BANK OF CANADA
BANQUE DU CANADA

Staff Working Paper/Document de travail du personnel—2022-43

Last updated: October 11, 2022

Grasping De(centralized) Fi(nance) Through the Lens of Economic Theory

by Jonathan Chiu,[1] Charles M. Kahn[2] and Thorsten V. Koeppl[3]

[1] Banking and Payments Department, Bank of Canada
jchiu@bank-banque-canada.ca

[2] Department of Finance, University of Illinois
c-kahn@illinois.edu

[3] Department of Economics, Queen's University
tk15@queensu.ca

DOI: https://doi.org/10.34989/swp-2022-43 | **ISSN** 1701-9397

Acknowledgements

Thorsten V. Koeppl acknowledges support from SSHRC Insight Grant 435-2022-0028.

Abstract

In this article, we use a simple stylized model of collateralized lending to analyze the value proposition and limitations of decentralized finance (DeFi). DeFi uses a decentralized ledger to run smart contracts that automatically enforce the terms of a lending contract and safeguard the collateral. DeFi can lower the costs associated with intermediated lending and improve financial inclusion. Limitations are the volatility of the crypto collateral and stablecoins used for settlement, the possible incompleteness of smart contracts and the lack of a reliable oracle. A proper infrastructure reducing such limitations could improve the value of DeFi.

Topics: Digital currencies and fintech; Payment clearing and settlement systems

JEL code: G2

1 Introduction

Crypto assets and crypto applications started with the release of Bitcoin in 2008. As the first *cryptocurrency*, Bitcoin enabled secure storage and an exchange of digital value without the use of a designated third party. However, from the start, the economic benefit of cryptocurrencies has been questioned: Within a stable, efficient monetary system, it is not clear what the value proposition of a cryptocurrency really is.

In 2015, the Ethereum blockchain was introduced to develop the idea of running *smart contracts* on a decentralized ledger. At first, the Ethereum blockchain was mainly a way to issue new tokens. However, it became clear that the blockchain could serve as a host for decentralized financial applications, based on the technology that runs smart contracts on secure distributed ledgers. Using these smart contracts, individuals can then directly engage in financial transactions without the use of third parties. This process, commonly referred to as *decentralized finance* (DeFi), enables the elimination of costly, third-party-run infrastructure when lending or trading.[1]

In this viewpoint article, we provide a primitive analysis of the DeFi value proposition, as well as its limitations. We ask two main questions: What are the necessary conditions for DeFi to provide value over traditional, intermediated lending relationships? And what are the main limitations DeFi applications currently face? While DeFi is used for a variety of applications, we focus on applications for lending, which compete directly with real world intermediaries such as banks or financing companies.[2]

We begin with a simple setting where there is a need for borrowing and lending, but where frictions, in the form of a double-sided commitment problem, make direct lending between two parties expensive. Third-party intermediaries can alleviate these problems by guaranteeing the execution of the contract, but they require a fee to ensure that they themselves

[1] Harvey et al. (2021) and Schär (2021) provide a non-technical, detailed discussion of DeFi architecture and applications.

[2] In particular, we do not look at decentralized exchanges, which are another promising application, but which mainly facilitate the trading of crypto assets and thus do not necessarily compete with traditional intermediaries in the mainstream.

have proper incentives.

This is where DeFi comes into play. Instead of relying on high fees, it can run a platform that—based on a distributed ledger and smart contracts—can guarantee the execution of a borrowing contract. Hence, DeFi can either substitute for traditional intermediation or allow for better, bilateral loans between contracting parties. The value of DeFi lies therefore in both disintermediation and financial inclusion.[3]

This value proposition of DeFi, however, runs into several key limitations. First, DeFi requires stablecoins with low volatility and fairly stable collateral values to function properly. Unfortunately, we are currently not quite there yet.[4] However, the introduction of a wholesale central bank digital currency (CBDC) and the tokenization of government securities provide alternatives that could alleviate these shortcomings.

Second, DeFi applications may be too rigid in their execution of smart contracts. One role intermediaries play is to adjust contract execution in the case of unforeseen contingencies. In the future, however, technological advances may make it possible to reduce the incompleteness of smart contracts or automate possible renegotiation of such contracts.

Third, DeFi relies on external entities providing information—so-called *oracles*. We are not aware of a solution to fully decentralize an oracle that provides real time information, especially unquantifiable "soft" information, to a DeFi application in a tamper-proof way. One alternative would be to have a designated party provide such infrastructure. In some cases, financial markets might regard a central bank as a reliable neutral provider.

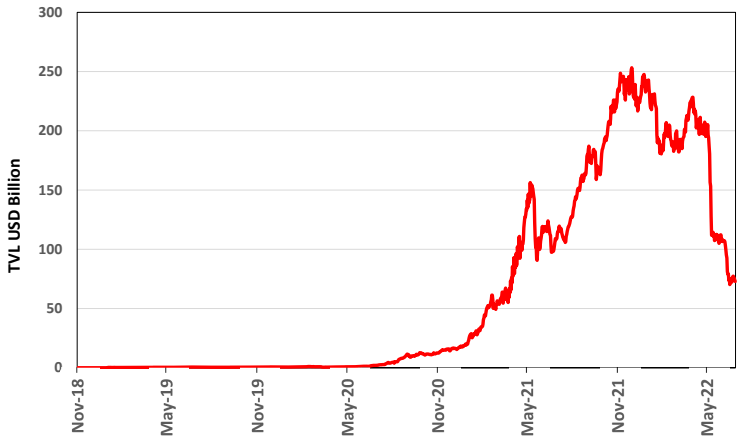
In the last few years, there has been a tremendous growth in DeFi in terms of both its scale and scope. As shown in Figure 1.1, the total value locked (TVL) into DeFi increased dramatically starting with the so-called "DeFi Summer" in 2020. After reaching its peak at USD 250 billion in late 2021, the DeFi market saw a sharp decline in its TVL in the

[3]Chiu and Koeppl (2019) provide an early analysis of such DeFi applications for settling securities based on a proof-of-work blockchain compared with using costly intermediaries.

[4]The TerraUSD crash has been a reminder that unbacked stablecoins have difficulties maintaining their exchange rate pegs, while backed stablecoins (e.g., Tether, USD Coin, Dai) tend to be more stable. Notwithstanding their backing, all stablecoins became more volatile during the Terra crash in 2022.

second quarter of 2022, largely due to the general price crash in crypto assets during this period. Nonetheless it remains at around USD 70 billion as of June 30, 2022. DeFi has also been expanding its scope. Figure 1.2 shows the decompositions of the TVL across different DeFi protocols. When combined, lending protocols and the closely related collateralized debt positions (CDP)[5] constitute the most important portion of the market, closely followed by decentralized exchanges (Dexes). Aave is currently the largest lending protocol, and MakerDAO is the largest CDP.

