Cryptocurrency as Collateral in DeFi Lending Platforms

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

October 2024

Abstract

We model DeFi lending where cryptocurrencies serve as collateral to secure financial transactions, with their values derived from their role as a medium of exchange for consumption, yet subject to information frictions. Overcollateralization mitigates these frictions, enabling greater gains from trades between borrowers and lenders in DeFi lending. Lending backed by volatile or bubbly cryptocurrencies can be stable and does not inherently lead to fragility. Instead, specific DeFi institutional arrangements, such as the rigidity of DeFi contracts, can result in multiple self-fulfilling equilibria where lending and prices vary significantly. Introducing flexible contract updates can restore equilibrium uniqueness, highlighting an efficiency-stability-decentralization tradeoff.

Keywords: Decentralized Finance; DeFi, Smart Contracts; Money; Bubbles; Dynamic Price Feedback; Financial Fragility; Information Frictions; Adverse Selection; DeFi trilemma, Stability, Efficiency, and Decentralization Tradeoff.

JEL classification: G10, G01

*Chiu (jchiu@bankofcanada.ca), Ozdenoren (eozdenoren@london.edu), Yuan (k.yuan@lse.ac.uk), and Zhang (oo7zsx@gmail.com). The views expressed in this paper are solely those of the authors and may differ from official Bank of Canada views.

1 Introduction

Since the release of Bitcoin in 2009, the primary application of blockchain technology has been the creation of various cryptocurrencies. These cryptocurrencies act as mediums of exchange on decentralized ledgers, operating without centralized authorities. However, since the launch of Ethereum in 2015, cryptocurrencies have evolved beyond mere payment instruments. Ethereum's blockchain, with its own programming language, allows developers to build and deploy smart contracts—immutable, deterministic computer programs—and decentralized applications (dApps). This innovation has given rise to Decentralized Finance (DeFi), which encompasses a variety of financial service protocols and applications on the blockchain. These applications are anonymous, permissionless financial arrangements implemented via smart contracts, aiming to replace traditional financial intermediaries (TradFi).

In this paper, we examine how financial services, particularly lending services, traditionally provided by intermediaries that collect information, create trust, and offer credit, can be built on cryptocurrencies, including those considered to be of questionable quality and subject to information frictions. We explore how these financial services can be offered in a trustless, permissionless, anonymous, and decentralized manner to realize gains from trade. Additionally, we investigate whether DeFi lending exhibits different types of financial fragility compared to traditional financial systems, such as bank runs in Diamond and Dybvig (1983).

To achieve this, we model cryptocurrencies explicitly as an intrinsically worthless medium of exchange (i.e., fiat money) within the canonical new monetarist framework of Lagos and Wright (2005). Moreover, we introduce a new role for these types of fiat money, where they are used as collateral essential to secure anonymous DeFi transactions. In fact, most collateral assets available and acceptable in DeFi are fiat money in the form of cryptocurrencies, enabled by smart contract technologies on the blockchain. Unlike in traditional finance, money is collateralizable in DeFi because it is cost-effective to store, trace, and trade on the blockchain. To model this additional collateral role, we extend the Lagos and Wright (2005) framework by incorporating the concept of a lending contract backed by market value of tradable collateral in Ozdenoren, Yuan, and Zhang (2023). Unlike in Ozdenoren, Yuan, and Zhang (2023), where the collateral is a traded financial asset that pays dividends, in our model, the collateral is intrinsically worthless and its value as collateral is derived from its role as a medium of exchange in facilitating consumption. To the best of our knowledge, this is one of the first models in the economic literature to explore the collateral role of fiat money, linking payment and financial services through a single instrument, motivated by rapid innovations in DeFi.[1]

[1]There is a contemporaneous paper by Ozdenoren, Yuan, and Zhang (2024) that studies the use of central bank digital

Although, as in many other models of fiat money, in our model cryptocurrency valuation is a bubble, the fragility in DeFi lending that we highlight is not due to this fact but rather due to institutional features of DeFi. We explicitly model the role of DeFi arrangements in determining the size and the sustainability of this cryptocurrency bubble. In fact, one contribution of our paper is to show that lending backed by a volatile or bubbly asset can be stable and does not inherently lead to fragility; instead, it is the specific contractual arrangements in lending platforms that make it so. For example, as demonstrated in section 4.2 if the haircuts on lending contracts are set flexibly, the fragility disappears. Specifically, our model incorporates the following four unique DeFi lending institutional features: anonymous/decentralized borrowing and lending contracts, information friction about collaterals, contract rigidity, and fast moving capital due to interoperability among DeFi protocols.

First, DeFi lending protocols offers anonymity associated with borrowing and lending. Anonymous lenders deposit their cryptocurrency (e.g., Tether) via a lending smart contract to the lending pool of the corresponding cryptocurrency (e.g., Tether pool) under a lending protocol (e.g., AAVE). In return, they receive a deposit receipt (IOU) in the form of an AAVE token (e.g., aTether) which accumulates interest continuously. Since borrowers are anonymous, credit checks and other borrower-specific evaluations are not feasible. Anonymous borrowers, however, can borrow a cryptocurrency (e.g., Tether) from the corresponding liquidity pool (e.g., Tether pool) by pledging *any* crypto collateral accepted by the protocol via a borrowing smart contract. Collateral assets have to be tokenized and compatible with smart contracts. The borrowing and lending interactions in a lending protocol are peer to pool. That is, both the borrower and the lender interact with a shared liquidity pool, which is governed by a separate smart contract. This setup eliminates the need for direct, peer-to-peer interaction, thus preserving the anonymity of both parties involved in the transaction.

Second, this decentralized arrangement gives rise to the information friction between borrowers and lenders of DeFi lending protocols. This information friction can take different forms, including asymmetric information or differences in opinion about the value of cryptocurrencies. Unlike TradFi where borrowers' identities are observable, in DeFi it is both impractical and infeasible for lenders to know the identities or future needs of the borrowers who pledge cryptocurrency in a DeFi lending pool.[2] Hence, DeFi is particularly susceptible to asymmetric information between borrowers and lenders regarding the value of a cryptocurrency, especially regarding the private consumption value of a cryptocurrency. In our model, we assume that borrowers have private information about their future need for the cryp-

currency as safe assets.

[2]Makarov and Schoar (2021) analyze Bitcoin flows associated with the shadow economy and highlight the challenges of enforcing Know-Your-Customer (KYC) norms.

tocurrency's payment services, which may be for legal transactions, gray market activities, cross-border payments, etc. Therefore, the source of information asymmetry arises from the convenience yield of the cryptocurrency as a medium of exchange, which is privately realized by the borrowers.

We also acknowledge that, although not formally modeled in the main text, there can be other sources of information frictions due to the decentralized and anonymous nature of DeFi protocols. For instance, the collateral composition of a liquidity pool is often opaque. Borrowers can choose to pledge any acceptable collateral assets, while lenders cannot control or easily monitor the composition of the underlying collateral pool. Consequently, borrowers are better informed about the collateral quality than lenders. [3]

Third, DeFi lending contract is inherently rigid. In DeFi applications, smart contracts replace human judgment and the rules for setting key parameters (e.g., interest rate formulas and haircuts) are pre-programmed using smart contracts. Interest rate formulas are based on algorithm to clear the market by crossing demand and supply curves. Haircuts are determined for each type of crypto collaterals. Since the protocol is governed by holders of governance tokens in a decentralized fashion, even a slight modification of the smart contract can involve a lengthy decision process among the governance token holders. Consequently, terms of smart contracts, especially haircut rules, are modified only occasionally and appear inflexible and rigid.[4]

Fourth, DeFi capital is fast moving DeFi. Differently from traditional finance where markets are segmented, the DeFi ecosystem is closely inter-connected and inter-operable which makes fast moving

[3]This latter observation is consistent with the empirical finding in Heimbach and Huang (2023) who show that borrowers with high leverage are more likely to tilt towards pledging volatile collateral when their debt positions are about to be liquidated. Borrowers can also have an information advantage relative to the lending protocol when smart contracts rely on an inaccurate price oracle. The price feed of an oracle has to trade off latency and accuracy. For example, the reference implementation to Uniswap's oracle averages prices over a twenty-four hour window, meaning that short-lived shocks to the price are largely ignored and even a large and sustained shock (e.g., 20% for an hour) will move the oracle price by less than 1%. When the price falls because of falling fundamentals, the oracle price will lag the "true" price of the asset significantly. Since crypto is a volatile asset class, with frequent intraday spikes and drops, informed borrowers can take out large loans backed by a crypto asset with a sudden inflated price from a delayed oracle and default on loan obligations, leaving the lending protocol with a collateral whose value is far below the face value of the loan. In Appendix E, we discuss some exploit incidents during the Terra collapse in May 2022 and other price exploits due to inflated on-chain collateral prices.

[4]These limitations of smart contracts have been pointed out in a survey article by John, Kogan, and Saleh (2023). We find that, for example, AAVE protocol had only 13 risk parameter changes in its first two years of operation. There are calls for technological improvements to make decentralized governance semi-automatic and data driven. However, up till now choosing these parameters has been a manual process (See Xu (2022)).

arbitrage capital possible. Based on cryptography, cryptocurrencies are created as payment tokens for secure settlements. With the introduction of DeFi lending protocols, they also serve as collaterals where the collateral values are determined in the decentralized exchange protocols. The movement of tokens across these on-chain protocols are fast and seamless, in contrast to slow moving capital in the traditional financial system. For example, M.Griffoli et al. (2023) demonstrate that the lending volume of a crypto asset within DeFi lending protocols exhibits a positive correlation with the crypto asset's dominance status in DeFi exchange protocols.

Our dynamic model of DeFi lending incorporates the above mentioned four features. In our model (1) borrowing is decentralized; (2) loans are over-collateralized and backed by the market value of cryptocurrencies which are payment instruments for consumption goods; (3) contracts have pre-specified and rigid terms (such as the rule for haircuts); (4) lending activities in the DeFi protocol and cryptocurrency prices in the decentralized exchanges are mutually dependent and endogenously determined. Moreover, borrowing rates are set mechanically in a market-clearing condition (to meet a certain utilization ratio) and liquidation of collateral occurs at market price automated by a liquidation smart contract.[5]

We micro-found the value of cryptocurrencies and the information advantage of their owners using the canonical island setup. Agents in each island have specific consumption needs known only to themselves before the state is realized. Cryptocurrencies are necessary mediums of exchange for consumption goods. The value of these cryptocurrencies change over time because consumption needs of the buyers change, leading to time varying matching probabilities with the consumption good sellers. Cryptocurrency holders are privately informed about their own consumption needs and hence the cryptocurrency's value. This information friction results in a classic lemons problem (Akerlof (1970)) and potentially severely reduces the gains from trade by driving out the high quality borrowers. Therefore, it is optimal for DeFi platforms to impose a haircut on the crypto asset to decrease the information sensitivity of the loan and mitigate the adverse selection problem, making the lending backed by cryptocurrencies exposed to information frictions feasible.[6]

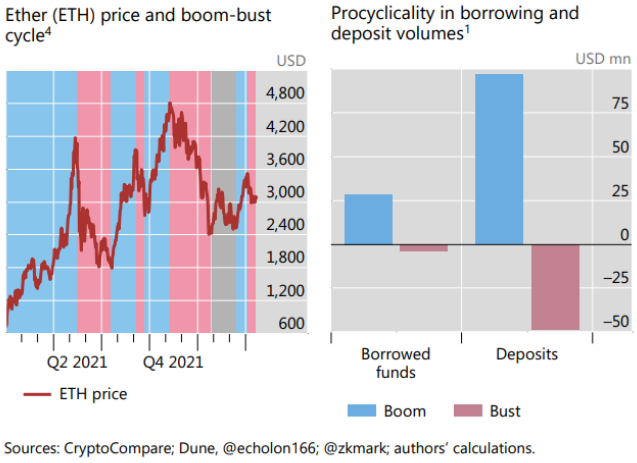
There is a feedback loop between crypto prices and the amount of DeFi lending in this dynamic model. Optimistic expectations about future crypto asset prices improves DeFi lending and bolsters

[5]In the main text, the liquidation mechanism does not explicitly model firesales. Lehar and Parlour (2022) empirically demonstrate that firesales from the liquidation mechanism in DeFi lending protocols, if occurs, lead to permanent negative as opposed to transient price impacts as normally expected. In an online appendix, we incorporate firesales into the model and show that it is crucial to account for information frictions to rationalize and quantify their puzzling empirical findings of permanent price impacts and demonstrate the robustness of the main framework.

