FIN. STREET

HOW TO DEFI?

LEARN HOW TO GET STARTED WITH DECENTRALIZED FINANCE

Table of CONTENTS

WHAT IS DECENTRALIZED FINANCE (DEFI)?

Decentralized Finance or DeFiis the movement that allows users to utilize financial services such as borrowing, lending, and trading without the need to rely on centralized entities. These financial services are provided via Decentralized Applications (Dapps), in which a majority of them are deployed on the Ethereum platform.

> *DeFi is not a single product or company but is instead a set of products and services that acts as a replacement for institutions ranging from banking, insurance, bonds and money markets. DeFi Dapps enable users to combine their services to open up multiple possibilities. It is often called money LEGOs due to its composability.*

In order for DeFi Dapps to work, it usually requires collateral to be locked into smart contracts. The cumulative collateral locked in DeFi Dapps is often referred to as the Total Value Locked. According to DeFi Pulse, the Total Value Locked at the start of 2019 measured around $275 million but in February 2020, it reached a high of $1.2 billion. The large growth of Total Value Locked serves as an indicator of the rapid growth of the DeFi ecosystem.

The DeFi Ecosystem

With such rapid growth, it would be impossible for us to cover everything DeFi has to offer in this book. That is why we have selected a few categories and DeFi Dapps that we believe are important and crucial for beginners to understand before steppinginto the DeFi ecosystem.

These DeFi Dapps stand to revolutionize traditional financial services by removing the need for any middlemen. However, it should be noted that DeFi in its current state is still highly nascent and experimental with many projects being rapidly improved upon daily. As time goes on, DeFi may develop further and look entirely unrecognizable from what it is today. Nevertheless, it is useful to understand the early beginnings of DeFi and one can still take advantage of the features offered DeFi Dapps today with the right know-how.

How Decentralized is DeFi?

It is not easy to answer how decentralized DeFi is. For simplicity's sake, we will separate the degrees of decentralization into three categories: centralized, semi-decentralizedand completely decentralized.

Centralized

- Characteristics: Custodial, uses centralized price feeds, centrally-determined interest rates, centrally-provided liquidity for margin calls
- Examples: Salt, BlockFi, Nexo and Celsius

Semi-Decentralized

- Characteristics: Non-custodial, decentralized price feeds, permissionless initiation of margin calls, permissionless margin liquidity, decentralized interest rate determination, decentralized platform development/updates
- Examples: Compound, MakerDAO, dYdX, bZx

Completely Decentralized

- Characteristics: Every component is decentralized
- Examples: No DeFi protocol is completely decentralized yet.

Currently, most DeFi dapps are sitting in the semi-decentralized category. A further breakdown of the decentralization components can be read in Kyle Kistner's articlein the Recommended Readings. Now that you have a better understanding of what being decentralized means, let's move on to key categories of DeFi.

DeFi Key Categories

In this book, we will be covering the following 8 major categories of DeFi:

Stablecoins

The prices of cryptocurrencies are known to be extremely volatile. It is common for cryptocurrencies to have intraday swings of over 10%. To mitigate this volatility, stablecoins that are pegged to other stable assets such as the USD were created.

Tether (USDT) was one of the first centralized stablecoins to be introduced. Every USDT is supposedly backed by $1 in the issuer's bank account. However, one major downside to USDT is that users need to trust that the USD reserves are fully collateralized and actually exist.

Decentralized stablecoins aim to solve this trust issue. Decentralized stablecoins are created in a decentralized manner via an overcollateralization method, operate fully on decentralized ledgers, are governed by decentralized autonomous organizations, and its reserves can be publicly audited by anyone.

While stablecoins are not really a financial application themselves, they are important in making DeFi applications more accessible to everyone by having a stable store of value.

Lending and Borrowing

Traditional financial systems require users to have bank accounts to utilize their services, a luxury that 1.7 billion people currently do not have. Borrowing from banks comes with other restrictions such as having agood credit score and having sufficient collateral to convince the banks that one is credit-worthy and able to repay a loan.

Decentralized lending and borrowing remove this barrier, allowing anyone to collateralize their digital assets and use this to obtain loans. One can also earn a yield on their assets and participate in the lending market by contributing to lending pools and earning interest on these assets. With decentralized lending and borrowing, there is no need for a bank account or a credit-worthiness check.