Figure 1.1: Total Value Locked (TVL) in DeFi (Source: DeFiLlama)



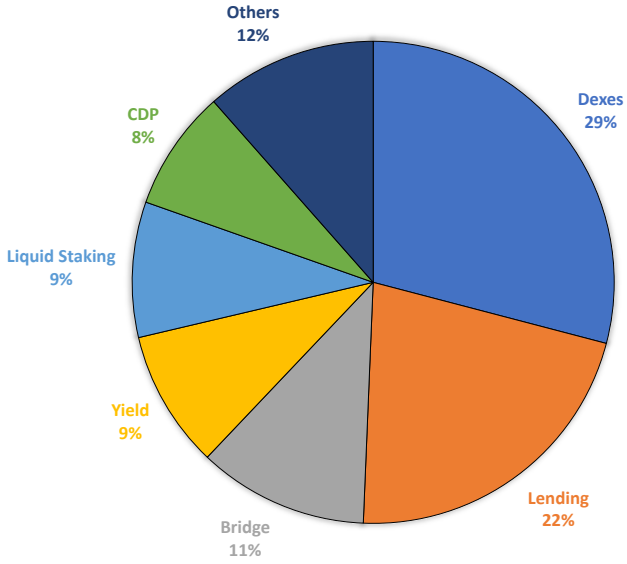
The economics literature on DeFi is just emerging. Many existing studies focus on decentralized exchanges and explore how automated market makers function differently from centralized exchanges; see Aoyagi and Ito (2021), Capponi and Jia (2021), Lehar and Parlour (2021), Park (2021). Another line of research investigates the economics of decentralized stablecoins such as Dai issued by the MakerDAO protocol (d'Avernas, Bourany, and Vandeweyer (2021), Li and Mayer (2021), Kozhan and Viswanath-Natraj (2021)).

Economic papers on DeFi lending are more limited in number. Lehar and Parlour (2022) empirically study how decentralized lending platforms affect the prices of crypto assets through liquidations of loans or collateral. Chiu et al. (2022) theoretically model a dynamic feedback between price and liquidity in DeFi lending and study the implications for fragility.[6] Our

[5]The key difference between the two is that a lending protocol lends out tokens deposited by lenders, while a CDP lends out tokens (typically stablecoins) minted by itself.

[6]There is also a related literature studying applications of smart contracts and the economic trade-offs

Figure 1.2: Decomposition of DeFi TVL in 2022 Q1 (Source: DeFiLlama)



viewpoint article contributes to this literature by using a simple, stylized model of borrowing to show what DeFi lending has to offer in terms of lower costs and better financial inclusion.

The article is organized as follows. In Section 2, we provide an overview of DeFi. Section 3 presents a simple model where lending involves either direct intertemporal trading or a centralized intermediary. Section 4 studies DeFi as an alternative arrangement and discusses its value proposition and limitations. Section 5 concludes by suggesting how proper infrastructure for DeFi may be built. Omitted proofs can be found in the Appendix.

2 What Is DeFi? An Overview

DeFi is an umbrella term for a variety of applications and projects in finance that attempt to reduce the reliance on costly, third-party intermediaries. These trusted actors are often replaced by smart contracts, which are immutable computer programs that guarantee execution of the contract. The concept of a smart contract was first introduced into computer science by Nick Szabo, who describes them as "building blocks for digital markets" embedding contracts into software and making their breach expensive (Szabo, 1996). He likened

involved; see, for example, Bakos and Halaburda (2021), Cong and He (2019), Lee et al. (2022).

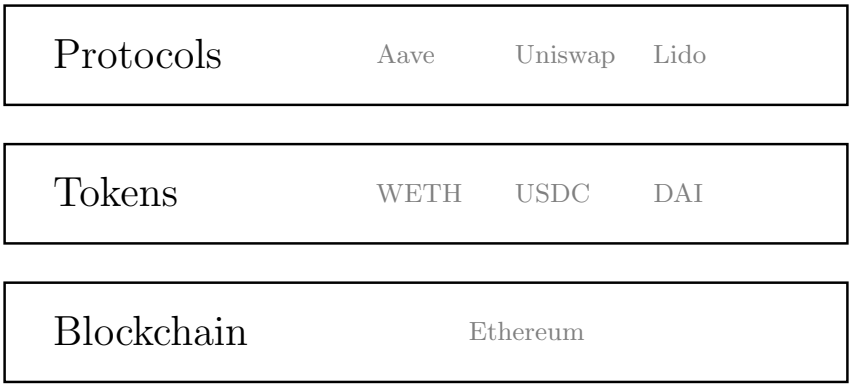
the idea to replacing a shopkeeper in a store with a pre-programmed vending machine.

The key development for DeFi was to link this idea to blockchain and distributed networks with the introduction of the Ethereum project. Smart contracts are run on a blockchain, which is a ledger simultaneously stored and updated across a distributed network of independent computers. As long as the blockchain is tamper-proof, smart contracts can be guaranteed to execute within this network without the use of a third-party intermediary.

2.1 DeFi Architecture

DeFi is designed as a multi-layered architecture with three primary layers (see Figure 2.1). The bottom one consists of the blockchain where the settlement of contracts occurs. The middle one creates assets as tokens that can be stored and transferred on the blockchain. The final one at the top contains the actual DeFi protocols that deploy the smart contracts. Above all these layers, there is an additional interface where potential users can access the application. Such applications can also integrate different protocols and offer wallets, which are local programs to run applications in a user-friendly way.

Figure 2.1: Basic DeFi Layers and Examples



Most DeFi protocols are run as a *permissionless* environment where anyone can use the protocol without third-party consent. Contracts can then freely interact with each other, be built on top of other existing contracts and even function across different protocols. As a result, DeFi protocols are *composable*. For example, one can write a smart contract that builds on a lending protocol and an exchange protocol to create a margin trade protocol.

We now briefly discuss the different layers of the DeFi architecture in further detail.

2.1.1 Settlement Layer

Bitcoin was the first blockchain application with a financial focus. As its script is rather simple, Bitcoin is mainly a system for recording ownership and transferring value. It is not designed as a foundational layer for other protocols to build on. In contrast, Ethereum, founded by the Ethereum Foundation, was specifically built to support the execution of smart contracts.[7]

Currently, Ethereum is the main blockchain for DeFi protocols, with over 50% of value in DeFi locked into it. While the majority of smart contracts are written on Ethereum, there are many other blockchains such as Algorand, Avalanche, Binance Smart Chain, Cosmos, Polkadot and Solana. These blockchains are designed to tackle issues such as scalability, interoperability and the cost of achieving consensus when a blockchain is updated with new information.

2.1.2 Token Layer

The process of tokenization allows users to create tokens building on the blockchain layer at the bottom. On Ethereum, the most popular standards are ERC20 for creating fungible (i.e., fully interchangeable) tokens and ERC721 for creating non-fungible tokens.

A token plays various roles in a protocol. For example, it can represent an IOU of a lending pool issued to a lender, or governance rights issued to an equity holder in a protocol. Tokens can also represent real-world assets. In particular, tokens can be designed as stablecoins intended to represent a stable value with respect to a unit of account.

Stablecoins can be backed by an asset off the blockchain, such as the US dollar or securities denominated in USD. Prominent examples are USD Coin (USDC) issued by Circle, Tether (USDT) issued by Bitfinex and Binance USD (BUSD) issued by Binance. Such an arrange-

[7]Ethereum has its own native cryptocurrency, Ether, which also serves to pay fees ("gas") for running the smart contracts.

ment typically requires a centralized, trusted third-party in the real world to hold reserves of the underlying asset to back the token. Hence, strictly speaking, these efforts a re not decentralized solutions.

Alternatively, one can issue a stablecoin that is backed by on-chain assets. A prime example is the stablecoin Dai, created by MakerDAO. This coin is backed by Ether (ETH) and other cryptocurrencies, for example USDC. The value of Dai is pegged to the US dollar and is based on over-collateralization, specifically a 33% haircut. More generally, one can create other synthetic tokens to replicate the income flows of real-world assets such as a stock index or standardized derivatives.[8]

2.1.3 Protocol Layer

DeFi protocols are built on top of the settlement and token layers. As previously noted, these protocols can serve a variety of purposes, the main ones being

- decentralized lending platforms
- decentralized exchanges for crypto assets
- customized derivatives
- asset management for crypto assets

with the first two being the most important examples.