[6]As mentioned before, the haircut rule can also be motivated by unobservable heterogenous private valuation which we provide in an online appendix.

current crypto prices, realizing more gains from trades, while pessimistic expectations about future crypto asset prices weakens DeFi lending and justifies lower current crypto prices, resulting in smaller gains from trades. We find that due to this feedback loop, rigidity in smart contracts could potentially lead to multiple self-fulfilling equilibria giving rise to the a new form of fragility of DeFi lending for a certain range of haircuts. Sudden stops, such as a transition from a positive to a negative expectation, are possible, driven by abrupt changes in self-fulfilling beliefs. Hence, the model's implications for DeFi lending and cryptocurrency prices align with the pro-cyclical pattern shown in Figure 1. 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)).[7]

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



Source: Aramonte et al. (2022)

It is widely acknowledged that crypto-currencies can be inherently fragile due to their money-like nature and susceptibility to the formation of rational bubbles.[8] The source of fragility in our model is different from the fragility of money and fall within the broad category identified by in Ozdenoren, Yuan, and Zhang (2023), referred to as market runs but on DeFi lending platforms. The economic mechanism leading to market runs in our paper differs significantly because of unique decentralized institutional features of DeFi lending. In our setup, the underlying collateral asset is fiat money and the haircut rule is assessed based on the price of money with some degree of rigidity. More important,

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

[8]For example, Schilling and Uhlig (2019) and others have studied the pricing of cryptocurrencies as payment instruments.

in contrast with traditional Diamond and Dybvig (1983) bank runs, market runs result from (mis-)coordination between present and future market participants. This (mis-)coordination is less likely for overcollateralized borrowing that occurs at centralized exchanges in the crypto space, such as Binance, or in TradFi, such as margin trading on stock exchanges, where lending contracts are governed by a central party. As mentioned earlier, decentralized autonomous organizations (DAOs) take more time to react to changes in the market environment compared to a central governance body, leading to a negative feedback spiral between cryptocurrency prices and the amount of DeFi lending.

Next, we investigate potential tools to address fragility by examining scenarios where the platform can flexibly update the smart contract terms, particularly the haircut, in a nonlinear manner in response to market price changes. We show that with flexible contracts, it is possible to support a unique equilibrium with high and stable lending volumes and asset prices. However, flexible contracts are costly and difficult to implement in the decentralized environment, pinpointing the inherent fragility of the DeFi lending protocols. To improve stability, it is necessary to give up certain degree of decentralization in DeFi. For example, platforms may re-introduce human actors to provide real-time risk management – an arrangement that forces the decentralized protocol to rely on a trusted third party. Our findings could potentially guide private developers, policymakers and regulators who are concerned about the financial stability implications of DeFi in designing safe-guarding rules and regulations (FSB 2022; IOSCO 2022).[9] While decentralization in participation and governance is fundamental to DeFi's exciting prospects in democratizing finance, our findings also highlight that decentralization also imposes limitations on DeFi's size, efficiency, complexity and flexibility, questioning its ability to significantly challenge the TradFi.

DeFi shares certain features with other collateralized borrowing markets, like Treasury repo and the housing/mortgage sector since in all these markets the pricing of the collateral assets is closely linked with the amount of borrowing. However, there are significant differences in the types of frictions existing in these other markets and DeFi. The Treasury repo market operates without contract rigidity. It has considerable liquidity, with flexible haircut/leverage adjustments throughout the day to reflect the prevailing information and risk environment, making the occurrence of multiple equilibria unlikely. In the mortgage/housing market, while information frictions exist and borrowing contracts are generally rigid due to regulatory constraints, an additional friction is at play -- slow-moving capital. The high transaction costs for arbitraging housing prices result in prolonged impacts from fire sales, potentially causing fragility in this market segment. However, in DeFi, arbitrage capital moves swiftly due to

[9]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

reduced arbitrage costs facilitated by flash loans and protocol interoperability. Consequently, when fire-sales occur in isolation within the DeFi space, their price impact tends to be transient. Our model indicates that only when paired with information friction and contract rigidity does the price impact of fire-sales acquire a lasting component. Thus, the self-fulfilling beliefs and dynamic DeFi market runs elucidated by our model constitute a critical economic mechanism underlying the potential DeFi fragility.

The rest of the paper is organized as follows. We describe the model setup in Section 2 and solve for a representative agent's optimization problem taking the cryptocurrency prices and the haircut as given in Section 3. In Section 4, we establish the conditions for the stability and fragility of DeFi lending, discuss how flexible contract design can improve stability and efficiency. Section 5 reviews related literature, provides additional discussion and concludes. In Appendix A, we present detailed proofs. In Appendices B-E, we provide brief descriptions of the features and frictions of DeFi lending protocols, using Aave as a real-world example, to motivate the model assumptions.[10]

2 The Model Setup

Crypto assets are used both as collateral and as a means of payments in the crypto sphere. We develop a model where crypto assets facilitate investment and consumption activities and investigate how the interaction between these two functions determines the efficiency and stability of the DeFi lending market.There are an infinite number of islands that represent physically segmented marketplaces, interconnected blockchains or different DeFi platforms where investment and consumption take place. On each island there are a continuum of two kinds of agents: buyers and sellers who trade in an investment goods market and a consumption goods market, with buyers on the demand side and sellers on the supply side. The transactions are facilitated by a crypto asset which has a fixed supply of A units and does not pay any dividends.

Time is infinite and discrete, indexed by t. Each time period is divided into four sub-periods. Buyers are long lived. They discount future utility with per-period discount factor $0 < \beta < 1$. (Hence no discounting between sub-periods.) Sellers live for one period. They enter the economy in the beginning of a period and leave at the end of the period and are replaced by new sellers in the next period.

In sub-period 1, an investment goods market opens where buyers can obtain investment goods from sellers to realize investment gains. Owing to limited commitment problems between buyers and sellers

[10] In the Online Appendix, we present a model where asymmetric information is about private valuation, a model of sentiment equilibria and incorporate a firesale shock to crypto prices, 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.

(arising from anonymity or other reasons), buyers need to pay sellers using a security backed by the crypto asset. As discussed below, the optimal arrangement will be a debt security which can be interpreted as a loan conducted on a DeFi lending platform using crypto assets as collateral. In subperiod 3, buyers purchase consumption goods using crypto assets as a means of payments. Both markets are decentralized. In sub-period 1, each buyer is matched with at least two sellers who engage in Bertrand competition. In sub-period 3, each buyer is matched with a seller, with the terms of trade determined by take-it-or-leave-it offers from buyers. In the second and fourth sub-periods, a frictionless asset market opens for agents to exchange crypto assets for a perishable numeraire good that can be produced subject to a linear disutility function.These crypto asset markets determine the crypto asset prices and allow buyers to replenish their crypto portfolios. We next describe each market in more detail.

Investment goods market/the lending platform In the first sub-period, buyers receive an investment opportunity. In order to benefit from this opportunity, a buyer needs to obtain investment goods which can be produced by sellers. There are gains from trade as sellers can produce the investment good at unit marginal cost while buyers' marginal return from investment is $z > 1$. Through the DeFi lending platform, buyers can borrow the investment goods from sellers in sub-period 1. Hence, we will also label buyers and sellers as borrowers and lenders respectively. In reality, the investment goods can be stablecoins mint/held by lenders. In DeFi lending protocols such as Aave, borrowers predominantly borrow stable coins such as USDT and USDC using risky crypto assets as collaterals (e.g., ETH, BTC, YFI, YNX). As stablecoins are regarded as medium of exchange and unit of account in DeFi, they are used to fund various transactions or to increase leverage in crypto investment. We can interpret z as the value accrued to borrowers when using stable coins obtained from lenders for speculative or productive purposes.[11]

In the DeFi setting, borrowers are anonymous and there is a commitment problem. To overcome the commitment problem, buyers need to pay sellers with a security backed by the collateral asset. Ozdenoren, Yuan, and Zhang (2023) show that the optimal security for this exchange is a debt security. Building on their result, we assume that buyers obtain investment goods by paying the lenders with a debt contract backed by a crypto asset. We refer to this market as Market I.

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

Consumption goods market

In the third sub-period buyers on an island purchase a consumption good from the sellers on that island. With probability λ the island is type L and with probability $1-\lambda$ it is type H. If the island is type L the probability that the buyer meets a seller is γ_L, and if the island is type H the probability that the buyer meets a seller is γ_H where $\gamma_L < \gamma_H$. One interpretation of the lower matching probability of a type L island is that buyers on a type L island need a good that is specialized to their needs and it is more difficult for them to find a seller that produces a good that matches their requirements. Buyers pay for the consumption good with the cryptocurrency.[12] We refer to these markets as Markets L and H.

Sellers produce the consumption good at unit marginal cost. A buyer's utility from consuming c units of the consumption good is $u(c)$. The utility function u is positive, twice differentiable, increasing and concave, i.e. $u(c) > 0$ for $c > 0$, $-\infty < u''(c) < 0 < u'(c)$ for $c > 0$. To guarantee equilibrium existence we further assume that utility is increasing sufficiently rapidly near zero consumption so that $u'(0^+) > 1 + \frac{1-\beta}{\beta(\lambda\gamma_L+(1-\lambda)\gamma_H)}$ and $\lim_{c\to\infty}[u'(c) + cu''(c)] = 0$.

Information environment and asset markets Buyers learn their island's type privately in subperiod 1, and in particular, the island's type is not observed by the sellers of the investment good and, there is asymmetric information between the buyers and sellers of the investment good in subperiod 1. This type of private information is relevant for the crypto-environment since the owners have better information about future convenience benefits generated by the crypto asset to themselves. After subperiod 1, each island's type in that period becomes common knowledge and information is symmetric across all agents.

In subperiod 2 agents trade the crypto asset in a frictionless market. We denote this crypto asset market by AM-L or AM-H depending on the information available about the island's type. We denote the price of the crypto asset in AM-L and AM-H by ϕ^L and ϕ^H. The price in this asset market depends on the island's type because, as we noted above, the island's type becomes commonly known after subperiod 1. In the fourth, and final, subperiod, agents, once again, trade the crypto asset in a frictionless market which we denote by AM-I. We denote the price of the crypto asset in AM-I by ϕ^I.

[12] As will become clear, there is no asymmetric information in the consumption goods market so agents do not need to use asset backed securities. An alternative interpretation is that buyers pay with a security that promises resale price of the asset.

