A 2023 PRIMER FOR CRYPTO CREDIT MARKETS

AUGUST 2023

Authors: Andreas Park, *University of Toronto*
Jona Stinner, *Witten/Herdecke University*

Lending and borrowing play critical roles in the economy, enabling individuals, businesses, and governments to access capital necessary for investments, expansions, and projects. The ability to lend and borrow efficiently facilitates the allocation of capital, and without borrowing, economic growth would be severely limited. On the other hand, without lending facilities, there would be no borrowing.

A blockchain is a digital value management tool and facilitates the financial infrastructure for the digital economy. However, understanding blockchain-based lending and borrowing can be challenging. We review the existing solutions in this paper.

The market for blockchain-based lending and borrowing has evolved through several stages. In the first stage, centralized services led by trading platforms dominated the market. In the second stage, blockchain innovators developed decentralized solutions that relied on collateral. In the third and current stage, a combination of centralized and decentralized solutions enables uncollateralized loans.

In this primer we review the central concepts such as centralized and decentralized platforms, the economic tools that platforms use to attract liquidity, and related concepts such as yield farming and aggregation.

CENTRALIZED LENDING

In the context of lending, there are two main types of arrangements: direct and intermediated.

Direct lending involves the lender and borrower agreeing on a contract, with peer-to-peer lending being a popular example. Previously, direct lending was a rare occurrence reserved for personal relationships, but with the emergence of FinTech platforms like LendingClub, it has become more accessible. Standardized contracts, such as bonds, can also be considered a form of direct lending, even though they may include unique features like covenants. While bonds are typically issued by large entities, some countries, such as Denmark, allow homeowners to issue their mortgages as a bond-like product. The core feature of the bond market is that the claims are tradable.

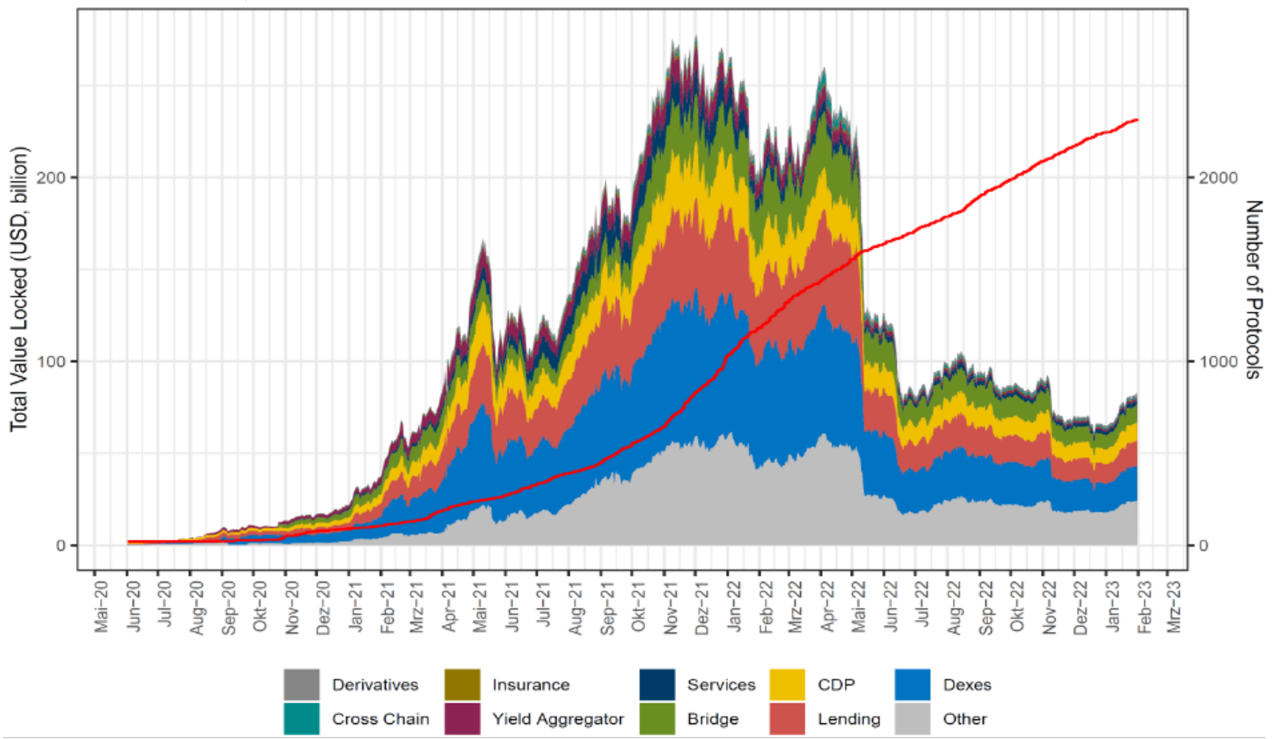
On the other hand, intermediated lending involves investors depositing funds into a pool and the pool organizer making lending decisions. Banks are the most prevalent type of intermediated lender, as their sizable pools facilitate crucial functions such as size, time, and risk intermediation. Pooling enables banks to combine small deposits into large loans, convert short-term deposits into long-term loans, and diversify risk. Indirect offerings, such as mortgage-backed securities, allow investors to purchase a claim on an asset pool, but they are considered capital market investment products, and they are not the subject of this paper.

In traditional finance, intermediated lending involves the intermediary taking custody of the investor's assets and issuing a receipt or IOU. This means that the intermediary controls the client's assets and plays a crucial role in making risk assessments when granting loans. Depositors rely on the intermediary to make responsible assessments, which is why banks are tightly regulated.

