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

May 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 makes crypto prices more sensitive to fundamental shocks, and asset prices and lending activities can fluctuate 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 and many conference participants for their valuable comments and suggestions. We also 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

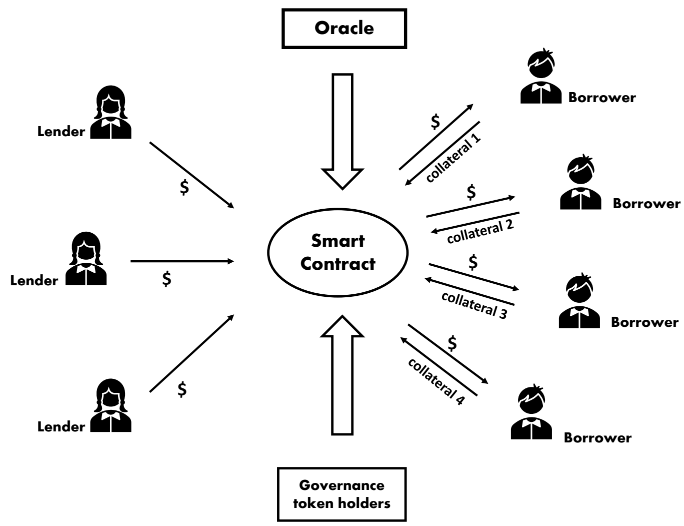
Decentralized finance (DeFi) is an umbrella term for a variety of financial service protocols and applications (e.g., decentralized exchanges, lending platforms, asset management) on blockchain. These are anonymous permissionless financial arrangements that aim to replace traditional intermediaries by 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 governed by holders of governance tokens in a decentralized fashion.

[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.

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 (Forthcoming)). 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 asset prices, which help us understand how information frictions and smart contract rigidity contribute

[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.

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 setupin 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	**Compround**	**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

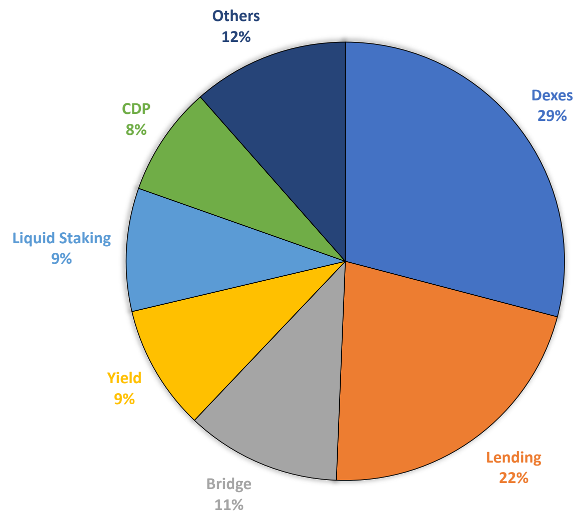
Data Source: DefiLlamma; Aavewatch; Compound.finance; Venus.io; Glassnode.

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:

Key players. The Aave eco-system consists of different players. Depositors can deposit a crypto

[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.

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 5 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 to the protocol, token holders need to make proposals, discuss with the community, and obtain enough

[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.

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

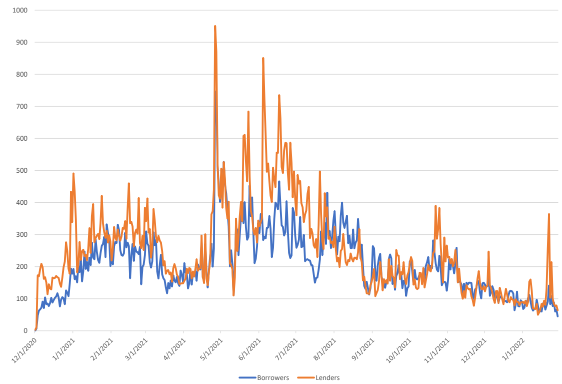
The economy is set in discrete time and lasts forever.[8] There are many infinitely-lived borrowers with identical preferences and access to the same information. We refer to a representative borrower as agent B. There are many crypto assets. Each borrower can hold at most one unit. There are also potential lenders who live for a single period and are replaced every period. 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.

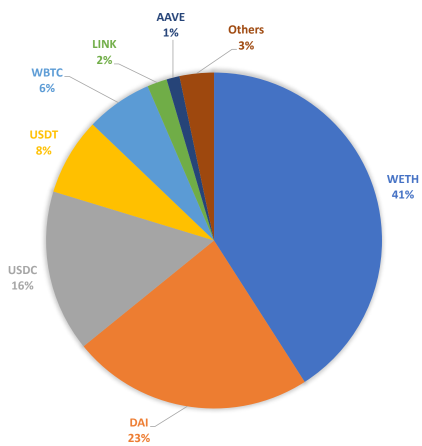
[8] In reality, interest payment on the borrowing in the lending protocols is continuously compounded and can be terminated at any time. Therefore, we can interpret that each time period in our model is relatively short.

(a) Total Value (USD) Locked in Aave

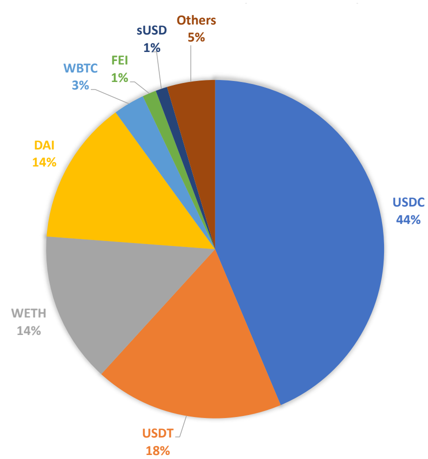


(b) Number of Unique Users per Day

Figure 3: Aave v2 TVL and Users Over time

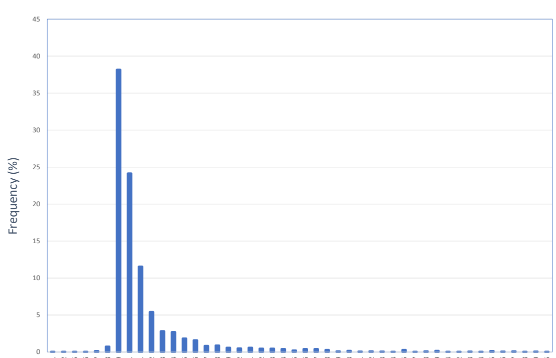


(a) Avg. Deposit Composition (Jan 2021-Jan 2022)

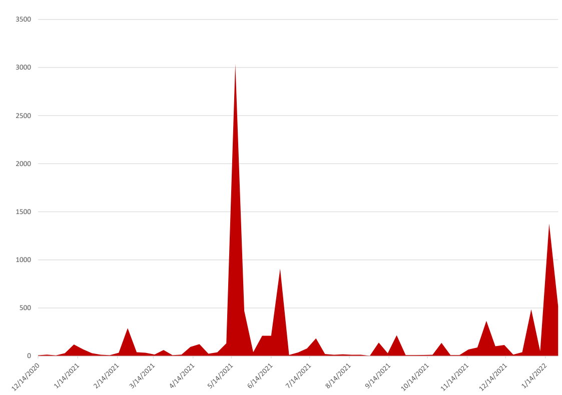


(b) Avg. Loan Composition (Jan 2021-Jan 2022)

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 Agent B has a need for funding that can be provided by agent Ls. There are gains from trade as the value per-unit of funding to agent B is $z > 1$, while the per-unit cost of providing funding by agent Ls is normalized to one. At the end of the period, agents B 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, 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. Collateral is locked and released if and only if a repayment is received. With a pre-programmed contract replacing human beings, incentive problems can be avoided.