Smart contracts In practice, DeFi lending is conducted anonymously and relies on smart contracts to initiate and settle collateralized debt[13] Collateral is locked into smart contracts and released to the borrower when repayment is received. Smart contracts are automated and all terms (e.g., interest rate formula and haircuts) are pre-programmed contingent on a small set of quantifiable real-time information. Due to decentralized governance of DeFi lending protocols, terms of smart contracts are modified only occasionally and appear inflexible and rigid.[14]

Formally, in our model, these smart contracts constitute a debt contract that specifies, at each time t, the haircut and interest rate (h, R_t) set by the lending protocol. The haircut defines the debt limit per unit of collateral according to:

$$q_t \leq \Phi_t(1-h) \tag{1}$$

where $\Phi_t = \left(\lambda\phi^L + (1-\lambda)\,\phi^H\right)$ is the contractual price underlying the DeFi debt contract. The borrowing limit is set by applying a pre-specified haircut on Φ_t. In DeFi lending the contractual price Φ_t comes from an Oracle that scans price quotes from many (centralized or decentralized) exchanges. We denote the face value of the loan by D_t and the interest rate on the loan by $R_t \equiv D_t/q_t$. We assume that lenders break even:

$$q_t = \frac{1}{a_{L,t}\lambda + a_{H,t}\,(1-\lambda)}\left[a_{L,t}\lambda\mathbb{E}_L \min\left\{D_t, \phi_t\right\} + a_{H,t}\,(1-\lambda)\,\mathbb{E}_H \min\left\{D_t, \phi_t\right\}\right] \tag{2}$$

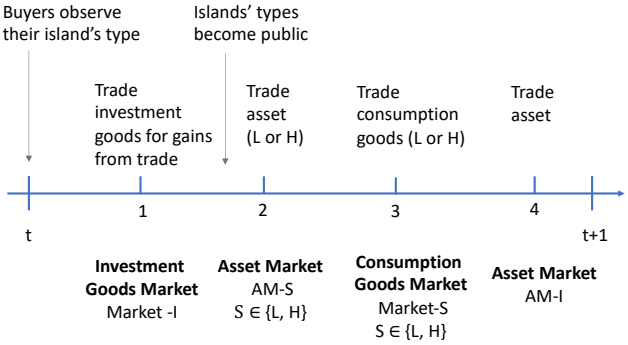
where $a_{L,t}$ and $a_{H,t}$ are the amount of collaterals pledged by low and high quality borrowers, respectively. The debt can be settled anytime within each period. In the case of $D_t < \phi_t$, collateral will be liquidated at the market price automated by the liquidation smart contract. Note that (2) represents the mechanical interest rate rule in the borrowing smart contract that clears the market (up to a utilization ratio, in this case, without loss of generality, 100%). In practice, there are two smart contracts: one for borrowing rates and one for lending rates, each designed to maintain a specific utilization ratio of the liquidity pool. For clarity, we assume lenders break even and focus solely on the smart contract that specifies the rule to set the borrowing rate. Given that the haircut and face value determine the interest rate through (1) and (2), we will denote the smart contract as (h, D_t) for the remainder of this paper..

Timeline Figure 2 summarizes the event timeline of this economy within each time period.

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

[14]We find that AAVE protocol, one of the largest DeFi lending protocol only had 13 risk parameter changes in its first two years of operation (See Appendix for the exact dates of these changes).

Figure 2: Timeline



Note that in this timeline, the lending platform in the investment good market is subject to information friction but types become publicly known in the asset markets and consumption goods market. A privately informed borrower could conduct an outright sale in an exchange (that is, an asset market), instead of obtaining a loan against it on a lending platform. However, it is optimal for the borrower to sell a debt contract on the lending platform rather than an equity contract in an asset exchange because the price discount of an equity contract due to adverse selection is larger in the asset exchanges which is shown in Ozdenoren, Yuan, and Zhang (2023).[15]

2.1 Equilibrium Concept

Definition 1. A stationary equilibrium consists of asset prices ϕ^L, ϕ^H and ϕ^I such that:

1) Given the prices, in the asset market AM-s where $s \in \{I, L, H\}$, buyers choose the optimal amount of crypto assets to bring to next sub-period.

2) Given the prices and their asset holding, in Markets L and H, buyers choose how much to consume and how much asset to retain optimally.

3) Given the prices and their asset holding, the face value D is set so that both types of buyers choose the amount of collateral to pledge optimally and the lenders break even.

[15] Ozdenoren, Yuan, and Zhang (2023) show that the optimal security for privately informed borrowers to sell in a similar setting consists of a debt contract (which both high and low quality borrowers sell) and a residual equity contract (which only the low quality borrowers sell). Empirically, there are other technical frictions in selling crypto assets on decentralized and centralized exchanges on blockchains. Transferring crypto assets to an off-chain centralized exchange is often subject to a long time lag before the assets can be traded, while transactions on an on-chain decentralized exchange are often subject to market illiquidity and price slippage.

4) Asset markets clear, i.e. buyers' demand for the asset in AM-s where $s \in \{I, L, H\}$ equals the asset supply A.

3 Solving the Model

We first solve for a representative buyer's optimization problem in each market taking the crypto asset prices and the haircut as given. As usual we solve the model backwards beginning with the crypto asset market AM-I in subperiod 4, moving back to consumption goods markets L and H in subperiod 3, crypto asset markets AM-L and AM-H in subperiod 2 and finally investment goods market in subperiod 1.

3.1 Buyer's optimization problem at AM-I

We refer to a buyer's continuation value from owning a units of the crypto asset in the asset market AM-I by $W_t^I(a)$ and from entering Market I at time $t+1$ with a units of crypto asset by $V_{t+1}^I(a)$.[16] The buyer chooses the amount of crypto assets, $\tilde{a}$, to bring to Market I and balances her budget by selling n units of numeraire goods:

$$W_t^I(a) = \max_{n,\tilde{a}} -n + \beta V_{t+1}^I(\tilde{a})$$

subject to $\phi_t^I \tilde{a} \leq \phi_t^I a + n$.

Substituting for n we get,

$$W_t^I(a) = \phi_t^I a + \left[\max_{\tilde{a}} -\phi_t^I \tilde{a} + \beta V_{t+1}^I(\tilde{a})\right] = \phi_t^I a + W_t^I(0)$$

where

$$W_t^I(0) = \max_{\tilde{a}} -\phi_t^I \tilde{a} + \beta V_{t+1}^I(\tilde{a}).$$

Taking the first order condition we obtain the buyer's optimal asset holding in AM-I as:

$$\phi_t^I = \beta \frac{\partial}{\partial a} V_{t+1}^I\left(a^I\right). \tag{3}$$

[16] Recall that AM-I takes place in the fourth subperiod of period t and precedes Market I that takes place in the first subperiod of period $t+1$. By assumption agents discount the payoff that they obtain in time $t+1$Market I when they compute their continuation values in time t AM-I.

3.2 Buyer's optimization problem at Markets L and H

We denote buyers' continuation values from owning a units of the cryptocurrency asset in Market s where $s \in \{L, H\}$ by $V_t^s(a)$. Recall that in Market s a buyer is matched with a seller with probability γ_s. We assume that the buyer makes the seller a take-it-or-leave-it offer of $(a - \tilde{a})$ units of the cryptocurrency in exchange for c units of the consumption good. Hence, if the seller accepts the offer, the buyer retains $\tilde{a}$ of the cryptocurrency with which he enters AM-I. The seller, on the other hand, enters AM-I with $(a - \tilde{a})$ units of the cryptocurrency, which she sells at price ϕ_t^I and obtains $\phi_t^I(a - \tilde{a})$ units of the numeraire good. If the seller refuses the offer, then the seller obtains reservation value of zero. Hence, we can write the buyer's value function as:

$$V_t^s(a) = \max_{c,\tilde{a} \geq 0} \gamma_s \left[u(c) + W_t^I(\tilde{a})\right] + (1 - \gamma_S) W_t^I(a)$$

subject to $c \leq \phi_t^I(a - \tilde{a})$. Note that the constraint can be viewed as either the budget constraint for the buyer or the participation constraint of the seller. Since the constraint must be satisfied with equality we can substitute for c and write the buyer's value function as:

$$V_t^s(a) = \max_{\tilde{a} \geq 0} \gamma_s \left\{u\left[\phi_t^I(a - \tilde{a})\right] + \phi_t^I \tilde{a}\right\} + (1 - \gamma_s)\phi_t^I a + W_t^I(0).$$

The first order condition for the buyer's optimization problem is:

$$u'\left[\phi_t^I(a - \tilde{a})\right] \geq 1 \tag{4}$$

with equality if $\tilde{a} > 0$. There are two cases to consider.

Case 1: $u'(\phi_t^I a) < 1$. In this case, the agent has left over assets after he pays for consumption goods. Denote c^* to be such that $u'(c^*) = 1$, we obtain the value function expression as follows:

$$\begin{aligned} V_t^s(a) &= \gamma_S \left\{u(c^*) + \phi_t^I a - c^*\right\} + (1 - \gamma_s)\phi_t^I a + W_t^I(0) \\ &= \phi_t^I a + \gamma_s(u(c^*) - c^*) + W_t^I(0). \end{aligned}$$

Case 2: $u'(\phi_t^I a) \geq 1$. In this case, the agent spends all the assets that he has brought to purchase consumption goods. The value function is then

$$V_t^s(a) = \gamma_s u(\phi_t^I a) + (1 - \gamma_s)\phi_t^I a + W_t^I(0).$$

3.3 Buyer's optimization problem at AM-L and AM-H

In the asset markets AM-L and AM-H, agents trade the cryptocurrency asset with symmetric information. In particular, they know whether buyers and sellers will buy consumption goods in Market L or H

in the next subperiod. We refer to a buyer's continuation value from owning a units of the crypto asset in AM-s, $s \in \{L, H\}$, by $W_t^s(a)$ and from entering consumption goods Market s with a units of crypto asset by $V_t^s(a)$. Hence,

$$W_t^s(a) = \max_{n,\tilde{a}} -n + V_t^s(\tilde{a})$$

subject to

$$\phi_t^s \tilde{a} \leq \phi_t^s a + n,$$

where n denotes the amount of numeraire good.[17] Since the budget constraint must hold with equality, we substitute for n in the payoff function and obtain,

$$W_t^s(a) = \phi_t^s a + \left[\max_{\tilde{a}} -\phi_t^s \tilde{a} + V_t^s(\tilde{a})\right] = \phi_t^s a + W_t^s(0)$$

where

$$W_t^s(0) = \max_{\tilde{a}} -\phi_t^s \tilde{a} + V_t^s(\tilde{a}).$$

Taking the first order condition we obtain the buyer's optimal asset holding in AM-S as:

$$\phi_t^s = \frac{\partial}{\partial a} V_t^s(a^s). \tag{5}$$

We can now use the expressions for $V_t^s(a)$ to solve for ϕ_t^s and $W_t^s(a)$. Recall that there are two cases.

Case 1: $u'(\phi_t^I a) < 1$. In this case,

$$\frac{\partial}{\partial a} V_t^s(a) = \phi_t^I$$

so we obtain $\phi_t^s = \phi_t^I$ and

$$W_t^s(a) = \phi_t^I a + W_t^s(0). \tag{6}$$

Case 2: $u'(\phi_t^I a) \geq 1$. In this case,

$$\frac{\partial}{\partial a} V_t^s(a) = \phi_t^I \left[\gamma_s u'(\phi_t^I a) + (1 - \gamma_s)\right]$$

so we obtain

$$\phi_t^s = \phi_t^I \left[\gamma_s u'(\phi_t^I a) + (1 - \gamma_s)\right] \text{ and}$$
$$W_t^s(a) = \phi_t^I \left[\gamma_s u'(\phi_t^I a) + (1 - \gamma_s)\right] a + W_t^S(0). \tag{7}$$

[17] Recall that buyers can produce the numeraire good one-to-one from labor. If $\tilde{a} > a$, the buyer purchases $(\tilde{a} - a)$ units of the asset and pays with the numeraire good. The production of the numeraire creates disutility which is given by $-n$ in the payoff function. Similarly, if $\tilde{a} < a$, the buyer sells $(a - \tilde{a})$ units of the asset and receives numeraire in exchange (so $n < 0$) which gives utility $-n$.

3.4 Partial Equilibrium of Market I

Now, we move to the first subperiod when Market I takes place. In this market there is asymmetric information. Buyers (borrowers) know their island's type but sellers do not know. This asymmetric information creates adverse selection in the market. If the island is type H, borrowers on the island know that the asset price will be ϕ_t^H next period. They would borrow the investment good, and secure the borrowing by giving up a security claim on the asset, only if the lenders gives enough of the investment good in exchange. However, lenders need to break even, and they need to take into account that the island may be type L in which case the asset price will be ϕ_t^L. Hence, there is a classic lemons problem in Market I.