In the crypto world, the first entities that engaged in borrowing and lending were centralized platforms like Bitfinex or Poloniex. While they are called "exchanges," they function more like brokerages, taking deposits of cash and digital assets and facilitating the sale of digital assets. Many also offer loans, such as for margin trading and short selling, invest in the tokens for which they facilitate trading, and even run market-making programs.

One concern with these centralized platforms is that they take custody of customers' assets and list these assets on their balance sheets.[i] Clients then become creditors and are exposed to risk if the exchange defaults. Ideally, trading businesses would establish accounts at custodians in the client's name. However, many platforms allegedly combined all assets in omnibus accounts, possibly commingling them with their own holdings and using an internal system to track holdings. As a result, platforms could use customer funds to make loans, which exposes the customer to risk. For example, centralized crypto exchanges offer loans through margin trading and short selling. In the

Figure 1: Total Value Deposited in All DeFi Protocols



The figure depicts the total deposits in DeFi projects, denominated in billion USD (left-axis), and the number of total protocols (right axis). "Other" includes 23 categories, each accounting for less than 0.01% of total deposits.

Data Source: https://defillama.com/docs/api

i Since April 2022, according to the SEC's Accounting Bulletin No. 121, crypto-exchanges are required to list their clients's assets on their balance sheets. This practice differs from brokerages which leave the value of clients' assets off their balance sheets.

infamous case of FTX, the Alameda hedge fund was able to take on significant risks and accumulated losses that ultimately left the FTX depositors on the hook. Since there is no oversight of the platforms, it is difficult to assess the extent to which customers were affected by improper handling of deposits.

The second generation of crypto lending platforms, such as Celsius, entered the market with a specific value proposition of providing users with interest payments on their crypto assets. These platforms assume custody of users' cryptocurrency deposits and lend them out to borrowers for a specified period. They often promise higher deposit rates than traditional banks while assuring the safety of the returns. However, concerns have been raised that the high rates of return may not be sustainable, and the platform may expose depositors to substantial and inadequately managed risks.

The collapse of the stablecoin UST in May 2022 triggered a chain reaction that caused one of the largest centralized crypto lenders to file for Chapter 11. The UST collapse led to the collapse of the Luna network and the hedge fund Three Arrows Capital (3AC). The Celsius Network, which is centralized despite its name, was one of a number of crypto lenders that had made significant loans to 3AC and subsequently went bankrupt. Depositors found themselves in the position of junior creditors in Celsius' bankruptcy proceedings, highlighting the potential risks associated with centralized crypto lending platforms.

Conceptually, there is nothing novel and economically interesting about centralized lending platforms. They made risky loans to risky entities that paid handsomely in bullish markets but crashed miserably when markets went down. The main deviation from conventional finance is the type of asset utilized and the absence of regulatory supervision.

In what follows, we will focus on the innovative part of the crypto ecosystem: decentralized blockchain-based lending platforms. A fundamental distinction between DeFi (Decentralized Finance) and the traditional finance world is the custody arrangement of assets. Namely, users hold assets in self-custody, and lending platforms are non-custodial. To understand the concept and its implications, we will first review the different custody arrangements.

CRYPTO-VENUE CUSTODY

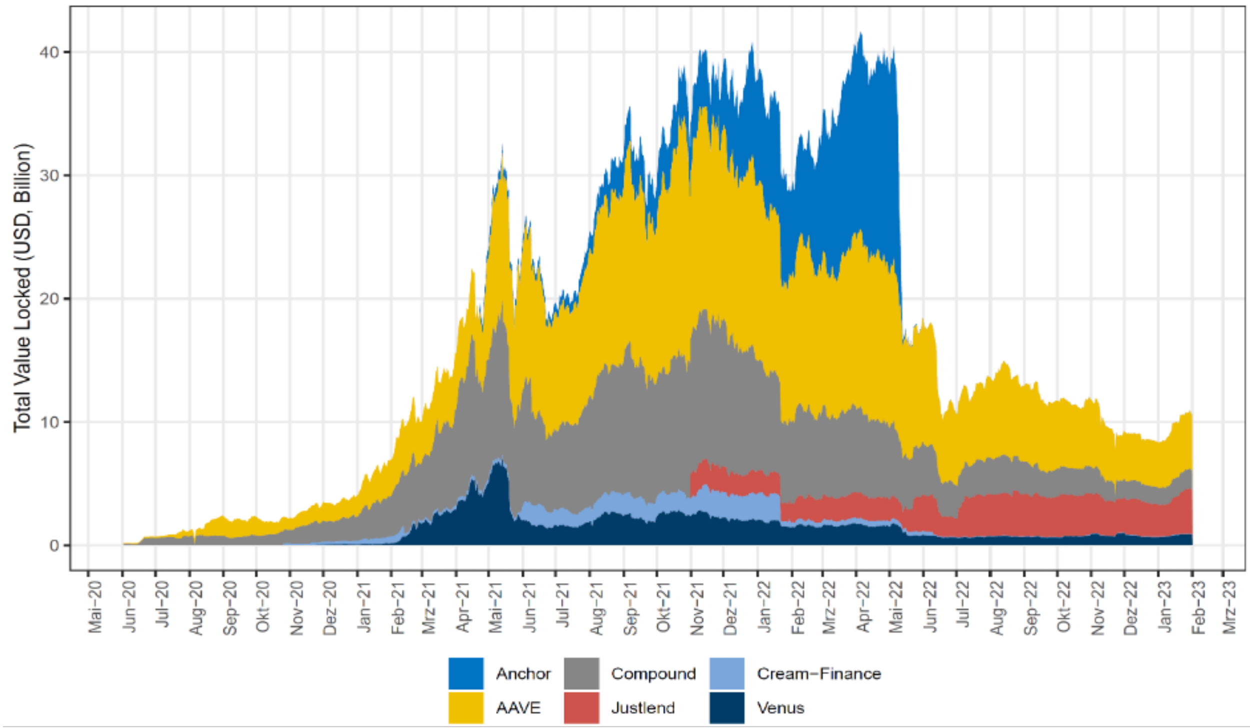
On public blockchains, crypto-asset ownership is associated with a public address, similar to an account number. There are two types of accounts on second-generation blockchains like Ethereum:[i] externally owned accounts (EOAs) and smart contract accounts. EOAs have a public address derived from a public key, which is generated from a private key in the process of asymmetric cryptography. The private key controls the crypto-assets and is used to sign transactions (comparable to a password). Smart contract accounts are pieces of code registered on the blockchain and entirely governed by their publicly visible code.

