Spring 2022

Yield Generation Using Decentralized Financial (DeFi) Applications

Nathan Walton
University of South Carolina - Columbia

Yield Generation Using Decentralized Financial (DeFi) Applications

By

Nathan Walton

Submitted in Partial Fulfillment
of the Requirements for
Graduation with Honors from the
South Carolina Honors College

May 2022

Approved:

DocuSigned by:
66410F5ACED0464...

5/3/2022

Reid Tymcio
Director of Thesis

Hugh Hoikwang Kim
Second Reader

Steve Lynn, Dean
For South Carolina Honors College

Abstract:

Decentralized financial (DeFi) applications are a new generation of financial service applications, composed of coded smart contracts, and deployed on a blockchain network. These applications offer several methods of generating yield on deposited funds, much like a traditional bank. In this paper I provide a definition of several key terms and a breakdown of the primary mechanisms through which yield is generated. Additionally, I examine three of the main types of DeFi applications, the services they provide, and how they execute these services. I then provide an overview of four strategies involving cash and leverage and estimate the potential benefits and risks of each strategy. Finally, the risks involved with participation in the DeFi ecosystem are discussed.

Table of Contents

1 Background and Definitions:

Ethereum: Ethereum was first envisioned in 2014 by founder Vitalik Buterin as a "Next-Generation Smart Contract and Decentralized Application Platform" (Buterin 2014). The goal was to improve upon the existing Bitcoin network by creating a blockchain with a built in Turing-complete programming language to create contracts that can be used to execute transactions by writing the logic into computer code. These coded contracts are commonly called smart contracts. They are used to define what actions the computer takes. Buterin envisions a world where financial products and currencies are not owned by a central government or bank, but rather by the users of these financial products and currencies. This is accomplished by facilitating the creation of token systems and program-based financial products using smart contracts.

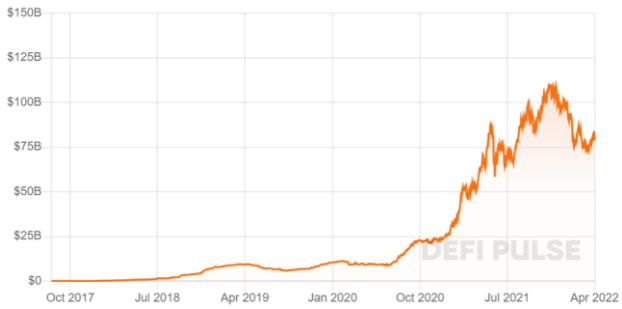
Traditional Finance: The earliest forms of market exchange were peer to peer trades based on credit. This system was highly inefficient since it required sellers to trust that buyers would pay their debts and buyers to trust that sellers were providing goods as advertised. Eventually, "money" emerged as a medium of exchange, unit of account, and a store of value that facilitated trade between multiple parties in a single currency. Gold coins are an early example of money. Today, the monetary system is made up of non-collateralized currencies (fiat) that are issued and controlled by central banks and transactions are facilitated by modern financial institutions (Harvey et. al. 2020).

Money: Money, by definition, functions as a medium of exchange, unit of account, and store of value. Key characteristics of money as a medium of exchange include divisibility, resistance to counterfeiting, high market value in relation to volume and weight. These characteristics facilitate the enabling of trade between multiple parties. It also must be fungible.

In other words, one piece of money must be perceived the same as another piece of money. This is why items such as diamonds cannot serve as money, as each diamond has a unique perception of its quality. Finally, money must serve as a store of value. Essentially, it must be able to be stored and retrieved easily over time, and still be usable as a medium of exchange. Modern theory has taken these base requirements of money and expanded on them by imposing the general perception that money must be backed by a government in order to be accepted as legal tender.

Decentralized Finance (DeFi): DeFi refers to a collection of applications that live on smart contract enabled blockchains, primarily Ethereum. These applications fall into several distinct categories, the most basic being exchanges, lending/borrowing services, and yield aggregators. Each of these applications serves a function similar to traditional brokerages, banks, and asset managers. For the purposes of this paper, total value locked (TVL) is defined as the mark to market value in USD held in DeFi protocol smart contracts. On Jan. 1, 2020, TVL was $10.4B. On Jan. 1, 2022, TVL was $98.9B (DeFi Pulse).

Figure 1



Note: B, billion

Source: DeFi Pulse

ERC-20: The ERC-20 token standard was proposed in November of 2015. At its most base level it allows users to create a “token” on the Ethereum network. These tokens can

represent anything within the network. The ERC-20 proposal laid down the standard to implement several of the characteristics of money in the Ethereum environment. First and foremost, it allows for fungibility. ERC-20 tokens have properties that behave exactly the same as the ETH token, meaning that one token will always be equal to all other tokens. Additionally, the proposal implemented functionality that allowed smart contracts (programs) to transfer tokens from one account to another, get current token balances, get total supply of the token on the network, and approve if an amount of token can be spent by a third-party account. The ERC-20 standard serves as the base for the following token types.

Stablecoins: Stablecoins are tokens whose intrinsic nature is to offer price stability. They are intentionally designed to have a value pegged to a reference point. This reference point can be another crypto asset, a fiat currency, or even the price of a commodity. The most popular implementation of stablecoins is as assets pegged to the USD. Stablecoins can exist in a variety of formats. Two of the biggest tokens by market cap are USDC and USDT, both of which are asset backed. Asset backed are collateralized by reserves worth a dollar value equivalent to the number of stablecoins issued. The reserves of off chain custodians are housed by an institution such as a bank or company. Stablecoin protocols can also host their reserves on-chain, such is the case with DAI, the stablecoin issued by MakerDAO. MakerDAO allows users to create, or "mint" one USD worth of DAI with the deposit of 1.50 USD worth of ETH to their smart contract treasury.

Stability of these two tokens is dependent on different principals. The stability of DAI is from arbitrage traders, liquidators, collateral and MakerDAO's ability to mint MKR token to ensure DAI stays on target. The stability of USDC is from arbitrage traders and large institutions buying USDC using dollars. This provides an interesting dynamic because MakerDAO can

always issue more MKR token to ensure the stability, as long as people are willing to buy MKR in exchange for dollars. USDC relies on trust that institutions will always have enough dollars to trade for digitized dollars.