The DeFi lending protocol sets a debt contract that specifies the haircut and face value (h, D_t).[18] The haircut, h, puts a limit on how much borrowers can borrow, denoted by q_t given by the constraint (1). The face value D_t, on the other hand, is set so that lenders break even.

Suppose a borrower enters Market I with a units of the crypto asset. The borrower takes the contract (h, D_t) and prices as given, and decides how many units of the crypto asset backed security to sell given the island's type. Since the security is backed by the crypto asset, the borrower can sell at most a units of the security. The actual payment of the debt security on a type s island is $\min(D_t, \phi_t^s)$. In particular, if $\phi_t^s < D_t$, type s buyer defaults. We assume that in case of default, the borrower pays the lender the collateral price ϕ_t^s and retains a units of the crypto asset in AM-s next sub-period.[19] Hence, the value of the borrower from holding a units of the crypto asset in Market I is given by:

$$\begin{aligned} V_t^I(a) = \lambda \max_{0\le \tilde{a}_L \le a} \left[z q_t \tilde{a}_L - \min(D_t, \phi_t^L)\tilde{a}_L \right] + (1-\lambda) \max_{0\le \tilde{a}_H \le a} \left[z q_t \tilde{a}_H - \min(D_t, \phi_t^H)\tilde{a}_H \right] \\ + \lambda W_t^L(a) + (1-\lambda) W_t^H(a) \end{aligned}$$

Since $W_t^s(a) = \phi_t^s a + W_t^s(0)$ we can rewrite the value function as:

$$\begin{aligned} V_t^I(a) = \lambda \max_{0\le \tilde{a}_L \le a} \left[z q_t \tilde{a}_L - \min(D_t, \phi_t^L)\tilde{a}_L \right] + (1-\lambda) \max_{0\le \tilde{a}_H \le a} \left[z q_t \tilde{a}_H - \min(D_t, \phi_t^H)\tilde{a}_H \right] \\ + \lambda \phi_t^L a + (1-\lambda)\, \phi_t^H a + \lambda W_t^L(0) + (1-\lambda) W_t^H(0) \end{aligned} \tag{8}$$

Next we solve the partial equilibrium in Market I where we characterize the equilibrium choices of the two types of buyers but take the asset prices as given. To simplify the problem we make two

[18] Setting the face value D_t is equivalent to setting the loan rate R_t since $R_t = D_t/q_t$.

[19] This assumption innocuous and we make it for notational convenience. The crypto asset trades at price ϕ_t^S in AM-S (and there is no discounting between sub-periods). We could equivalently assume that the lender sells the asset in AM-S and the borrower rebalances his asset portfolio.

observations. First, due to the linearity of the objective function, the optimal values of $\tilde{a}_L$ and $\tilde{a}_H$ are either 0 or a. Second, in equilibrium, the low type borrower always borrows so that $\tilde{a}_L = a$.

To pin down $\tilde{a}_L$, $\tilde{a}_H$ and D_t,we need to consider only two cases. The first is a pooling equilibrium where $\tilde{a}_L = \tilde{a}_H = a$ so that both types of borrowers trade the debt security in exchange for the investment good. The second is a separating equilibrium where $\tilde{a}_L = a$ and $\tilde{a}_H = 0$ so that only the low type trades the debt security in exchange for the investment good. We next derive the face value of debt D_t in each case and characterize a necessary and sufficient condition under which the corresponding equilibrium exists.

Pooling case: The face value of the debt D_t^P is given by the break even condition for the sellers:

$$q_t = \lambda \min(D_t^P, \phi_t^L) + (1-\lambda)\min(D_t^P, \phi_t^H). \tag{9}$$

The face value of debt in the pooling equilibrium depends on whether the low type defaults or not. When low type defaults, $\min(D^P, \phi_t^L) = \phi_t^L$; otherwise, $\min(D_t^P, \phi_t^L) = D_t^P$. Substituting q_t in (9) with the upper bound of loan amount q_t in (1), we obtain an equation for the debt face value in the pooling equilibrium:

$$D_t^P = \begin{cases} \frac{(1-h)\left(\lambda\phi_t^L + (1-\lambda)\phi_t^H\right) - \lambda\phi_t^L}{(1-\lambda)} & \text{if } \frac{\phi_t^H}{\phi_{tt}^L} > \frac{1-\lambda(1-h)}{(1-h)(1-\lambda)} \\ (1-h)\left(\lambda\phi_t^L + (1-\lambda)\phi_t^H\right) & \text{o.w.} \end{cases} \tag{10}$$

The debt is traded in the pooling equilibrium if and only if

$$zq_t = z\left\{\lambda \min(D_t^P, \phi_t^L) + (1-\lambda)\min(D_t^P, \phi_t^H)\right\} \geq \min(D_t^P, \phi_t^H).$$

Defining

$$\overline{\zeta}\left(h, \phi^L, \phi^H\right) \equiv \begin{cases} \frac{(1-\lambda)\phi^L}{(1-h)(\lambda\phi^L + (1-\lambda)\phi^H) - \lambda\phi^L} & \text{if } \frac{\phi^H}{\phi^L} > \frac{1-\lambda(1-h)}{(1-h)(1-\lambda)} \\ 1 & \text{o.w.} \end{cases}$$

and

$$\zeta \equiv 1 - \frac{z-1}{\lambda z}$$

we can write the pooling condition as,

$$\overline{\zeta}\left(h, \phi^L, \phi^H\right) \geq \zeta. \tag{11}$$

Separating case: The face value of the debt D_t^S is given by the break even condition for lenders:

$$q_t = \min(D_t^S, \phi_t^L). \tag{12}$$

In the separating case we can assume w.l.o.g. that the low type does not default, i.e. $D_t^S \leq \phi_t^L$. This is because, in the case of default, setting the face value of debt to $D_t^S = \phi_t^L$ is equivalent to setting a higher face value. Hence, substituting q_t in (12) with the upper bound of loan amount q_t in (1), we obtain an equation for the debt face value in the separating equilibrium:

$$D_t^S = (1-h)\left(\lambda\phi_t^L + (1-\lambda)\,\phi_t^H\right) \tag{13}$$

The debt is traded in the separating equilibrium if and only if

$$\overline{\zeta}\left(h, \phi^L, \phi^H\right) \leq \zeta. \tag{14}$$

4 Dynamic DeFi Lending Equilibrium: Multiplicity and Uniqueness

The analysis in the previous section takes the asset prices as given. In this section, we characterize the stationary equilibrium where asset prices are endogenously determined. We first demonstrate that, with contract rigidity, 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 (Market I) justified by different cryptocurrency prices. The multiple crypto currency prices are in turn justified by the different equilibria in Market I. We then show that if debt contract terms can be flexibly updated, a unique stationary equilibrium is obtained and fragility is eliminated.

4.1 Characterization of Stationary Equilibria

We focus on steady state and drop time subscripts for the remainder of the section and solve for the equilibrium steady state asset prices: ϕ^L, ϕ^H ϕ^I. For simplicity we also set $A = 1$.

To begin we show that $u'(\phi^I) < 1$ is inconsistent with a stationary equilibrium. From (6) if $u'(\phi^I) < 1$ than $\phi^L = \phi^H = \phi^I$. As a result, $\min(D, \phi^L) = \min(D, \phi^H) = q = (1-h)\phi^I$. Substituting these terms in (8), we have

$$V^I(a) = (z-1)(1-h)\phi^I a + \phi^I a + \lambda W^L(0) + (1-\lambda)W^H(0)$$

and

$$\phi^I = \beta \frac{\partial}{\partial a} V^I(1) = \beta\left[1 + (z-1)(1-h)\right]\phi^I.$$

Hence, in steady state of stationary equilibrium, $\phi^L = \phi^H = \phi^I = 0$. But this is inconsistent with $u'(\phi^I) < 1$ since $u'(\phi^I) = u'(0) > 1$.

For the remainder of our analysis we focus on the case where $u'(\phi^I) \geq 1$. From (7) we have:

$$\phi^s = \phi^I\left[\gamma_s u'(\phi^I) + (1-\gamma_s)\right].$$

Lemma 1. *The ratio of the asset prices at AM-L and AM-H, ϕ^L/ϕ^H, is increasing in ϕ^I.*

The ratio of the asset prices at AM-L and AM-H captures the degree of adverse selection since the lenders who buy the asset backed security do not know whether the asset price will be low (ϕ^L) or high (ϕ^H) in the next subperiod. As the ratio ϕ^L/ϕ^H increases (and gets closer to one), adverse selection decreases. Lemma 1 shows that the degree of adverse selection is decreasing in ϕ^I. As we show in the rest of this section, this feedback between asset prices that works through adverse selection is key to supporting multiple equilibria.

Next, we consider the two cases where the debt security is traded in a pooling and separating equilibrium in Market I where ϕ^I_P and ϕ^I_S correspond to the asset price in AM-I in the pooling and the separating equilibrium respectively.

In the pooling case, we substitute the pooling debt price (9) into (8) and differentiating with respect to a we obtain:

$$\phi^I_P = \beta(z-1)\left[\lambda \min(D^P, \phi^L) + (1-\lambda)\min(D^P, \phi^H)\right] + \beta\left[\lambda\phi^L + (1-\lambda)\phi^H\right].$$

Recall that in the pooling case low type defaults if and only if $\frac{\phi^H(x)}{\phi^L_t(x)} > \frac{1-\lambda(1-h)}{(1-h)(1-\lambda)}$. Using this fact and substituting the face value from (10) we obtain:

$$\phi^I_P = \beta\left[(z-1)(1-h)+1\right]\left(\lambda\phi^L + (1-\lambda)\phi^H\right), \tag{15}$$

In the separating case, substituting the separating debt price (12) into (8) and differentiating with respect to a we obtain:

$$\phi^I_S = \beta\lambda(z-1)\min(D^S, \phi^L) + \beta\left[\lambda\phi^L + (1-\lambda)\phi^H\right].$$

Substituting the face value from (13) we obtain:

$$\phi_S^I = \beta\left[\lambda(z-1)(1-h)+1\right]\left(\lambda\phi^L + (1-\lambda)\,\phi^H\right). \tag{16}$$

Next proposition delivers the existence of a stationary equilibrium and shows that there can be multiple equilibria.

Proposition 1. *There exists either a unique pooling equilibrium, a unique separating equilibrium or two equilibria one pooling and separating. Moreover, when the pooling and separating equilibria coexist, asset prices ϕ^I, ϕ^H and ϕ^L are higher in the pooling equilibrium than in the separating equilibrium.*

The detailed proof is provided in the appendix. We give a rough sketch here. First let $\phi^s(x) = x\left[\gamma_s u'(x) + (1-\gamma_s)\right], s \in \{L, H\}$ and define two functions: one for the pooling and the other for the separating case as follows:

$$\phi_P^I(x) = \beta\left[(z-1)(1-h)+1\right]\left(\lambda\phi^L(x) + (1-\lambda)\,\phi^H(x)\right), \tag{17}$$

$$\phi_S^I(x) = \beta\left[\lambda(z-1)(1-h)+1\right]\left(\lambda\phi^L(x) + (1-\lambda)\,\phi^H(x)\right). \tag{18}$$

We then show that there exists a fixed point for the pooling price in (17) and a fixed point for a separating price in (18). We demonstrate that at least one, and sometimes both, of these fixed points satisfy the respective pooling and separating conditions to complete the proof.

By examining further the boundary conditions for the pooling and the separating equilibrium, we characterize the conditions under which the economy admits multiplicity in asset prices for a given haircut.