Decentralized exchanges set up marketplaces to facilitate the spot trades of cryptocurrencies. These protocols have mainly arisen to permit the direct conversion of different cryptocurrencies without the use of traditional currencies. Many of the exchanges replicate real-world arrangements such as over-the-counter markets or limit-order books. A more novel type of decentralized exchange is the so-called "automated market maker" (AMM) which automates the price-finding mechanism based on the actual trades made on an exchange.

[8]Other attempts to create stablecoins are based solely on the principle of a "currency board" that actively intervenes to support a peg. However, such attempts have sometimes spectacularly failed (see, for example, the crash associated with the Terra/LUNA protocol).

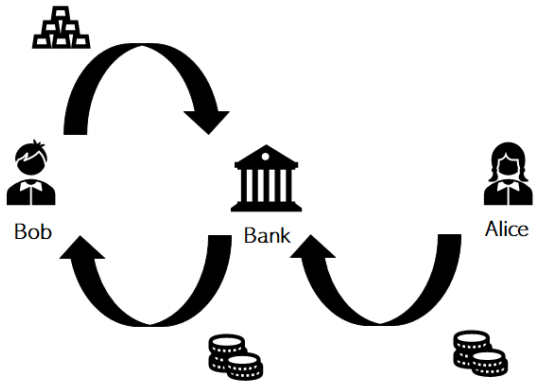
Decentralized lending platforms such as Aave, C.R.E.A.M. Finance, dYdX and Compound function very much like traditional banking intermediaries, taking in deposits in stablecoins and allowing borrowers to obtain funds in these stablecoins against crypto collateral. The main attraction of these platforms is that crypto users can use their investments as collateral to achieve additional functionality from their crypto holdings.

Other protocols generate value by introducing financial products that are hard to replicate with traditional arrangements. A prime example is *flash* loans. Unsecured credit can be provided under the condition that the loan must be repaid *atomically* within a single block of the underlying blockchain. This means that the borrower receives the funds, uses and repays them—all within the same blockchain transaction or in linked transactions within the same block. Hence, either all transactions are carried out, or none are. Flash loans help, for example, in arbitraging away price difference across different exchanges. For instance, if two AMM pools price a token differently, an investor can obtain a flash loan from a lending protocol, buy and sell in the two pools, and then repay the loan immediately, making a profit from the price discrepancy. While flash lending improves market efficiency, it can also be abused to launch so-called "flash attacks." For example, an attacker can use a flash loan to create an artificially large transaction on an illiquid exchange. The attacker can thereby temporarily manipulate the price and potentially profit from it, if a lending protocol relies on this price on the exchange to value collateral assets.

2.2 An Illustrative Example

Consider an example of arranging a secured loan using an intermediary such as a bank. As illustrated in Figure 2.2, suppose Bob wants to borrow cash from Alice. He is willing to pledge some assets as collateral. A financial intermediary—"the bank"—takes a cash deposit from Alice and lends the cash to Bob against his collateral held in custody. The collateral will be returned to Bob when he repays the loan. The bank will liquidate the collateral if Bob defaults. Bob has an incentive to default whenever the value of the collateral drops enough in value. A traditional arrangement that involves an intermediary is often referred to as *centralized finance* (CeFi).

Figure 2.2: Secured Loan Example



How does a typical DeFi lending protocol replicate this loan arrangement? Assume that the borrower takes out a loan in a stablecoin and secures the loan with a crypto asset. Lenders deposit their tokens individually into a lending pool that is governed by a lending protocol. To access funds in the lending pool, the borrower locks crypto collateral into a smart contract. The borrowing terms are calculated based on a pre-programmed function including the haircut on the collateral, the repayment schedule and the interest rate.

The smart contract is then executed according to its rules. Settlement is *atomic* in the sense that the collateral is only returned when all obligations are met by the borrower. Typically, the contract is over-collateralized to safeguard against default, but as the value of the collateral can fluctuate, the need to liquidate becomes an issue.

To deal with liquidation, two elements are required. First, the crypto asset that serves as collateral needs to be priced automatically using a price feed. This component of the arrangement, called an *oracle*, can be incorporated in the protocol or can come from a different DeFi application. Second, a *liquidation bot* is needed to monitor open borrowing positions and—using a smart contract—automatically liquidates under-collateralized positions.

This example makes it clear that decentralization is often a matter of degree, where different steps in this lending relationship may or may not be decentralized. First, the borrower and the lender need to be matched. This requires an effective matching engine or pool to be set up where lenders contribute funds and borrowers can access funds within the

protocol. Second, the digital form of funds—stablecoins in our example, but possibly other cryptocurrencies—are genuine representations of real-world cash balances. This requires a reliable tokenization process and, in the case of stablecoins, a reliable way to manage them. Third, the protocol needs to keep custody of the digital assets and allocate their ownership reliably. This requires a well-designed smart contract and a tamper-proof blockchain on which the contract is deployed. Fourth, there needs to be a mechanism to settle the contract unambiguously. This may involve the liquidation of collateral when the price of the collateral drops, which, as pointed out, necessitates an oracle and liquidation bots. Each of these components can be implemented by either an intermediary or a smart contract. Most DeFi applications decentralize the custody and settlement. Decentralizing other elements, such as tokenization or the oracle, is much harder to achieve.

2.3 A Short Preview

In the next two sections, we present a formal discussion of the value and limitations of both CeFi and DeFi. To do so, we focus on the example of decentralized lending just outlined and compare three different lending arrangements where a borrower has collateral, but needs to obtain liquidity against the collateral. One arrangement is a direct trading relationship with a lender. The problem is that both sides to a collateralized loan contract cannot commit to the terms of the contract. The borrower may default, while the lender may not return the collateral.

A second lending arrangement solves the problem by having a financial intermediary take custody of the collateral and execute the contract terms for a fee. The fee is necessary to give incentives to this third party to safeguard the collateral and execute the contract properly.

An alternative way, the third arrangement, is to use a smart contract. DeFi can then be seen simply as a different arrangement for custody and execution of the contract. We assume that the contract has a lower cost than using the third party. However, the collateral being used and, possibly, the stablecoin used for settlement as well, have higher volatility than their real counterparts. This gives rise to a trade-off for the value offered by the smart contract.

Beyond the issue of volatility, such DeFi arrangements tend to suffer from several limitations associated with the execution of the smart contract. Firstly, guaranteed execution comes at the cost of too little flexibility ex post. Secondly, the contract needs an oracle that provides price feeds that are necessary for executing the contract. These are potential areas where public infrastructure can increase the value proposition of DeFi in the future.

3 CeFi—Intermediated Lending

3.1 Setup

We start off by looking at a simple borrowing environment that requires collateral to secure a loan. There are two periods, $t = 0, 1$. Agents are risk neutral. We focus on two agents, a lender and a borrower.

There is a single nonstorable consumption good, y, which serves as numeraire. The lender has preferences given by

$$y_0 + y_1$$

and is endowed with e_L units of numeraire goods in period $t = 0$. The borrower values the numeraire good more than the lender in period $t = 0$,

$$(1 + v)y_0 + y_1,$$

where $v > 0$. The borrower is endowed with e_B units of the numeraire good in $t = 1$, but has no endowment of the good in period 0. We assume that e_L and e_B are sufficiently large for them to conduct the financial arrangements discussed below. Since the borrower and lender have different intertemporal marginal rates of substitution, there are gains from trade.