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 these stablecoins 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 each yields a random, idiosyncratic payoff at the end of period t which we denote as $s_t \in [0, 1]$. The payoff state, s_t, 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). We assume that s_t is distributed according to probability distribution F_Q where $Q \in \{L, H\}$ denotes the quality of the asset. Quality $Q_t = L$ with probability $\lambda \in (0, 1)$ and draw i.i.d. at the beginning of the each period. Therefore, crypto assets with a larger λ have lower average quality. As there are many crypto assets, each period fraction λ of the assets are of $Q = L$.[10]

We denote the density of F_Q by f_Q and its survival function, $1 - F_Q(s)$, by $\widetilde{F}_Q(s)$. We assume both distributions have strictly positive density in their domain $[0, 1]$, and F_H stochastically dominates F_L according to the likelihood ratio, i.e., $f_L(s)/f_H(s)$ is decreasing in $s \in [0, 1]$.

At the beginning of each period, the borrower of a crypto asset privately learns the asset's quality in that period. The asset's quality and the state are both publicly revealed at the end of each period. For

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

[10] An alternative interpretation of the model is that there is only one crypto asset but the quality Q changes each period.

simplicity, we assume that the asset quality is i.i.d., past quality does not provide any information about the future. Allowing persistent shock will not affect the main results of the paper. 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. The end-of-period ex-payoff price of a crypto asset in period t is denoted as ϕ_t. Each borrower can hold at most one unit of crypto asset. The dynamic structure is based on Lagos and Wright (2005).

DeFi Debt At the beginning of the period, the smart contract is updated before he receives information about the asset quality. The contract, $y(s, \phi_t)$, promises a payment at the end of each period backed by payoff and the price of the crypto asset. As discussed, DeFi lending typically uses a debt contract: $y(s, \phi_t) = \min(s_t + \phi_t, D)$ where $D \in [\underline{s} + \phi_t, \bar{s} + \phi_t]$ denotes the debt threshold. The amount of borrowing, that is, the size of the loan per unit of collateral pledged, q_t, is determined by the zero profit condition on the lenders discussed below. The design chooses the largest possible face value of the debt subject to the constraint that the loan size cannot exceed the value of the pledged crypto asset discounted by a haircut h:

$$D = \max\{\widetilde{D} : q_t(\widetilde{D}) \leq \frac{E_t\left[s; \widetilde{D}\right] + \phi_t}{1+h}\} \tag{1}$$

As shown below, q_t and $E_t[s]$ depend on the mix of borrowers choosing to borrow from the contract after observing the asset quality, which in turn depends on the choice of D.

After observing the asset quality, agent B raises funding from a DeFi protocol by executing the smart contract. We denote by $a_{it,Q}$ the quantity of collateral a borrower pledges when the the crypto asset that backs the debt is of quality Q. Quantities pledged by each type must be optimal given the price, i.e., for each $Q \in \{L, H\}$,

$$a_{t,Q} \in \arg\max_{a \in [0,1]} a\left(zq_t - E_Q y_t\left(s, \phi_t\right)\right). \tag{2}$$

Note that the choice a is quality dependent, meaning that lenders face adverse selection in the DeFi lending market. The loan size q does not depend on the underlying asset quality because lenders are not able to distinguish between low and high quality when they compete to offer the loan. Of course, in equilibrium, lenders take into account the average quality of the collateral mix backing the loan.

Formally, the price of contract $y(s, \phi_t)$ is given by:

$$q_t = \frac{1}{1+r} \left\{ \frac{1}{a_{t,L}\lambda + a_{t,H}(1-\lambda)} \left[a_{t,L}\lambda E_L y_t(s,\phi_t) + a_{t,H}(1-\lambda) E_H y_t(s,\phi_t) \right] \right\} \tag{3}$$

where r is the rate of return lenders expect to make on the loan which is determined by lenders' outside alternatives. For now, we assume $r = 0$. If the quality Q were known, the lender would expect a return $E_Q y$ from the debt contract y. Since Q is not known, the lender's expected return on the RHS is given by the weighted average derived according to the equilibrium mix of borrowers. Competition then implies that the equilibrium loan size q offered by lenders is equal to the expected return.

Similarly, the expected value of dividend in (1) equals

$$E_t[s] = \left[a_{t,L}\lambda E_L s + a_{t,H}(1-\lambda) E_H s \right] / \left(a_{t,L}\lambda + a_{t,H}(1-\lambda) \right).$$

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

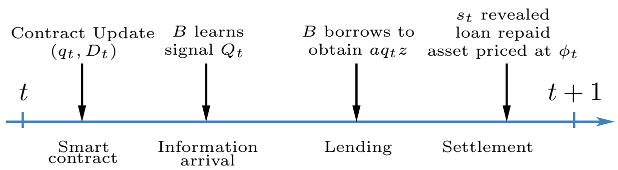
$$\begin{aligned} \phi_t = \beta \Bigg\{ \lambda \left[\int_{\underline{s}}^{\bar{s}} \left(a_{t+1,L}\left(zq_{t+1} - y_{t+1}(s,\phi_{t+1,})\right) + (s+\phi_{t+1}) \right) dF_L(s) \right] \\ + (1-\lambda) \left[\int_{\underline{s}}^{\bar{s}} \left(a_{t+1,H}\left(zq_{t+1} - y_{t+1}(s,\phi_{t+1})\right) + (s+\phi_{t+1}) \right) dF_H(s) \right] \Bigg\}, \end{aligned} \tag{4}$$

where β is the discount factor, $0 < \beta < 1/z$. The asset price is determined by the collateral value of the asset in the future, which in turn depends on the extent of asymmetric information in future DeFi lending markets. Specifically, the continuation value of an asset depends on the information state Q in the next period. Given Q, the value of the asset is simply the sum of the collateral value $E_Q a_Q(zq - y)$, the expected dividends $E_Q s$, and the resale value ϕ.

Timing In each period, lenders compete to lend to borrowers via the smart contract subject to the haircut rule, determining q and D. Agent B receives private information and decides whether to borrow by pledging collateral to the smart contract. Once borrowing is done, both Q and s_t are revealed and the asset price is determined. Finally, agent B repays the lenders or defaults and loses the collateral, and consumption takes place. At the end of the period, agent B can work to buy at most one unit of the crypto asset. Figure (6) shows the timeline.

To summarize, given haircut h, an equilibrium consists of asset prices $\phi_{t,}$, debt thresholds D_t, loan size q_t and collateral quantities $\{a_{t,L}, a_{t,H}\}$ that solves equations (2)-(4).

Figure 6: Timeline



4 Equilibrium in Lending Market

We begin the analysis by describing the equilibrium in the DeFi lending market.[11] To study the borrowers' decision, we first define the degree of *information insensitivity* as the ratio of the expected value of the debt under the low versus the high distribution, i.e., $E_L y(s, \phi)/E_H y(s, \phi)$. Note that a debt contract $y(s, \phi) = \min\{s + \phi, D\}$ has the property that $E_L y(s, \phi) \leq E_H y(s, \phi)$. As this ratio increases, the expected values of the debt under the low versus high distribution become closer, and the adverse selection problem becomes less severe.

