485 DeFi protocols running on different blockchains (e.g., Ethereum, Terra, BSC, Avalanche, Fantom, Solana) as of April 2022. The TVL of these protocols are 237 billion USD with lending protocols accounting for about 20%. (Figure 2).[4] Table 1 reports some basic statistics about the three main lending protocols: Compound operating on Ethereum, Venus on the BSC and Aave on multiple chains. Operating on multiple blockchains, Aave is the largest among the three in terms of TVL, deposits and borrows, and market capitalization of its governance tokens. Below, we give a brief overview of some key features of the Aave lending protocol. More details can be found in the appendix.

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

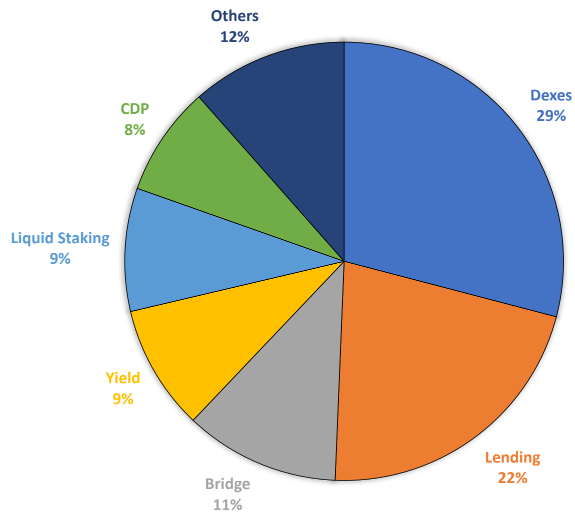
	Aave	**Compound**	**Venus**
Total value locked (USD)	13.35 B	6.35 B	1.51 B
Blockchain	Multi	Ethereum	BSC
Total deposits (USD)	15.37 B	9.51 B	1.51 B
Total borrows (USD)	5.93 B	3.21 B	0.82 B
Governance Token	AAVE	COMP	XVS
Market Cap (USD)	2.38 B	0.99 B	0.13 B

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

Aave is an open source and non-custodial liquidity protocol where users can earn interest on deposits and borrow crypto assets. It is one of the largest DeFi protocols, with the following features:

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

Figure 2: Composition of TVL of all DeFi Protocols on all Chains (April 2022)



Data Source: DefiLlamma.

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

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

Ricky collateral. Aave currently accepts over 20 different crypto assets as collateral including WETH, WBTC, USDC and UNI. Most non-stablecoin collateral assets have very volatile market value. As shown in table 4 in the Appendix, the prices of stablecoins such as USDC and DAI (top panel), are not so volatile and they are typically loaned out by lenders. Other crypto assets, which are used as collaterals to back the borrowings, are extremely volatile relative to collateral assets commonly used in traditional finance (bottom panel). For example, ETH, which accounts for about 50% of use non-stablecoin deposits in Aave, has a daily volatility of 5.69%. The maximum daily price drop was over 26% during the sample period. The most volatile one is CRV, the governance token for the decentralized exchange and automated market maker protocol Curve DAO. For CRV the maximum price change within a day was over 40%. For risk management purposes, Aave has imposed very high haircuts on these crypto assets. For example, the haircuts for YFI and SNX are respectively 60% and 85%.[5]

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

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

Decentralized governance. Like many other DeFi protocols, Aave has released the governance to the user community by setting up a decentralized autonomous organization or DAO. Holders of the AAVE token can vote on matters such as adjustments of interest rate functions, addition or removal of assets, and modification of risk parameters such as margin requirements. To implement such changes

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

to the protocol, token holders need to make proposals, discuss with the community, and obtain enough support in a vote. This process helps protect the system against censorship and collusion. However, decentralized governance by a large group of token holders is both time and resource costly. Hence it is not possible to update the protocol or the smart contract terms very frequently. As a result, relative to a centralized organization, a DeFi protocol may be slower to make necessary adjustments to respond to certain unexpected external changes (e.g., changes in market sentiments) in a timely manner.[6]

Figures 3-5 show some basic statistics describing the Aave lending protocol. In April 2022, Aave supports the lending of 31 tokens and the total market size is about 11 billion USD. As shown in Figure 3 (a), the total value locked in Aave has increased substantially from mid 2020 to mid 2021, and has gone through a few ups and downs since then. The numbers of active lenders and borrowers, reported in panel (b), have also fluctuated over time. Figure 4 shows the average compositions of deposits and borrows. Aave does not show explicitly which deposited crypto assets are used as collaterals. These graphs however suggest that stablecoins such as USDC and USDT are borrowed disproportionately relative to their deposits. Stablecoins account for over 75% of loans. At the same time, the frequencies of borrowing assets like ETH and BTC (WETH and WBTC in the figures) are lower than those of depositing them, suggesting that they are mostly used as collaterals. It is also observed that the leverage of these loans is relatively high since the distribution of the health factors is skewed towards the left in Figure 5 (a), with 40% with a health factor below 1.[7] Liquidations happen frequently as a result of the volatile collateral prices and high leverage. Panel (b) shows the time series of collateral liquidations.

3 The Model Setup

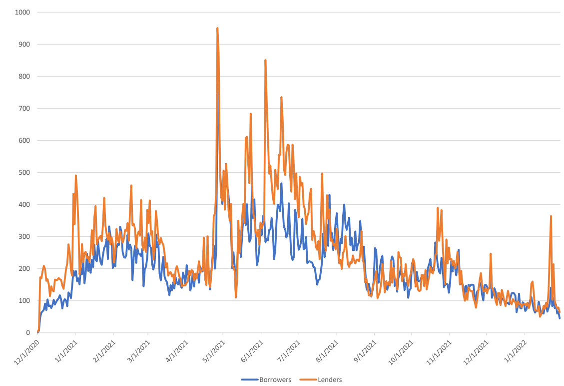
The economy is set in discrete time and lasts forever.[8] There are many infinitely-lived borrowers with identical preferences. There is a fixed set of crypto assets. Each borrower can hold at most one unit. There are also potential lenders who live for a single period and are replaced every period. DeFi lending is facilitated by an intermediary. All agents can consume/produce linearly a numeraire good at the end of each period.

[6] A risk assessment report 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." (Source: https://gauntlet.network/reports/aave)

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

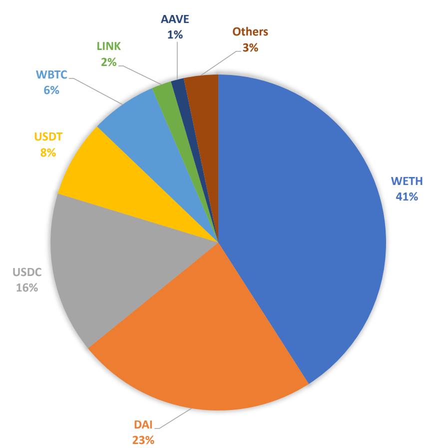
[8] In reality, interest payment on the borrowing in the lending protocols is continuously compounded and can be terminated at any time. Therefore, we can interpret that each time period in our model is relatively short.