Exchanges

To exchange one cryptocurrency to another, one can use exchanges such as Coinbase or Binance. Exchanges like these are centralized exchanges, meaning they are both the intermediaries and custodians of the assets being traded. Users of these exchanges do not have full control of their assets, putting their assets at risk in case the exchanges get hacked and are unable to repay their obligations.

Decentralized exchanges aim to solve this issue by allowing users to exchange cryptocurrencies without giving up custody of their coins. Without storing any funds on

centralized exchanges, users do not need to trust the exchanges to stay solvent.

Derivatives

A derivative is a contract whose value is derived from another underlying asset such as stocks, commodities, currencies, indexes, bonds, or interest rates.

Traders can use derivatives to hedge their positions and decrease their risk in any particular trade. For example, imagine you are a glove manufacturer and want to hedge yourself from an unexpected increase in rubber price. You can buy a futures contract from your supplier to deliver a specific amount of rubber at a specific future delivery date at an agreed price today.

Derivatives contracts are mainly traded on centralized platforms. DeFi platforms are starting to build decentralized derivatives markets.

Fund Management

A derivative is a contract whose value is derived from another Fund management is the process of overseeing your assets and managing its cash flow to generate a return on your investments. There are two main types of fund management—active and passive fund management. Active fund management has a management team making investment decisions to beat a particular benchmark such as the S&P 500. Passive fund managementdoes not have a management team but is designed in such a way to mimic the performance of a particular benchmark as closely as possible.

In DeFi, some projects have started to allow for passive fund management to take place in a decentralized manner. Thetransparency of DeFi makes it easy for users to track how their funds are being managed and understand the cost they will be paying.

Lottery

As DeFicontinues to evolve, creative and disruptive financial applications will emerge, democratizing accessibility and removing intermediaries. Putting a DeFi spin onto lotteries allow for the removal of custodianship of the pooled capital unto a smart contracton the Ethereum Blockchain.

With the modularity of DeFi, it is possible to link a simple lottery Dapp to another DeFi Dapp and create something of more value. One DeFi Dapp that we will explore in this book allows participants to pool their capital together. The pooled capital is then invested into a DeFi lending Dapp and the interest earned is given to a random winner at a set interval. Once the winner is selected, the lottery purchasers get their lottery tickets refunded, ensuring no-loss to all participants.

Payments

A key role of cryptocurrency is to allow decentralized and trustless value transfer between

two parties. With the growth of DeFi, more creative payment methods are being innovated and experimented.

One such DeFi project that is explored in this book aims to change the way we approach payment by reconfiguring payments as streams instead of transactions we are familiar with. The possibility of providing payments as streams open up a plethora of potential applications of money. Imagine “pay-as-you-use” but on a much more granular scale and with higher accuracy.

The nascency of DeFi and the rate of innovation will undoubtedly introduce new ways of thinking on how payments work to address many of the current financial system’s shortfalls.

Insurance

Insurance is a risk management strategy in which an individual receives financial protection or reimbursement against losses from an insurance company in the event of an unfortunate incident. It is common for individuals to purchase insurance on cars, home, health, and life. But is there decentralized insurance for DeFi?

All of the tokens locked within smart contracts are potentially vulnerable to smart contract exploits due to the large potential payout possible. While most projects have gotten their codebases audited, we never know if the smart contracts are truly safe and there is always a possibility of a hack which may result in a loss. The risks highlight the need for purchasing insurance especially if one is dealing with large amounts of funds on DeFi. We will explore several decentralized insurance options in this book.

DECENTRALIZED STABLECOINS

The prices of cryptocurrencies are extremely volatile. To mitigate this volatility, stablecoins that are pegged to other stable assets such as the USD were created. Stablecoins help users to hedge against this price volatility and was created to be a reliable medium of exchange. Stablecoins have since quickly evolved to be a strong component of DeFi that is pivotal to this modular ecosystem.

> *There are 19 stablecoins currently listed on CoinGecko. The top 5 stablecoins has a market capitalization totaling over $5 billion.*

We will be looking into USD-pegged stablecoins in this chapter. Not all stablecoinsare the same as they employ different mechanisms to keep their peg against USD. There are two types of pegs, namely fiat-collateralized and crypto-collateralized. Most stablecoins employ the fiat-collateralized system to maintain their USD peg.