Proposition 2. *Pooling and separating equilibria co-exist if and only if*

$$\overline{C} > \frac{\gamma_L}{\gamma_H} > \underline{C}, \tag{19}$$

where

$$\overline{C} = \frac{1-\lambda}{\lambda}\frac{(1-h)\left[(\lambda z - z + 1) - \beta\lambda^2(z-1)\right] - \lambda\beta}{1-(1-h)\left[(\lambda z - z + 1) + \beta\lambda\,(1-\lambda)\,(z-1)\right] - (1-\lambda)\,\beta},$$
$$\underline{C} = \frac{1-\lambda}{\lambda}\frac{(1-h)\left[(\lambda z - z + 1) - \beta\lambda(z-1)\right] - \lambda\beta}{1-(1-h)\left[(\lambda z - z + 1) + \beta\,(1-\lambda)\,(z-1)\right] - (1-\lambda)\,\beta}.$$

In other words, when the ratio of matching probability with a consumption good seller in a low state versus in a high state is in an intermediate range, there exist both a pooling equilibrium with high asset prices, greater funding and production, and a separating equilibrium with depressed asset prices,

reduced funding and production. It is important to note that DeFi lending does not always admit multiple equilibria. Proposition 2 outlines the condition for stability and fragility in DeFi lending.

The economic mechanism for equilibrium multiplicity in Proposition 2 is distinct from the one in Diamond and Dybvig (1983) that features (mis-)coordination among a cross-section of depositors. The runs we identify are market runs as opposed to traditional bank runs, and are due to the *dynamic coordination* with future agents. They are driven by self-fulfilling pessimistic beliefs in crypto prices and DeFi lending activities. When the switch between these multiple equilibria is driven by a sunspot, multiplicity results in fragility. In an online-appendix, we construct sentiment equilibria where the economy switches between multiple self-fulfilling regimes based on non-fundamental sunspot states (Asriyan, Fuchs, and Green (2019)). We show that the total DeFi lending is "pro-cyclical" in the sense that it is positively correlated with the asset price.

In the same online appendix, we address an empirical puzzle presented by Lehar and Parlour (2022). They demonstrate that the liquidation mechanism in DeFi lending protocols, when collaterals are sold on decentralized exchanges, results in permanent negative price impacts. They highlight the fire-sale channel as a potential source of instability in the DeFi system. Their finding of a permanent price impact is puzzling for two reasons. First, by definition, firesales are not driven by fundamental shocks and should not have any permanent price impact. Second, the fast moving capital in DeFi should mitigate the amplification effects of fire sales, rendering any price impacts temporary.[20] Our model shows that even if the direct negative price impact of fire sale is temporary, it can become permanent because of the existence of multiple equilibria. A lower asset price from DeFi liquidation sale leads to heightened adverse selection about the asset quality, causing agents dynamically "coordinate" their pessimistic beliefs and making the equilibrium switch more likely. That is, the negative price impact of firesales only becomes permanent combined with information friction. Therefore, our model rationalizes not only the empirical findings of permanent price impact in Lehar and Parlour (2022) but also outlines the conditions for such occasions.[21]

4.2 Uniqueness under Flexible Design of Debt limit

We have shown that under a rigid haircut, for a certain range of parameter values, DeFi lending can lead to multiplicity. In this section, we show that a flexible contract design supports a unique equilibrium

[20]The DeFi literature has documented active arbitrage activities cross-chains or on-chains enabled by Miner Extractable Value (MEV) bots or flash loans, indicating that DeFi capitals are fast moving (Qin, Zhou, and Gervais (2022)).

[21]In our model, the collateralized lending market is competitive and lenders break even. This means that there are liquidations but the ratios of non-performing loan are low across equilibrium outcomes.

and generates higher social surplus from lending compared to the case with a rigid haircut.

Under flexible design, we modify the equilibrium concept in Definition 1 so that the haircut on the smart contract is no longer subject to constraint (1). Instead, we assume that the DeFi protocol chooses the haircut to maximize the expected amount of loans made by the platform given prices ϕ^L and ϕ^H.[22] That is, the DeFi platform chooses the function $h\left(\phi^L, \phi^H\right)$ to maximize:

$$\left(\lambda + (1-\lambda)\, a_H\left(\phi^L, \phi^H\right)\right) q\left(h\left(\phi^L, \phi^H\right), \phi^L, \phi^H\right) \tag{20}$$

where the loan size is:

$$q\left(h, \phi^L, \phi^H\right)) = \left(1 - h\left(\phi^L, \phi^H\right)\right)\left(\lambda\phi^L + (1-\lambda)\,\phi^H\right)$$

and

$$a_H\left(\phi^L, \phi^H\right) = \begin{cases} 1 & \text{if } \overline{\zeta}\left(\phi^L, \phi^H\right) \geq \zeta \\ 0 & \text{otherwise} \end{cases}. \tag{21}$$

Definition 2. A stationary equilibrium with flexible haircut consists of asset prices ϕ^L, ϕ^H and ϕ^I such that $h\left(\phi^L, \phi^H\right)$ solves the platform's maximization problem and (1)-(4) in Definition 1 hold.

The next proposition shows that the flexibility in setting the haircut optimally in response to changes in the asset price leads to a unique stationary equilibrium. Although the haircut is set flexibly, in the unique equilibrium the platform chooses the same haircut in every period.

Proposition 3. *There exists a unique stationary equilibrium with flexible haircut in which equilibrium asset prices are given by* $\overline{\phi}^I$, $\overline{\phi}^L$ *and* $\overline{\phi}^H$. *In any equilibrium, the intermediary takes the asset prices* ϕ^I, ϕ^L *and* ϕ^H *as given and chooses the haircut according to the following rule:*

$$h\left(\phi^L, \phi^H\right) = \begin{cases} \frac{(1-\lambda)\left(\zeta\phi^H(x) - \phi^L(x)\right)}{\zeta(\lambda\phi^L(x) + (1-\lambda)\phi^H(x))} & \text{if } \check{\phi}^I \leq \phi^I \leq \hat{\phi}^I \\ 0 & o.w. \end{cases}.$$

Additionally, if $\overline{\phi}^I < \check{\phi}^I$ *then the equilibrium is separating, otherwise it is pooling and the equilibrium with flexible haircut Pareto dominates the equilibrium with a rigid haircut.*

The construction of the proof is detailed in the Appendix. To understand the haircut function, first suppose ϕ^I is very high which makes the debt contract informationally insensitive and the adverse selection very mild. The platform can guarantee the high type's participation in the debt market without

[22] DeFi protocol may benefit from larger amount of loans for various reasons. For example, if the intermediary charges a fixed per unit fee than maximizing loan amount is tantamount to maximizing the protocol's profit.

a haircut which generates high debt volume and raises the surplus from lending. If ϕ^I is lower than a threshold ($\hat{\phi^I}$), the debt contract becomes informationally more sensitive and the platform eventually needs to set a positive haircut. As ϕ^I becomes even lower, the platform keeps increasing the haircut to maintain a pooling outcome. However, when ϕ^I is extremely low (below $\check{\phi^I}$), adverse selection becomes too severe and it is too costly for the intermediary to entice high type to participate in the debt market by setting a very high haircut. In this case, the intermediary chooses to forgo haircut and target lending to the low types only. This flexibility in adjusting haircut implies that, given any asset prices, the loan size are weakly greater than those under the rigid DeFi contract.

The dynamic feedback between asset prices and the haircut is the key economic force that leads flexible contracting to eliminate the equilibrium multiplicity. To understand this, let us go through the following thought experiment. In the multiple equilibria region of the rigid haircut regime, the high type of borrowers has two choices: either to participate or not and the outcome depends on asset prices. When asset prices are high, the high type will participate due to low adverse selection, resulting in a pooling equilibrium; otherwise, they will not, leading to a separating equilibrium. To see that with flexible contracting, the separating equilibrium will not survive as an equilibrium, let us suppose that asset prices are such that they lead to a separating equilibrium with fixed haircut. Now since the haircut can be flexibly adjusted, the platform is able to raise the haircut to ensure that the debt contract is information insensitive and entice the participation of the high type in the debt issuance. In this pooling outcome, the collateral asset generates more funding, realizes more gains from trade, and becomes more valuable. Higher asset prices, in turn, lower the adverse selection and relax the high type's participation constraint further. Consequently, the haircut can be lowered, triggering the dynamic feedback loop between asset prices and the haircut. This unravelling process ends until the asset prices and DeFi lending reach the pooling equilibrium level.[23]

The above result is obtained when the collateral is a fiat money, significantly different from that in Ozdenoren, Yuan, and Zhang (2023) which features an optimal security design backed a financial asset that pays dividend. Additionally, we show that the fragility in DeFi lending that we highlight is not due to the bubble-like property of cryptocurrency but rather due to institutional features of DeFi. It suggests that the rigid haircut rule (1) imposed by the DeFi smart contract is the source of DeFi lending instability in the form of multiple equilibria and lowers welfare. Can a DeFi lending smart contract be pre-programmed to replicate the flexible contract design? This can be challenging in practice. First, a

[23]At this pooling equilibrium with flexible haircut, the resulting equilibrium haircut is not higher but may be lower than the fixed haircut that we started with depending on the severity of adverse selection.

flexible contract cannot be implemented using simple linear haircut rule that is typically encoded in DeFi contracts. Second, the optimal haircut on the debt threshold shown in the above proposition depends on information that may not be readily available on-chain (e.g., z, λ). Alternatively, the lending protocol can replace the algorithm by a human risk manager who can adjust risk parameters in real time according to the latest information. Relying fully on a trusted third party, however, can be controversial for a DeFi protocol. Our results highlight the difficulty in achieving stability and efficiency in a decentralized environment subject to informational frictions.

5 Related Literature and Discussion

We have developed a dynamic equilibrium model for studying decentralized lending protocols such as Aave and Compound. While there is a young and growing literature on DeFi (see the survey paper by Makarov and Schoar (2022)), there is relatively limited work on DeFi lending platforms. Besides those mentioned earlier, most studies focus on the special institutional arrangements in DeFi lending. Mueller (2022) find that the liquidation mechanism in the DeFi lending protocol increases cost and risk for leveraged investment. Heimbach and Huang (2023) examine leverage decisions (e.g., collateral use, leverage ratio) of DeFi borrowers and their determinants. Rivera, Saleh, and Vandeweyer (2023) study the programmable interest rate function in the DeFi lending protocols that implements optimal competitive equilibrium.

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 stable coins 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 puzzling permanent impact of collateral liquidations on asset prices. For a general overview of DeFi architecture and applications, see Harvey et al. (2021) and Schar (2021). Chiu, Kahn, and Koeppl (2022) study the value propositions and limitations of DeFi. Vulnerabilities that make DeFi lending protocols fragile (e.g., price oracle exploits by borrowers) are studied in the recent computer science literature. These computer science papers focus mainly on the efficiency of design features of these protocols (e.g., see Gudgeon et al. (2020), Perez et al. (2021), Qin et al. (2020), Qin et al. (2021)).

The key difference of our model from the existing DeFi literature is that we formally model cryp-

tocurrencies as payment instruments. Cryptocurrencies are built on the blockchain technology which makes it nearly impossible to counterfeit or double-spend. Additionally, we model the collateral value of cryptocurrency on their role as a medium of exchange explicitly.

Our model studies the fragility implication of the asymmetric information about the asset's future payoff between the borrowers and the lenders. One might question the nature of this information asymmetry: is it possible for the cryptocurrency owners to know more about the future payoff than the other participants in the DeFi system? In the model, we micro-found this friction by modeling the difference in the convenience yield across cryptocurrencies for different types of consumption goods (e.g, resulting from improved searching and matching technology among buyers and sellers), crypto owners are privately informed about the convenience yield because they know their own future need for consumption goods transaction.

As discussed previously, borrowers can also have information advantage relative to the lending protocol when the smart contract relies on a stale price feed from the Oracle. Since crypto asset prices are volatile and most lenders have little knowledge of the collateral mix used by the borrowers, the owners of the cryptocurrencies, who are also borrowers, are more likely to have better information about the crypto asset value. That is, information asymmetry is also empirically plausible.

Furthermore, there may be multiple sources of information frictions. To highlight the robustness of the feedback mechanism in the model presented in the main text, we have also provided a model where asymmetric information is about unobservable private valuation in an online appendix.