(a) Total Value (USD) Locked in Aave

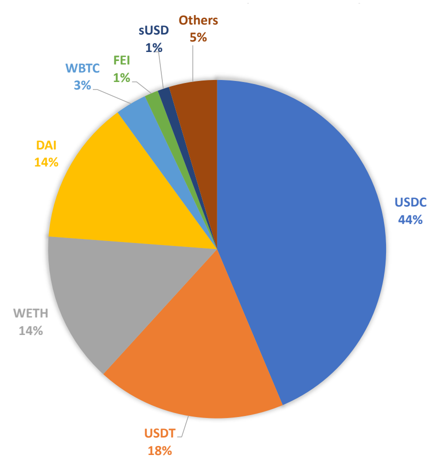


(b) Number of Unique Users per Day

Figure 3: Aave v2 TVL and Users Over time

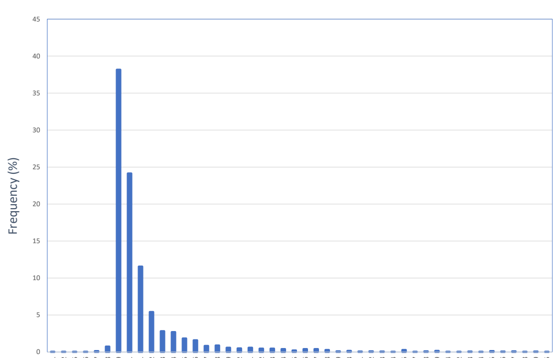


(a) Avg. Deposit Composition (Jan 2021-Jan 2022)

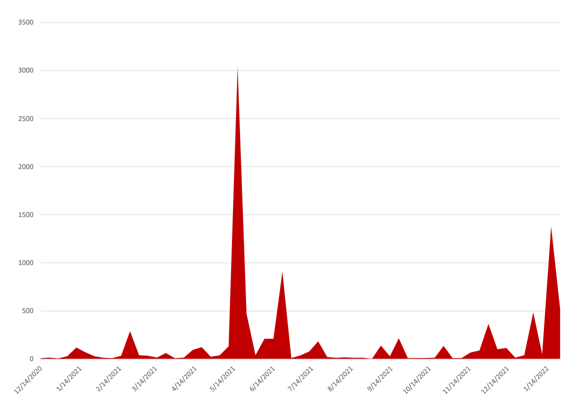


(b) Avg. Loan Composition (Jan 2021-Jan 2022)

Figure 4: Asset Compositions in Aave v2



(a) Health Factor (January 2022)



(b) Number of Liquidtions per Week

Figure 5: Liquidation Risk in Aave v2

Gains from Trade A borrower has a need for funding that can be provided by lenders. There are gains from trade as the value per-unit of funding to a borrower is $z > 1$, while the per-unit cost of providing funding by lenders is normalized to one. At the end of the period, borrowers can produce the numeraire good to repay the lenders subject to linear disutlility. The fundamental friction that gives rise to DeFi lending is that agents are anonymous and cannot commit to future actions. This implies that loans need to be collateralized on crypto assets. In addition, centralized intermediaries that provide custodial services also cannot commit to returning the assets. This friction supports the role for DeFi lending which relies on a smart contract to implement a collateralized loan. The DeFi intermediary helps determines the terms of trade only. Collateral is locked into a smart contract and released to the borrower if and only if a repayment is received. With a pre-programmed contract replacing human beings, incentive problems can be reduced.

In DeFi lending platforms such as Aave, borrowers predominantely borrow stablecoins such as USDT and USDC using risky collaterals such as ETH, BTC, YFI, YNX. They use stablecoins to fund various transactions due to their status of medium of exchange and unit of account in DeFi. We can interpret z as the value accrued to the borrowers when using the stablecoins borrowed from the lenders for purchasing assets or converting them into fiat.[9]

Crypto Asset's Properties and Information Environment For simplicity, we assume that all crypto assets are ex-ante identical but, at the beginning of a period, each of them 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. A high-quality asset will pay divided $\delta_H = \delta$ at the end of the period and will survive to the next period with probability $s_H = 1$. The dividend δ captures both pecuniary payoff that the asset generates (e.g., staking returns to the holder), and other private benefits that accrue from holding the crypto asset (e.g., governance right). With probability λ, the quality of the asset is low. A low-quality asset does not pay any dividends today ($\delta_L = 0$) and it will survive to the next period with probability $s_L \in [\underline{s}, \bar{s}]$ which will be drawn from a distribution F before the end of the period. Here, $1 - s_L$ captures whether the quality shock has persistent effects on the dividend flow of the crypto asset.[10]

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

[10] In the Appendix, we also explore an alternative setup where there is aymmetric information concerning borrowers' private, insltead of common, valuation. The main results hold.

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 to borrow and borrow how much from DeFi lending. The borrower then receives the private return from the loan, and observes the realization of s_L. Given the information, the borrower decides whether to repay the loan or default. The asset's quality and the state s_L are both publicly revealed at the end of each period. In the next period, some low-type assets do not survive and are replaced by new ones that are ex-ante identical. Also, for simplicity, we have assumed that borrowers receive private information every period. In the Appendix, we consider the general case where private information arrives only infrequently with probability χ, which can capture the degree of information imperfection.

Asset Price At the end of each period, agents meet in a centralized market to trade the assets by transferring the numeraire good. At this point, the private information is resolved. The end-of-period ex-dividend price of a crypto asset that will survive to the next period is denoted as ϕ_t. The pre-dividend price is thus $\Phi_t = \delta + \phi_t$ for a good asset and $s_L\phi_t$ for a bad asset with survival probability s_L. In the centralized market, each borrower can acquire at most one unit of crypto asset to the next period.[11]

DeFi Lending & Borrowers As discussed in the introduction, DeFi lending typically uses a debt contract with the haircut h pre-determined by the lending protocol. The haircut defines the debt limit per unit of collateral

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

In the benchmark model, we assume that the haircut is fixed over time and examine the case of a flexible haircut in an extension. In each period, the intermediary sets the gross loan rate R_t in the lending contract: if the borrower borrows ℓ_t units of funding, the face value of the debt is $R_t\ell_t$.

After observing the asset quality, the borrower raises funding from a DeFi protocol by executing the lending contract. Given (R_t, D_t), a type $i = H, L$ borrower chooses how much collateral a_t to pledge and how much loan ℓ_t to borrow from the pool:

$$\max_{a_t,\ell_t} z\ell_t - \mathbb{E}\min\{\ell_t R_t, a_t(\delta_i + s_i\phi_t)\}$$

subject to a collateral constraint

$$\ell_t R_t \leq a_t D_t.$$

By borrowing ℓ_t and pledging a_t, the borrower obtains $z\ell_t$ from the loan but needs to either repay $\ell_t R_t$ or lose the collateral value $a_t(\delta_i + s_i\phi_t)$. The collateral value discounted by the haircut needs to be

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

sufficiently high to cover the loan repayment. Note that, without loss of generality, we can assume that the collateral constraint is binding: $\ell_t R_t = a_t D_t$.[12] So the solution for the borrowing decision is given by

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

Hence, it is optimal to set $a_t \in \{0,1\}$. When the term inside the square bracket is positive, the borrower pledges $a_t = 1$ to borrow $\ell_t = D_t/R_t$ and promises to repay D_t. Default happens whenever $D_t > \delta_i + s_i\phi_t$. When the term inside the square bracket is non-positive, the borrower does not borrow: $a_t = \ell_t = 0$. Since $\delta_H > \delta_L$ and $s_H > s_L$, it is easy to verify that $a_{Lt} \geq a_{Ht}$ and $\ell_{Lt} \geq \ell_{Ht}$. That is, the low-type borrowers have higher incentives to borrow than the high-type. When both types borrow, we have a *pooling* outcome. When only the low-type borrowers borrow, we have a *separating* outcome.