A wallet is a software tool that stores private keys and enables the signing of transactions. There are many forms of wallets, with the most common being browser plugins or smartphone apps. Although the terms "wallet" and "public address" are often used interchangeably, a single wallet can handle many addresses. When the user controls the private keys, a wallet is called self-custody.

To use a crypto asset at a centralized marketplace, users must transfer the asset to the respective venue. To facilitate this operation, centralized exchanges issue their users a unique public address, but the custody of the private keys for this address rests with the exchange. Therefore, these public addresses are called custodial wallets because the exchange has custody of the private keys.

i First generation blockchains such as Bitcoin are simple decentralized ledgers that can do little more than record transfers from one address to another. In contrast, most second-generation blockchains permit the execution of arbitrary operations and allow, in particular, code executions, also referred to as smart contracts.

Figure 2: Total Value Deposited in Lending Protocols



The figure shows total deposits in the six largest DeFi loan projects across chains, expressed in billions of USD.

Data Source: https://defillama.com/docs/api

After a user transfers crypto assets to their exchange/custodial wallet, there is usually a second step whereby the assets are transferred from the custodial wallet to one of the exchange's omnibus wallets. When the transfer is made to the custodial wallet, the user loses control of the asset, and all further transfers are recorded in the exchange's own siloed system rather than on the blockchain. For this reason, assets in omnibus wallets are often called "off-chain." Since trades are arranged and recorded on the exchange's proprietary infrastructure, these venues are referred to as centralized.

CUSTODY IN DECENTRALIZED LENDING

Decentralized lending is typically automated and uses smart contracts to manage loan terms. Users can access these smart contracts through web-based applications, which are commonly referred to as Dapps. Dapps are permission-free, and the smart contract code and operation scheme is publicly visible on the blockchain.

DeFi lending applications differ from traditional centralized intermediation as they function on decentralized blockchain networks, which means that all operations are governed by smart contract code, and the code is executed "decentrally" by the blockchain's validators. This eliminates the need for centralized power over transactions, but also puts full responsibility on the user (e.g., errors made by the user cannot be reversed). The advantage is that transactions are censorship-resistant and deposits are non-custodial, meaning that no third party can abuse their power and steal funds.

Participation in DeFi is open to anyone with an internet connection, whereas traditional intermediation is typically restricted to agents meeting eligibility requirements. This enables people without access to financial services to use DeFi platforms but does not exclude criminals who try to avoid KYC standards. Although anonymity also applies to physical cash, the concern with criminals using blockchain networks is the scalability.

The non-custodial nature of smart contracts has significant implications, as it allows users to maintain control over their funds and grants access only to fully transparent execution schemes.[i] This reduces agency conflicts and moral hazard, as the terms and conditions are pre-programmed and enforced by the blockchain, ensuring that all parties adhere to their agreed-upon obligations.

In contrast, traditional intermediation faces agency conflicts and opaque decision-making. Banks are subject to supervision because they pool user deposits, which can result in potential conflicts of interest. Brokerages must outsource custody of assets to protect their clients' assets effectively.

THE PRINCIPLES OF DEFI LENDING

There are two broad types of DeFi lending applications. The first type relies on liquidity pools, where users deposit assets into a pool and derive a monetary benefit. Liquidity seekers can then interact with the pools based on several rules.

The second type of DeFi lending application is the so-called minting protocol. These contracts allow users to create a specific token by entering into a collateralized debt position.

To explain the processes of a first-type DeFi lending application in more detail, let's take the example of the Compound protocol. Users deposit tokens, such as the cryptocurrency ETH, into a lending pool. Borrowers can access this pool based on posted collateral with the requirement to later repay their loan with interest to unlock and redeem the collateral. The interest borrowers pay flows back to depositors, who receive a receipt token, known as cETH. This token signifies the depositor's claim as a fraction of the pool at the time of the deposit.

The MakerDAO protocol belongs to the second type of DeFi lending application. Users deposit collateral, such as ETH, into a smart contract known as a vault to mint new DAI tokens. These tokens represent a collateralized loan, and borrowers must repay the DAI loan with interest to retrieve their collateral. Unlike Compound, vaults are not pooled, and there are no receipt tokens. MakerDAO's DAI is a stablecoin, as the protocol mechanisms target a price peg of 1 DAI to 1 USD.