Moreover, by incorporating information friction, our model explains how firesale might have permanent price impact even when DeFi capital is fast moving. The price-funding liquidity feedback channel, compounded by firesale, as demonstrated in the model, could potentially destabilize the DeFi ecosystem.

Additionally, 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), Fostel and Geanakoplos (2012) and Ozdenoren, Yuan, and Zhang (2023). In Ozdenoren, Yuan, and Zhang (2023), the focus is on how flexible and optimal security design eliminates equilibrium multiplicity when the collateral is a dividend paying asset. Our model is significantly different because the collateral in our paper is a form of medium of exchange. We build instead upon the new monetarist framework of Lagos and Wright (2005) to value cryptocurrencies. In addition, we take contract rigidity seriously, match it with institutional details of the DeFi system. Moreover, the haircut rule in our model is also different, which is based on cryptocurrency price, closely following the practice of DeFi lending contracts. The fragility discussed in this paper falls within the broad category identified by in Ozdenoren,

Yuan, and Zhang (2023), referred to as "market runs." These occur in the context of market-based financial intermediation and are driven by dynamic (mis-)coordination and self-fulfilling beliefs. This type of fragility contrasts with the "bank runs" within bank-based intermediation described in Diamond and Dybvig (1983), which are driven by cross-sectional (mis-)coordination. While both papers address market-based runs, the economic mechanism leading to fragility in this paper differs uniquely because in our paper the underlying collateral asset is fiat money and the haircut rule is assessed based on the price of money.

To summarize, this paper investigates the operation of DeFi lending protocols and demonstrates that it is feasible to reduce the information sensitivity of cryptocurrencies with questionable qualities, facilitating financial transactions that benefit both borrowers and lenders. We also identify a unique source of fragility that arises with the adoption of these protocols. Cryptocurrencies are inherently volatile as payment instruments. However, with the advent of DeFi lending services, these tokenized crypto-assets can also serve as collateral, and under certain conditions, promote stable lending that maximizes social surplus. As DeFi lending expands and more crypto assets are used as collateral, system-wide leverage, liquidity, value creation, and interconnectedness increase. We show that the distinctive institutional characteristics of DeFi, combined with underlying information frictions, introduce a unique source of fragility triggered by self-fulfilling cycles and subsequent market runs. These issues warrant attention from both practitioners and regulators.

References

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

Aoyagi, J. and Y. Itoy (2021). *Coexisting Exchange Platforms: Limit Order Books and Automated Market Makers*.

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 (2019). "Liquidity Sentiments". *American Economic Review* 109.11, pp. 3813–48.

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

Chiu, J., C. Kahn, and T. Koeppl (2022). *Grasping De(centralized) Fi(nance) through the Lens of Economic Theory*.

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

Diamond, Douglas W. and Philip H. Dybvig (1983). "Bank runs, deposit insurance, and liquidity". *Journal of Political Economy* 91.3, pp. 401–419.

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.

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

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

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

Gudgeon, Lewis et al. (2020). "DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency". In: AFT '20. New York, NY, USA: Association for Computing Machinery, pp. 92–112. ISBN: 9781450381390.

Harvey, C.R. et al. (2021). *DeFi and the Future of Finance*. Wiley. ISBN: 9781119836018.

Heimbach, Lioba and Wenqian Huang (2023). *DeFi Leverage*. Tech. rep. BIS.

John, Kose, Leonid Kogan, and Fahad Saleh (2023). "Smart Contracts and Decentralized Finance". *Annual Review of Financial Economics* 15, pp. 523–542.

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.

Lehar, Alfred and Christine A Parlour (2022). *Systemic Fragility in Decentralized Markets*. Tech. rep. BIS.

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.

Makarov, Igor and Antoinette Schoar (2021). *Blockchain Analysis of the Bitcoin Market*. MIT Sloan Working Paper 6479-21. MIT Sloan School of Management.

Makarov, Igor and Antoinette Schoar (2022). *Cryptocurrencies and Decentralised Finance*. BIS Working Papers 1061. Bank for International Settlements.

M.Griffoli, Tommaso et al. (2023). *The Making of Dominant Currencies: Evidence in DeFi*. Tech. rep. LSE.

Mueller, Peter (2022). *DeFi Leveraged Trading: Inequitable Costs of Decentralization*. Tech. rep. Fordham.

Ozdenoren, Emre, Kathy Yuan, and Shengxing Zhang (2023). "Dynamic Asset-Backed Security Design". *The Review of Economic Studies* 90.6, pp. 3282–3314.

— (2024). *Money as Safe Assets: Design of CBDCs*. LSE Working Papers. LSE.

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

Perez, Daniel et al. (2021). "Liquidations: DeFi on a Knife-Edge". In: *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 15, 2021, Revised Selected Papers, Part II*. Berlin, Heidelberg: Springer-Verlag, pp. 457–476. ISBN: 978-3-662-64330-3.

Qin, Kaihua, L Zhou, and Arthur Gervais (2022). "Quantifying blockchain extractable value: How dark is the forest?" In: *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE.

Qin, Kaihua et al. (2020). *Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit*.

Qin, Kaihua et al. (2021). "An empirical study of DeFi liquidations". In: *Proceedings of the 21st ACM Internet Measurement Conference*. ACM.

Rivera, Thomas, Fahad Saleh, and Quentin Vandeweyer (2023). *Equilibrium in a DeFi Lending Market*. Tech. rep. McGill University.

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

Schilling, Linda and Harald Uhlig (2019). "Some simple bitcoin economics". *Journal of Monetary Economics* 106, pp. 16–26.

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

A Proofs

A.1 Proof of Lemma 1

Proof.

$$\frac{\partial\left(\frac{\phi^L}{\phi^H}\right)}{\partial\phi^I} > 0 \Leftrightarrow \frac{\partial\phi^L}{\partial\phi^I}\phi^H - \frac{\partial\phi^H}{\partial\phi^I}\phi^L > 0$$

$$\begin{aligned}\frac{\gamma_L\left[u'(\phi^I)+\phi^I u''(\phi^I)\right]+(1-\gamma_L)}{\gamma_H\left[u'(\phi^I)+\phi^I u''(\phi^I)\right]+(1-\gamma_H)} > \frac{\phi^L}{\phi^H} &= \frac{\gamma_L u'(\phi^I)+(1-\gamma_L)}{\gamma_H u'(\phi^I)+(1-\gamma_H)} \\ &\Leftrightarrow \left[\gamma_L u'(\phi^I)+(1-\gamma_L)\right]\gamma_H < \left[\gamma_H u'(\phi^I)+(1-\gamma_H)\right]\gamma_L \\ &\Leftrightarrow (1-\gamma_L)\gamma_H < \gamma_H(1-\gamma_L)\end{aligned}$$

□

A.2 Proof of Proposition 1

Proof. W.l.o.g. set $A=1$. Let $\phi^s(x) = x\left[\gamma_s u'(x)+(1-\gamma_s)\right], s\in\{L,H\}$ and

$$\phi_P^I(x) = \beta\left[(z-1)(1-h)+1\right]\left(\lambda\phi^L(x)+(1-\lambda)\phi^H(x)\right),$$

$$\phi_S^I(x) = \beta\left[\lambda(z-1)(1-h)+1\right]\left(\lambda\phi^L(x)+(1-\lambda)\phi^H(x)\right).$$

Note that $\phi_P^I(x) > \phi_S^I(x)$ for all $x>0$ (and both expressions are equal and zero at $x=0$).

Observe that

$$\frac{\partial\phi_P^I(x)}{\partial x} = \beta\left[(z-1)(1-h)+1\right]\left(\lambda\frac{\partial\phi^L(x)}{\partial x}+(1-\lambda)\frac{\partial\phi^H(x)}{\partial x}\right)$$

$$\frac{\partial\phi_S^I(x)}{\partial x} = \beta\left[\lambda(z-1)(1-h)+1\right]\left(\lambda\frac{\partial\phi^L(x)}{\partial x}+(1-\lambda)\frac{\partial\phi^H(x)}{\partial x}\right)$$

Substituting

$$\frac{\partial\phi^s}{\partial x} = \gamma_s\left[u'(x)+xu''(x)\right]+(1-\gamma_s),\ s\in\{L,H\}$$

we obtain:

$$\frac{\partial\phi_P^I(x)}{\partial x} = \beta\left[(z-1)(1-h)+1\right]\left(\left(\lambda\gamma_L+(1-\lambda)\gamma_H\right)\left[u'(x)+xu''(x)\right]+\lambda(1-\gamma_L)+(1-\lambda)(1-\gamma_H)\right)$$

$$\frac{\partial\phi_S^I(x)}{\partial x} = \beta\left[\lambda(z-1)(1-h)+1\right]\left(\left(\lambda\gamma_L+(1-\lambda)\gamma_H\right)\left[u'(x)+xu''(x)\right]+\lambda(1-\gamma_L)+(1-\lambda)(1-\gamma_H)\right)$$

Moreover, $\frac{\partial^2 \phi_S^I(x)}{\partial x^2} < 0$ since $-\frac{xu'''(x)}{u''(x)} < 2$, and $\frac{\partial \phi_P^I(x)}{\partial x}\mid_{x=0} > \frac{\partial \phi_S^I(x)}{\partial x}\mid_{x=0} > 1$ since

$$u'(0) > 1 + \frac{1}{(\lambda\gamma_L + (1-\lambda)\gamma_H)}\left(\frac{1}{\beta\left[\lambda(z-1)(1-h)+1\right]} - 1\right)$$

By assumption $\lim_{x\to\infty} \frac{\partial \phi^S(x)}{\partial x} \to 1 - \gamma_S < 1$. Hence,

$$\lim_{x\to\infty} \frac{\partial \phi_P^I(x)}{\partial x} = \beta\left[(z-1)(1-h)+1\right](\lambda(1-\gamma_L) + (1-\lambda)(1-\gamma_H)) < 1$$

So $\phi_P^I(x)$ and $\phi_S^I(x)$ each have exactly one strictly positive fixed point.

Let $\hat{\phi}_P^I > 0$ and $\hat{\phi}_S^I > 0$ be these two fixed points where $\hat{\phi}_P^I > \hat{\phi}_S^I$. Let

$$\overline{\zeta}(x) = \begin{cases} \frac{(1-\lambda)\phi^L(x)}{(1-h)(\lambda\phi^L(x)+(1-\lambda)\phi^H(x))-\lambda\phi^L(x)} & \text{if } \frac{\phi^H(x)}{\phi_t^L(x)} > \frac{1-\lambda(1-h)}{(1-h)(1-\lambda)} \\ 1 & \text{o.w.} \end{cases}.$$

Since $\frac{\phi^L(x)}{\phi^H(x)}$ is increasing in x, $\frac{(1-\lambda)\phi^L(x)}{(1-h)(\lambda\phi^L(x)+(1-\lambda)\phi^H(x))-\lambda\phi^L(x)}$ is increasing in x. Thus, we must have either $\overline{\zeta}\left(\hat{\phi}_P^I\right) > \zeta$ or $\overline{\zeta}\left(\hat{\phi}_S^I\right) < \zeta$ or both, which implies that either there exists a pooling equilibrium where $\phi^I = \hat{\phi}_P^I$ or a separating equilibrium where $\phi^I = \hat{\phi}_S^I$ or both types of equilibria co-exist.