The borrower also has an endowment of one unit of a durable asset x in period 0. The asset matures at the end of period 1, when it provides a payoff to its holder. For the typical holder, the payoff of the asset is $p_1^x(s)$ in units of the numeraire good, where $s = \ell, h$ denotes

the state of the world in period $t = 1$. We assume the two states are equally probable and

$$p_1^x(h) = (1 + \delta)p^x$$
$$p_1^x(\ell) = (1 - \delta)p^x$$

so that the price of the asset is p^x in period 0. The state s is revealed at the beginning of period 1, so that the price of the asset in period 1 is given by $p_1^x(s)$.[9]

Since the asset is transferable, it also has the potential to serve as collateral. However, we assume that the asset is not perfectly liquid. There are two components to this assumption. First, when the borrower or lender sells the asset on the open market, there is a transaction cost of L per unit initially invested.[10] Second, we assume that for the lender, the asset yields no payoff if held in period 1; instead, he or she must sell the asset to obtain any value, thereby incurring the transaction cost. On the other hand, the borrower receives full benefit from the asset in period 1 and therefore does not need to sell it. In addition, we assume that

$$p^x(\ell) > L, \tag{1}$$

$$p^x(h) - p^x(\ell) > L. \tag{2}$$

The sequence of events is as follows. In period 0, the lender can transfer some of the endowment good to the borrower in exchange for the borrower's asset. In period 1, the borrower can in return transfer some endowment to the lender in exchange for the asset held by the lender. Since the numeraire good serves the role of a means of payment, which is used to settle trades, we will label it as cash.

Assumptions In period 0, in addition to spot transactions, the borrower and the lender can establish two-period agreements. In effect, these arrangements have the borrower receiving cash in period 0 in return for temporarily handing over the collateral asset to the lender. We assume that such trades are subject to these frictions:

[9] We treat these prices as exogenous in the sense that they are not influenced by the use of the asset as collateral in the lending relationship.

[10] To keep comparisons consistent across arrangements, we assume that the transaction cost only applies when dealing with the open market, not in direct interactions between the borrower and the lender.

1. State-contingent contracts whose terms depend on the realized value of the collateral asset x are too costly to write.

2. Neither the lender nor the borrower can commit to period 1 exchanges that are not ex post rational.

3.2 Direct Trading

We next look at the possibilities for the lender and borrower to directly trade with each other.

Spot sale of collateral Suppose the borrower sells the collateral in period 0 to the lender in order to finance consumption. Since the lender will resell it on the market, incurring the cost L, the lender will pay $p^x - L$.[11] Thus, the borrower's payoff is

$$(1 + v)(p^x - L). \tag{3}$$

The borrower gains from a spot sale whenever this payoff is greater than the expected payoff from retaining the asset or, in other words, if

$$p^x > L\frac{1+v}{v}, \tag{4}$$

which we assume throughout the analysis.

Direct Collateralized Lending Suppose now that the borrower asks for a cash loan C in period 0 against a promised repayment R in period 1 and hands over the asset as collateral to the lender to secure the loan. Our assumptions imply that both the lender and the borrower need an incentive to settle the trade and that not settling the trade is costly due to the cost L. The borrower defaults whenever the repayment is more costly than the value of the collateral:

$$R \geq p^x(s). \tag{5}$$

[11] This is without loss of generality since the borrower could equivalently sell the asset on the market at the same price.

The lender does not hand back the collateral if the repayment is too low, taking into account the liquidation cost

$$R \leq p^x(s) - L. \tag{6}$$

Given condition (2), the outcome is equivalent to a spot sale of the collateral unless one of the following mutually exclusive conditions holds:

$$p^x(\ell) \geq R > p^x(\ell) - L \tag{7}$$

or

$$p^x(h) \geq R > p^x(h) - L. \tag{8}$$

When condition (7) is satisfied, the loan is repaid in state ℓ, but the lender refuses to return the collateral for the state h, leading to liquidation. When condition (8) is satisfied, the loan is repaid in state h, but the borrower defaults in state ℓ, leading to liquidation. Since payoffs for the borrower are increasing in the cash advanced, we have the following result.[12]

Lemma 1. *The borrower offers the contract* (C, R) *with*

$$C = p^x - \frac{L}{2} \tag{9}$$

and $R \in \{p^x(h), p^x(\ell)\}$*, which yields a payoff equal to*

$$(1 + v)(p^x - \frac{L}{2}) \tag{10}$$

for the borrower.

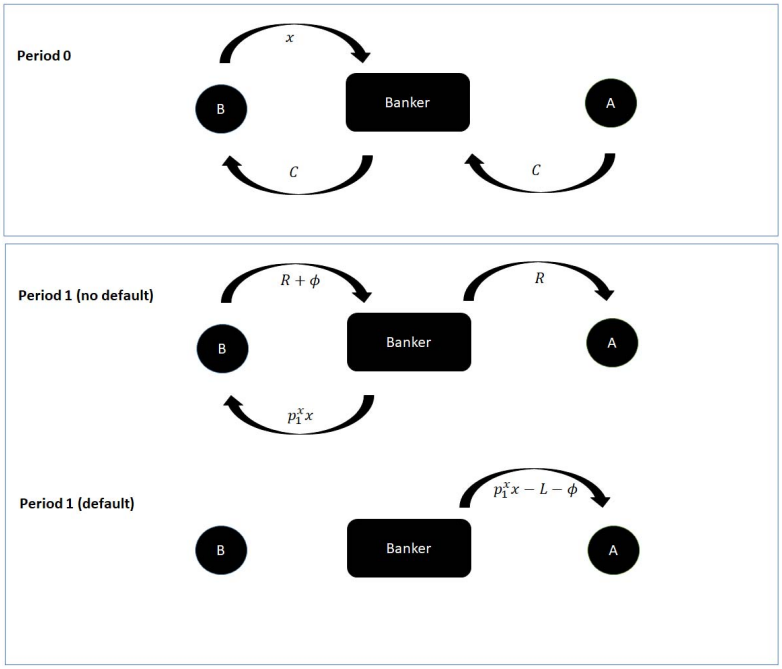
Since the lender gets zero expected profits, the social welfare is equal to the borrower's payoff, so that direct lending always dominates the spot sale of collateral. We turn next to the question of whether an intermediary can achieve an even better outcome.

[12]See the Appendix for a formal proof.

3.3 CeFi Loans

We consider now a third agent, a banker who is hired to intermediate loans. The banker has no personal funds; instead, the banker receives funds from the lender and lends them out to the borrower in period 0. The terms of the contract are again denominated by (C, R) and the borrower pledges asset x as collateral with the bank (see Figure 3.1).

Figure 3.1: CeFi Loan Arrangement



Like the lender, the banker has no direct use for the collateral. The banker, however, can commit not to steal the collateral and sell it, but to execute the loan agreement. The banker charges a fee $\phi > 0$ (payable by the borrower in cash in period 1). The fee reflects the fact that the bank is considered a *trusted third party*.[13]

[13]The fee is exogenous in our framework. However, it can be interpreted as the flow return to the charter value of the bank in a more general model. The outline of such a model is as follows. Denote the banker's discount factor by β. Assume that the bank incurs a one-time entry cost $\phi/(1-\beta)$ to acquire the bank charter. For simplicity, suppose the banker handles one loan each period. Then potential competition from other entrants ensures that the banker is limited to a fee of ϕ per loan, and the bank's profit is dissipated.