Finally, stablecoins can maintain their peg algorithmically. In this case, there is no reserve backing. Algorithmic stablecoins are the highest risk form of the token class.

Stablecoins have a variety of use cases. Often the primary two uses are for tax purposes and to reduce exposure to more volatile underlying crypto tokens.

Liquidity Provider (LP) tokens: LP tokens are created when a user deposits liquidity into a pool on an exchange. These LP tokens represent the proportional share of the total pool that a depositor has rights to. A key difference is that rather than borrowers who pay interest on their loans, there are traders who pay a fee every time they make a trade. Each exchange charges its own swap fee, which is then distributed pro-rata back to liquidity providers. These tokens generally possess the same property of composability as ERC-20.

Governance tokens: Governance tokens can be thought of as an evolution of traditional common stock shares. Some governance tokens, like Uniswap' s UNI token, only give holders the ability to vote in the on-chain governing process. These tokens do not provide any sort of income, and aside from voting abilities, the only native incentive to hold this type of governance token is price appreciation. Other governance tokens provide the same voting power but come with an additional benefit. They can be staked (deposited) to earn a percentage of the revenue generated by a protocol.

2 Yield Mechanisms

Principal: In the realm of DeFi base yield is generated through three base mechanisms: borrowing demand, liquidity mining, and revenue sharing. A fourth mechanism, built upon these

three methods is yield aggregation, in which a separate smart contract takes advantage of the composability of DeFi platforms to automate the yield farming process and often maximize potential yield generated (Cousaert et. al. 2021).

Liquidity Mining: Often new protocols will incentivize users to adopt their protocol by rewarding early adopters with native tokens. These native tokens often have governance properties. Tokens with these governance properties have some intrinsic value as the token represents a voting say in the strategy of the protocol in the future. Additionally, since these tokens are often distributed in the early stages of the protocol life cycle, they are given additional value by speculative traders looking to make a profit.

Revenue Distribution: Certain tokens entitle a user to a portion of the revenue that a protocol generates through fees. Uniswap V3 LP tokens act as receipts for liquidity deposited into the pool and are redeemable for the holder's proportion of the pool plus the fees generated from swaps in the pool. Other decentralized exchanges employ different mechanisms to achieve a similar outcome, though there is a dark side. Rather than reward the liquidity providers with the full fee taken from each swap, this model distributes a fraction of the fee to the LP's and distributes the rest of the rewards to users who deposit the platform governance token into a smart contract. Often times, the biggest depositors of governance tokens are venture capitalists who funded the platform inception.

Demand for Leverage: Following the laws of supply and demand, as the demand for loans from DeFi lending platforms grows as does the interest rate that borrowers must pay on these loans, thus leading to higher lending rates for depositors. In a bullish market, borrowers are inclined to use lending platforms to take on leverage. They do this through creating what is known as a "leveraging spiral" or recursive leverage, in which traders deposit a token like ETH

into a lending platform, borrow a stablecoin like DAI against that deposit, swap their DAI into ETH, and repeat the process (Vadgama et. al. 2022). Compound Finance is one of the most popular lenders in DeFi. On April 1, 2021, the 7-day moving average of the borrow rate on DAI was 9.55%, compared to 4.42% on April 1, 2022. This specific type of yield is distributed to platform users in the form of cTokens or tokens created by the Compound platform that reflect the value of the underlying deposited asset as well as interest accumulated on the deposit.

Yield Aggregation: A more novel method of yield generation is through yield aggregation platforms. Protocols such as Yearn, and Pickle generate yield by pooling user funds into "vaults" or other similarly named vehicles. In the case of Yearn, users deposit funds into a "vault" in exchange for yTokens or yvTokens. These tokens are redeemable for the initial deposit into the vault plus any accrued yield. To use plain language, funds are deposited into a program that executes a pre-defined trading strategy to generate yield for all users with funds deposited into the contract. Yield aggregation platforms charge a fee for their services.

3 Protocol Types

3.1 Decentralized Exchanges

Principal: The decentralized exchange (DEX) serves the same function as a traditional asset exchange with a key difference. In the traditional model liquidity has been owned by a group of professional trading firms. This concentrated liquidity opens markets to the risk of asset manipulation and restriction during periods of high volatility. DEX pools allow any market participant to provide liquidity. This lowers the barriers to entry for new tokens to be created and helps increase resistance to manipulation and censorship. Most major DEXs function in one of two primary ways: either using an automated market maker (AMM) or through a decentralized order book exchange.

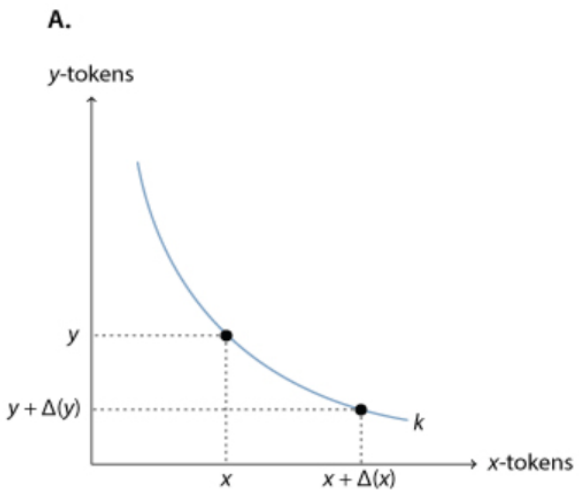


Figure 2

Constant Product Market Maker: The most common method for a DEX to enable trading is through the use of a constant product market maker (CPMM). The CPMM is a smart contract that facilitates trades by hosting a pool of two or more assets. These pools of funds are known as liquidity pools. In order to make a trade, a user deposits one asset into the pool and receives their desired asset. The smart contract calculates the exchange rate (price) based on the liquidity pool's token reserve ratio, defined as the amount of token A vs the amount of token B in the pool. In its most basic form, the constant product model can be expressed by the function $xy = k$, where x and y denote the smart contract's token reserves and k is a constant. The constant k changes between trades.. The constant is also subject to fluctuations from fees taken as incentives to liquidity providers. These fees will be exempt from the following analysis. Considering that the prior equation must hold, each trade f, we get $(x + \Delta x) \cdot (y + \Delta y) = k$. It can then be easily shown that $\Delta y = (k/(x + \Delta x)) - y$. Consequently, Δy will assume negative values for any $\Delta x > 0$. Thus, any trade will result in an increase the pool's quantity of x and decrease the pool's quantity of y. This is modeled by the convex curves shown in Figure 2. A liquidity pool using this model cannot be depleted, as tokens will get more expensive with lower reserves. When the token supply of either one of the two tokens approaches zero, its relative price rises infinitely as a result (Schär 2021).