□

A.3 Proof of Proposition 2

Proof. As a first step we find $\phi^I(\zeta)$ such that

$$\frac{(1-\lambda)\phi^L\left(\phi^I(\zeta)\right)}{(1-h)\left(\lambda\phi^L\left(\phi^I(\zeta)\right) + (1-\lambda)\phi^H\left(\phi^I(\zeta)\right)\right) - \lambda\phi^L\left(\phi^I(\zeta)\right)} = \zeta$$

where $\phi^s\left(\phi^I\right) = \phi^I\left[\gamma_s u'(\phi^I) + (1-\gamma_s)\right]$ for $s = L, H$. Rearranging we obtain:

$$u'(\phi^I(\zeta)) = 1 + \chi \tag{A.1}$$

where

$$\chi = \frac{\lambda - (\lambda z - z + 1)(1-h)}{(\lambda z - z + 1)(1-h)\left[(1-\lambda)\gamma_H + \lambda\gamma_L\right] - \lambda\gamma_L}$$

and:

$$\phi^L\left(\phi^I(\zeta)\right) = \phi^I(\zeta)\left[1 + \gamma_L\chi\right] \text{ and } \phi^H\left(\phi^I(\zeta)\right) = \phi^I(\zeta)\left[1 + \gamma_H\chi\right].$$

Let $\phi^I(\zeta) = (u')^{-1}[1+\chi]$, $\phi^L(\phi^I(\zeta)) = [1+\chi\gamma_L](u')^{-1}[1+\chi]$,and $\phi^H(\phi^I(\zeta)) = [1+\chi\gamma_H](u')^{-1}[1+\chi]$. Using the definitions for $\phi_P^I(x)$ and $\phi_S^I(x)$ we obtain:

$$\phi_P^I\left(\phi^I(\zeta)\right) = \beta\left[(z-1)(1-h)+1\right](1 + \chi\left[\lambda\gamma_L + (1-\lambda)\gamma_H\right])(u')^{-1}[1+\chi] \tag{A.2}$$

$$\phi_S^I\left(\phi^I(\zeta)\right) = \beta\left[\lambda(z-1)(1-h)+1\right]\left(1+\chi\left[\lambda\gamma_L+(1-\lambda)\gamma_H\right]\right)\left(u'\right)^{-1}\left[1+\chi\right] \tag{A.3}$$

There exists multiple equilibria iff $\phi_P^I\left(\phi^I(\zeta)\right) > \phi^I(\zeta) > \phi_L^I\left(\phi^I(\zeta)\right)$. Hence, there exists multiple equilibria iff

$$\frac{1}{\beta\left[(z-1)(1-h)+1\right]} < 1+\chi\left[\lambda\gamma_L+(1-\lambda)\gamma_H\right] < \frac{1}{\beta\left[\lambda(z-1)(1-h)+1\right]}.$$

Plugging in for χ and rearranging gives (19). □

A.4 Proof of Proposition 3

Proof. Note that $\overline{\zeta}\left(h,\phi^L,\phi^H\right)$ and the intermediary's objective (20) are respectively increasing and decreasing in $h\left(\phi^L,\phi^H\right)$. Let $h^*\left(\phi^L,\phi^H\right)$ the smallest haircut for which a pooling equilibrium exists, i.e. the smallest haircut such that $\overline{\zeta}\left(h^*\left(\phi^L,\phi^H\right),\phi^L,\phi^H\right) \geq \hat{\zeta}$. Note that there are two cases:

1) If $\frac{\phi_L}{\phi_H} \geq \hat{\zeta}$ then $h^*\left(\phi^L,\phi^H\right) = 0$. The planner optimally chooses $h\left(\phi^L,\phi^H\right) = 0$ and the equilibrium is pooling.

2) If $\frac{\phi_L}{\phi_H} < \hat{\zeta}$ then $h^*\left(\phi^L,\phi^H\right) > 0$. In this case, the planner either chooses $h\left(\phi^L,\phi^H\right) = h^*\left(\phi^L,\phi^H\right)$ and the equilibrium is pooling or $h\left(\phi^L,\phi^H\right) = 0$ and the equilibrium is separating.

To show that a flexible contract design supports a unique equilibrium, we first study the pooling case. In a pooling equilibrium prices are given by a fixed point of the following equations:

$$\phi_P^I(x) = \beta\left[(z-1)(1-h^*\left(\phi^L(x),\phi^H(x)\right))+1\right]\left(\lambda\phi^L(x)+(1-\lambda)\phi^H(x)\right)$$

and

$$\phi^s(x) = x\left[\gamma_s u'(x)+(1-\gamma_s)\right]$$

where $s \in \{L,H\}$. Moreover, letting $\hat{\phi}^I$ be such that

$$\frac{\phi^L\left(\hat{\phi}^I\right)}{\phi^H\left(\hat{\phi}^I\right)} = \frac{\gamma_L u'(\hat{\phi}^I)+(1-\gamma_L)}{\gamma_H u'(\hat{\phi}^I)+(1-\gamma_H)} = \zeta,$$

we can write

$$h^*\left(\phi^L(x),\phi^H(x)\right) = \begin{cases} \frac{(1-\lambda)\left(\zeta\phi^H(x)-\phi^L(x)\right)}{\zeta(\lambda\phi^L(x)+(1-\lambda)\phi^H(x))} & \text{if } x < \hat{\phi}^I \\ 0 & \text{o.w.} \end{cases}.$$

Substituting we obtain:

$$\phi_P^I(x) = \begin{cases} \beta\left[\frac{\lambda}{\zeta}\phi^L(x)+(1-\lambda)\phi^H(x)\right] & \text{if } x < \hat{\phi}^I \\ \beta z\left[\lambda\phi^L(x)+(1-\lambda)\phi^H(x)\right] & \text{o.w.} \end{cases}.$$

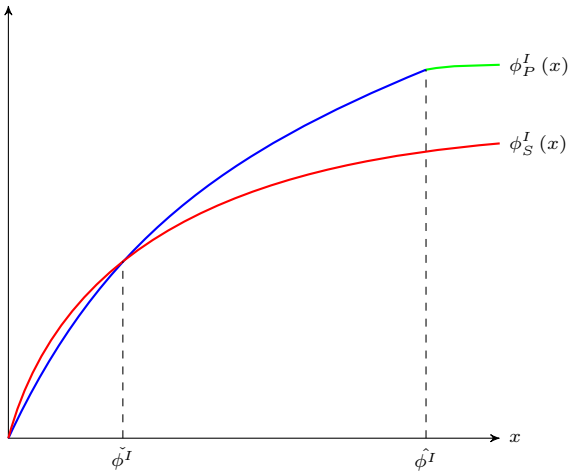


Figure 3: $\phi_P^I(x)$ and $\phi_S^I(x)$

Note:

$$\frac{\partial \phi_P^I(0)}{\partial x} = \beta\left[\frac{\lambda}{\zeta}\left(\gamma_L u'(0) + (1-\gamma_L)\right) + (1-\lambda)\left(\gamma_H u'(0) + (1-\gamma_H)\right)\right] > 1$$

since

$$u'(0) > 1 + \frac{1-\beta}{\beta\left(\lambda\gamma_L + (1-\lambda)\gamma_H\right)} > 1 + \frac{1-\beta\left[\frac{\lambda}{\zeta} + (1-\lambda)\right]}{\beta\left[\frac{\lambda}{\zeta}\gamma_L + (1-\lambda)\gamma_H\right]},$$

$$\phi_P^I(\infty) = \beta z\left(\lambda(1-\gamma_L) + (1-\lambda)(1-\gamma_H)\right) < 1,$$

left derivative at $\hat{x}$ is larger than the right derivative:

$$\frac{\partial \phi_P^I\left(\hat{\phi}^{I^-}\right)}{\partial x} > \frac{\partial \phi_P^I\left(\hat{\phi}^{I^+}\right)}{\partial x}$$

and,

$$\frac{\partial^2 \phi_P^I(x)}{\partial x^2} = \begin{cases} \beta\left(\frac{\lambda}{\zeta}\gamma_L + (1-\lambda)\gamma_H\right)\left[2u''(x) + xu'''(x)\right] & \text{if } x < \hat{\phi}^I \\ \beta z\left(\lambda\gamma_L + (1-\lambda)\gamma_H\right)\left[2u''(x) + xu'''(x)\right] & \text{o.w.} \end{cases} < 0$$

since $-\frac{xu'''(x)}{u''(x)} < 2$. See Figure 3 for an illustration of $\phi_P^I(x)$.

Next, we turn to the separating case. In a separating equilibrium prices are given by a fixed point of the following equations:

$$\phi_S^I(x) = \beta\left[\lambda(z-1)+1\right]\left(\lambda\phi^L(x) + (1-\lambda)\phi^H(x)\right)$$

and

$$\phi^s(x) = x\left[\gamma_s u'(x) + (1-\gamma_s)\right]$$

where $s \in \{L, H\}$.

Comparing $\phi_S^I(x)$ and $\phi_P^I(x)$ we find that:

$$\phi_S^I(x) \gtreqless \phi_P^I(x) \Leftrightarrow \frac{\phi^L(x)}{\phi^H(x)} \lesseqgtr \frac{\lambda z - z + 1}{\lambda z + 1}.$$

Let $\check{\phi}^I$ be such that

$$\frac{\phi^L\left(\check{\phi}^I\right)}{\phi^H\left(\check{\phi}^I\right)} = \frac{\gamma_L u'(\check{\phi}^I) + (1-\gamma_L)}{\gamma_H u'(\check{\phi}^I) + (1-\gamma_H)} = \frac{\lambda z - z + 1}{\lambda z + 1}.$$

By Corollary 1, $\check{\phi}^I < \hat{\phi}^I$ since $\frac{\lambda z - z + 1}{\lambda z + 1} < \zeta$. Hence, $\phi_S^I(x) \gtreqless \phi_P^I(x) \Leftrightarrow x \gtreqless \check{\phi}^I$. See Figure 3 for an illustration of $\phi_S^I(x)$ and $\phi_P^I(x)$.

From the above properties of $\phi_S^I(x)$ and $\phi_P^I(x)$, we see that both functions have exactly one fixed point. Denote them by $\overline{\phi}_S^I$ and $\overline{\phi}_P^I$ respectively. There are three possibilities. Either $\overline{\phi}_P^I < \overline{\phi}_S^I < \check{\phi}^I$, or $\overline{\phi}_P^I > \overline{\phi}_S^I > \check{\phi}^I$, or the knife-edge case $\overline{\phi}_P^I = \overline{\phi}_S^I = \check{\phi}^I$. In the knife-edge case we assume that the intermediary chooses the pooling contract. From (20), we observe that given ϕ^I, the intermediary prefers the separating contract to the pooling contract if $h^*\left(\phi^L\left(\phi^I\right), \phi^H\left(\phi^I\right)\right) > 1-\lambda$ or, after some algebra, $\phi^I < \check{x}$. Hence, there exists a unique equilibrium with flexible haircut such that if $\overline{\phi}_P^I < \overline{\phi}_S^I < \check{\phi}^I$ then the equilibrium is a separating one where the haircut is $h = 0$ and the equilibrium prices are $\overline{\phi}_S^I$, $\phi^L\left(\overline{\phi}_S^I\right)$ and $\phi^H\left(\overline{\phi}_S^I\right)$, and if $\overline{\phi}_P^I \geq \overline{\phi}_S^I \geq \check{\phi}^I$ then the intermediary chooses the haircut $h = h^*\left(\phi^L\left(\overline{\phi}_P^I\right), \phi^H\left(\overline{\phi}_P^I\right)\right)$ and the equilibrium prices are $\overline{\phi}_P^I$, $\phi^L\left(\overline{\phi}_P^I\right)$ and $\phi^H\left(\overline{\phi}_P^I\right)$. Clearly, asset prices and the loan size are higher with flexible haircut. As a result buyers' utilities from consumption is higher and the intermediary is better off with flexible haircut and the lenders are indifferent (since they break even either way.) □

B Protocol For Loanable Funds: Features and Frictions

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

Key players. The Aave eco-system consists of various types of participants. Depositors can deposit a crypto asset into the corresponding pool of the Aave protocol and collect interest over time. Borrowers can borrow 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 unpaid loan will grow, which might result in the deposited assets becoming more likely to be liquidated by liquidators. 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. This collateral liquidation mechanism of LTV and health ratio is akin to initial margin and maintenance margin in the traditional margin borrowing. The part of difference of the maintenance margin is given to liquidators as incentive to activate the dormant liquidation (smart) contract for a levered position whenever its health factor falls below 1.[24] The collateral assets are valued based on price feed provided by Chainlink's decentralized oracles.