DeFi Lending & Lenders The intermediary has no initial funding. It obtains funding q_t from the lenders to finance loans to borrowers. When the loan matures, the intermediary will pass the future cash flows – either the repayment of the borrowers or the resale value of the collateral (in case of a default) – to the lenders, after collecting an intermediation fee (discussed below). Hence, a lender's expected return from the debt contract offered to a type-i borrower is

$$y_H(\delta + \phi) = \min\{D_t, \delta + \phi_t\},$$
$$\mathbb{E}y_L(s_L\phi) = \mathbb{E}\min\{D_t, s\phi_t\}.$$

That is, the lender expects to get D_t when the borrower repays, and get the value of the collateral when the borrower defaults. Note that the borrower's borrowing decision (a_{it}, ℓ_{it}) is quality dependent, meaning that lenders face adverse selection in DeFi lending. Since lenders are not able to distinguish between low and high quality borrowers at the time of lending, the choice of funding size q_t does not depend on the underlying asset quality. Of course, in equilibrium, lenders take into account the expected quality of the collateral mix backing the loan. Formally, the lender's zero-profit condition implies that the funding provided by a lender is given by

$$q_t = \frac{1}{1+f}\left\{\frac{1}{a_{L,t}\lambda + a_{H,t}(1-\lambda)}\left[a_{L,t}\lambda\mathbb{E}y_L(s_L\phi_t) + a_{H,t}(1-\lambda)\,y_H(\delta+\phi_t)\right]\right\} \tag{3}$$

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

where $f < z - 1$ is a fixed fee charged by the intermediary per unit of loan.[13] Since the collateral quality is unknown, the lender's expected return on the RHS is given by the weighted average derived according to the equilibrium mix of borrowers.

Finally, the interest rate is set by the intermediary who takes the price ϕ_t and the haircut h as given and solves

$$\max_{R_t} f[\lambda \ell_{Lt} + (1-\lambda)\, \ell_{Ht}] \tag{4}$$

ensuring that (i) $\{a_i, \ell_i\}$ solves the optimization problem of type $i \in \{L, H\}$ (condition 2), and (ii) lenders make zero-profit (condition 3).

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

$$\begin{aligned} \phi_t = \beta \Bigg\{ \lambda \left[\int_{\underline{s}}^{\bar{s}} (z\ell_{L,t+1} - \min\{\ell_{L,t+1}R_{t+1}, a_{L,t+1}s_L\phi_{t+1})\} + s_L\phi_{t+1})\, dF(s_L) \right] \\ + (1-\lambda)\, [z\ell_{H,t+1} - \min\{\ell_{H,t+1}R_{t+1}, a_{H,t+1}(\delta + \phi_{t+1})\} + \delta + \phi_{t+1}] \Bigg\}, \end{aligned} \tag{5}$$

where β is the discount factor such that $0 < \beta < 1/z$. The continuation value of the asset, conditional on i, is simply the sum of three terms: the collateral value $\mathbb{E}a_i(zq - y_i)$, the dividend value δ_i, and the resale value $s_i\phi$. Importantly, the collateral value of the asset is related to endogenous variables $(\ell_{it+1}, a_{it+1}, R_{t+1})$ which in turn depend on the extent of asymmetric information in future DeFi lending markets.

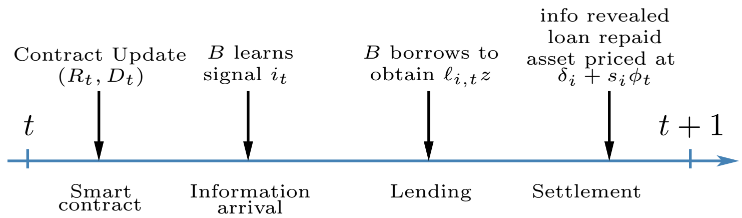
Timing The time-line is summarized in Figure (6). In each period, the debt limit D_t is determined given h. The intermediary sets R_t to attract lenders and borrowers to trade loans subject to the haircut rule. A borrower receives private information about the quality of the asset and decides whether to borrow by pledging collateral to the smart contract. Once borrowing is done, both i and s_L are revealed and the asset price is determined. Finally, the borrower repays the loan, or defaults and loses the collateral. At the end of the period, consumption takes place and the borrower can work to acquire assets for the next period.

To summarize, 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

[13] In equilibrium, the lenders' funding will be lent to the borrowers, $q = \ell$. When the loan matures the intermediary takes qf either from the repayment or from the resale value of the collateral. The remaining amount goes to the lender. The assumption of $f < z - 1$ ensures that the net gain from loans is positive.

that (i) borrowers' loan decisions are optimal (condition 2), (ii) lenders earn zero profits (condition 3), (iii) R_t solves intermediary's problem (condition 4), and (iv) the asset pricing equation is satisfied (condition 5).

Figure 6: Timeline



4 Equilibrium in Lending Market

We begin the analysis by describing the equilibrium in the DeFi lending market for a given asset price ϕ.[14] To study the borrowers' decision, we first define the degree of *information insensitivity* as the ratio of the expected value of the debt contract for different types, i.e., $\mathbb{E}y_L(s_L,\phi)/\mathbb{E}y_H(\phi)$. Note that a debt contract has the property that $\mathbb{E}y_L(s_L,\phi) \leq \mathbb{E}y(\phi)$. As this ratio increases, the expected values of the debt under the low versus high 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, both types borrow the same amount: $\ell_L = \ell_H = \frac{D}{R} = q$. Condition (3) implies that the equilibrium funding supplied by lenders is

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

We can define an implicit interest rate

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

In the separating case, only the low-type borrowers borrow: $\ell_H = 0, \ell_L = \frac{D}{R} = q$. The funding from lenders is given by

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

We can define an implicit interest rate

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

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

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

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

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

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

5 Multiple Equilibria in Dynamic DeFi Lending

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

5.1 Characterization of Stationary Equilibria

5.1.1 Pooling equilibrium

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

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

The loan size is given by

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

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

$$\frac{\mathbb{E}y_L(s_L, \phi^P)}{\mathbb{E}y_H(\phi^P)} \geq \zeta. \tag{7}$$

5.1.2 Separating Equilibrium

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

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

The loan size are given by $\ell_H = 0$ and

$$\ell_L = q^S = \frac{1}{1+f}\mathbb{E}\left[\min\{D^S, s_L\phi^S\}\right],$$

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

$$\frac{\mathbb{E}y_L(s_L, \phi^P)}{\mathbb{E}y_H(\phi^P)} < \zeta. \tag{9}$$

5.2 Existence and Uniqueness

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

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

The above lemma implies that there exists at most one pooling and one separating stationary equilibrium. If they co-exist, the price in the pooling equilibrium is higher than that in the separating equilibrium. It is also easy to show that both prices are higher than the fundamental price of the asset in autarky, $\underline{\phi} = \frac{\beta(1-\lambda)\delta}{1-\beta(\lambda\mathbb{E}(s_L)+(1-\lambda))}$. This means that the introduction of DeFi lending raises the equilibrium asset price above its fundamental level. To show the existence of equilibrium, we now consider the incentive constraints (7) and (9). In particular, we define a function:

$$\hat{\zeta}(\phi) \equiv \frac{\mathbb{E}y_L(s_L, \phi)}{\mathbb{E}y_H(\phi)}$$

that measures the degree of information insensitivity. The above lemma implies that $\hat{\zeta}(\phi^P) > \hat{\zeta}(\phi^S)$. Hence, we have the following proposition.