Collateralized lending is the foundation of the first generation of DeFi lending protocols. Blockchains use pseudonymous accounts that anyone can create, meaning that by default, there is no link between accounts and individuals, no credit reporting, and no recourse mechanism if a loan goes unpaid. Therefore, collateral is the only way to secure a loan.

Starting in 2021, several projects began offering undercollateralized or uncollateralized loans. The most prominent provider of this type to date is Maple Finance, located in Australia, and a 2021 Creative Destruction Lab's Blockchain Stream graduate. Maple Finance verifies institutional borrowers and links their identities to wallets, making the loans de facto enforceable with traditional means. Their clients mostly include firms that operate in the blockchain industry, such as crypto-miners and market makers. This lending model is conceptually similar to peer-to-peer lending with known identities.

For the remainder of this paper, we will describe the processes involved in DeFi lending, focusing on lending pools and ignoring MakerDAO and uncollateralized lending for simplicity.

i The code underlying most Dapps is decentrally governed by the community and can be changed upon approval. Some changes, such as code parameters can be changed directly with blockchain-based voting whereas others may require human intervention, provided the smart contract account has been set up to allow change. Changeable contracts, however, face additional risk of exploits and attacks. See Gervais et al. (2020) for a discussion.

LENDING POOL PROTOCOLS

As of February 2023, the total locked-up value in pooled lending protocols is $14 billion, representing about 24% of all the value locked in DeFi applications.[i] To provide some context, decentralized exchanges are the largest category with a total value locked (TVL) of $21 billion (see Figure 1). The four largest lending protocols by TVL are Aave, Justlend, Compound, and Venus, which together make up 81% of all lending platforms (see Figure 2).

While these platforms have some minor differences, they share a common architecture, which we describe next.

THE PERSPECTIVE OF DEPOSITORS

Users who contribute crypto assets to the non-custodial liquidity pools receive interest income. Upon supplying funds to a pool, users receive a token that signifies their contribution. There are two models. In Aave, users receive so-called "atokens," while in Compound, they receive "ctokens" (e.g., aETH, aUDST, cETH, etc.). Both tokens are transferable, meaning that a depositor can transfer their claim to another user. However, the protocols account for interest differently. In Aave, interest collected on the reserves that the atokens represent is directly distributed to atoken holders by continuously increasing their wallet balance. In Compound, tokens represent pool ownership and are realized as capital gains.

For example, consider a user who deposits $10 each into an Aave and Compound pool, each with values of $90, respectively. In Aave, the pool size is irrelevant for the number of tokens issued. The user receives 10 aUSDT tokens. Deposit interest is computed continuously and recorded by increasing the user's wallet balance. If the user collects 5% interest after a certain period, the wallet would contain 10.5 aUSDT tokens, exchangeable for 10.5 USDT tokens by returning the atokens to the contract. Returned tokens are "burned" (i.e., they are removed from circulation). Burning is usually accomplished by sending tokens to an address with no private keys.

For Compound, assume there were 900 cUSDT tokens in circulation at the deposit time. The user would receive 100 cUSDT tokens representing a 10% ownership in the pool at the time of deposit. Suppose the pool collects 5% interest so that the pool represents 1,050 cUSD. The depositor can reclaim their deposit by returning the 100 cUSDT tokens to the contract and will receive 10.5 USDT tokens in return. Effectively, the exchange rate of a cUSDT to a USDT changes from 1:10 to 1:10.5.

In functional terms, a cUSDT deposit is similar to a T-bill investment, whereas an Aave deposit resembles a deposit with almost continuous compounded interest.

THE PERSPECTIVE OF BORROWERS

Four key principles underpin DeFi loans. The first is that the borrower must provide collateral to secure the loan. Second, the value of the collateral must surpass the loan's value. Third, if the collateral value drops below a certain threshold relative to the amount owed, it can be liquidated. Fourth, liquidation is not triggered by a central party or the protocol, but can be initiated by anyone, and is incentivized by the process design.

The quality of the underlying collateral determines a user's borrowing capacity. Interest rates can be variable or fixed; loans commonly have no term limit. However, interest accrues over time and contributes to the borrower's liability relative to their collateral. As a result, if the value of funds owed relative to the collateral increases over time, the protocol may allow the liquidation of the loan.

i See https://defillama.com/categories

Most DeFi lending protocols accept multiple collateral tokens with varying fundamental characteristics, valuations, and volatility. Each asset is classified by a collateral factor, which dictates the maximum outstanding debt relative to the collateral. This factor is inversely related to the risk exposure and price volatility of the collateral.

For example, if an asset has a collateral factor of 0.8, a depositor can borrow up to 80 cents for every dollar of collateral. This threshold is also referred to as the *borrowing* capacity. When multiple assets are used as collateral, the total borrowing capacity is determined by the weighted sum of their respective collateral factors. These factors are set by the protocol and can be voted on by the owners of the governance tokens.

Borrowers receive the asset they borrow from the general pool of assets, and the smart contract keeps track of their loan-to-collateral ratio. The borrowed asset is held in the borrower's wallet and can be used at their discretion. Repaying the loan involves sending the borrowed amount plus interest back to the lending pool using the repayment option in the web app. In some cases, borrowers can also use their collateral to repay the loan, which requires the platform to run a token swap function similar to an automated market maker.

The interest rates for a liquidity pool are determined programmatically as a function of the utilization rate, which is the ratio of outstanding debt to supplied deposits.