Risky collateral. Aave currently accepts over 20 different crypto assets as collateral including WETH, WBTC, USDC and UNI. Most non-stablecoin collateral assets have very volatile market value. As shown in table 3 in the Appendix, the prices of stablecoins such as USDC and DAI (top panel), are not so volatile and they are typically loaned out by lenders. Other crypto assets, which are used as collaterals to back the borrowings, are extremely volatile relative to collateral assets commonly used in traditional finance (bottom panel). For example, ETH, which accounts for about 50% of use non-stablecoin deposits in Aave, has a daily volatility of 5.69%. The maximum daily price drop was over 26% during the sample period. The most volatile one is CRV, the governance token for the decentralized exchange and automated market maker protocol Curve DAO. For CRV the maximum price change within a day was over 40%. For risk management purposes, Aave has imposed very high haircuts on these crypto assets. For example, the haircuts for YFI and SNX are respectively 60% and 85%.[25]

[24] In practice, small loans are often not liquidated when the high gas fees make a liquidation unprofitable.

[25] 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-

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

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

Decentralized governance. Like many other DeFi protocols, Aave has released the governance to the user community by setting up a decentralized autonomous organization or DAO. Holders of the AAVE token can vote on matters such as adjustments of interest rate functions, addition or removal of assets, and modification of risk parameters such as margin requirements. To implement such changes to the protocol, token holders need to make proposals, discuss with the community, and obtain enough support in a vote. This process helps protect the system against censorship and collusion. However, decentralized governance by a large group of token holders is both time and resource costly. Hence it is not possible to update the protocol or the smart contract terms very frequently. As a result, relative to a centralized organization, a DeFi protocol may be slower to make necessary adjustments to respond to certain unexpected external changes (e.g., changes in market sentiments) in a timely manner. This problem is well documented. For instance, a risk assessment report of Aave in April 2021 pointed out that "As market conditions change, the optimal parameters and suggestions will need to dynamically shift as well. Our results suggest that monitoring and adjustment of protocol parameters is crucial for reducing risk to lenders and slashing in the safety module."[26] In practice, since the setup of Aave v2 in late 2020 until May 2022, the risk parameters have been updated only 13 times (see Table 2 in the Appendix for some of the key changes). All were conducted after Aave DAO elected Gauntlet, a centralized entity, to provide dynamic risk parameters recommendations.

These features of Aave are common among the DeFi lending protocols, highlighting three key frictions

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.

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

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

C Further Details about Aave Lending Protocol

According to DeFiLlama, there are 1485 DeFi protocols running on different blockchains (e.g., Ethereum, Terra, BSC, Avalanche, Fantom, Solana) as of April 2022. The TVL of these protocols are 237 billion USD with lending protocols accounting for about 20%. (Figure 4).[27] 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.

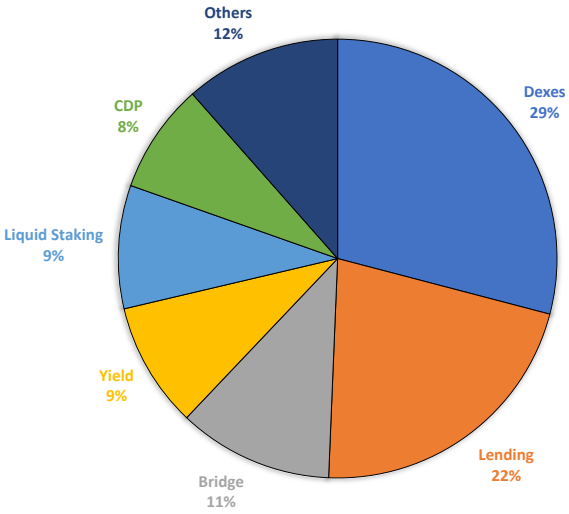
C.1 Tokens

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.[28] **aTokens** are interest-bearing tokens that

[27] 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.

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

Figure 4: Composition of TVL of all DeFi Protocols on all Chains (April 2022)



Data Source: DefiLlamma.

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).

C.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 unpaid 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.[29]

The **variable rate** is the rate based on the current supply and demand in Aave. **Stable rates** act as a fixed rate.[30] The current model parameters for stable and variable interest rates are given in Figure 5. Figure 6 shows Dai's rate schedule as an example.

Figure 5: 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

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

[30] 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 6: Stable vs Variable Rates for Dai

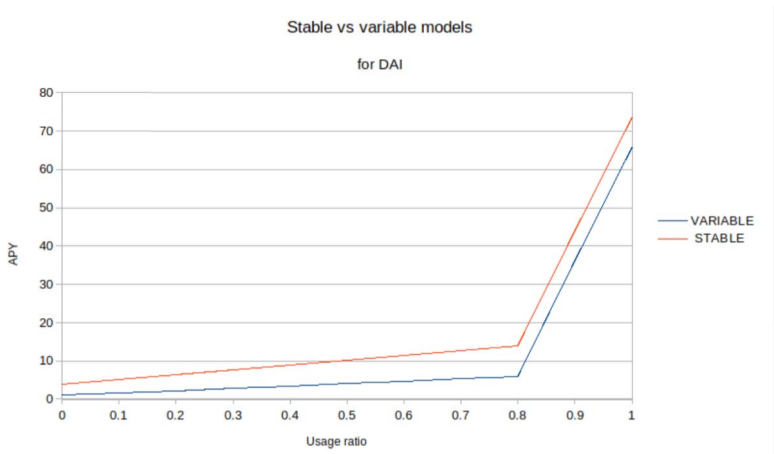


Figure Source: Aave.com

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 7.

C.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 undercollateralized 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 factor** *(Hf)*. When $Hf < 1$, a loan is considered undercollateralized and can be liquidated. When the

Figure 7: 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

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 7).[31] When the liquidation is completed successfully, the health factor of the position is increased, bringing the health factor above 1.

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

C.5 Shortfall Event

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

[31] 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.

Table 2: Historical AAVE V1 Risk Parameter Changes

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

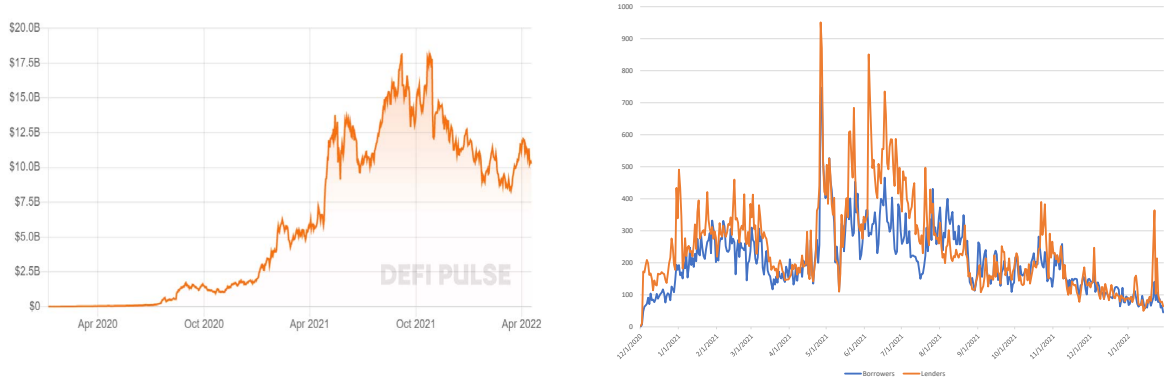
incentives, AAVE holders will deposit their tokens into the SM. In return, they receive rewards (periodic issuance of AAVE known as Safety Incentives (SI)) and fees generated from the protocol (see reserve factor above).

C.6 Recovery Issuance

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

C.7 Some Basic Statistics

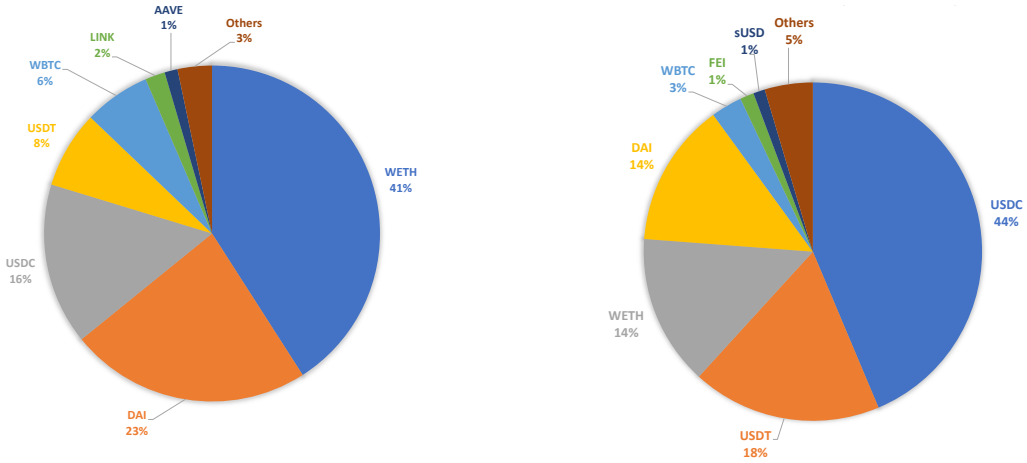
Figures 8-10 show some basic statistics describing the Aave lending protocol. In April 2022, Aave supports the lending of 31 tokens and the total market size is about 11 billion USD. As shown in Figure 8 (a), the total value locked in Aave has increased substantially from mid 2020 to mid 2021, and has 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 9 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



(a) Total Value (USD) Locked in Aave

(b) Number of Unique Users per Day

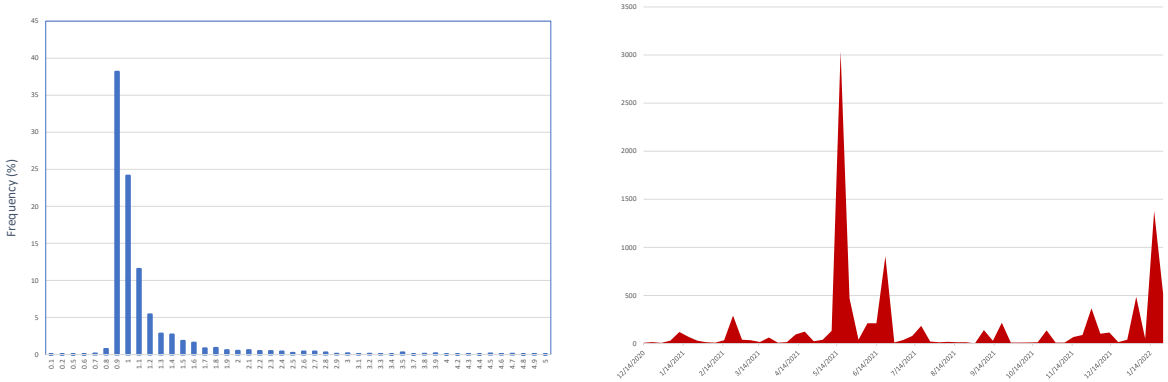
Figure 8: Aave v2 TVL and Users Over time



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

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

Figure 9: Asset Compositions in Aave v2



(a) Health Factor (January 2022)

(b) Number of Liquidtions per Week

Figure 10: Liquidation Risk in Aave v2

is relatively high since the distribution of the health factors is skewed towards the left in Figure 10 (a), with 40% with a health factor below 1.[32] Liquidations happen frequently as a result of the volatile collateral prices and high leverage. Panel (b) shows the time series of collateral liquidations.

D Volatility of Collateral Value

See Table 3.

E Price Exploits

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

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

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

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

of XVS while lenders were unable to exclude XVS being used as a collateral. Similar exploits happened to Ethereum-based lending protocols Cheese Bank (with $3.3 million loss in November 2020), Vesper Finance (with $3 millions loss in November 2021), and Inverse Finance (with $15.6 million loss in April 2022).

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

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

Source: CoinGecko.