We assume that lenders are strategic and compete à la Bertrand which ensures that equilibrium in the DeFi market is generically unique. That is, lenders simultaneously make offers in terms of q taking into account which types of borrower would borrow. Agent B observes these offers, and decides how much of the collateral to be pledged to back the loan.[12] Due to Bertrand competition, lenders make zero surplus in expectation, and the equilibrium q is given by (3). The quantities sold by each type of agent B, a_Q, is optimal for that type and satisfies (2). The next proposition characterizes the equilibrium in the DeFi lending market.

Proposition 1. *If* $E_L y(s, \phi)/E_H y(s, \phi) > \zeta \equiv 1 - (z-1)/(\lambda z)$, *then* $q = \lambda E_L y(s, \phi) + (1-\lambda) E_H y(s, \phi)$ *and* $a_L = a_H = 1$. *If* $E_L y(s, \phi)/E_H y(s, \phi) < \zeta$, *then* $q = E_L y(s, \phi)$, $a_L = 1$ *and* $a_H = 0$.[13]

Proposition 1 implies that the equilibrium features a pooling (separating) outcome when the debt contract is sufficiently informationally insensitive (sensitive). In particular, when $E_L y(s, \phi)/E_H y(s, \phi)$ 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 $q = \lambda E_L y(s, \phi) + (1-\lambda) E_H y(s, \phi)$. When $E_L y(s, \phi)/E_H y(s, \phi)$ 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 $q = E_L y(s, \phi)$. As the implicit interest rate is given by

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

[12] In this formulation agent B has all the bargaining power, but this is not crucial for any of our results.

[13] When $E_L y/E_H y = \zeta$, there are multiple equilibria. In particular, both pooling and separating (and even semi-separating) equilibria are possible. To simplify exposition in this knife edge case, we select the pooling equilibrium.

D/q, a loan traded in a pooling equilibrium requires a lower interest payment for the borrower than one traded at the separating equilibrium. The above proposition also indicates that in addition to the parameters that characterize type heterogeneity, the gains from trade parameter, z, is also an important determinant of adverse selection: a lower z 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 $E_L y(s,\phi)/E_H y(s,\phi)$ is slightly below 1, as z approaches 1 (so that ζ is close 1), the DeFi lending will be in a separating equilibrium. In other words, when 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

In this section, we demonstrate that this economy is fragile and 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 themselves justified by the different equilibria in the DeFi lending. We first solve the equilibrium for a debt contract collateralized by a generic crypto asset.

Given the debt contract $y(s,\phi_t) = \min(s_t + \phi_t, D)$ where $D = \delta + \phi_t$. We will see below that the haircut rule (1) will be binding in equilibrium (i.e., $q_t^Q = \frac{E_Q s + \phi_{t.}}{1+h}$). By Proposition 1 and (1), the loan size is given by $q_t^P = \frac{\lambda E_L s + (1-\lambda) E_H s + \phi_t}{1+h}$ if $(E_L y)/(E_H y) \geq \zeta$ and $q_t^S = \frac{E_L s + \phi_{t.}}{1+h}$ otherwise. Using (4), we obtain the price of the collateral asset in the asset market as

$$\phi_t = \begin{cases} \beta \left[(z+h)\, q_{t+1}^P \right] & \text{if } \frac{E_L y}{E_H y} \geq \zeta, \\ \beta \left[\lambda\, (z+h)\, q_{t+1}^S + (1-\lambda)\, (E_H s + \phi_{t+1}) \right] & \text{if } \frac{E_L y}{E_H y} < \zeta. \end{cases} \tag{5}$$

Intuititively, in a pooling outcome, all assets are collateralized to obtain DeFi loans. In a separating outcome, only assets held by the low type are collateralized while those held by the high type remain idle.

Next, we characterize stationary equilibria where DeFi lending is either always traded in a pooling equilibrium, or it is always in a separating equilibrium. Since we are focusing on stationary equilibria we drop the time subscripts.

5.1 Pooling Equilibrium

Plugging q^P into (5) we observe that a pooling equilibrium, in which both types of agent B borrow in the lending market, exists if and only if

$$\frac{E_L \min(\delta, s) + \phi^P}{E_H \min(\delta, s) + \phi^P} \geq \zeta, \tag{6}$$

where the asset prices in the pooling equilibrium are given by

$$\phi^P = \beta\,(z+h)\left(\frac{\lambda\left(E_L s + \phi^P\right) + (1-\lambda)\left(E_H s + \phi^P\right)}{1+h}\right).$$

Solving for the pooling prices we obtain the equilibrium asset price

$$\phi^P = \frac{\beta\,(z+h)\,(\lambda E_L s + (1-\lambda) E_H s)}{1+h-\beta\,(z+h)}. \tag{7}$$

By plugging (7) into (6) we see that a pooling equilibrium exists if and only if the high type borrowers have incentives to borrow:

$$\zeta \int_0^\delta \widetilde{F}_H\,(s)\,ds - \int_0^\delta \widetilde{F}_L\,(s)\,ds \leq (1-\zeta)\,\frac{\beta\frac{z+h}{1+h}}{1-\beta\frac{z+h}{1+h}}\,(\lambda E_L s + (1-\lambda) E_H s)$$

where the debt threshold $D = \phi + \delta$ is pinned down by the lender's break even condition:

$$q^P = \lambda \int_0^\delta \widetilde{F}_L(s)ds + (1-\lambda)\int_0^\delta \widetilde{F}_H(s)ds + \phi = \frac{\lambda E_L s + (1-\lambda) E_H s + \phi}{1+h}.$$

The first equality is derived from (2) while the second equality is implied by the haircut rule (1), where δ is set to make it binding.

5.2 Separating Equilibrium

A separating equilibrium, in which only the low type of agent B borrows in the DeFi lending market, exists if and only if

$$\frac{E_L \min(\delta, s) + \phi^S}{E_H \min(\delta, s) + \phi^S} < \zeta, \tag{8}$$

where the asset prices in the separating equilibrium are given by,

$$\phi^S \quad = \quad \beta\left(\frac{\lambda\,(z+h)\left(E_L s + \phi^S\right)}{1+h} + (1-\lambda)\left(E_H s + \phi^S\right)\right),$$

Solving for the separating price we obtain:

$$\phi^S \quad = \quad \frac{\beta\frac{z+h}{1+h}\lambda E_L s + \beta(1-\lambda) E_H s}{1-\beta(\lambda\frac{z+h}{1+h} + 1 - \lambda)} \tag{9}$$

By plugging (9) into (8) we see that a separating equilibrium exists if and only if the high type borrowers choose not to borrow:

$$\zeta \int_0^{\delta} \widetilde{F}_H(s)\, ds - \int_0^{\delta} \widetilde{F}_L(s)\, ds > (1-\zeta)\, \frac{\beta \frac{z+h}{1+h} \lambda E_L s + \beta(1-\lambda) E_H s}{1 - \beta(\lambda \frac{z+h}{1+h} + 1 - \lambda)}$$

where the debt threshold $D = \phi + \delta$ is again pinned down by the lender's break even condition:

$$q^S = \int_0^{\delta} \widetilde{F}_L(s) ds + \phi = \frac{E_L[s] + \phi}{1+h}.$$