Top 5 Cryptocurrency Stablecoins (Feb 2020)		
Rank	Bank	Market Cap. ($ million)
1	Tether (USDT)	4284
2	USD Coin (USDC)	443
3	Paxos Standard (PAX)	202
4	True USD (TUSD)	142
10	Dai (DAI)	123

For simplicity, we will look at two USD stablecoins, Tether (USDT) and Dai (DAI) to showcase the differences in their pegging management.

Tether (USDT) pegs itself to $1 by maintaining reserves of $1 per Tether token minted. While Tether is the largest and most widely used USD stablecoin with daily trading volumes averaging approximately $30 billion in the month of January 2020, Tether reserves are keptin financial institutions and users will have to trust Tether as an entity to actually have the reserve amounts that they claim. Tether is therefore a **centralized, fiat-collateralized stablecoin.**

Dai (DAI) on the other hand, is collateralized using cryptocurrencies such as Ethereum (ETH). Its value is pegged to $1 through protocols voted on by a decentralized autonomous organization and smart contracts. At any given time, the collateral to generate DAI can be easily validated by users. DAI is a **decentralized, crypto-collateralized stablecoin.**

Based on the top 5 stablecoins' market capitalization, Tether dominates the stablecoin market with approximately 80% of market share. Although DAI's market share only stands at about 3%, its trading volume has been increasing at a much faster rate. DAI's trading volume increased by over 4,000% relative to Tether's growth of 126% since the start of January 2020.

DAI is the native stablecoin used most widely in the DeFi ecosystem. It is the preferred USD stablecoin used in DeFi trading, lending and more. To understand DAI further, we will introduce you to its platform, Maker.

Maker

What is Maker?

Maker is a smart-contract platform that runs on the Ethereum blockchain and has three tokens: stablecoins, Sai and Dai (both algorithmically pegged to $1), as well as its governance token, Maker (MKR).

Sai (SAI) is also known as Single Collateral Dai and is backed only by Ether (ETH) as collateral.

Dai (DAI) was launched in November 2019 and is also known as Multi-Collateral Dai. It is currently backed by Ether (ETH) and Basic Attention Token (BAT) as collaterals with plans to add other assets as collaterals in the future.

Maker (MKR) is Maker's governance token and users can use it to vote for improvements on the Maker platform via the Maker Improvement Proposals. Maker is a type of organization known as a Decentralized Autonomous Organization (DAO). We will look further into this under the governance subsection.

What are the Differences between Sai and Dai?

Maker initially started out on 19 December 2017with the Single Collateral Dai. It was minted using Ether (ETH) as the sole collateral. On 18 November 2019, Maker announced the launch of the new Multi-Collateral Dai, which can be minted using either Ether (ETH) and/or Basic Attention Token (BAT) as collateral, with plans to allow other cryptocurrencies to back it in the future. To reiterate,

Single-Collateral Dai	**=**	**Legacy Dai**	**=**	**Sai**
Multi-Collateral Dai	**=**	**New Dai**	**=**	**Dai**

Moving forward, Multi-Collateral Dai will be the de-facto stablecoin standard maintained by Maker and eventually, SAI will be phased out and no longer supported by Maker. For brevity, we will only be using Multi-Collateral Dai (DAI) to walk through examples in the following sections.

How does Maker Govern the System?

Recall our brief mention on Decentralized Autonomous Organization (DAO)? That's where the Maker (MKR) token comes in. MKR holders have voting rights proportional to the amount of MKR tokens they own in the DAO and can vote on parameters governing the Maker Protocol.

The parameters that the MKR holders vote on are vital in keeping the ecosystem healthy, which in turn helps ensure that Dai remains pegged to $1. We will briefly go through three key parameters which you will need to know in the Dai stablecoin ecosystem:

1. Collateral Ratio

The amount of Dai that can be minted is dependent on the collateral ratio.

Ether (ETH) collateral ratio=150%

Basic Attention Token (BAT) collateral ratio=150%

Essentially, what it means with a collateral ratio of 150% is that to mint $100, you need to deposit a minimum of $150 worth of ETH or BAT.

2. Stability Fee

It is equivalent to the 'interest rate' which you are required to pay along with the principal debt of the vault. The stability fee is at 8% as of February 2020.