Decentralized order book: There are a variety of ways decentralized order books can be implemented. While they all use smart contracts for on-chain transaction settlement, they have slight differences in how the order books themselves are hosted.

One approach is the on-chain order book, where every buy/sell order is stored in the smart contract. This approach is highly unfavorable as it causes traders to incur massive amounts of network fees. This disadvantage becomes significantly more costly when markets are volatile as there are many more cancelled orders which incur a fee (Schär 2021).

Another is the off-chain order book, where the book is hosted off chain and then trades are settled on-chain. Off-chain order books are hosted and updated by centralized third parties generally referred to as relayers. These parties provide takers with price and volume information that they need to select an order they would like to fill. Though some centralization and dependencies are introduced into the system using this approach, the risks are mitigated by limiting the role of the relayer to that of a communicator. They are never in control of funds, perform matching, or execute trades. Decentralized order books are not commonly used in DeFi due to high fees and security concerns.

3.2 Lending Platforms

Principal: DeFi lending platforms serve a similar purpose to TradFi lenders. They incentivize users who wish to deposit their assets so that others can borrow assets. Unlike traditional lenders, all the parameters of the loan, like interest, maturity, and asset prices, are contained within a smart contract. These smart contracts also include clauses to facilitate trust between parties. DeFi lenders set themselves apart from each other through differentiation in mechanisms used. Though the underlying economic principals differ, the basic mechanisms remain constant.

Collateralization Ratio: Currently, there are no major DeFi lending platforms which offer uncollateralized loans. Without access to centralized consumer credit scores or other information about a borrower's credit worthiness protocols have no way of identifying default risk. Because of this, platforms such as Aave, Compound, and MakerDAO require loans to be overcollateralized, meaning that a borrower cannot take out a loan larger than the amount of collateral that they have posted to the platform. A common metric to measure the health of a loan is the collateralization ratio, or collateral-to-borrow ratio[5]. Each asset that is usable as collateral on a protocol has its own collateralization ratio based upon the price volatility of the asset. For example, say a user wants to borrow 100 USD worth of USDC using ETH as collateral at a collateralization ratio of 1.25, the user must deposit 125 USD worth of ETH.

Liquidations: Liquidations are the fundamental mechanism by which platforms ensure that loans remain overcollateralized by a margin large enough to ensure that price volatility does not place the collateral value in jeopardy. For security reasons the Ethereum blockchain does not allow positions to be automatically liquidated by a smart contract (Perez 2021). Because of this, an incitive is given to third party actors to make what is known as a liquidation call. Any network participant can liquidate a position that meets the liquidation parameters of the platform. To make a liquidation call the third party essentially buys the collateral from the protocol at a discount, thus paying back the borrowed funds.

Interest Rates: Each protocol has their own model for deriving the rates on each asset. The most common model is known as a "kinked rate" model in which interest rates sharply change past some defined threshold (Gudgeon et. al. 2020). This threshold is commonly based upon what is known as a utilization ratio, defined as the ratio of total loans to gross deposits.

When this ratio passes a certain point deemed optimal by platform governance the interest rate slope sharply increases.

Interest and Reward Distribution: A common model for interest distribution is through the use of what I will be calling xTokens. Employed by Aave in the form of aTokens and Compound in the form of cTokens these are assets which represent a user's proportional share of a lending pool as well as accrued interest. xTokens represent an ownership stake in the underlying market. For each unit of token deposited into the market the user receives an amount of xToken representative of their proportion of the lending pool. These tokens continuously accrue interest which makes the intrinsic value of the xToken higher than the underlying asset. xTokens are always redeemable for the original deposit amount plus accrued interest.

3.3 Yield Aggregators

Principal: A yield aggregator is a type of protocol that aggregates user funds and invests them in a variety of yield generating services/strategies. Essentially a smart contract based fund manager, the yield aggregator automatically executes an investment strategy on behalf of users. There is no set model for yield aggregators as each platform offers unique products. These products simplify and amplify the yield generation process.

Composability and Examples: Yield aggregators take advantage of the premise of composability across DeFi by integrating many different protocols. One of the most popular yield aggregators, Yearn, offers a product known as "Vaults." One specific example is the "Curve MIM-UST" Vault. Users provide liquidity to the MIM-UST pool on Curve and then deposit the LP tokens to the Vault, which then deposits them to Convex Finance where they earn rewards in the form of CVX. The earned tokens are then collected and reinvested back into the strategy.

Another example is the Pickle Finance. A user can deposit funds a “Pickle Jar” where they are then used to execute a trading strategy and generate yield. The profits of this yield are then reinvested back into the strategy. Pickle takes the process one step farther. When the user deposits their LP tokens into the Pickle Jar they receive pTokens which can then be reinvested into a “Farm” where they earn additional yield.

Fees: Yield aggregation protocols charge a fee for their services. In the case of Yearn it is a simple two and twenty structure. A two percent fee is taken from all assets in a pool, and a 20 percent fee is taken from any excess yield generated by the pool. Pickle operates in a significantly different manner, where they only charge fees on the reward tokens farmed in the aggregation strategy. Each yield aggregator has their own fee structure, and this is part of what makes them such a unique product.

4 Yield Farming Strategies

4.1 Overview and Assumptions

To interact with DeFi apps, one must have a “wallet” on the host network. This wallet serves as a user’s identity across all apps that they visit. By connecting their wallet to the smart contracts powering the dApp, they are allowing the program to view their unique identity and the amount of assets available to transact with. One of the most popular wallet applications is Metamask.