5.3 Properties of Equilibria and Multiplicity

We first discuss the effects of DeFi lending on asset prices by rewritting them as multiples of the fundamental price of the asset in autarky, $\underline{\phi} = \beta \frac{\lambda E_L s + (1-\lambda) E_H s}{1-\beta}$:

$$\phi^P = \Psi^P(z,h) \cdot \underline{\phi}$$
$$\phi^S = \Psi^S(z,h) \cdot \underline{\phi}$$

where the multipliers are given by

$$\Psi^P(z,h) = \frac{(z+h)(1-\beta)}{1+h-\beta(z+h)},$$
$$\Psi^S(z,h) = \frac{1 + \frac{z-1}{1+h} \frac{\lambda s_L}{\lambda s_L + (1-\lambda) s_H}}{1 - \lambda \frac{\beta}{1-\beta} \frac{z-1}{1+h}},$$

Since $\Psi^P \geq \Psi^S \geq 1$, the introduction of DeFi lending raises the equilibrium asset price above its fundamental level. In addition, DeFi lending can increase the volatility of asset prices when there are shocks to fundamentals. First, it magnifies fundamental shocks to ϕ^0 (e.g., $E_L s$, $E_H s$). Second, it introduces new DeFi specific shocks, e.g., asset price goes up with a rise in z and a drop in h. Note that, the multipling effects exist even without adverse selection (i.e., $F_L = F_H$).

We now demonstrate that, subject to adverse selection, DeFi lending is inherently fragile in the sense there are belief-driven multiple equilibria. The following proposition shows that there is always a range of parameters such that, if the haircut is not high enough, then multiple equilibria exist.

Proposition 2. *Let* $\kappa_P = \frac{\zeta - \beta z(1-(1-\zeta)\lambda)}{1-\beta z(1-(1-\zeta)\lambda)}$ *and* $\kappa_S = \frac{\zeta - \beta(1-(1-\zeta z)\lambda)}{1-\beta(1-(1-\zeta z)\lambda)}$.

(i) If $E_L s / E_H s \geq \kappa_S$*, then there is a unique equilibrium with the pooling outcome and the collateral price given by (7).*

(ii) If $\kappa_S > E_L s/E_H s > \kappa_P$ *and* $h < \overline{h}$ *(where* $\overline{h}$ *depends on the primitives) then there are multiple equilibria. One of them is a separating equilibrium with the collateral price given by (9). The other one*

is a pooling equilibrium with the collateral price given by (7). If $h \geq \overline{h}$ then there is a unique equilibrium with the pooling outcome and the collateral price given by (7).

(iii) If $\kappa_P \geq E_L s/E_H s$ and if $h < \overline{h}$ (where $\overline{h}$ depends on the primitives) then there is a unique equilibrium with the separating outcome with the collateral price given by (9). If $h \geq \overline{h}$ then there is a unique equilibrium with the pooling outcome and the collateral price given by (7).

To understand this proposition, we first start with the case where the haircut is zero. In that case, the equilibrium conditions imply that a pooling equilibrium exists when $E_L s/E_H s \geq \kappa_P$, and a separating equilibrium exists when $E_L s/E_H s \leq \kappa_S$. We show in the appendix that $\kappa_P < \kappa_S$ which, by continuity, implies multiplicity for $E_L s/E_H s \in (\kappa_P, \kappa_S)$ when h is sufficiently low. Multiple equilibria in part (ii) arise due to a dynamic price feedback effect. When the collateral asset price is high, the degree of information insensitivity of the debt contract, $\left(E_L s + \phi^P\right) / \left(E_H s + \phi^P\right)$, is above the threshold ζ. Hence, the adverse selection problem is mild and the high-type agent B is willing to pool with the low type and borrow in the lending market. In turn, if agents anticipate a pooling equilibrium in future periods, the liquidity value of the asset 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, $\left(E_L s + \phi^S\right) / \left(E_H s + \phi^S\right)$, is below the threshold ζ. Therefore, the adverse selection problem is severe and the high type agent B 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.

In region (ii) 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)). In particular, equilibrium asset prices ϕ^k, debt thresholds D^k, loan sizes q^k will all fluctuate with the sentiment state indexed by $k \in \{1, ..., K\}$ which evolves over time subject to stochastic transitions. With a sufficiently low haircut and sentiments sufficiently persistent, one can construct a sentiment equilibrium in which the economy switches between separating and pooling outcomes according to non-fundamental sunspot states.

The above proposition suggests that increasing the haircut can ameliorate the above feedback loop, restoring uniqueness. When the haircut is high, debt threshold is low, making the debt contract less informationally sensitive. This means that high quality asset owner retains some of the upside from the collateral asset. As a result, high quality borrowers may be willing to borrow, eliminating the separating equilibrium. However, imposing a high haircut is costly because borrowers can borrow less from the lenders, reducing the surplus from DeFi lending. The optimal debt threshold is set to balance this trade-off and is examined in the next section.

5.4 Uniqueness under Flexible Design of Smart Contracts

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, $y(s,\phi_t) = \min(D, s+\phi_t)$ for $0 \le D \le \bar{s}+\phi_t$ to maximize

$$V_t = \max_{0\le D\le \bar{s}+\phi_t} \lambda \left[\int_{\underline{s}}^{\bar{s}} \left(\max\{zq_t - y(s,\phi_t), 0\} + (s+\phi_t)\right) dF_L(s)\right] \\ + (1-\lambda)\left[\left(\int_{\underline{s}}^{\bar{s}} \max\{zq_t - y(s,\phi_t), 0\} + (s+\phi_t)\right) dF_H(s)\right], \tag{10}$$

where

$$q_t = E_t y(s,\phi_t) \\ = \begin{cases} E_L y(s,\phi_t), & \text{if } z\left[\lambda E_L + (1-\lambda)E_H\right] y(s,\phi_t) < E_L y(s,\phi_t), \\ \left[\lambda E_L + (1-\lambda)E_H\right] y(s,\phi_t), & \text{if } z\left[\lambda E_L + (1-\lambda)E_H\right] y(s,\phi_t) \ge E_L y(s,\phi_t). \end{cases} \tag{11}$$

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 loan size that the lenders are willing to offer 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 3. *Under flexible design,*

(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.[14] 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.

5.5 Numerical Example

We conclude this section by using a numerical example to illustrate the impacts of haircut on lending volume and the asset price. We also consider a slightly more general model setup. The benchmark model assumes that the gain from trade parameter z is fixed for all borrowers, generating two stark outcomes where either all borrowers are active or only the low type borrowers are active. Here, this example generalizes the model to capture a more realistic case with heterogenous z: borrowers receive i.i.d. shocks on their gain from trade, $z_t \sim G(z)$, which is privately observed by the borrowers. This generalization implies a smooth adjustment of the borrower mix as parameter values vary.

In the numerical example, we assume that the flow payoff of the asset follows a two-point distribution on 0 and 1, $F_L(s) = (1 - \pi_L)\mathbb{I}(s \geq 0) + \pi_L \mathbb{I}(s \geq 1)$, $F_H(s) = \mathbb{I}(s \geq 1)$. Parameters in the numerical

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

values are loosely calibrated to match the magnitude of ETH price fluctuations in the data.[15] We set $\beta = 0.95$, $\lambda = 0.7$, and $G(z) = \frac{z-1}{0.06}$ for $1 \leq z \leq 1.06$. The focus of the exercise is to compare equilibrium lending volume and asset prices with some benchmarks.