Since the borrower pledges the collateral with the bank, there is no incentive problem for the lender anymore. Hence, the only incentive problem is the borrower defaulting on the loan, which happens whenever

$$R + \phi \geq p^x(s). \tag{11}$$

3.4 Optimal CeFi Loan Contract

Suppose the contract maximizes the borrower's payoff.[14] When $R+\phi > p^x(h)$, the borrower always defaults and the contract terms are similar to those of a spot sale, with an additional cost ϕ. When $p^x(h) \geq R+\phi > p^x(\ell)$, the borrower defaults when the collateral value is low. One can easily show that the contract terms are then similar to those of direct lending, again with an additional cost ϕ. Since the bank charges a positive fee, there is no value offered by the banker intermediating the loan in these cases.

Thus the banker offers a loan contract (C, R) that solves

$$\max_{C,R}(1+v)C + p^x - R - \phi \tag{12}$$

subject to

$$C \leq R \tag{13}$$

$$R + \phi \leq p^x(\ell). \tag{14}$$

The objective function captures that the borrower receives $(1+v)C$ in period 0 and earns $p^x - R - \phi$ in period 1. The first constraint captures the lenders' participation in the loan arrangement, whereas the second one is necessary so that the borrower does not default.

If the banker absconds with the collateral, the bank loses its reputation and future business. In order to induce honest behavior, the fee must thus satisfy

$$\phi \geq (1-\beta)(p^x - L).$$

For a given $\phi > 0$, this restriction is always satisfied for β sufficiently close to 1.

[14]The borrower's payoff is equivalent to social welfare for all lending arrangements since she receives all surplus and banking has zero profits.

Since $v > 0$, we have that the objective function is increasing in R after substituting the first constraint. Hence, we have the following result.

Lemma 2. *The optimal CeFi loan arrangement is given by*

$$C = R = p^x(\ell) - \phi \tag{15}$$

so that the payoff for the borrower is

$$(1+v)p^x(\ell) - (1+v)\phi + p^x. \tag{16}$$

The bank adds value since it can solve the two-sided commitment problem. Hence, there is a trade-off between incurring the banker's fee ϕ and the cost of inefficiently liquidating the collateral L when there is default in the optimal direct lending arrangement. We have the following result.

Proposition 3. *CeFi lending is optimal if and only if*

$$L \geq \bar{L} = \left(\frac{v}{1+v}\right)(p^x(h) - p^x(\ell)) + 2\phi. \tag{17}$$

Discussion A bank loan is thus preferred, whenever the costs of default are large relative to the costs of using a trusted third party. It is interesting to also look at the loan size relative to the ex ante value of the collateral. This can be summarized by the haircut defined as

$$H = 1 - \frac{C}{p^x}. \tag{18}$$

A larger haircut means that the loan is more over-collateralized. The haircut on the bank loan and direct lending are given by

$$H = \frac{1}{p^x}\left(\frac{1}{2}(p^x(h) - p^x(\ell)) + \phi\right) \tag{19}$$

and

$$H = \frac{1}{p^x}\frac{L}{2}, \tag{20}$$

respectively. The haircut on the bank loan is thus always larger since

$$L < (p^x(h) - p^x(\ell)) + 2\phi. \tag{21}$$

Define next the quality of the collateral good by the volatility of its price

$$\delta = \frac{p^x(h) - p^x(\ell)}{2p^x}. \tag{22}$$

Holding the expected payoff p^x constant, the loan size for direct lending is unaffected by changes in volatility, but the haircut associated with the bank loan increases. Consequently, collateral that is more volatile decreases the attractiveness of a bank loan.

4 DeFi—Decentralized Lending

4.1 Setup

We now consider a DeFi platform that offers contracts without relying on a trusted third-party. Instead, the platform uses a blockchain to store and execute an atomic, smart contract. The environment remains the same as in the previous section, except for the introduction of two new assets.

First, there is now a second asset c, which is a crypto asset that can be stored on the blockchain and kept safe within a smart contract. This solves the problem that the lender can seize the collateral in period 1. Consequently, using a smart contract, the borrower and lender can avoid the fee ϕ.[15] The payoff in period 1 of this asset is given by

$$p_1^c = \begin{cases} (1+\varepsilon)p^c & \text{w.p. } 0.5 \\ (1-\varepsilon)p^c & \text{w.p. } 0.5. \end{cases}$$

In order to facilitate a clear comparison, we assume that $p^c = p^x$ and that both assets face the same liquidation cost L. We can then allow the borrower to exchange one unit of asset x against one unit of the crypto assets c at the start of period 0.

[15] More generally, one could assume that there are costs associated with deploying the smart contract on the blockchain. In what follows, we interpret ϕ as the cost saved by employing a smart contract in lieu of a bank.

Second, there exists a stablecoin s which is used on the blockchain to settle the smart contract.[16] The stablecoin is necessary because cash cannot be tokenized on the blockchain. The stablecoin is liquid, in that there are no costs to purchasing or selling it.

The value of stablecoins fluctuates according to

$$p_1^s = \begin{cases} (1+\eta)p^s & \text{w.p. } 0.5 \\ (1-\eta)p^s & \text{w.p. } 0.5 \end{cases}$$

where $\eta < \varepsilon$. Hence, the crypto collateral is more volatile than the stablecoin and, consequently,

$$\frac{1+\varepsilon}{1+\eta} > \frac{1-\varepsilon}{1-\eta}. \tag{23}$$

Stablecoins in period 0 trade at their expected value p^s. Finally, we assume that the distributions of payoffs for the two assets and the stablecoin are independent.

4.2 DeFi Loans

The borrower now receives a loan (S, R) from the lender, where S is the size of the loan in stablecoins and R is the promised repayment, also in stablecoins. The loan is executed automatically by an atomic smart contract. Hence, the smart contract can avoid the fee ϕ associated with a bank loan. If the borrower repays the loan, the smart contract returns the collateral to the borrower. If the loan is not repaid, the smart contract automatically liquidates the collateral, incurring the deadweight loss L (see Figure 4.1).[17]

It is always optimal for the borrower to convert the entirety of the loan into consumption in period 0, then wait until period 1 to purchase the stablecoins to repay the loan. The borrower defaults if and only if the obligation to repay the loan in stablecoins exceeds the

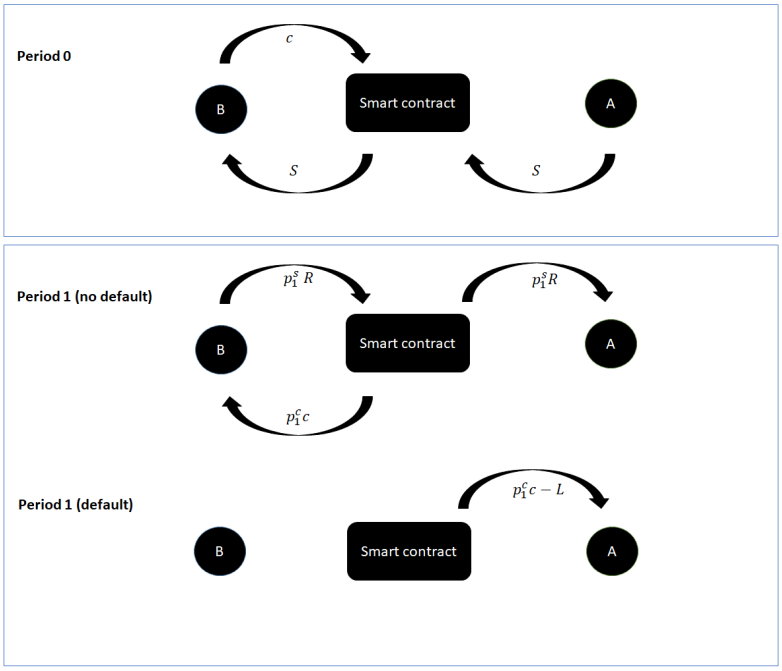
[16] We assume that stablecoins, just like cash in CeFi, cannot be pledged as collateral in DeFi. In reality, many major stablecoins (e.g., USDT, BUSD) are not accepted by DeFi lending platforms as collateral.