As the pool lends the asset to borrowers, depositors face an increasing solvency risk as pool utilization increases. However, certain mechanisms are designed to retain pool value, so depositors seeking liquidity should be able to sell their receipt tokens.

INTEREST RATES

An Example For Health Factors

A user deposits 1 ETH at a price of $1,500 as collateral. The collateral on Aave for ETH is 80%, which means that the user can borrow up to $1,200. Suppose the user borrows 1,000 USDT.

The borrower’s health factor is

1500 x 0.8/1000=1.2.

After a while, the price of ETH drops to $1,200 per USDT. With a collateral bound of 80%, the maximum that the user could borrow is $960. This shift is reflected in the health factor which is now

1200 x 0.8 /1000=0.96.

Since the health factor is below 1, the loan can now be liquidated.

Aave allows keepers to repay as much as 50% of the original loan and collect an additional fee of 5%. Therefore, the keeper repays 500 USDT and seizes an equivalent amount of collateral ETH plus an additional 50 USDT (=5% of 500 USDT) worth of collateral as a fee.

Pools are designed to disincentivize full utilization via a stepwise linear function for the interest rate (see Figure 3). The interest rate follows a linear function of the utilization, and If utilization is low, this rate will have a low slope. When utilization passes a threshold, the function becomes much steeper. This setup aims for three effects:

- New borrowers may be deterred from taking up a new loan due to the high rate.
- Existing borrowers face a higher rate that makes their loans more expensive. They face

a risk of liquidation because accrued interest lowers their borrowing capacity and may lead to their collateral being liquidated.

- The value of deposits increases, which should motivate depositors not to withdraw their funds and attract outsiders to supply additional deposits.

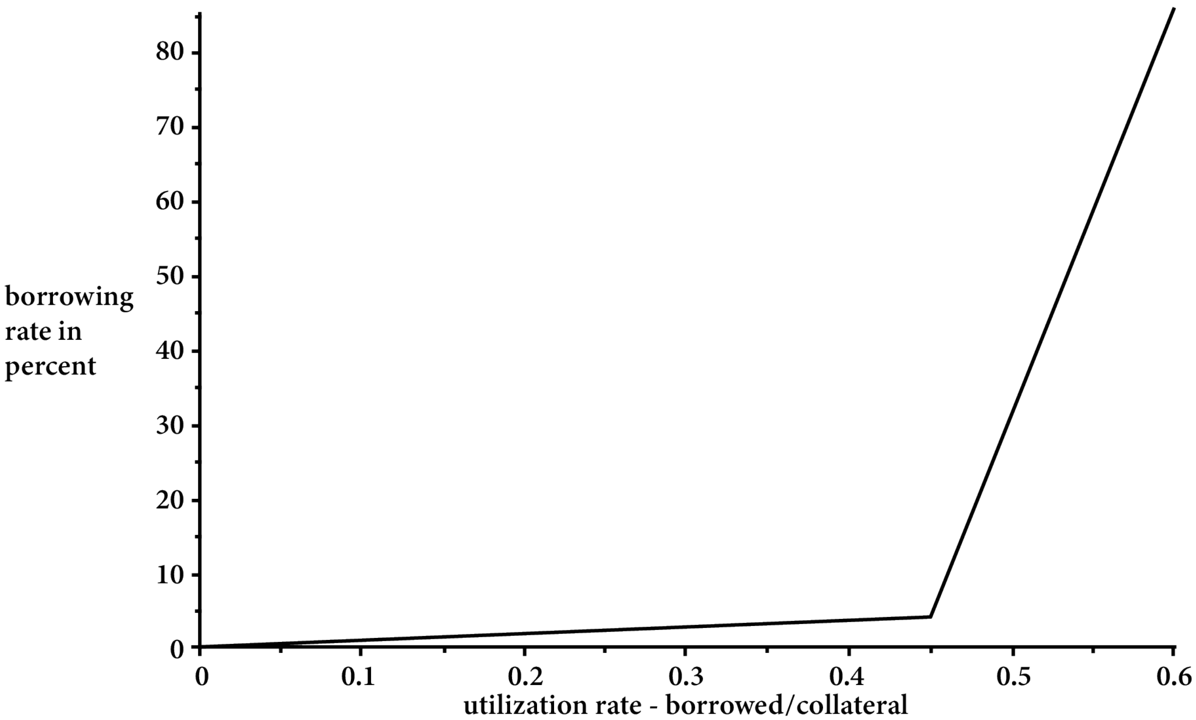
POOL SOLVENCY AND LIQUIDATIONS

To ensure the integrity and stability of lending pools, lending protocols use a process known as a liquidation event, which occurs when the value of a borrower's collateral falls below a minimum threshold.

Specifically, liquidation becomes eligible when the collateral multiplied by the asset's *liquidation threshold*, a number between 0 and 1, declines below the outstanding debt. In other words, the liquidation threshold is the point at which a position is under-collateralized. The liquidation threshold is higher than the *borrowing capacity* to ensure that there is enough collateral to pay liquidators their reward.

For example, the Aave protocol specifies that the threshold for wrapped Bitcoin (WBTC) is 75%. The inverse of this number, 133%, is the extent to which a position must be over-collateralized: for every $3 of a loan based on wrapped Bitcoin as collateral, there must be collateral worth at least $4.