First, the equilibrium lending volume is compared with the volume under full information:

$$vol_0 = \lambda E_L s + (1-\lambda) E_H s + \widehat{\phi}$$

where $\widehat{\phi}$ is the asset price under complete information

$$\widehat{\phi} = \frac{\beta E z}{1 - \beta E z} \left[\lambda E_L s + (1-\lambda) E_H s \right].$$

The equilibrium volume is lower than the volume under complete information as borrowers with low z and/or high signal may not want to pool with other borrowers. The discount on volume reflects the illiquidity due to asymmetric information and haircut. The volume discount is formally defined as

$$\text{volume discount} = \left[\frac{vol}{vol_0} - 1 \right] \times 100.$$

Second, the equilibrium asset price is compared with the autarky value of the asset

$$\underline{\phi} = \frac{\beta}{1-\beta} \left[\lambda E_L s + (1-\lambda) E_H s \right].$$

The equilibrium price is greater than the autarky value because of the additional liquidity value when the asset is used as collateral in DeFi lending. We follow the literature to measure the liquidity premium of the asset which is formally defined as

$$\text{liquidity premium} = \left[\frac{\phi}{\underline{\phi}} - 1 \right] \times 100.$$

Figure 7 illustrates the effect of increasing haircut on the volume discount and on the liquidity premium as asset quality, represented by π_L, varies.

The figure in the right panel suggests that haircut reduces the liquidity value of the collateral asset: as haircut increases, the liquidity premium decreases at all levels of asset quality. The left panel shows the responses of the volume discount. When the asset quality takes extreme values (π_L closes to 0 or 1), haircut has a monotonic effect on the lending volume: increasing the haircut lowers the lending volume. Interestingly, for an intermediate level of asset quality, a moderate increase in the haircut actually increases the lending volume. This result is consistent with the general idea that, while setting the haircut too high can limit the gain from trade, a moderate haircut can help restore financial stability when high type borrowers are not willing to pool with low type borrowers if the haircut is set too low.

[15] In particular, parameterization targets include the quartiles of the price of ETH and the empirical transition matrix across different states associated with these quartiles.

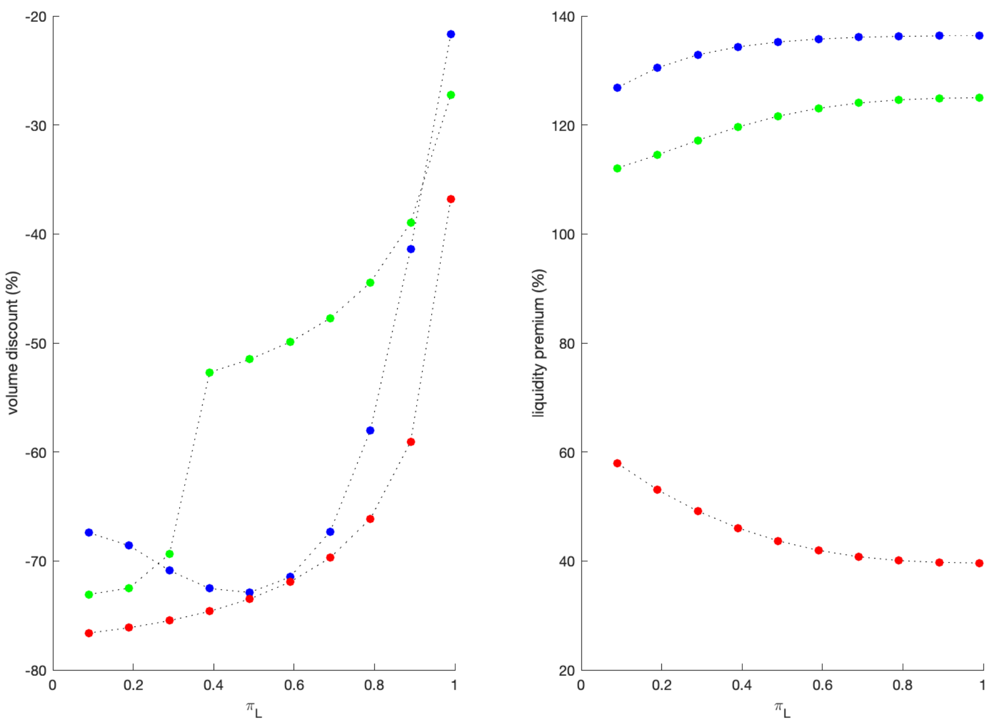


Figure 7: Comparative statics over asset quality measured by π_L, when haircut $h = 1\%$, $h = 5\%$, and $h = 10\%$.

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 8 shows that lending accounts for about 23% of DeFi TVL. We run an OLS

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

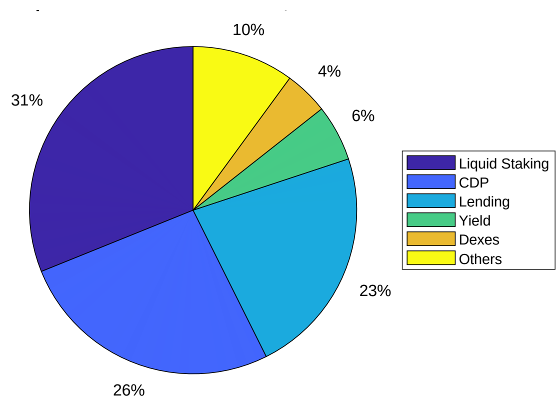
where $ETHP$ is the price of ETH, $LTCP$ is the price of Litecoin (LTC), $BURN$ is the amount of ETH burned since the London Fork as a percentage of ETH supply, $DEFI$ is the fraction of WETH locked into DeFi protocols, and $LEND$ is the fraction of WETH locked into DeFi lending. Since Litecoin has limited 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.

6.2 Effects of Collateral Quality and Crypto Prices on USDT Loans

Our model predicts that low-type borrowers have high incentives to borrow while high-type borrowers' incentives increases with the price of collateral. We examine this prediction using Aave v2 lending data. We focus on the USDT lending pool because it is the second largest in terms of total loans. Also, USDT cannot used as collateral and hence the mapping to our model is cleaner. We run an OLS

$$log(USDT) = \alpha_0 + \alpha_1 log(Price) + \alpha_2 Dummy + \alpha_3 D_I + \alpha_4 D_I \cdot log(Price),$$

Figure 8: 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	

where $USDT$ is the total USDT loan volume, $Price$ is a price index of crypto assets[16], $Dummy = 1$ for days after April 26 (the date when Aave provided incentives to users who borrow/lend certain tokens). Finally, the dummy D_I captures the severity of liquidation: $D_I = 1$ when the fraction of USDT loans liquidated is at least two standard deviations above the mean. As expected, results in Table 3 suggests that USDT loans increase with both crypto prices and incentives captured by $Dummy$. Consistent with our theory, loans increase when the liquidation risk goes up (e.g., lower collateral quality due to higher λ) but the effect is mitigated when crypto prices are higher (captured by the interaction term).

[16]It is a weighted sum of crypto assets accepted by Aave with weights given by their Aave deposits.