[17] In principle, the liquidation costs for crypto assets can be different from L. It may be more costly to liquidate crypto assets (for example, due to slippage when the asset is sold through an illiquid AMM) or less costly (for example, due to the fungibility of some crypto assets).

value of the collateral, or

$$p_1^s R > p_1^c. \tag{24}$$

Figure 4.1: DeFi Loan Arrangement



Assume for the rest of this section that L is sufficiently large so that any default by the borrower is suboptimal.[18] Then the contract requires

$$R \leq \frac{1-\varepsilon}{1+\eta}\frac{p^c}{p^s} \tag{25}$$

so that there is no default risk. Thus the optimal contract solves

$$\max_{S,R}(1+v)p^s S + p^c - p^s R \tag{26}$$

subject to (25) and

$$S \leq R. \tag{27}$$

[18]The Appendix provides an analysis where it can be optimal for the DeFi loan to include some default by the borrower, if L is sufficiently small. Interestingly, we also show there that DeFi optimally rules out default whenever the stablecoin is not volatile ($\eta = 0$).

The objective function captures that the borrower swaps asset x for the crypto asset, receives $(1+v)Sp^c$ in consumption in period 0, and repays the obligations from the DeFi loan, $p_1^c - p_1^s R$, in period 1. This yields

$$R = S = \frac{1-\varepsilon}{1+\eta}\frac{p^c}{p^s} \tag{28}$$

for the optimal DeFi loan, with the borrower's payoff given by

$$v\left(\frac{1-\varepsilon}{1+\eta}\right)p^c + p^c. \tag{29}$$

Hence, we have the following result establishing that DeFi saves costs while preventing default.

Proposition 4. *Suppose $L \geq \bar{L}$ and $p^c = p^x$. DeFi without default dominates CeFi if and only if*

$$\phi \geq \left(\frac{v}{1+v}\right)\left((1-\delta) - \frac{1-\varepsilon}{1+\eta}\right)p^c. \tag{30}$$

The optimal DeFi contract has the advantage of saving the banker's fee ϕ. DeFi is thus optimal as long as the cost ϕ of relying on a trusted third party to execute the lending arrangement is large enough. This captures the promise of DeFi to reduce the cost of lending. To the contrary, DeFi relies on crypto collateral and stablecoins for settlement that are both potentially more volatile. If the cash price of traditional collateral is more volatile than the cash price of crypto collateral, then DeFi dominates even if the banker's fee were zero. Finally, when the lending arrangement or collateral assets become more valuable, DeFi becomes less attractive. This points to a role for DeFi for less important lending markets.

Consider now a situation where ϕ is too high so that CeFi is dominated by direct trading. DeFi can still be better than direct trading since it can rule out default for the contracting parties without using the banker. This is summarized in the following result.[19]

[19]For L sufficiently small and $\eta > 0$, it can be the case that a DeFi contract with some default is best. See the Appendix for the analysis.

Proposition 5. *Suppose $L < \bar{L}$ and $p^x = p^c$. DeFi without default dominates direct trading if and only if*

$$L \geq 2\left(\frac{v}{1+v}\right)\left(\frac{\varepsilon+\eta}{1+\eta}\right)p^x. \tag{31}$$

Hence, DeFi also provides value in that it expands intermediation to lending contracts that did not rely on intermediation before due to the high costs of using formal lending contracts. In this sense, DeFi also fosters financial inclusion.

4.3 The Limitations of DeFi

Volatility of Stablecoins and Crypto Collateral It is instructive to consider more carefully the effect of volatility on DeFi. To do so, we can compare haircuts for DeFi and CeFi lending. The haircut for a CeFi loan can be written as

$$\delta + \frac{\phi}{p^x}, \tag{32}$$

while the haircut for a DeFi loan without default is given by

$$1 - \frac{Sp^s}{p^c} = 1 - \frac{1-\varepsilon}{1+\eta}. \tag{33}$$

The lower the haircut on the DeFi loan, the more likely it is to be preferable to the CeFi loan. If returns on ordinary and crypto collateral are the same and the DeFi haircut is smaller than the CeFi haircut, then the DeFi loan is guaranteed to be superior.

The haircut formula makes it clear that volatility of stablecoins and crypto collateral are important factors for the value proposition of DeFi. In general, crypto assets seem to be more volatile than traditional, real assets used for collateral, such as Treasury bills. As the volatility of the crypto collateral increases, the DeFi contract becomes less attractive relative to the bank loan.

For example, ETH, being the native token on Ethereum, is often used as collateral in DeFi lending. ETH is substantially more volatile than traditional collateral assets, with its value

sometimes fluctuating by 25% within a day. Such volatility can result in wide spreads for loans, liquidations and losses from lending.[20]

Incomplete Contracts While a smart contract allows for guaranteed execution, it may have to be incomplete. Consider a situation where with probability $(1-\theta)$ the borrower loses the endowment e_B in period 1. In this event, even if the borrower has an incentive to repay the loan, they cannot do so, being unable to acquire the settlement asset. Note that this information is "soft" in the sense that one needs to verify the circumstances why the borrower does not repay the loan.

The optimal DeFi loan is now given by

$$\max_{S,R}(1+v)p^sS+\theta(p^c-p^sR) \tag{34}$$

subject to

$$p^sS \leq \theta p^sR+(1-\theta)(p^c-L) \tag{35}$$

$$R \leq \frac{1-\varepsilon}{1+\eta}\frac{p^c}{p^s} \tag{36}$$

with the solution yielding the following payoff for the borrower:

$$v\left(\theta\frac{1-\varepsilon}{1+\eta}+(1-\theta)\right)p^c-(1+v)(1-\theta)L+p^c. \tag{37}$$

To the contrary, a CeFi contract allows the bank to condition on the "soft" information and forgive the loan repayment in that contingency, while returning the collateral to the borrower. This avoids the liquidation cost. Assuming the fee ϕ also includes the expected costs of verifying the borrower's condition, we obtain

$$\max_{C,R}(1+v)C+p^x-\theta(R+\phi) \tag{38}$$

subject to

$$C \leq \theta R \tag{39}$$

$$R+\phi \leq (1-\delta)p^x \tag{40}$$

[20]On February 23, 2021, a record-high $115 million in DeFi lending positions were wiped out following a large price decline of ETH.

for the CeFi lending arrangement. Hence, the borrower's payoff is given by

$$v\theta(1-\delta)p^x - (1+v)\theta\phi + p^x. \tag{41}$$

This yields the following result.