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

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

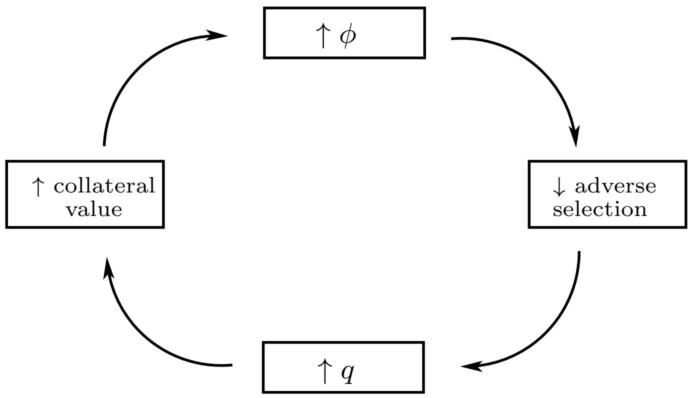
5.3 Haircut and Multiplicity

In Proposition 2, multiplicity in the middle region part arises due to a dynamic price feedback effect described in Figure 7. When the collateral asset price is high, the degree of information insensitivity of the debt contract, $\hat{\zeta}(\phi^P)$, is above the threshold ζ. Hence, the adverse selection problem is mild and the high-type borrowers are willing to pool with the low type. In turn, if agents anticipate a pooling equilibrium in future periods, the expected liquidity value of the asset in the next period is large, hence the asset price today is high. Conversely, when the asset price is low, the degree of information insensitivity of the debt contract, $\hat{\zeta}(\phi^S)$, is below the threshold ζ. Therefore, the adverse selection problem is severe and the high type retains the asset and chooses not to borrow. In turn, if agents anticipate a separating equilibrium in future periods, the liquidity value of the asset is limited thus the asset price today is low. As a result, the asset prices are self-fulfilling in this economy.

As discussed earlier, the haircut is a key parameter controlling the degree of information sensitivity. In particular, setting a lower haircut makes the debt contract informationally more sensitive, magnifying the adverse selection problem. Hence, defining two thresholds

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

Figure 7: Dynamic Feedback Loop



we have the following result.

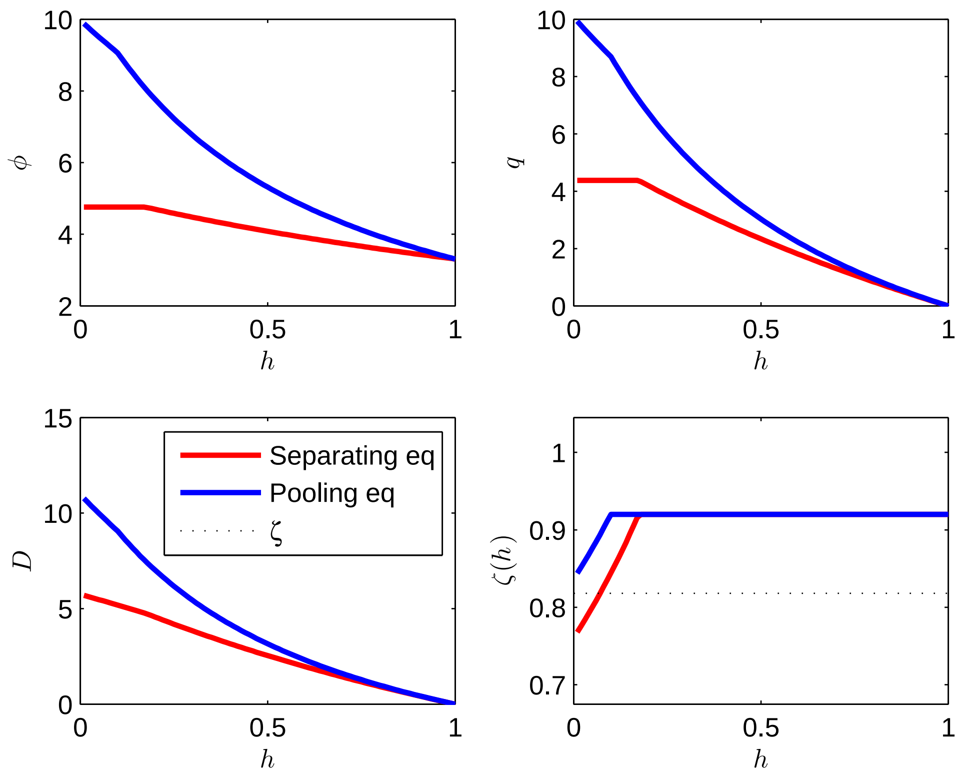
Proposition 3. *When* $\mathbb{E}(s) \in (\kappa_P, \kappa_S)$, there are multiple equilibria for h not too large.

5.3.1 A Simple Example

We now use a simple numerical example to briefly discuss the effects of h on the equilibrium outcome. The full analysis is given in the Appendix. Suppose s_L is drawn from a two point distribution such that $s_L = 1$ with probability π, and $s_L = 0$ with probability $1 - \pi$. Consider the separating equilibrium. When $s_L = 0$, a low-type borrower always defaults. When $s_L = 1$, the low-type defaults if $D^S > \phi^S$ and repays if $D^S < \phi^S$. In the former case ($D^S > \phi^S$), the loan size is equal to the expected value of the asset, $\pi\phi^S$, which does not depend on the haircut. Hence, condition (8) implies that the asset price is also independent of h. However, according to condition (9), an increase in h, makes it harder to support a separating equilibrium as the contract becomes less information sensitive. In the latter case ($D^S < \phi^S$), the loan size is equal to πD. Hence, the asset price is decreasing in h. A separating equilibrium exists whenever $\pi < \zeta$ as h does not affect the information sensitivity of the contract. The pooling equilibrium can be analyzed similarly.

Figure 8 plots the effects of h on the asset price, the loan size, the debt limit and the degree of information insensitivity of the contract. The red and blue curves indicate respectively the separating and pooling equilibria, assuming their existence. The parameter values used are $z = 1.1$, $\lambda = 0.5$, $\beta = 0.9$, $\delta = 1$, $\pi = 0.92$, $f = 0$, which satisfy the condition $\mathbb{E}(s) \in (\kappa_P, \kappa_S)$ in Proposition 3. The bottom right plot compare the degrees of information insensitivity to the threshold ζ which is captured by the horizontal dash line. When h is close to zero, the dash line appears above the red curve and below the blue curve, confirming the multiplicity result in Proposition 3. The other three plots also confirm the earlier result that the asset price, loan size and debt limit are higher in a pooling equilibrium. In this example, multiplicity can be ruled out and pooling can be supported by setting $h > \hat{h} = 7.1\%$ where $\zeta = \zeta^S(\hat{h})$.