Table 3: **Collateral Quality and Crypto Prices and DeFi Loans**

	Estimate	Std. Err.	T-Stat	p
Intercept	17.965	0.04604	390.2	0
Log(Price)	3.0229	0.10183	29.686	1.4336e-112
Dummy	2.4009	0.05249	45.739	3.6679e-181
D_I	0.20707	0.045868	4.5144	7.9198e-06
$D_I \cdot$ Log(Price)	-1.2501	0.20117	-6.2142	1.0849e-09
No. obs. :	507			
R^2	0.901	Adj. R^2	0.901	

6.3 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.[17] 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 9 shows how the composition changes over time. Note that tokens have different USD prices. Hence, changing prices will affect their (nominal) shares in the pool. To remove the effects of token price changes on the composition, we fix their prices at the median level over the sample period (Jan 2021- April 2022). So the results derived below capture only variations in token quantities and not in their prices.

We study how sentiment is related to the overall quality of the collateral pool proxied by the weighted average of the ratings of all outstanding collateralizable deposits.[18] We run an OLS regressing log(Rating) on a dummy and log(FGI) as follows

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

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

Figure 9: Composition of Collateralizable Asset Mix

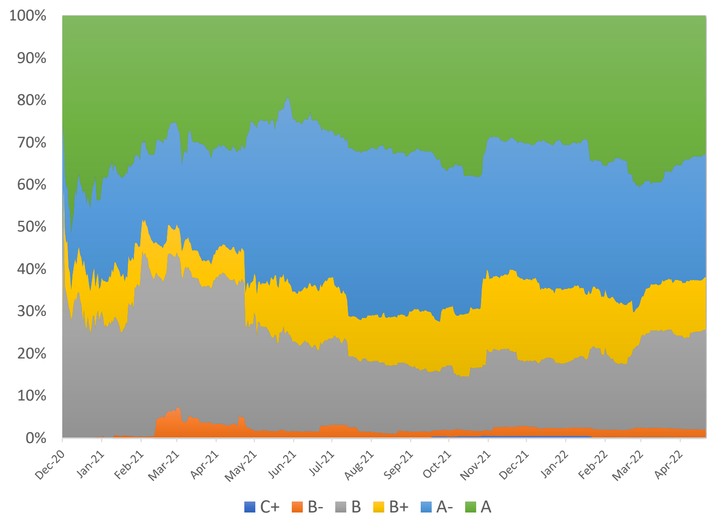


Figure Source: Dune Analytics

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

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.

Table 4: **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	

6.4 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

Figure 10: Effects of FG Index on Average Risk Rating

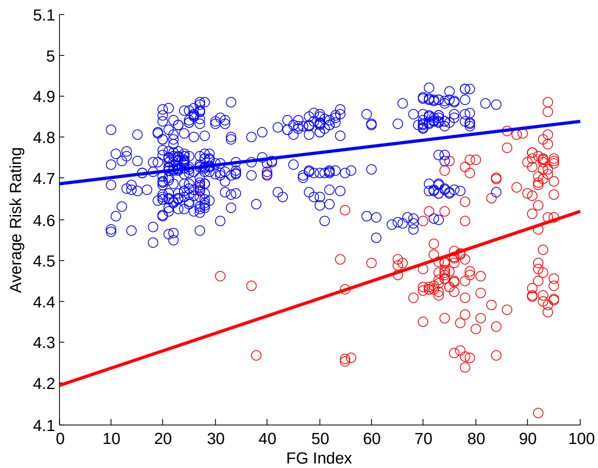


Figure Source: Dune Analytics

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

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*. SSRN.

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

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

Capponi, A. and R. Jia (2021). *Decentralized Stablecoins and Collateral Risk*.

d'Avernas, A., T. Bourany, and Q. Vandeweyer (2021). *Are Stablecoins Stable?* SSRN.

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 (Forthcoming). *Decentralized Stablecoins and Collateral Risk.*

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".

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".

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

Let $\overline{q} \equiv \lambda E_L y + (1-\lambda) E_H y$. Note that $z\overline{q} - E_H y \gtreqless 0$ iff $E_L y / E_H y \gtreqless \zeta$.

Consider the case $E_L y / E_H y > \zeta$. Suppose that the equilibrium price q is strictly less than $\overline{q}$. In this case a lender can deviate and bid $\overline{q} - \epsilon$ where $\epsilon > 0$. For ϵ small enough, $z\left(\overline{q} - \epsilon\right) - E_H y > 0$. Hence given this q both types borrow and the deviation generates strictly positive surplus. This means that the equilibrium q must be at least $\overline{q}$. At $\overline{q}$ or above, both types borrow, hence the only q that is consistent with the zero profit condition is $q = \overline{q}$.

Now consider the case $E_L y / E_H y < \zeta$. In this case high type will borrow only if q is sufficiently larger than $\overline{q}$. However, when $q > \overline{q}$, lenders make negative profit. Hence equilibrium q must be below $\overline{q}$. If q is below $\left(E_L y\right)/z$ then neither type borrows. In this case, one of the lenders can deviate and bid $E_L y - \epsilon$ where $\epsilon > 0$. For ϵ small enough, $z\left(E_L y - \epsilon\right) - E_L y > 0$ so the low type borrows and the deviating lender makes strictly positive surplus. If q is at least $\left(E_L y\right)/z$ but less than $E_L y$ then the low type borrows from the lender who sets that q. In this case, one of the lenders who bids $E_L y$ or less can deviate and bid slightly above q. This lender then wins and increases her surplus. At q greater than or equal to $E_L y$ (and below $\overline{q}$), the low type alone borrows. Hence the only q that is consistent with zero profit condition is $q = E_L y$.

A.2 Proof of Proposition 2

By the discussion in the text we know that a pooling equilibrium exists if and only if $E_L s / E_H s \geq \kappa_P$, and a separating equilibrium exists if and only if $E_L s / E_H s < \kappa_S$. To complete the proof of the proposition we need to show $\kappa_P < \kappa_S$. To see this note that,

$$[\zeta - \beta z (1 - (1 - \zeta) \lambda)] - [\zeta - \beta (1 - (1 - \zeta z) \lambda_L)] = -\beta \lambda_L (z - 1) \left(\frac{1 - \lambda}{\lambda} \right)$$

and similarly,

$$[1 - \beta z (1 - (1 - \zeta) \lambda)] - [1 - \beta (1 - (1 - \zeta z) \lambda_H)] = -\beta \lambda_H (z - 1) \left(\frac{1 - \lambda}{\lambda} \right).$$

Using the equalities above and the fact that $\lambda_L > \lambda_H$ we obtain:

$$\begin{aligned} \kappa_P = \frac{\zeta - \beta z (1 - (1 - \zeta) \lambda)}{1 - \beta z (1 - (1 - \zeta) \lambda)} &< \frac{\zeta - \beta z (1 - (1 - \zeta) \lambda) + \beta \lambda_L (z - 1) \left(\frac{1 - \lambda}{\lambda} \right)}{1 - \beta z (1 - (1 - \zeta) \lambda) + \beta \lambda_H (z - 1) \left(\frac{1 - \lambda}{\lambda} \right)} \\ &= \frac{\zeta - \beta (1 - (1 - \zeta z) \lambda_L)}{1 - \beta (1 - (1 - \zeta z) \lambda_H)} = \kappa_S. \end{aligned}$$

A.3 Proof of Uniqueness Under a Flexible Smart Contract

Denote the debt contract $y(s, \phi) = \min(\delta, s) + \phi$, for all $s \in [\underline{s}, \bar{s}]$ where $\delta = D - \phi$. Denote $\delta^*(\phi_{t+1})$ the maximum δ so that the incentive constraint of the high type borrower is satisfied

$$z [\lambda E_L y(s, \phi_{t+1}) + (1 - \lambda) E_H y(s, \phi_{t+1})] \geq E_H y(s, \phi_{t+1})$$

in which case there is a pooling equilibrium. When the information friction is severe enough, $\delta^*(\phi_{t+1}) < \bar{s}$.