Figure 3: The Borrowing Interest Rate



The figure depicts an example for the borrowing interest rate in Aave. It is a piecewise linear function of the credit utilization rate Ui, defined as the ratio of the borrowed amount to the collateral. For volatile crypto assets such as ETH, the "optimal" (or, rather, target) utilization ratio *U** is 45%. The function is $R_0+R_1xU_i/U^*$ for $Ui<U^*$ and $R_0+R_1+R_2x(U_i-U^*)/(1-U^*)$for $U_i>U^*$, where $R_0=0$, $R_1=4\%$, and $R_2=300\%$.

Source: https://docs.aave.com/risk/liquidity-risk/borrow-interest-rate

A user can take loans and provide collateral in a variety of digital assets. To account properly, the solvency of a user across all open positions is expressed using the so-called health factor. The health factor for each user is calculated as the weighted sum of the collateral value multiplied with the liquidation threshold relative to the value of outstanding debt. A health factor below 1 means that a position is liquidatable.

The health factor determines the viability of a user's credit position. Repaying interest can increase the health factor, as the outstanding loan increases due to accrued interest over time. Once the health factor falls below one, the loan is liquidatable, and anyone can trigger the liquidation by repaying the outstanding debt, including interest, and seizing the collateral.

Prospective liquidators or "keepers" monitor open loans and are incentivized to trigger the liquidation by receiving a fee. Aave, for example, allows keepers to liquidate up to 50% of the borrowed amount plus a fee between 5% and 15%, depending on the collateral. The fee for liquidators (or bonus from the liquidator's perspective) contributes to the system's health. The keeper can only apply their fee to one type of collateral, although loans can be backed with different collateral tokens.

The liquidation process is automated and works based on a computer code that monitors loans and triggers liquidation when profitable. However, the process may not always work correctly, for example, when network fees are high. To address this risk, a portion of the interest accrues to the protocol to fund a reserve pool.

Users rarely utilize the full borrowing capacity of their capital, as the protocols warn users of possible liquidation when withdrawing collateral or taking up a large loan relative to the collateral that would result in a low health factor. In early February 2023, the median health factor across all loans was 2.24 and 1.76 for Aave and Compound, respectively. The liquidation process is crucial to maintaining the integrity of DeFi lending pools because if a loan exceeds the collateral, the pool as a whole would be at risk.

An Example for Loan Liquidations from the Ethereum Blockchain

On April 17, 2021, a user deposited ETH 0.6 into the Aave V2 ETH lending pool. At the time, this amount was worth USD 1,406. And the pool stated a lending rate (APY) of 0.19%.

On April 28, the user borrowed USDC 1,000 from the Aave USDC pool, using her deposit as collateral. At this time, the USDC pool's total liquidity was B1.73 and the outstanding debt B1.58, so that the pool utilization rate was 89.8%. Based on the pricing function, the user's variable borrowing rate was 3.99% p.a.

At the time of borrowing, the 0.6 ETH collateral was worth $1,636 and the liquidation threshold of USDC equal to 0.825. The user's health factor therefore was

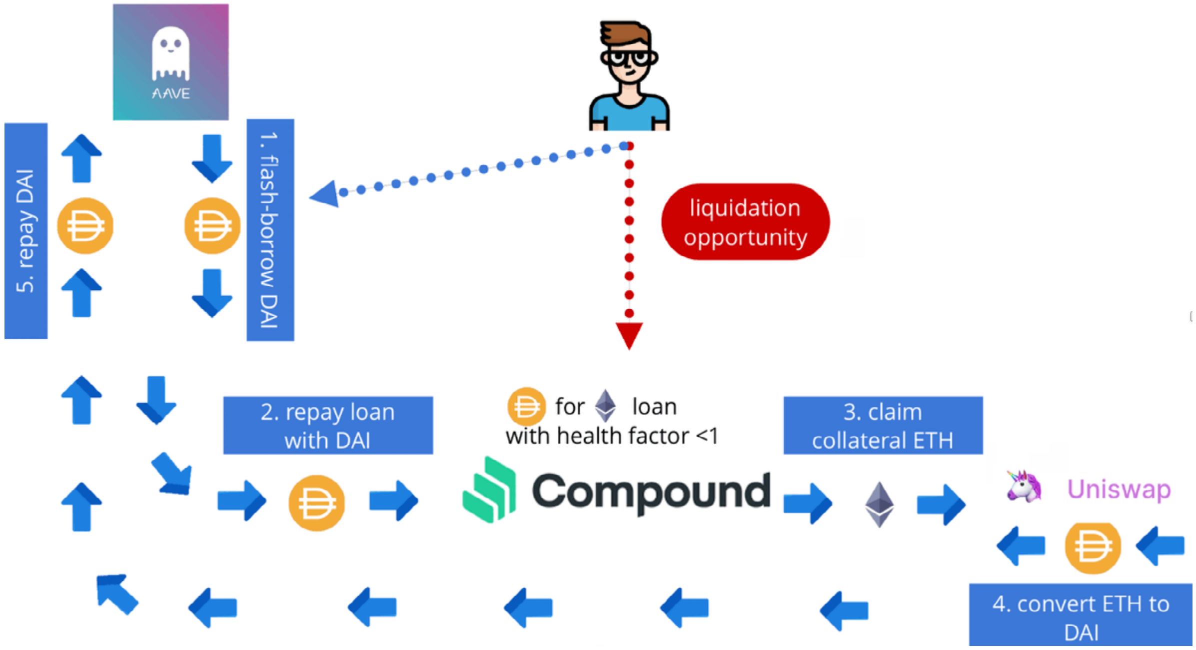
0.825 x 1636/1000 = 1.35.