The following sections will assume that the reader has the Metamask (or other supported wallet) extension installed to their web browser and has a sufficient quantity of the network token to pay for transaction fees (gas).

4.2 Cash Trades

Overview: The premise of earning interest on funds deposited into a bank has existed since the dawn of banking. This strategy will be explored three ways. First through the lending of a stablecoin, second through the lending of another token like ETH, and third through depositing in a yield aggregator. Naturally the stablecoin strategy is the least risky as it provides minimal to no exposure to market priced assets.

Rate Models: To initiate a lending strategy on a lending platform, in this case Aave, the user must visit the website that hosts the dApp. From here they review the various assets available to use as collateral on the platform as well as the deposit APY currently associated with that asset. The deposit rates on Aave are constantly subject to change as they are highly dependent on the utilization rate of the asset, amongst other factors. However, Aave does also offer fixed-rate loans, which are useful when rates are historically low. These fixed rate loans are also dependent upon the utilization rate as well as other factors.

Utilization rate is defined as the ratio of the amount of funds currently borrowed to the amount deposited on the platform. As the utilization rate increases and there is less capital available, the model reflects high interest rates. This encourages the repayment of outstanding variable-rate loans and additional capital deposits. When the utilization rate is low, reflecting a lower demand for capital, the model reflects lower interest rates to encourage the borrowing of funds.

Interest rate models on Aave follow the “kinked rate” model discussed earlier. This model leads to a very rapidly increasing borrow rate once the utilization rate passes a certain point, around 75%. This helps ensure that the Aave treasury is not exposed to outsized risk.

Yearn Finance has a much different approach to their rates. Yearn generates yield for vault depositors by executing one of or a combination of several different strategies. This leads to inconsistent yields at any given time. Yearn yields also auto-compound every time rewards from a strategy are harvested and redeposited into a vault. Due to these factors, Yearn estimates an APY and provides this number on the dashboard.

It was found that often the lending rates on stablecoins on platforms like Gemini diverge from lending rates on the dollar. For example the lending rates for dollars and ETH on Aave currently are 2.25% and 0.71%. The lending rates on Gemini are 3.43% and 1.26%. In a traditional sense this would imply that the demand for currency is higher on Gemini thus they can lend the currency at a higher rate. However, an argument can be made that this additional yield is associated with the risk that Gemini offers uncollateralized loans.

Stablecoin Lending Model: In its simplest form the future value of money is defined mathematically as $FV = I * (1 + R * T))$ where R is the annual interest rate, T is the number of years, and FV is the value at the end of these years. Due to the multi-faceted nature of the interest rate model it is nearly impossible to predict what rates will look like in the future or when they will change. These factors are key in projecting the total yield generated by a lending strategy. For this reason the analysis in Figure 3 holds these assumptions: 1) The interest rate shown at the time of deposit is stable. 2) The value of governance token rewards offered in addition to the deposit rate is negligible. The top line is the number of months that the funds remain deposited, and on the left is the APY shown to users at the time of deposit. The current deposit rate is 2.73%.

	6	12	18	24	36	42	48	54	60
1%	$1,005.00	$1,010.00	$1,015.00	$1,020.00	$1,030.00	$1,035.00	$1,040.00	$1,045.00	$1,050.00
1.50%	$1,007.50	$1,015.00	$1,022.50	$1,030.00	$1,045.00	$1,052.50	$1,060.00	$1,067.50	$1,075.00
2.00%	$1,010.00	$1,020.00	$1,030.00	$1,040.00	$1,060.00	$1,070.00	$1,080.00	$1,090.00	$1,100.00
2.25%	$1,011.25	$1,022.50	$1,033.75	$1,045.00	$1,067.50	$1,078.75	$1,090.00	$1,101.25	$1,112.50
2.50%	$1,012.50	$1,025.00	$1,037.50	$1,050.00	$1,075.00	$1,087.50	$1,100.00	$1,112.50	$1,125.00
2.75%	$1,013.75	$1,027.50	$1,041.25	$1,055.00	$1,082.50	$1,096.25	$1,110.00	$1,123.75	$1,137.50
3.00%	$1,015.00	$1,030.00	$1,045.00	$1,060.00	$1,090.00	$1,105.00	$1,120.00	$1,135.00	$1,150.00
3.50%	$1,017.50	$1,035.00	$1,052.50	$1,070.00	$1,105.00	$1,122.50	$1,140.00	$1,157.50	$1,175.00
4.00%	$1,020.00	$1,040.00	$1,060.00	$1,080.00	$1,120.00	$1,140.00	$1,160.00	$1,180.00	$1,200.00
5.00%	$1,025.00	$1,050.00	$1,075.00	$1,100.00	$1,150.00	$1,175.00	$1,200.00	$1,225.00	$1,250.00

Figure 3

Ethereum Lending: While similar to the stablecoin lending model the profit calculation for lending ETH depends on another key factor: the price of Ethereum at both deposit and withdrawal. Ethereum denominated deposits earn interest not in dollar terms but in Ethereum terms. For example, a $1000 deposited at 1% APY earns $10 in a year, and 1000 ETH deposited at 1% APY earns 10 ETH in a year. However, if the price of ETH at the time of deposit is $1 and the price at the time of withdrawal is $2, the deposit actually yielded 2% APY in dollar terms not including the capital gains on the initial investment. The analysis in Figure 4 holds the following assumptions: 1) The interest rate shown at the time of deposit does not compound. 2) The funds will be deposited for one year. 3) The value of governance token rewards is negligible. 4) Deposited ETH was purchased at current market price of ~$3,000 ETH/USD. The top line is the price of Ethereum at end of a year and the left is the APY shown to users at the time of deposit.