Corollary 6. *Assume $p^x = p^c$. When smart contracts are incomplete, DeFi is better than CeFi if and only if*

$$\phi \geq \left(\frac{v}{1+v}\right)\left(1-\delta-\frac{1-\varepsilon}{1+\eta}\right)p^x + \left(\frac{1-\theta}{\theta}\right)\left(L - \frac{v}{1+v}p^x\right). \tag{42}$$

Relative to the original case, DeFi becomes less attractive whenever the last term is positive. As the DeFi smart contract cannot replicate the state contingency of the bank loan, there needs to be an advantage for it to become optimal. When stablecoins are stable ($\eta \to 0$), such an advantage can arise if the crypto collateral is less volatile and its liquidation costs are sufficiently small. In reality, however, crypto assets tend to be more volatile than most real assets that serve as collateral. Hence, as more contract flexibility is required, DeFi tends to lose its value when L is relatively large.

The Oracle Problem DeFi contracts rely on price feeds that correctly specify the value of the collateral and the stablecoin. To see the problems that can arise from mispricing, consider an example where $p^c = p^x = p^s = 1$ and, in particular, the borrower is aware that $p^c = 1$, but the oracle misspecifies the price of the collateral as[21]

$$\rho > 1. \tag{43}$$

The borrower can then take out a DeFi loan at $\tilde{R} = \rho\frac{1-\varepsilon}{1+\eta}$, which results in a lower haircut than with the correct price. Assume now for simplicity that

$$\rho > \left(\frac{1+\varepsilon}{1-\varepsilon}\right)\left(\frac{1+\eta}{1-\eta}\right) \tag{44}$$

[21] More generally, ρ represents a distortion of the relative price $\frac{p^c}{p^s}$.

so that the DeFi loan defaults for sure. The borrower's payoff is then given by

$$(1+v)\rho\left(\frac{1-\varepsilon}{1+\eta}\right), \tag{45}$$

but the surplus from lending is only given by

$$v\rho\left(\frac{1-\varepsilon}{1+\eta}\right) - L, \tag{46}$$

the difference being the lender's payoff.

Recall that, under the optimal CeFi arrangement, the borrower's payoff is

$$v(1-\delta) - (1+v)\phi, \tag{47}$$

which is equivalent to total surplus. This implies that the borrower would prefer the DeFi loan, even though this is not socially optimal whenever

$$(1+v)\rho\left(\frac{1-\varepsilon}{1+\eta}\right) > v(1-\delta) - (1+v)\phi > v\rho\left(\frac{1-\varepsilon}{1+\eta}\right) - L. \tag{48}$$

Since the first inequality always holds by assumption (44), we have the following result.

Corollary 7. *Suppose $L > (1+v)\phi$. If the oracle overprices the crypto collateral, there is inefficient adoption of DeFi.*

When the crypto collateral is mispriced, the borrower would like to take advantage by using a DeFi loan and then default on the loan. Since the lender bears the liquidation cost from the unanticipated default, there is now a wedge between the borrower's payoff and social welfare. In the extreme case, where lending does not add much value ($v \to 0$), the borrower would still prefer DeFi lending, even though there would be no surplus generated at all from lending per se. This is akin to the borrower arbitraging against the oracle.[22]

[22]Such a situation occurred for example during the TerraUSD collapse in May 2022. As a result of the extreme volatility in the price of LUNA tokens, the price feed used for DeFi smart contracts denominated in the LUNA token was significantly higher than the actual market value of the token. Attackers exploited the price discrepancy to obtain loans collateralized by an inflated LUNA token from the underlying Venus protocol. This led to a loss of about $11.2 million for the protocol until the protocol increased the haircut of LUNA from 45% to 100%, essentially stopping lending against LUNA collateral altogether.

Further Limitations—Externalities and Anonymity When there are many borrowers and lenders paired on the DeFi platform, there can be an interdependency between individual smart contracts via *price externalities*. Suppose the value of the crypto collateral depends on the selling pressure in the market according to $\alpha(n)p^c(s)$, where n is the fraction of collateral being liquidated in the market.[23]

For $\alpha(0) = 1$ and $\alpha'(n) < 0$, there is a fire sale externality. Given the period 0 belief that $n = 0$, the individually optimal DeFi contract between a borrower and a lender sets $R = \frac{1-\varepsilon}{1+\eta}$. In period 1, however, if some borrowers switch their belief to $n > 0$, then all borrowers are induced to default. This leads to a self-fulfilling fire sale equilibrium, which is socially inefficient due to the liquidation cost L. Such a scenario is less likely to occur with CeFi arrangements, as the banker may have an incentive to avoid liquidation of collateral, if this were to compromise the fee.

Another limitation of DeFi is that—in principle—borrowers are anonymous on the platform. This anonymity tends to arise from the fact that individuals can assume several identities on DeFi platforms. Hence, rationing of credit is limited because individual borrowers cannot be uniquely identified.

Interestingly, this also precludes the use of more complicated, nonlinear contracts. The reason is that these would give rise to arbitrage where borrowers can achieve better outcomes by taking out smaller, but more individual, loans. Hence, DeFi contracts tend to be linear in their pricing.

5 Building a Proper Infrastructure for DeFi

Some of the limitations of DeFi could be alleviated by building a proper third-party-provided infrastructure. An institution—possibly public—that took on certain tasks could improve the functionality of DeFi applications. This is ironic, since DeFi is supposed to be built on a fully decentralized infrastructure. The first of such tasks is to improve the quality of the assets used in DeFi, both stablecoins and collateral assets. For stablecoins, the obvious issue

[23]This price externality is particularly likely to occur with an illiquid pool on a decentralized exchange.

is to ensure their stability. One possibility is for a central bank to issue a CBDC that can be tokenized and transacted on public blockchains. DeFi applications would then have access to a standardized, riskless settlement asset.

Alternatively, central banks could simply ensure that the issuers of stablecoins have access to their balance sheets. As a consequence, stablecoins could operate as a narrow bank where the issued coins are fully backed by deposits at the central bank. This would clearly remove any ambiguity with respect to the backing of a coin. But it would also foster private innovation to create tokenizable and programmable stablecoins. Prudential regulation would be necessary, since DeFi could otherwise be used as a means for regulatory arbitrage without adding any value per se.

There are also opportunities to improve the quality of the collateral that can be used by DeFi applications. One way to foster the adoption of DeFi is to tokenize standard collateral such as government-issued securities. Developing this capacity is a public good, which in turn could foster incentives to tokenize private assets within the same infrastructure.

Finally, the provision of oracles, like the provision of any other information, is a classic public good. For some oracles, a public institution with little incentive to manipulate the information could prove a more trustworthy guarantor of quality; for other oracles, a private institution might be the best provider.

In short, DeFi holds the promise to make financial arrangements more efficient and more inclusive. A natural way to lever these promises into concrete success is by building a proper infrastructure to support innovative, private applications. Such infrastructure, however, is likely to rely on some designated third party, making the notion of a fully decentralized system somewhat of an illusion (Aramonte et al., 2021).

References

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

Aramonte, S., W. Huang and A. Schrimpf (2021) "DeFi Risks and the Decentralisation Illusion", *BIS Quarterly Review*, December.

Bakos, Y. and H. Halaburda (2021) "Blockchains, Smart Contracts and Connected Sensors: Substitutes or Complements?", NYU Stern School of Business, August 1.