Between April 28 and July, the ETH price dropped to 1,153, causing the health factor to drop to 0.825x1153/1000=0.95.

Two liquidators became active and repaid a debt proportion of USDC 756.43 and seized ETH 0.42 collateral, earning a liquidation bonus of 5.5% or USD 104.6 before fees.

Following the partial liquidation, the user repaid the outstanding debt of USDC 252.19, collected the remaining collateral of ETH 0.17, including ETH 0.00015 interest, and withdrew both from the Aave protocol.

Figure 4: Loan Liquidation with Flash Loans



A bot recognizes a liquidatable loan on Compound. To collect the reward, the bot takes up a Flash loan from Aave (step 1), repays the loan in Compound (step 2), seizes the collateral (step 3), exchanges the collateral for the borrowed token in the automated market maker UniSwap (step 4) and repays the Aave flash loan (step 5).

FLASH LOANS

Flash loans are a type of credit that requires no collateral, has instant maturity, and can utilize any available liquidity. A flash loan is taken up and repaid in a single block transaction using a smart contract. Services like collateralswap and defisaver provide user-friendly off-the-shelf solutions for flash loans. Notably, the blockchain infrastructure only settles a sequence of dependent transactions if all elements can be executed. This feature makes flash loans conceptually risk-free because they are only taken up and executed if they can be repaid in the same transaction. A user seeking a flash loan can not default since the entire credit arrangement fails when the repayment amount is insufficient to cover the debt and interest.

Flash loans are an essential component of the DeFi ecosystem as they enable risk-free arbitrage, an important mechanism for market efficiency and integrity.

For example, if there is a price discrepancy between the marginal prices on two swap exchanges, an arbitrageur can take out a flash loan for an overpriced token, sell the token on the high-price exchange, buy it back on the low-price exchange to equalize the prices, and then repay the loan. These operations are strung together, submitted, and executed as a single package. If the arbitrage profit is insufficient to cover the loan and interest, the transaction (i.e., the flash loan) fails, and the user loses any attached transaction fees.

A second example, illustrated in Figure 4, relates to loan liquidations. As described above, loan liquidations are typically triggered and executed by liquidation bots as atomic liquidation scripts (i.e., strings of transactions). In the example, a keeper identifies a liquidatable loan on Compound. The bot does not have the capital to repay the loan. However, the bot can take up a Flash loan from Aave (step 1), repay the loan in Compound (step 2) and seize the collateral (step 3), exchange the collateral for the borrowed token in an AMM like UniSwap (step 4) and repay the Aave flash loan (step 5). Every step is contingent on the next step: if someone pre-empts the bot and repays the loan, the Flash loan would not be taken up. If the exchange rate from the AMM trade is unfavourable, the liquidation would not occur and the Flash loan would not be taken up. The only risk that arbitrageurs face is that the transaction fails, in which case they still have to pay the gas fee or transaction fee.

LIQUIDITY MINING

Sufficient liquidity is crucial for the mechanics of liquidity pools and offers several benefits to users. Liquidity pools with enough liquidity are less vulnerable to illiquidity risks, which means that users can participate in frictionless lending even during times of high demand. In smaller pools, large loans or liquidity withdrawals can disrupt utilization rates. This can result in increased volatility of lending rates and may impact the pool's overall lending activity level.

The amount of assets deposited in a protocol, or TVL, is an important indicator of a protocol's popularity and revenue-generating potential. It is also used as a key benchmark by DeFi data comparison websites, which attracts users. In short, liquidity is the key driver for the adoption and success of a platform.

As a result, DeFi protocols compete for liquidity, and liquidity incentives are vital to attracting deposits. Network or protocol tokens have emerged as a strategic incentive tool, as they are claims on a portion of the fee income the protocol generates. The protocol can attract more capital by providing incentives to early liquidity providers and demanders, which can increase fee income and create a virtuous cycle of growth. Of course, this process must be designed carefully so that token issuance stops when the protocol becomes self-sustaining.

A liquidity incentive program is often called a *liquidity mining program*, and users seeking the associated returns are called *liquidity miners*. and reward borrowers and depositors with native or governance tokens. Procedurally, the lending protocol generates a fixed quantity of native tokens or draws on an existing deposit of tokens. The allocation schemes vary, but typically users are rewarded for open deposit and borrow positions. The awarded tokens can have various features. Most commonly, they are governance tokens that allow holders to vote on changes to the platform. Usually, these tokens do not directly represent cash flow rights, but some token holders may envision, for instance, paying themselves a portion of the reserve funds at a future date.

A Liquidity Mining Example: Compound

Compound launched its governance token COMP in June 2020 with an extensive liquidity mining program. The program was introduced with a reserve contract, holding 4,229,949 COMP tokens. Currently 0.1765 tokens are allocated per Ethereum block to protocol users. This program is scheduled to last for four years. Within each qualifying pool, an equal share of the tokens goes to borrowers and lenders.

In February 2023, the reserve allocated approximately 1300 COMP per day, worth $71,500 USD (about $55 per token). The community of COMP holders decides on the allocation across pools through voting. About 97% of COMP tokens are distributed to pools that contain stablecoins such as USDC or DAI.

For more information on the current allocation scheme see:

https://compound.finance/governance/comp

YIELD FARMING

Yield farming has gained a bad reputation partly due to an episode of the Odd Lots podcast, a popular Bloomberg-sponsored series covering a wide range of finance and market-related topics every week. In the episode, Sam Bankman-Fried, the founder and former CEO of the now-defunct crypto exchange FTX, described yield farming as throwing money into a magic pot from which one can get more than one put in. Essentially, he described yield farming as a Ponzi scheme. While there are undoubtedly fraudulent schemes in the blockchain space, there is a legitimate case for yield farming.