	$ 2,000	$ 2,250	$ 2,500	$ 2,750	$ 3,000	$ 3,250	$ 3,500	$ 3,750	$ 4,000
0.05%	$ 667.00	$ 750.38	$ 833.75	$ 917.13	$1,000.50	$1,083.88	$1,167.25	$1,250.63	$1,334.00
0.10%	$ 667.33	$ 750.75	$ 834.17	$ 917.58	$1,001.00	$1,084.42	$1,167.83	$1,251.25	$1,334.67
0.15%	$ 667.67	$ 751.13	$ 834.58	$ 918.04	$1,001.50	$1,084.96	$1,168.42	$1,251.88	$1,335.33
0.20%	$ 668.00	$ 751.50	$ 835.00	$ 918.50	$1,002.00	$1,085.50	$1,169.00	$1,252.50	$1,336.00
0.25%	$ 668.33	$ 751.88	$ 835.42	$ 918.96	$1,002.50	$1,086.04	$1,169.58	$1,253.13	$1,336.67
0.30%	$ 668.67	$ 752.25	$ 835.83	$ 919.42	$1,003.00	$1,086.58	$1,170.17	$1,253.75	$1,337.33
0.35%	$ 669.00	$ 752.63	$ 836.25	$ 919.88	$1,003.50	$1,087.13	$1,170.75	$1,254.38	$1,338.00
0.40%	$ 669.33	$ 753.00	$ 836.67	$ 920.33	$1,004.00	$1,087.67	$1,171.33	$1,255.00	$1,338.67
0.45%	$ 669.67	$ 753.38	$ 837.08	$ 920.79	$1,004.50	$1,088.21	$1,171.92	$1,255.63	$1,339.33
0.50%	$ 670.00	$ 753.75	$ 837.50	$ 921.25	$1,005.00	$1,088.75	$1,172.50	$1,256.25	$1,340.00

Figure 4

Yearn Strategies: The USDC yVault implements five strategies to generate yield and optimizes between strategies given different market conditions.

Aave Flashmint Folding allows the contract to simultaneously supply and borrow USDC on Aave to maximize earnings. Flashmints are used to mint DAI from MakerDAO to close an undercollateralized position on Aave. This boosts the rewards earned. Earned rewards are harvested and sold for USDC which is redeposited into the strategy.

The Curve Yield Seeker supplies USDC to Curve Finance to earn CRV, the governance token of Curve. Similarly, the Single Sided Balancer strategy provides USDC to a stable pool on balancer and collects rewards in the form of Balancer's native token, BAL. Earned tokens are harvested and redeposited back into the strategy, which automatically switches to the most profitable pool.

Notional Finance is a DeFi product offering various maturity fixed-income products. The Notional Reinvest strategy supplies USDC at various maturities to earn a fixed rate yield on the USDC. At maturity, earned yield is harvested and deposited back into the strategy.

Quantification: Due to the nature of yVaults, it is nearly impossible to determine a definitive APY on deposits. However, Yearn estimates that the current APY on the USDC yVault is 2.71%. See the sensitivity model under the stable lending section for estimates of profitability.

4.3 Leverage Trades

Overview: The concept of leverage, or using borrowed capital to increase position size, is not new. A user deposits a certain amount of collateral, borrows a percentage of the deposited collateral, and reinvests the borrowed capital, thus gaining increased exposure to the underlying

asset. This increased exposure is the equivalent of magnifying a position's gains and losses. It inherently comes with increased risk for both parties.

Liquidation: The borrower must be weary of Aave's liquidation mechanism. Aave implements what they call the "Health Factor" calculated as:

$$\frac{\Sigma Collateral\ in\ ETH * Liquidation\ Ratio}{Borrowings\ in\ ETH}$$

When the health factor of the borrowers account drops below one, a third-party liquidator can call the liquidate function in the Aave application. This allows the liquidator to then step in and pay back up to 50% of the borrowed funds using the debt asset. Aave also incentivizes liquidators to actively search for opportunities by offering them a discount on the collateral, 5% in the case of ETH. Aave also allows the user to chose whether they want to receive aTokens (leave the money deposited in Aave) or the underlying asset after a successful liquidation call. In practice, this mechanism offers part of an undercollateralized position for sale at a discount, provided the buyer has sufficient funds to make the purchase of the collateral using the debt asset. An example: Bob deposits 10 ETH and borrows 5 ETH worth of USDC. Bob's health factor drops below one. A liquidator can pay up to 50% of Bob's debt (2.5 ETH worth of DAI). In return the liquidator can claim the ETH collateral plus a 5% bonus. This entitles the liquidator to 2.5 + 0.125 ETH for repaying 2.5 ETH worth of DAI.

Levered Borrowing Strategy: Execution involves three distinct steps. First, ETH must be deposited into the lending platform as collateral, earning interest, in this case at 0.33%. Second, an amount of ETH is borrowed. The current borrow APY is 4.93%. Finally, the borrowed funds are supplied as further collateral to earn interest. The cycle can be repeated many times, increasing overall exposure to the underlying asset. Each time it is repeated the position becomes more and more risky as there is more dollar denominated debt at stake. The model below reflects

the PnL of a leveraged ETH position at various leverage amounts and prices in USD at the time of closing the trade. Further the following assumptions are held to be true: 1) The market price at the time of deposit is 3000 ETHUSD. 2) The APYs are stable. 3) Transaction fees are negligible. 4) There is a one-year time horizon.

	$ 2,000	$ 2,250	$ 2,500	$ 2,750	$ 3,000	$ 3,250	$ 3,500	$ 3,750	$ 4,000
0.50	$1,435.95	$1,812.19	$2,188.43	$2,564.66	$2,940.90	$3,317.14	$3,693.38	$4,069.61	$4,445.85
1.00	$ 865.30	$1,366.95	$1,868.60	$2,370.25	$2,871.90	$3,373.55	$3,875.20	$4,376.85	$4,878.50
1.50	Liquidate	$ 921.71	$1,548.78	$2,175.84	$2,802.90	$3,429.96	$4,057.03	$4,684.09	$5,311.15
2.00	Liquidate	Liquidate	$1,228.95	$1,981.43	$2,733.90	$3,486.38	$4,238.85	$4,991.33	$5,743.80
2.50	Liquidate	Liquidate	Liquidate	$1,787.01	$2,664.90	$3,542.79	$4,420.68	$5,298.56	$6,176.45
3.00	Liquidate	Liquidate	Liquidate	$1,592.60	$2,595.90	$3,599.20	$4,602.50	$5,605.80	$6,609.10
3.50	Liquidate	Liquidate	Liquidate	Liquidate	$2,526.90	$3,655.61	$4,784.33	$5,913.04	$7,041.75
4.00	Liquidate	Liquidate	Liquidate	Liquidate	$2,457.90	$3,712.03	$4,966.15	$6,220.28	$7,474.40