The designer chooses δ 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 $\delta = \delta^*(\phi_{t+1})$. If the designer chooses to design a contract that leads to a separating outcome, then $\delta = \bar{s}$.

Next we look at the two cases:

Pooling case:

In a pooling equilibrium, denote the pooling debt threshold by δ. High type's incentive constraint is satisfied iff:

$$(z - 1) \left(\underline{s} + \phi + \int_{\underline{s}}^{\delta} \widetilde{F}_H(s) ds \right) \geq z \lambda \left(\int_{\underline{s}}^{\delta} \widetilde{F}_H(s) ds - \int_{\underline{s}}^{\delta} \widetilde{F}_L(s) ds \right).$$

In a pooling equilibrium, the designer's value is:

$$z\left(\underline{s}+\phi+\lambda\int_{\underline{s}}^{\delta}\widetilde{F}_L(s)ds+(1-\lambda)\int_{\underline{s}}^{\delta}\widetilde{F}_H(s)ds\right)+\lambda\int_{\delta}^{\bar{s}}\widetilde{F}_L(s)ds+(1-\lambda)\int_{\delta}^{\bar{s}}\widetilde{F}_H(s)ds.$$

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

$$\phi^P(\phi)=\beta\left[z\left(\underline{s}+\phi+\lambda\int_{\underline{s}}^{\delta}\widetilde{F}_L(s)ds+(1-\lambda)\int_{\underline{s}}^{\delta}\widetilde{F}_H(s)ds\right)+\lambda\int_{\delta}^{\bar{s}}\widetilde{F}_L(s)ds+(1-\lambda)\int_{\delta}^{\bar{s}}\widetilde{F}_H(s)ds\right]$$

where δ is such that

$$(z-1)\left(\underline{s}+\phi+\int_{\underline{s}}^{\delta}\widetilde{F}_H(s)ds\right)=z\lambda\left(\int_{\underline{s}}^{\delta}\widetilde{F}_H(s)ds-\int_{\underline{s}}^{\delta}\widetilde{F}_L(s)ds\right). \tag{A.1}$$

Separating case:

In this case, the designer would choose $\delta=\bar{s}$ to maximize gain from lending to the low type. The incentive constraint for the high type not to participate is

$$(z-1)\left(E_Hs+\phi\right)\geq z\lambda\left(E_Hs-E_Ls\right).$$

Taking ϕ as given, the asset price in the previous period under separating equilibrium is

$$\phi^S(\phi)=\beta\left[\lambda z(E_Ls+\phi)+(1-\lambda)(E_Hs+\phi)\right]$$

Next we look at which type of design is selected by the designer. The answer to this question depends on the asset price which itself depends on the chosen design. But before solving for the full equilibrium, we first take asset price as exogenous and see how the chosen design depends on the asset price. We consider the two cases separately.

Separating case:

In this case ϕ^S is linear in the next period price ϕ

$$\frac{\partial\phi^S}{\partial\phi}=\beta(\lambda z+1-\lambda)<1$$

When $\phi=0$, $\phi^S(0)>0$ as long as $E_Ls>0$. Together with $\frac{\partial\phi^S}{\partial\phi}<1$, we learn that $\phi=\phi^S(\phi)$ has a unique solution. Denote the solution ϕ^{S*}.

Pooling case:

In this case

$$\phi^P = \beta z \left(\underline{s} + \phi + \lambda \int_{\underline{s}}^{\delta(\phi)} \widetilde{F}_L(s)ds + (1-\lambda) \int_{\underline{s}}^{\delta(\phi)} \widetilde{F}_H(s)ds \right) \tag{A.2}$$
$$+ \beta \left(\lambda \int_{\delta(\phi)}^{\bar{s}} \widetilde{F}_L(s)ds + (1-\lambda) \int_{\delta(\phi)}^{\bar{s}} \widetilde{F}_H(s)ds \right)$$

where $\delta(\phi)$ is the solution to (A.1).

Note that

$$\frac{\partial \delta}{\partial \phi} = \frac{(z-1)}{(z\lambda - z + 1)\widetilde{F}_H(\delta) - z\lambda \widetilde{F}_L(\delta)}$$

It is clear that increasing ϕ relaxes the participation constraint if F_H and F_L satisfies the monotone likelihood ratio. So, $\frac{\partial \delta}{\partial \phi} > 0$, which means that the threshold δ must be high enough so that $(z\lambda - z + 1)\widetilde{F}_H(\delta) - z\lambda \widetilde{F}_L(\delta) > 0$.

$$\frac{\partial \phi^P}{\partial \phi} = \beta z + \beta \frac{(z-1)^2 \left(\lambda \widetilde{F}_L(\delta) + (1-\lambda)\widetilde{F}_H(\delta) \right)}{(z\lambda - z + 1)\widetilde{F}_H(\delta) - z\lambda \widetilde{F}_L(\delta)} > \beta z$$

$\phi^P(\phi)$ has a steeper slope than $\phi^S(\phi)$.

$$\frac{\partial^2 \phi^P}{\partial \phi^2} = -\beta \lambda (z-1)^2 \frac{f_L(\delta)\widetilde{F}_H(\delta) - f_H(\delta)\widetilde{F}_L(\delta)}{\left((z\lambda - z + 1)\widetilde{F}_H(\delta) - z\lambda \widetilde{F}_L(\delta) \right)^2} < 0.$$

$\phi^P(\phi)$ is concave.

When $\phi = 0$, $\phi^P(0) > 0$ as long as $E_L s > 0$. When ϕ is large enough, $\delta = \bar{s}$, $\frac{\partial \phi^P}{\partial \phi} = \beta z < 1$. And $\phi^P(\phi)$ is concave. Together, these properties imply that $\phi = \phi^P(\phi)$ has a unique solution. Denote the solution ϕ^{P*}.

When the designer chooses the design optimally, the asset price taking the next period price ϕ as given is

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

The equilibrium price is such that

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

Finally, we show that there is a unique equilibrium. Note that $\phi^P(\phi)$ has a steeper slope than $\phi^S(\phi)$. And when ϕ is large enough, $\widehat{\delta}(\phi)$ converges to $\bar{s}$, in which case $\phi^P(\phi) > \phi^S(\phi)$. Therefore, the two curves intersect at most once. Let $\widehat{\phi}$ to be the intersection point:

$$\phi^S(\widehat{\phi}) = \phi^P(\widehat{\phi}).$$

The equilibrium can fall into three cases. Case 1, $\phi^{P*} < \phi^{S*} < \widehat{\phi}$; case 2, $\phi^{P*} = \phi^{S*} = \widehat{\phi}$; case 3, $\widehat{\phi} < \phi^{S*} < \phi^{P*}$.