Figure 8: Effects of Haircut h



5.4 Sentiment Equilibrium

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

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

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

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

$$\phi^k = \beta \sum_{k=1}^{K} \sigma_{kk'} \beta \left\{ \lambda \left[\int_{\underline{s}}^{\bar{s}} \left(z\ell_L^{k'} - \min\{\ell_L^{k'} R^{k'}, a_L^{k'} s\phi^{k'}\} + s\phi^{k'} \right) dF_L(s) \right] \right.$$
$$\left. + (1-\lambda) \left[z\ell_H^{k'} - \min\{\ell_H^{k'} R^{k'}, a_H^{k'}(\delta + \phi^{k'})\} + \delta + \phi^{k'} \right] \right\}.$$

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

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

Example 1. Consider the two-point distribution example with $K = 3$ states and and $\bar{k} = 1$. We assume the following transition matrix:

$$\begin{pmatrix} \sigma & 1-\sigma & 0 \\ 0 & \sigma & 1-\sigma \\ 1-\sigma & 0 & \sigma \end{pmatrix}$$

so that the economy in state k will either stay unchanged or move to state $k+1$ (mod 3). We can interpret the three states as follows:

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

– $a_L^3 = 1, a_H^3 = 0$, $\ell_L^3 = q^3 = \pi \min\{(\delta + \phi^3)(1-h), \phi^3\}, \ell_H^3 = 0$

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

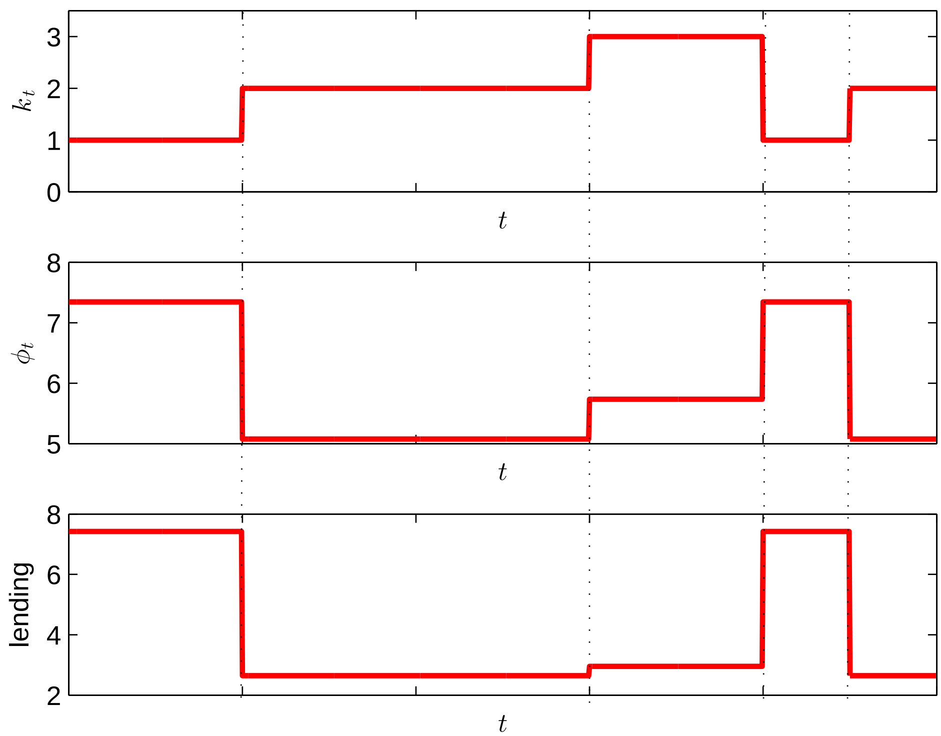
Example 2. Consider the two-point distribution example with $K = 10$ states. We assume the following transition matrix: If the economy is in state k in a given period, in the next period sentiment stays the same with probability σ. From states $k \in \{2, \ldots, K-1\}$ economy moves to state $k-1$ with probability $(1-\sigma)/2$ and to state $k+1$ with probability $(1-\sigma)/2$. From state 1 economy moves to state 2 with probability $1-\sigma$. From state K economy moves to state $K-1$ with probability $1-\sigma$. Figure 10 plots a simulation for 5000 periods when $\sigma = 0.95$ and $\bar{k} = 6$.

5.5 Uniqueness under Flexible Design of Debt limit

We have shown that DeFi lending subject to a rigid haircut can lead to multiplicity when the debt contract is too informationally sensitive. We now show that a flexible contract design can support a unique equilibrium and generate a higher social surplus from lending. Specifically, under flexible design of the smart contract, the design is no longer subject to the constraint (1). Instead, each period, the contract designer can design any feasible debt contract, $y(D, \widetilde{\delta}+\widetilde{s}\phi_t) = \min(D, \widetilde{\delta}+\widetilde{s}\phi_t)$ for $0 \le D \le \delta+\phi_t$. We use $(\widetilde{\delta}, \widetilde{s})$ to emphasize that these are random variables. The designer maximizes

$$\begin{aligned}
V_t = \max_{0 \le D \le \delta+\phi_t} & \lambda\left[\max\left\{\widetilde{z}\mathbb{E}y(D, \widetilde{\delta}+\widetilde{s}\phi_t) - y(D, \delta+\phi_t), 0\right\} + (\delta+\phi_t)\right] \qquad (10) \\
&+ (1-\lambda)\left[\max\left\{\widetilde{z}\mathbb{E}y(D, \widetilde{\delta}+\widetilde{s}\phi_t) - \mathbb{E}y(D, s_L\phi_t), 0\right\} + \int s_L dF(s_L)\phi_t\right],
\end{aligned}$$

Figure 9: Sentiment Equilibrium Example 1



where $y(D, \delta + \phi_t)$ is the value of the debt contract for the borrower who knows that the underlying asset quality is high,