Yield farming is the process of allocating capital to the protocols that provide the largest rewards. It is not about creating income out of thin air but rather using a new term to describe a fundamental mechanism of capitalism.

While users can deploy their assets in any way they see fit, in practice, this process is often organized by non-custodial asset managers known as "yield aggregators." These tools organize and execute the strategic allocation of users' assets to the protocols that offer the highest rewards. By doing so, they help users optimize their yield-earning potential. A yield-aggregation service, such as Yearn Finance, collects users' funds in smart-contract-based pools, which are then invested by the protocol according to a predefined yield-generating strategy. These protocols are decentralized in the sense that the deposit into the protocol is non-custodial because the code that performs the allocation runs on the blockchain as a smart contract.

Investments may include a wide range of strategies, varying from basic portfolio rebalancing to complex sequences that utilize leveraged trading. As is common in the DeFi space, the specific strategies are not secretive or a black box. Rather, users themselves can propose or contribute to a strategy. These strategies are first reviewed by the community and/or development team and eventually approved through a decentralized voting process. Users can send funds upon formalizing the strategy script in a smart contract, and the protocol independently executes the specified strategy. Although yield aggregators serve a legitimate and arguably traditional role in financial resource allocation, there is also a dark side. One concern is that yield aggregators often offer fabulous returns, as indicated by their APY, sometimes in multiples of hundreds. These numbers can be misleading due to a lack of transparency regarding their computation methods, currency denomination, underlying assumptions, time frame or horizon, and potential associated risks. For instance, one strategy may be highly leveraged and expose the user to the risk of a total loss. Another may involve rewards that rely on a long-term locked deposit where the high APY is driven by a token that experiences substantive short-term price rises, possibly due to market manipulations.

For the DeFi space to thrive in the future, it will arguably be necessary to develop commonly accepted and followed standards that clearly outline risks (not just the broad existence of risks) and explain how protocols arrive at their numbers and promises.

We introduce yield farming in this primer because it is arguably an important mechanism for creating liquidity in the DeFi space. Similar to mutual funds, yield farming strategies often take leveraged positions (and thus involve activity on lending protocols). Moreover, they gravitate towards liquidity mining programs. If a lending protocol decides to offer liquidity incentives, the returns from protocol activity increase substantially, often attracting large-scale exposure from yield aggregating services. Our own analysis, to be released later this year, shows that in some cases, the introduction of a liquidity mining program led to an increase in TVL by a factor of 10.

CONCLUSION

We have provided an overview of the key applications and mechanisms of lending markets in the crypto space. Centralized crypto lending is not particularly innovative as it mimics traditional finance based on a new asset class. Decentralized lending has yielded several innovative processes, illustrating how borrowing and lending can be arranged without formal intermediaries. However, two challenges remain. Firstly, the number of applications of these tools is restricted to crypto assets. To reach its potential, either there would have to be a digital economy where these assets have a purpose beyond trading crypto-assets, or existing assets would need to be deployed on public blockchains.

Secondly, almost all blockchain-based lending requires over-collateralization, which prevents efficient use of capital. It is hard to beat the current world of highly regulated banking and conversion of deposits to loans. While a potential future extension of collateral assets (e.g., to digital security certificates) may stimulate broader use cases, the key issue preventing under-collateralized lending is the lack of recourse. Going forward, digital IDs may solve this problem. However, it still is unclear how digital IDs, consumer privacy, and anti-money laundering provisions can be reconciled for public blockchain applications.

References

S. Cousaert, J. Xu and T. Matsui, "SoK: Yield Aggregators in DeFi," 2022 *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Shanghai, China, 2022, https://doi.org/10.1109/ICBC54727.2022.9805523

Augustin, P., Shin, D., & Chen-zhang, R. (2022). Reaching for Yield in Decentralized Financial Markets. *SSRN Electronic Journal.*

Capponi, A., & Ruizhe, J. (2021). The Adoption of Blockchain-Based Decentralized Exchanges. *Working Paper.*

Cong, L. W., Li, X., Tang, K., & Yang, Y. (2022). Crypto Wash Trading. *National Bureau of Economic Research*, (30783). https://doi.org/10.3386/w30783

Cousaert, S., Xu, J., & Matsui, T. (2022). SoK: Yield Aggregators in DeFi. *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022*. https://doi.org/10.1109/ICBC54727.2022.9805523

Gudgeon, L., Perez, D., Harz, D., Livshits, B., & Gervais, A. (2020). The Decentralized Financial Crisis. *CVCBT 2020*. https://doi.org/10.1109/CVCBT50464.2020.00005

Harvey, C. R., Santoro, J., & Ramachandran, A. (2021). DeFi and the Future of Finance. *Working Paper.*

Lehar, A., & Parlour, C. A. (2022a). Decentralized Exchanges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3905316

Lehar, A., & Parlour, C. A. (2022b). Systemic Fragility in Decentralized Markets. *SSRN Electronic Journal*.

Makarov, I., & Schoar, A. (2022). *Cryptocurrencies and Decentralized Finance (DeFi)*.

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

Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021). An empirical study of DeFi liquidations: Incentives, risks, and instabilities. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC, 1(1), 336–350*. https://doi.org/10.1145/3487552.3487811