In the first case, $\phi^{P*} < \phi^S(\phi^{P*})$ so pooling is not an equilibrium. In the third case, $\phi^{S*} < \phi^P(\phi^{S*})$ so separating is not an equilibrium. In all three cases, the equilibrium is unique. If the equilibrium is separating, the asset price is less than $\widehat{\phi}$. If the equilibrium is pooling, the asset price is more than $\widehat{\phi}$.

Given any end-of-period price ϕ, the price in the previous period and the volume of inputs traded using the smart contract is weakly greater than those under DeFi. Therefore, the steady state price and volume is weakly greater than those under DeFi. The borrower is better off under flexible design while lenders are not worse off. The stationary equilibrium therefore Pareto dominates the one under DeFi.

A.4 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 (denoted by state 0). Suppose the distribution is given by $F_0(s)$ such that $E_0(s) = \lambda E_L(s) + (1-\lambda)E_H(s)$.

Pooling Equilibrium

We have the following conditions:

(i) Asset pricing:

$$\begin{aligned}\phi^P = &(1-\chi)\{\beta\left[E_0\left(\left(zq_0 - y_0(s,\phi^P)\right) + \left(s+\phi^P\right)\right)\right]\} \\ &+ \chi\{\beta\lambda\left[E_L\left(\left(zq - y(s,\phi^P)\right) + \left(s+\phi^P\right)\right)\right] + \beta\left(1-\lambda\right)\left[E_H\left(\left(zq - y(s,\phi^P)\right) + \left(s+\phi^P\right)\right)\right]\}\end{aligned}$$

where we use q, y to denote contract terms when there is private information, and q_0, y_0 to denote contract terms when there is no private information.

(ii) Binding haircut constraint when there is private information:

$$q(1+h) = \lambda E_L s + (1-\lambda)E_H s + \phi^P$$

(iii) Break-even condition when there is private information:

$$q = \left[\lambda E_L y\left(s,\phi^P\right) + (1-\lambda)\,E_H y\left(s,\phi^P\right)\right]$$

(iv) Binding haircut constraint when there is no private information:

$$q_0(1+h) = E_0 s + \phi^P$$

(v) Break-even condition when there is no private information:

$$q_0 = E_0 y_0\left(s, \phi^P\right)$$

We can show that the condition for a pooling equilibrium in (5),

$$\phi^P = \beta(z+h)q,$$

is not affected by χ. The reason is that a pooling equilibrium is not informationally sensitive. The asset price for a pooling equilibrium is not changed:

$$\phi^P = \beta(z+h)\frac{\lambda E_L s + (1-\lambda)E_H s}{1+h-\beta(z+h)}.$$

Separating Equilibrium

We have the following conditions:

(i) Asset pricing:

$$\begin{aligned}\phi^S &= (1-\chi)\{\beta\left[E_0\left(zq_0 - y_0(s,\phi^S) + s + \phi^S\right)\right]\} \\ &\quad + \chi\{\beta\lambda\left[E_L\left(zq - y(s,\phi^S) + s + \phi^S\right)\right] + \beta\left(1-\lambda\right)\left[E_H\left(s+\phi^S\right)\right]\}.\end{aligned}$$

(ii) Binding haircut constraint when there is private information:

$$q(1+h) = E_L s + \phi^S$$

(iii) Break-even condition when there is private information:

$$q = E_L y\left(s, \phi^S\right)$$

(iv) Binding haircut constraint when there is no private information:

$$q_0(1+h) = E_0 s + \phi^S$$

(v) Break-even condition when there is no private information:

$$q_0 = E_0 y_0\left(s, \phi^S\right)$$

Hence the condition for the separating price in (5) becomes

$$\begin{aligned}\phi^S &= (1-\chi)\{\beta\left[E_0\left(\left(zq_0 - y_0(s,\phi^S)\right) + \left(s+\phi^S\right)\right)\right]\} \\ &+ \chi\{\beta\lambda\left[E_L\left(\left(zq - y(s,\phi^S)\right) + \left(s+\phi^S\right)\right)\right] + \beta\left(1-\lambda\right)\left[E_H\left(s+\phi^S\right)\right]\} \\ &= \ (1-\chi)\beta(z+h)q_0 + \chi\beta\lambda(z+h)q + \chi\beta\left(1-\lambda\right)\left[E_H\left(s+\phi^S\right)\right]\end{aligned}$$

due to (iv) and (v). Hence the asset price becomes

$$\phi^S = \beta\frac{\lambda\frac{z+h}{1+h}E_L(s) + (1-\chi)\frac{z+h}{1+h}(1-\lambda)E_H(s) + \chi\left(1-\lambda\right)E_H\left(s\right)}{1-\beta[(1-\chi(1-\lambda))\frac{z+h}{1+h} + \chi\left(1-\lambda\right)]}$$

Note that, when $\chi = 0$, $\phi^S = \phi^P$. Obviously, when $\chi = 1$, this is just the one in the benchmark case.

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.[19] **aTokens** are interest-bearing tokens that are minted upon deposit and and burned at withdraw. The aTokens' value is pegged to the value of the corresponding deposited asset at a 1:1 ratio, and can be safely stored, transferred or traded. Withdrawals 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

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

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.[20]

The **variable rate** is the rate based on the current supply and demand in Aave. **Stable rates** act as a fixed rate.[21] The current model parameters for stable and variable interest rates are given in Figure 11. Figure 12 shows Dai's rate schedule as an example.

The **deposit rate** is given by

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

where SB_t is the share of stable borrows, S_t is average stable rate, VB_t is the share of variable borrows, V_t is average variable rate, R_t is the reserve factor (a fraction of interests allocated to mitigate shortfall events discussed below). The **Loan to Value** (LTV) ratio defines the maximum amount that can be borrowed with a specific collateral. It's expressed in percentage: at $LTV = 75\%$, for every 1 ETH worth of collateral, borrowers will be able to borrow 0.75 ETH worth of the corresponding currency of the loan. The current risk parameters are given in Figure 13.

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:

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

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**

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

[21] 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 11: 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

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 13).[22] When the liquidation is completed successfully, the health factor of the position is increased, bringing the health factor above 1.

[22]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 12: Stable vs Variable Rates for Dai

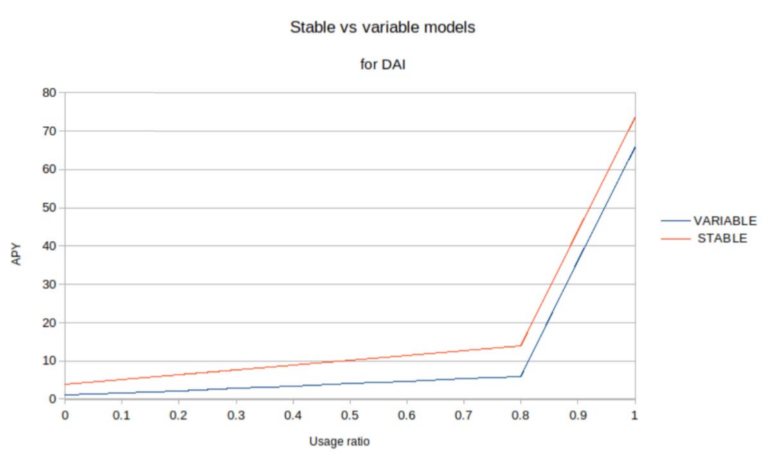


Figure Source: Aave.com

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 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.

Figure 13: 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

C Volatility of Collateral Value

Table 5: 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.