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

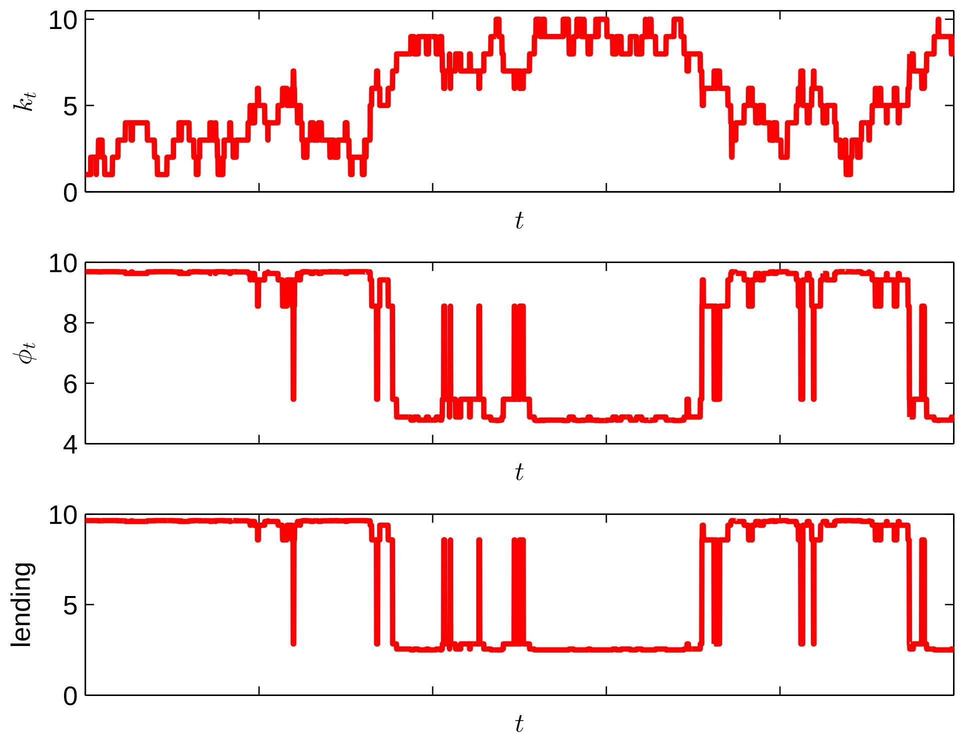
$\mathbb{E}y(D, s_L\phi_t)$ is the value of the debt contract for the borrower who knows that the underlying asset quality is low,

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

$\widehat{z}$ denotes the marginal product of obtaining funding from lenders deducting the intermediation fee f to the intermediary,

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

Figure 10: Sentiment Equilibrium Example 2



$\mathbb{E}y(D, \widetilde{\delta} + \widetilde{s}\phi_t)$ is the total expected value of the debt contract $y(D, \widetilde{\delta} + \widetilde{s}\phi_t)$ for lenders and the intermediary

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

Basically, given the price ϕ_t, the contract designer sets the debt threshold D to maximize the expected value of the contract to the borrower, taking into account how the design affects the funding that the lenders are willing to supply under the separating and the pooling cases. Given the optimal design, the asset price at the end of the previous period equals

$$\phi_{t-1} = \beta V_t. \tag{12}$$

An equilibrium under flexible design of smart contracts is $y(s, \phi_t)$, $q_t(y)$ for all feasible y, V_t, and ϕ_t, that satisfies (10), (11), and (12). The following proposition compares the outcomes under flexible contract design with those under a DeFi lending contract subject to the rigid haircut rule (1).

Proposition 5. *Under flexible optimal debt limit,*

(i) there exists a unique stationary equilibrium.

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

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

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

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

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

5.5.1 A Simple Example

In the example with a two-point distribution, the optimal flexible debt limit depends on parameter values. As shown in the Appendix, when $\pi < \zeta$, the pooling equilibrium does not exist. It is thus optimal for the intermediary to set $D_t^S = \phi_t$ to support a separating equilibrium. When $\pi \geq \zeta$, the pooling equilibrium exists and dominates the separating one. The intermediary's optimal choice is to set

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

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

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

6 Some Evidence

Here we report some evidence to support the case that our model can be useful for understanding the relationship between DeFi lending, crypto prices and market sentiment. We also discuss some evidence where borrowers pledged inflated collateral assets to obtain loans from lending protocols which later suffered big financial losses due to the bad debt.

6.1 Effects of DeFi Lending on ETH Price

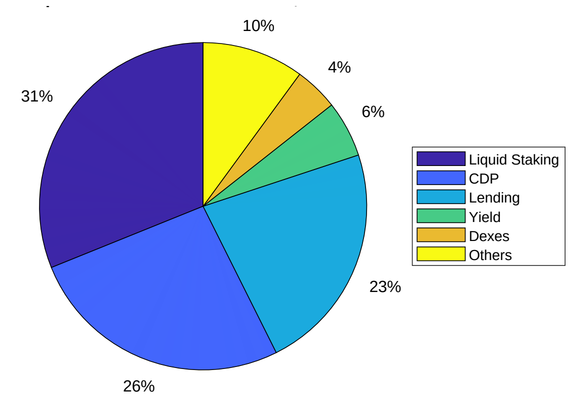
Our model predicts that DeFi lending should be positively correlated with crypto prices due to the price-liquidity feedback loop. Since the Ethereum blockchain is the main platform for DeFi, we use WETH TVL data from DeFiLlama to test this hypothesis. The sample is from 2018 January to 2022 March. Figure 11 shows that lending accounts for about 23% of DeFi TVL. We run an OLS

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

where $ETHP$ is the price of ETH, $LTCP$ is the price of Litecoin (LTC), $BURN$ is the amount of ETH burned since the London Fork as a percentage of ETH supply, $DEFI$ is the fraction of WETH locked into DeFi protocols, and $LEND$ is the fraction of WETH locked into DeFi lending. Since Litecoin has limited use in DeFi, we use its price to capture non-DeFi factors that can influence the price of ETH.

As expected, results in Table 2 suggests that the prices of ETH and LTC are highly correlated. Also, unsurprisingly, by removing tokens from the circulating supply, BURN has a positive effect on the ETH price. Finally, after controlling for the general effects of DeFi on the price of ETH, TVL in DeFi lending is still positively correlated with the price of ETH, consistent with the prediction of our model.

Figure 11: Composition of WETH TVL in DeFi (March 2022)



Data Source: DefiLlamma.

Table 2: **DeFi Lending and Crypto Prices**

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

6.2 Collateral Composition and Market Sentiment

Our model predicts that good market sentiment can help mitigate adverse selection, improving the quality of the collateral pool. We use the Aave platform data to examine the relationship between collateral composition and market sentiment. The market sentiment are measured by the "Crypto Fear & Greed Index" (FGI) for Bitcoin and other large cryptocurrencies.[16] The construction of the Index is based on measures of market volatility, market momentum/volume, social media, surveys, token dominance and Google Trends data. The Index is supposed to measure the emotions and sentiments from different sources, with a value of 0 indicating "Extreme Fear" while a value of 100 indicating "Extreme Greed". Since Aave does not provide collateral data, we need to use outstanding deposits of collateralizable tokens as a proxy. Basing on their internal risk assessment, Aave assigns risk ratings to each token ranging from C+ to A+. We use these risk parameters to measure the quality of these assets. Figure 12 shows how the composition changes over time. Note that tokens have different USD prices. Hence, changing prices will affect their (nominal) shares in the pool. To remove the effects of token price changes on the composition, we fix their prices at the median level over the sample period (Jan 2021- April 2022). So the results derived below capture only variations in token quantities and not in their prices.