Figure 5

Levered Yield Aggregation: Execution of this strategy is similar to the prior, with a couple caveats. The main one being that the borrowed funds are not recycled into the collateral pool to improve the health factor of the borrower. This inherently limits the amount of leverage a user can take on with this strategy, as Aave limits ETH borrows to about 82% of the collateral. Because of this feature this strategy operates in the following manner: ETH is deposited as collateral. Up to approximately .8 ETH can then be borrowed for every one ETH deposited. The borrowed ETH is then deposited in the Yearn Finance yETH vault earning an estimated 1.29% APY.

The yETH vault generates yield through four distinct strategies. Though each strategy uses different assets and protocols, the base premise is the same. Use the deposited ETH to earn rewards on other protocols. Sell the reward tokens and deposit the profits into the vault. Repeat.

The same assumptions are held as in the previous section. See Figure 6 for estimates of profitability as well as the liquidation point at various prices and leverage ratios.

	$ 2,000	$ 2,250	$ 2,500	$ 2,750	$ 3,000	$ 3,250	$ 3,500	$ 3,750	$ 4,000
0.10	$ 1,898.47	$ 2,174.62	$ 2,450.77	$ 2,726.91	$ 3,003.06	$ 3,279.21	$ 3,555.36	$ 3,831.50	$ 4,107.65
0.15	$ 1,844.41	$ 2,133.21	$ 2,422.02	$ 2,710.83	$ 2,999.64	$ 3,288.45	$ 3,577.26	$ 3,866.07	$ 4,154.88
0.25	$ 1,736.28	$ 2,050.41	$ 2,364.54	$ 2,678.67	$ 2,992.80	$ 3,306.93	$ 3,621.06	$ 3,935.19	$ 4,249.33
0.50	$ 1,465.95	$ 1,843.39	$ 2,220.83	$ 2,598.26	$ 2,975.70	$ 3,353.14	$ 3,730.58	$ 4,108.01	$ 4,485.45
0.75	Liquidate	Liquidate	Liquidate	$ 2,517.86	$ 2,958.60	$ 3,399.34	$ 3,840.09	$ 4,280.83	$ 4,721.58
0.85	Liquidate	Liquidate	Liquidate	Liquidate	Liquidate	$ 3,417.83	$ 3,883.89	$ 4,349.96	$ 4,816.03

Figure 6

4.4 Composability

This is by no means an exhaustive list of the potential trading pairs, protocols, and strategies through which one can generate yield. For each example given there are another 10 strategies that have not been modeled. This is one of the hallmark characteristics of DeFi apps. Due to the nature of ERC-20 tokens the positions and assets created by activity on the blockchain are all tradeable throughout the entire ecosystem.

Beyond the relatively basic examples laid out here, users can extend the trading system deeper into the environment. For example, say Trader A is bullish on an ERC-20 token called TKN. The trader could borrow ETH from Compound Finance. That trader could then provide ETH/TKN liquidity to a Uniswap liquidity pool, where they earn fees on the trades in that pool. The trader could then take the LP token they received in exchange for their liquidity and deposit it into an ETH/TKN Pickle Jar, where it is used to execute a yield aggregation strategy.

5 Risks

Things are not all peaches and cream in the decentralized financial universe. Many of the risks that currently exist for traditional financial services companies also exist in the decentralized world, as do a myriad of additional risk factors that one must account for before making the decision to participate. Traditional risk factors such as liquidity and insolvency are at play in addition to novel risk factors such as impermanent loss, software integrity, and

governance attacks, amongst others. As with any other market, macroeconomic factors play a large part directing the direction of price movement.

5.1 Liquidity Risk

Liquidity is generally referred to as the ease at which an asset is bought and sold without affecting its market price. The deeper the liquidity of a market, the less friction there is between buyers and sellers. Liquidity risk refers to a firm's, individual's, and now software's ability to repay their debts without suffering massive losses.

In order to understand liquidity risk for traditional banks it is imperative to understand what debts a bank has and how it generates the income used to pay these debts. When a bank receives a deposit, it is recorded as a debt, as the bank now owes the depositor their initial deposit plus whatever interest has accrued on that deposit. When a bank makes a loan, it is recorded as an asset, because the borrower is liable to the bank for the borrowed funds plus interest accrued on these loans. The liquidity problem arises when two events happen simultaneously. First, the borrower cannot continue paying their loan. They have defaulted. Second, the depositor requests that his funds be returned to him/her. This presents an issue for the bank because the deposited funds were used as the loan to the borrower. Seeing as the bank does not have possession of the depositor's funds (they were loaned out) they must draw upon their shareholders to repay the depositor.

While this is a simplification of the mechanism, imagine the following scenario. There are 100 depositors and 100 borrowers. All but 10% of the deposited money was loaned out to the borrowers. 75 of the borrowers can no longer repay their loans and all of the depositors want their money back. This is known as a bank run, when the bank does not have enough funds available to pay its depositors back at the moment they request their capital. In a world where

shareholders have limited funds, the bank can only afford a certain amount of bad loans, else they go insolvent, and cannot pay their debts. However, this is not the case in the United States. Due to the mechanisms of the Federal Reserve, U.S. Treasury, and Congress, the biggest banks in the world will always be able to make as many risky loans as they would like, as they will just print more money to prevent insolvency.

Decentralized lending protocols face a similar conundrum, however rather than having a group of shareholders to back bad debt, they have what is commonly called a pool. Creditors deposit assets into the pool and debtors borrow assets from the pool. Like a bank, the pool grows by accumulating the spread between the borrow rate and deposit rate. As we saw in the section on lending platforms and their interest rates, in a low-liquidity environment lending protocols adjust their rates as a method of incentivizing users to take an action (deposit capital or repay debt). This mechanism acts as a buffer to avoid potential illiquidity events.