Capponi, A. and R. Jia (2021) "The Adoption of Blockchain-based Decentralized Exchanges", arXiv preprint arXiv:2103.08842

Chiu, J. and T. V. Koeppl (2019) "Blockchain-based Settlement for Asset Trading", *Review of Economic Studies*, 32, pp. 1716–1753

Chiu, J., E. Ozdenoren, K. Yuan and S. Zhang (2022) "On the Inherent Fragility of DeFi Lending", Manuscript

Cong, L. W. and Z. He (2019) "Blockchain Disruption and Smart Contracts", *The Review of Financial Studies*, 32, pp. 1754–1797

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

Harvey, C. R., A. Ramachandran and J. Santoro (2021) *DeFi and the Future of Finance*, New York: John Wiley & Sons

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

Lee, M., Martin, A. and R. M. Townsend (2021) "Optimal Design of Tokenized Markets", SSRN: http://dx.doi.org/10.2139/ssrn.3820973.

Lehar, A. and C. A. Parlour (2021) "Decentralized Exchanges", SSRN: http://dx.doi.org/

10.2139/ssrn.3905316

Lehar, A. and C. A. Parlour (2022) "Systemic Fragility in Decentralized Markets", SSRN: https://ssrn.com/abstract=4164833

Li, Y. and S. Mayer (2021) "Money Creation in Decentralized Finance: A Dynamic Model of Stablecoin and Crypto Shadow Banking", SSRN: https://ssrn.com/abstract=3757083

Park, A. (2021) "The Conceptual Flaws of Constant Product Automated Market Making",

SSRN: https://ssrn.com/abstract=3805750

Schär, F. (2021) "Decentralized Finance: On Blockchain-and Smart Contract-based Financial Markets", Federal Reserve Bank of St. Louis Review vol. 103(2), pages 153–174, April.

Szabo, N. (1996) "Smart Contracts: Building Blocks for Digital Markets" *EXTROPY: The Journal of Transhumanist Thought*, 16 18.2:28

A Proof of Lemma 1

Note first that, by assumption, $p^x(h) - L > p^x(\ell)$.

Consider $R \in [p^x(\ell) - L, p^x(\ell)]$. The borrower then solves

$$\max_{C,R} \quad (1+v)C + \frac{1}{2}(p^x(\ell) - R) \tag{49}$$

subject to

$$C \leq \frac{1}{2}R + \frac{1}{2}(p^x(h) - L) \tag{50}$$

since the lender keeps the collateral in the high state. After substituting the constraint with equality, the objective function is increasing in R. Hence, we have that $R = p^x(\ell)$ and $C = p^x - L/2$.

Next, consider $R \in [p^x(h) - L, p^x(h)]$. The borrower's problem is now given by

$$\max_{C,R} \quad (1+v)C + \frac{1}{2}(p^x(h) - R) \tag{51}$$

subject to

$$C \leq \frac{1}{2}R + \frac{1}{2}(p^x(\ell) - L) \tag{52}$$

since the borrower defaults in state ℓ. The solution is $R = p^x(h)$, and again we have $C = p^x - L/2$.

For all other cases, the collateral is always liquidated. Hence, the outcome is identical to a spot sale, and thus dominated by this arrangement.

B Optimal DeFi Contracts with Default

For clarity, we focus on the case where $p^c = p^s = 1$. The results are unaffected by this assumption. When $R > \frac{1+\varepsilon}{1-\eta}$, the borrower always defaults. This is equivalent to a spot trade.

Consider now $R \in (\frac{1+\varepsilon}{1+\eta}, \frac{1+\varepsilon}{1-\eta}]$. Then, the borrower defaults unless the crypto collateral has a high value and the stablecoin has a low value. The borrower's problem is then given by

$$\max_{S,R}(1+v)S + \frac{1}{4}(1+\varepsilon-(1-\eta)R) \tag{53}$$

subject to

$$S \leq \frac{1}{4}(1-\eta)R + \frac{1}{2}((1-\varepsilon)-L) + \frac{1}{4}((1+\varepsilon-L). \tag{54}$$

The borrower's payoff from the optimal contract is then

$$v - (1+v)\frac{3}{4}L \tag{55}$$

which is worse than direct lending.

Consider next $R \in (\frac{1-\varepsilon}{1-\eta}, \frac{1+\varepsilon}{1+\eta}]$. Then, there is default whenever the crypto collateral has a low value. Thus, the borrower solves

$$\max_{S,R}(1+v)S + \frac{1}{2}((1+\varepsilon)-R) \tag{56}$$

subject to

$$S \leq \frac{1}{2}R + \frac{1}{2}((1-\varepsilon)-L) \tag{57}$$

so that the payoff from the contract is given by

$$\frac{v}{2}\left(\frac{1+\varepsilon}{1+\eta} + (1-\varepsilon)\right) - (1+v)\frac{L}{2} < v - (1+v)\frac{L}{2}. \tag{58}$$

Hence, the contract is again dominated by direct lending.

Consider then a repayment $R \in (\frac{1-\varepsilon}{1+\eta}, \frac{1-\varepsilon}{1-\eta}]$. Since there is default only when the crypto

collateral has a low value, but the stablecoin has a high value, the optimal contract solves

$$\max_{S,R}(1+v)S+\frac{1}{2}((1+\varepsilon)-R)+\frac{1}{4}((1-\varepsilon)-(1-\eta)R) \tag{59}$$

subject to

$$S\leq\frac{1}{2}R+\frac{1}{4}(1-\eta)R+\frac{1}{4}((1-\varepsilon)-L). \tag{60}$$

Hence, the borrower's payoff from such a contract is given by

$$v\left(1-\frac{\eta}{2}\right)\left(\frac{1-\varepsilon}{1-\eta}\right)-(1+v)\frac{L}{4}. \tag{61}$$

The borrower can thus reduce the default probability and potentially obtain a cheaper loan when the stablecoin has a lower value in period 1.

Finally, when $R\leq\frac{1-\varepsilon}{1+\eta}$, there is no default. This is the case analyzed in the main body of the paper. We can summarize our result as follows.

Lemma 8. *The optimal DeFi contract is given by no liquidation and*

$$R=S=\frac{1-\varepsilon}{1+\eta} \tag{62}$$

if and only if

$$\frac{L}{2}\geq\frac{v}{1+v}(1-\varepsilon)\left(\frac{\eta(2-\eta)}{1-\eta^2}\right). \tag{63}$$

Otherwise, the optimal contract includes some liquidation and satisfies

$$R=\frac{1-\varepsilon}{1-\eta} \tag{64}$$

$$S=\left(1-\frac{\eta}{2}\right)\left(\frac{1-\varepsilon}{1-\eta}\right)-\frac{L}{4}. \tag{65}$$

When liquidation costs are low, the optimal DeFi contract includes default in the worst possible state, i.e., when the value of the crypto collateral is low and the stablecoin's value is high. If there is no difference in the volatility of the two collateral assets, the DeFi contract with default always dominates direct lending. The reason is simply that the haircut is smaller due to the lower likelihood of default.

If the liquidation costs are large, the optimal DeFi contract does not include default. More interestingly, however, whenever the stablecoin has a small enough volatility ($\eta \to 0$), the optimal DeFi contract never allows for default.

These results are somewhat an artifact of our model. First, contracts are not state contingent. However, a DeFi contract with default can increase the state contingency relative to direct lending. Second, we assume risk neutrality and iid shocks to crypto collateral as well as stablecoins. The advantage of DeFi with some default may disappear if we relax these assumptions.