Figure 12: Composition of Collateralizable Asset Mix

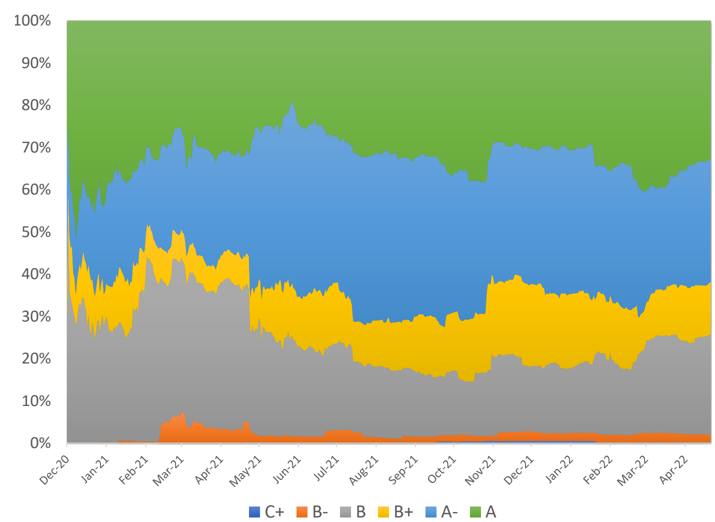


Figure Source: Dune Analytics

We study how sentiment is related to the overall quality of the collateral pool proxied by the weighted average of the ratings of all outstanding collateralizable deposits.[17] We run an OLS regressing log(Rating) on a dummy and log(FGI) as follows

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

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

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

where Dummy=1 for days after April 26. We report the result in Table 4. Both variables are significant, suggesting that the average rating of the collateral mix goes up when the sentiment captured by the FGI is high, as predicted by our model.

Figure 13: Effects of FG Index on Average Risk Rating

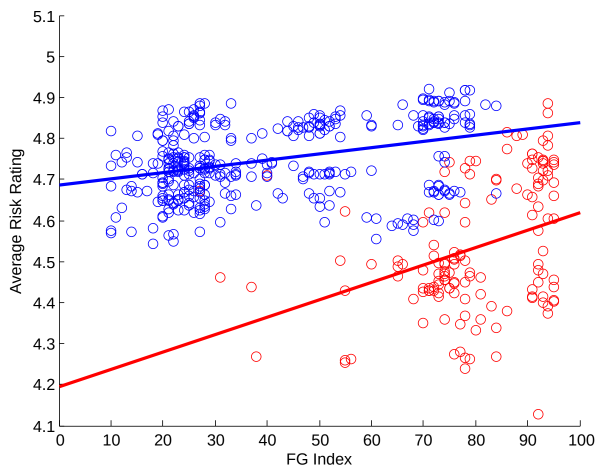


Figure Source: Dune Analytics

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

Table 3: **Sentiment and Collateral Rating**

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

6.3 Price Exploits

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

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

7 Conclusion

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

References

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

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

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

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

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

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.

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.

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

A Appendix

A.1 Proof of Proposition 1

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

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

which is equivalent to

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

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

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

A.2 Proof of Proposition 2

First, we define functions

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

Note that their difference is

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

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

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

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

which have the following properties:

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

and the difference between the two functions is

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

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

A.3 Proof of Proposition 3

Separating equilibrium

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

Debt limit:

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

Loan size:

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

Asset price:

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

Existence of separating equilibrium:

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

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

Debt limit:

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

Loan size:

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

Asset price:

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

Existence of separating equilibrium:

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

Hence, a separating equilibrium exists when

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

Pooling equilibrium

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

Debt limit:

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

Loan size:

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

Asset price:

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

Existence of pooling equilibrium:

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

As $h \to 0$, we have

Debt limit:

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

Loan size:

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

Asset price:

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

Existence of pooling equilibrium:

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

Hence a pooling equilibrium exists when

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

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

A.4 Two-point Distribution Example

A.4.1 Separating Equilibrium

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

In a separating equilibrium:

Debt limit:

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

Loan size:

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

There are two cases.

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

This is true when

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

We then have

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

The existence of separating equilibrium requires

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

We define a threshold

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

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

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

This is true when

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

We then have

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

The existence of separating equilibrium requires

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

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

A.4.2 Pooling Equilibrium

In a pooling equilibrium:

Debt limit:

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

Loan size:

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

There are two cases.

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

This is true when

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

We then have

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

The existence of separating equilibrium requires

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

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 pooling equilibrium requires

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

A.5 Proof of Uniqueness Under a Flexible Smart Contract

Denote the debt contract $y(D, \widetilde{\delta}+\widetilde{s}\phi) = \min(D, \widetilde{\delta}+\widetilde{s}\phi)$. Denote D^* the maximum face value so that the incentive constraint of the high type borrower is satisfied

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

in which case there is a pooling equilibrium. If the adverse selection is sufficiently severe, $D < \delta+\phi$.

The designer chooses D to maximize V_{t+1} taking as given $q_{t+1}(y)$ and ϕ_{t+1}. If the designer chooses to design a contract that leads to a pooling outcome, then $D = D^*$. If the designer chooses to design 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 $\bar{s}^* = D^*/\phi$. In this case, all terms in the IC constraint for H type are proportional to the asset price ϕ, which drops out of the constraint. So, the high type's incentive constraint is satisfied iff

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

Define the LHS-RHS as a function of $\bar{s}$, $\mathcal{F}(\bar{s}) \equiv \widehat{z}\left[\lambda\mathbb{E}_L\min(\bar{s},s)+(1-\lambda)\bar{s}\right] - \bar{s}$. The function has the following property:

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

So $\mathcal{F}(\bar{s})$ is concave and positive when $\bar{s}$ is close to 0. If the information friction is severe enough so that $\mathcal{F}(1) = \widehat{z}(\lambda\mathbb{E}_L s + 1-\lambda) - 1 < 0$, or equivalently $\mathbb{E}_L s < \frac{1-(1-\lambda)\widehat{z}}{\lambda\widehat{z}} = 1 + \frac{1}{\lambda\widehat{z}} - \frac{1}{\lambda} < 1$, the inequality is violated at $\bar{s} = 1$, and there exists a unique threshold $0 < \bar{s}^* < 1$ such that the inequality holds with strict equality, $\mathcal{F}(\bar{s}^*) = 0$. Since the asset price ϕ drops out, threshold $\bar{s}^*$ does not depend on ϕ.

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

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

which has the following property

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

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

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

If information friction is not so severe so that $\mathcal{F}(\bar{s}) > 0$ for all $\bar{s} \leq 1$, or equivalently, $1 > \mathbb{E}_L s > 1 + \frac{1}{\lambda \widehat{z}} - \frac{1}{\lambda}$, the face value of the debt is $D^* \geq \phi$. In this case, denote the optimal deisgn under pooling equilibrium to be $d^* + \phi = D^*$, $d^* \geq 0$.

The high type has the incentive to sell iff

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

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

If the information friction is severe enough, $d^* \leq \frac{\widehat{z}[\lambda \mathbb{E}_L s + (1 - \lambda)]}{1 - \widehat{z}(1 - \lambda)} \phi < \delta$, so the maximum d^* equals

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

where $\frac{\widehat{z}[\lambda \mathbb{E} s + (1 - \lambda)]}{1 - \widehat{z}(1 - \lambda)} \phi < \delta$.

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

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

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

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

When ϕ is large enough so $\frac{\widehat{z}[\lambda \mathbb{E}_L s + (1 - \lambda)]}{1 - \widehat{z}(1 - \lambda)} \phi > \delta$,

$$d^* = \delta$$

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

Because $\frac{\lambda}{\lambda-(\widehat{z}-1)(1-\lambda)} > 1$, $\phi^P(\phi)$ is concave with slope less than 1 when $\frac{\widehat{z}[\lambda\mathbb{E}_L s+(1-\lambda)]}{1-\widehat{z}(1-\lambda)}\phi > \delta$.