Liquidity risk is also dependent on the depth of liquidity in exchange markets. If liquidity is sufficiently low, then participants face the risk of not being able to exchange one asset for another that they will use to pay their debt. A good example of this can be seen in the real estate market. When liquidity in the housing market is high (there is a lot of buying and selling activity), buyers often will take on debt in the form of a mortgage to purchase the house that they want. The buyer now owes a certain amount of the money to the bank, and they have the value of their house to act as collateral for this debt. However, say the buyer can no longer pay the interest on their loan. Simultaneously, the housing market suddenly becomes illiquid, the homeowner cannot sell the house or is forced to sell it for a much lower price than they initially bought it. The bank now will collect (foreclose) the asset to cover a portion of the bad loan.

Many decentralized lenders employ a liquidation incentive. This incentive attempts to ensure that a protocol always has access to enough funds to repay creditors. If the value of borrowed funds drops below the value of the collateral, up to 50% of the borrower's collateral is sold at a discount to pay off their borrowed position. In this case say a participant deposits 1 ETH (~$3,000) into Aave and borrows .5 ETH worth of USDC (~$1500). The price of ETH drops to $2,250 and the UDSC is only worth .66 ETH. the value of the borrowed funds has dropped below the value of the deposited funds, thus the position is eligible for liquidation. This mechanism, when employed efficiently, ensures that the only market participant who suffers from insufficient liquidity is the over-collateralized debtor.

5.2 Divergence Loss

Impermanent loss is a euphemistic term used to refer to the return difference between providing funds to an AMM's liquidity pool and the alternative of holding the tokens. Impermanent loss is rarely impermanent nor is it always recognized as a loss. A more appropriate term is divergence loss.

When a market participant, Jim, provides liquidity, say in a USDC-ETH pool that is weighted 50-50, he deposits 50% of the position in USDC and 50% of the position in ETH. In the section on automated market makers, we noted the formula $xy = k$. In this case x is USDC and y is ETH. Say the pool holds 10 ETH and $10,000 USDC, k is constant at 100,000. Jim's position represents 10% of the pool, so 1 ETH and $1,000 USDC, or $2,000 total. The AMM pool is indifferent holding 20 ETH and 5000

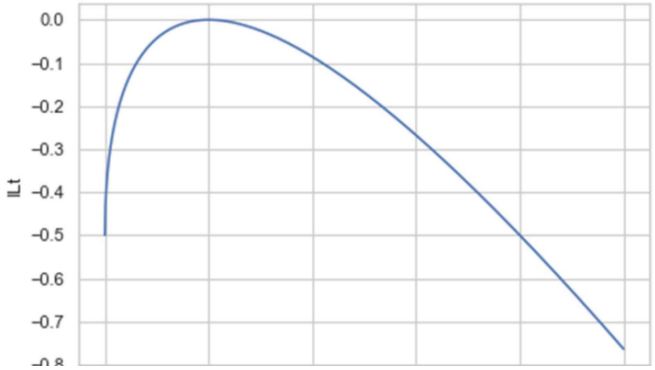


Figure 7

USDC or 5 ETH and 20,000 USDC. Recall the price shown to users of the pool is the ratio of one asset to another. At the time of deposit the price of ETH was 10,000/10 or $1,000 per ETH. Say the price increases to 4,000 USDC. While this is happening, arbitrage traders will be adding USDC and removing ETH until the ratio equals the current price. One this happens there are 5 ETH in the pool and $20,000. If Jim were to try and withdraw his funds, he would now only be entitled to .5 ETH and $2,000 USDC, totaling $4,000. Had Jim just held his 1 ETH and 1,000 USDC he would now have $5,000. Divergence loss faced at different price multiples is shown in Figure 7, where ILt is the divergence loss in % of initial position and xt is the multiple by which price changed.

This phenomenon is referred to as impermanent loss because theoretically, if the price of ETH were to fall to the level at which Jim made his initial deposit, he would face no divergence loss.

The quantification of potential divergence losses excludes one key factor: fees accrued from exchanges made using the pool. Fees that traders pay to make an exchange are accrued into the liquidity pool, so when the liquidity providers wish to withdraw their portion of the pool, they also withdraw their portion of the fees that have accrued to the pool. Without the fee accrual mechanism there would be no inventive to provide liquidity as opposed to simply holding the assets.

A study done in 2021 by members of the Bancor team found that the top 17 pools on Uniswap earned $199.3m in fees since inception. They also found that those pools suffered $260.1m in divergence losses, meaning in aggregate the LPs would have been better off by $60.8m had they simply held the tokens themselves.

5.3 Smart Contract Exploits

Owing to the irreversible nature of a blockchain, applications built on these networks using smart contracts must be entirely bug free. If a contract contains errors in its code or logic, then it can be exploited and funds can be stolen. Since there is no way of reversing the transaction, the funds are permanently lost.

These exploits are often caused by coding errors in the smart contracts. These errors can either be related to the more advanced aspects of virtual machine programming and coding language semantics, or to the logical operations of the smart contracts. For example, on Apr. 14, 2022 a called Unicorn Nodes executed an attack on its token holders. The contract that created the RNBW token, Unicorn Node's native token, had a back door built into it that allowed anyone to transfer another's balance of tokens. The creators of Unicorn Node used this bug in the contract to remove tokens from holders wallets and sell them on the open market.

More advanced attacks include attacks on protocol governance. These attacks are generally carried out in several steps, with the result being to change protocol governance in a way that allows for an exploit. First, the attacker submits a malicious governance proposal that changes the fundamental operation of the smart contract. Then they acquire a large enough voting share to control the governance vote on the malicious proposal and transfer the protocols funds to their own wallet. Recently this exact method was used to exploit the Beanstalk protocol for over $182m.

A blockchain network can also be exploited in what is known as a 51% attack. The base premise of blockchain security is that there are lots of computers that all come to an agreement that a transaction is valid. The transaction is then officially recorded to the blockchain. When the system is working properly malicious transactions cannot be recorded on the ledger because less

than half the total computers agree that the transaction is valid. However, if an attacker controls over half of the computers, then they can influence what is considered valid.