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

So in this case when $\mathbb{E}_L s > 1 + \frac{1}{\lambda\widehat{z}} - \frac{1}{\lambda}$, we can focus on analyzing the pooling equilibrium. From the analysis above, $\phi^P(\phi)$ is concave with slope less than 1 when $\frac{\widehat{z}[\lambda\mathbb{E}_L s+(1-\lambda)]}{1-\widehat{z}(1-\lambda)}\phi > \delta$. So 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 the optimal contract conditional on supporting a pooling equilibrium has a face value less than asset price, $D^* < \phi$, or equivalently

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

If the optimal contract supports a separating equilibrium, the designer would choose $D = \delta + \phi$ to maximize gains from lending to the low type. Because both the low type borrower and lenders expect the high type not to borrow, the low type chooses the maximum face value to maximize borrowing. In the special parametrization of the model, any face value between ϕ and $\delta + \phi$ generates the same revenue from borrowing because a low quality asset does not pay any dividend. More generally, low quality assets could pay positive dividend. So the maximum face value $D = \delta + \phi$ is a more robust form of debt design in the separating case.

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

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

Note that condition (A.3) implies that

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

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

In a separating equilibrium, the asset price

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

which has the following property

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

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

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

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

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

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

In either case, the equilibrium is unique.

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

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

when condition (A.6) holds. Otherwise, the equilibrium contract is a separating one with face value $D = \delta + \phi$. When $\mathbb{E}_L s > 1 + \frac{1}{\lambda\widehat{z}} - \frac{1}{\lambda}$, the equilibrium contract is a pooling one with face value $D = d + \phi$ where

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

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

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

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

Separating equilibrium

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

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

So the optimal debt limit is

$$D^S = \phi_t.$$

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

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

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

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

implying a unique fixed point

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

Pooling equilibrium

In a pooling equilibrium,

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

the optimal debt limit is the maximum value that satisfies

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

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

The solution solves

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

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

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

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

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

This happens when

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

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

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

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

Given this debt policy, the loan size is

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

and the asset price in the previous period is given by

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

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

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

implying a unique fixed point.

Optimal debt limit

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

$$D_t^S = \phi_t.$$

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

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

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

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

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

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 χ is sufficiently close to 1.

A.8 An Alternative Setup with Unobservable Private Valuation

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

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

The debt limit is given by $D = (\delta + \phi)(1 - h)$. We assume that $v > \delta$. As a result, all borrowers repay in the good state. Low type borrowers 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 multipicity result.

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

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

B More Details about Aave Lending Protocol

B.1 Tokens

Aave issues two types of tokens: (i) aTokens, issued to lenders so they can collect interest on deposits, and (ii) AAVE tokens, which are the native token of Aave.[18] **aTokens** are interest-bearing tokens that are minted upon deposit and and burned at withdraw. The aTokens' value is pegged to the value of the

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

corresponding deposited asset at a 1:1 ratio, and can be safely stored, transferred or traded. Withdrawals of the deposited assets burns the aTokens. **AAVE tokens** are used to vote and influence the governance of the protocol. AAVE holders can also lock (known as "staking") the tokens to provide insurance to the protocol/depositors and earn staking rewards and fees from the protocol (more details below).

B.2 Deposits and loans

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

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

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

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

where $U = Total\ Borrows/Total\ Liquidity$ is the share of the liquidity borrowed.[19]

The **variable rate** is the rate based on the current supply and demand in Aave. **Stable rates** act as a fixed rate.[20] The current model parameters for stable and variable interest rates are given in Figure 14. Figure 15 shows Dai's rate schedule as an example.

The **deposit rate** is given by

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

where SB_t is the share of stable borrows, S_t is average stable rate, VB_t is the share of variable borrows, V_t is average variable rate, R_t is the reserve factor (a fraction of interests allocated to mitigate shortfall events discussed below). The **Loan to Value** (LTV) ratio defines the maximum amount that can be

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

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

Figure 14: Current Rate Parameters

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

Table Source: Aave.com

borrowed with a specific collateral. It's expressed in percentage: at $LTV = 75\%$, for every 1 ETH worth of collateral, borrowers will be able to borrow 0.75 ETH worth of the corresponding currency of the loan. The current risk parameters are given in Figure 16.

B.3 Collateral and Liquidation

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

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

Figure 15: Stable vs Variable Rates for Dai

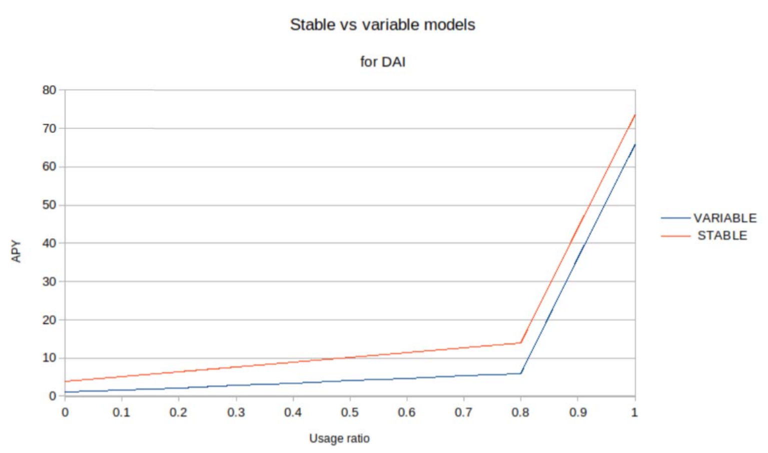


Figure Source: Aave.com

The difference between the LTV and the LQ is a safety cushion for borrowers. The values of assets are based on **price feed** provided by Chainlink's decentralized oracles. The LQ is also called the **health factor** *(Hf)*. When $Hf < 1$, a loan is considered undercollateralized and can be liquidated. When the health factor of a position is below 1, **liquidators** repay part or all of the outstanding borrowed amount on behalf of the borrower, while receiving an equivalent amount of collateral in return plus a liquidation "bonus" (see Figure 16).[21] When the liquidation is completed successfully, the health factor of the position is increased, bringing the health factor above 1.

B.4 Shortfall Event

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

[21] Example: Bob deposits 5 ETH and 4 ETH worth of YFI, and borrows 5 ETH worth of DAI. If Bob's Health Factor drops below 1 his loan will be eligible for liquidation. A liquidator can repay up to 50% of a single borrowed amount = 2.5 ETH worth of DAI. In return, the liquidator can claim a single collateral, as the liquidation bonus is higher for YFI (15%) than ETH (5%) the liquidator chooses to claim YFI. The liquidator claims 2.5 + 0.375 ETH worth of YFI for repaying 2.5 ETH worth of DAI.

Figure 16: Current Risk Parameters

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

Table Source: Aave.com

issuance of AAVE known as Safety Incentives (SI)) and fees generated from the protocol (see reserve factor above).

B.5 Recovery Issuance

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

C Volatility of Collateral Value

Table 4: The Volatility of Collateral Value (January 2021 - April 2022)

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

Source: CoinGecko.