On Mar. 29, 2022 the Ronin network blockchain, home of metaverse game Axie Infinity, was hacked for $625m. The hack was carried out when the attacker found a backdoor that allowed him access to 5 of the 9 Ronin validators. From there, they were able to execute transactions that drained the funds from the network and sent them to the attackers wallet.

Having funds stolen from a bank is not a new concept. It has simply been replicated in the digital world. Similarly, just as banks and corporations are audited smart contract auditing services are available. There are firms which will audit protocols smart contracts to ensure their safety and validity.

5.4 Interoperability

Part of the value proposition for DeFi applications is the fact that they are highly interoperable. A single user can utilize multiple different services or protocols with minimal friction. Compare sending money from one bank to another. Banks have communication networks that are subject to delays of days at a time. The Ethereum network allows users and protocols to transfer funds within minutes. This facilitates rapid and complex movements of capital between parties and applications on the network. While it is an attractive feature of any set of financial service providers, it also poses a relatively large risk.

Tightly coupled liquidity systems create a heavy degree of financial integration, which results in systemic dependencies between applications. The contagion, exploit, or sudden failure of one member of the intertwined system of exchanges, lenders, or aggregators could ripple throughout the entire network affecting the entire group of applications.

An example of this can be demonstrated by the mechanisms through which some liquidity providers leverage their positions. As interoperability has increased applications have been developed which allow LPs to use their liquidity positions as collateral, creating a secondary market for liquidity positions. Using LP tokens as collateral creates a feedback loop where if the price of the underlying asset experiences heavy volatility it can create a cascade of loan liquidations.

This is not too different from what happens in a traditional bank run. Depositors believe that the bank does not have the assets to repay the depositors. They are insolvent, and so the depositor attempts to withdraw their funds. Since the bank is not fully reserved all the depositors do not have access to their funds and are forced to take a loss. Similarly, if a lending protocol uses LP tokens as collateral for issued debt and the value of the LP tokens declines significantly, the protocol is now insolvent. It has issued more debt than the value of its collateral.

6 Conclusions

This paper has examined the basic principals of decentralized financial services applications, as well as estimated potential returns from using these applications, and the risks that come with these potential returns. I detailed the definitions of multiple different token types, including ERC-20 tokens, stablecoins, LP tokens, and governance tokens.

The economic mechanisms that allow protocols to generate yield were explored and then three types of protocol were discussed. Each discussion focused on the principals of the protocol type as well as an overview of how the type of protocol works and what its function is. It is worth noting, that because each application is written differently and has different features, almost no two will be the exact same. This applies not only across types but within the types as

well. They share many features, but each application has features and advancements that the founders believe give it a competitive advantage over other protocols.

Each protocol type was then incorporated into at least one trading strategy and the returns of these strategies were estimated. These estimates provide a guideline for the return of any given strategy given current market conditions and estimated APYs provided by the protocols. Protocols often have unique mechanisms by which they generate the yield. These mechanisms depend on a variety of market factors and participant behaviors. This naturally makes it impossible to forecast the actual amount of interest that will be accrued to the depositor.

Finally, the risks that are present when interacting with DeFi applications were compared to many of the risks that are present in traditional financial markets. While these risks present themselves in different ways conceptually many of them are very similar. There is also a greater magnitude of systemic risk in the DeFi ecosystem because it lacks the battle testing and liquidity depth that traditional financial markets have.

There are several areas that I believe could be conducive to further research. The first being the amount of leverage in the system. By finding the percent of funds that had been loaned to a user and then deposited as collateral one could determine the actual amount of tokens that had been initially deposited into contracts. Further studies could also be done on the ether token by estimating the monetary premium it has by becoming the dominant infrastructure of global digital finance and commerce.

Bibliography

Aave's Risk Framework. n.d. Retrieved From https://docs.aave.com/risk/

Berentsen, A., & Schär, F. (2019). Stablecoins: The quest for a low-volatility cryptocurrency. The economics of Fintech and digital currencies, 65-75.

Buterin, V. (2014). Ethereum whitepaper. ethereum.org. Retrieved March 24, 2022, from https://ethereum.org/en/whitepaper/

Cousaert, S., Xu, J., & Matsui, T. (2021, September 14). Sok: Yield aggregators in Defi. arXiv.org. Retrieved March 24, 2022, from https://arxiv.org/abs/2105.13891

Defi Pulse - The Decentralized Finance Leaderboard: Stats, charts and Guides: Defi Pulse. https://defipulse.com. (n.d.). Retrieved March 31, 2022, from https://www.defipulse.com/

ERC-20 Token Standard. (December 3, 2021) Retrieved from https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

Gudgeon, L., Werner, S., Perez, D., & Knottenbelt, W. J. (2020). DEFI protocols for loanable funds. *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. https://doi.org/10.1145/3419614.3423254

Harvey, C. R., Ramachandran, A. Santoro, J. (2020, December 15). Defi and the future of Finance. SSRN. Retrieved March 31, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3711777

Loesch, S., Hindman, N., Richardson, M. B., & Welch, N. (2021). Impermanent Loss in Uniswap v3. arXiv preprint arXiv:2111.09192.

Perez, D., Werner, S. M., Xu, J., & Livshits, B. (2021, October 3). *Liquidations: Defi on a knife-edge*. SpringerLink. Retrieved April 6, 2022, from https://link.springer.com/chapter/10.1007/978-3-662-64331-0_24

Schär, F. (2021, April 15). Decentralized finance: On blockchain- and Smart Contract-based Financial Markets. Economic Research - Federal Reserve Bank of St. Louis. Retrieved April 1, 2022, from https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

Vadgama, N., Xu, J., & Tasca, P. (2022). *Enabling the internet of value: How blockchain connects global businesses*. Springer Nature Switzerland AG.

Warren, W., & Bandeali, A. (2017, February 21). 0x: An open protocol for decentralized exchange on the Ethereum blockchain. 0xProject.com. Retrieved April 1, 2022, from https://www.0x.org/pdfs/0x_white_paper.pdf