3. Dai Savings Rate (DSR)

The Dai Savings Rate (DSR) is the interest earned by holding Dai over time. It also acts as a monetary tool to influence the demand of Dai. The DSR rate is set at 7.50% as of February 2020.

Motivations to Issue DAI:

Why would you want to lock up a higher value of ETH or BAT only to issue Dai with a lower value? You could have sold your assets directly to USD instead.

There are three possible cases:

1. You need cash now and you have an asset that you believe will be worth more in the future.
   - In this case, you could hold your asset in the Maker vault and get the money now by issuing Dai.

2. You need cash now but do not want to risk triggering a taxable event when selling your asset.
   - Instead, you will draw the loans by issuing Dai.

3. Investment Leverage
   - You are able to conduct investment leverage on your assets given that you believe the value of your assets would go up.

How do I get my hands on some Dai (DAI)?

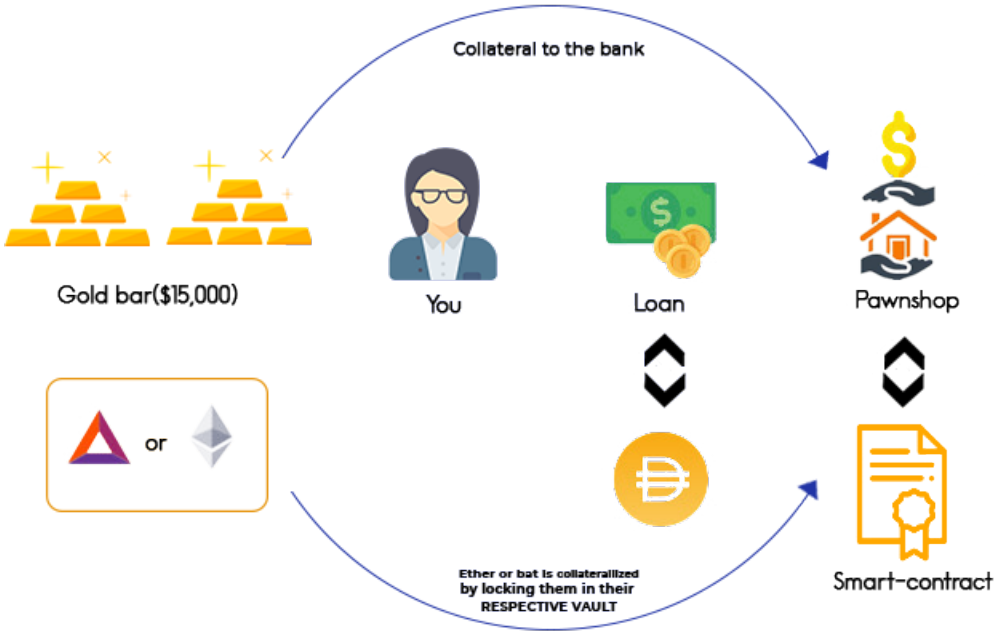
There are two ways you can get your hands on some Dai (DAI):

1. Minting Dai

2. Trading DAI

1. Minting Dai

We will walk through how DAI can be minted using a pawnshop analogy.



Let's assume that one day you are in need of $10,000 cash, but all you have are gold bars worth $15,000 at home. Believing that the price of gold will increase in the future, instead of selling the gold bars for cash, you decide to go to a pawnshop to borrow $10,000 cash by putting your gold bars as collateral for it. The pawnshop agrees to lend you $10,000 with an interest of 8% for the cash loan. Both of you sign a contract agreement to finalize the transaction.

Now let's change the terminology to get the narrative of DAI:

Gold bars (Collateral)	→	**Ether or Basic Attention Token (Collateral –Multi-Collateral Dai)**
Cash loan	→	**Dai (DAI)**
The pawnshop	→	**Maker**
Contract agreement	→	**Smart Contract (Vault)**
Loan interest	→	**Stability Fee**

What happens is that you will mint or 'borrow' Dai via the Maker platform by putting your Ether (ETH) or Basic Attention Token (BAT) as collateral. You will have to repay your 'loan' along with the 'loan interest' which is the stability fee when you want to redeem your ETH or BAT at the end of your loan.

To provide an overview, let's walk through how you can mint your own Dai.

On the Maker platform (www.oasis.app), you can borrow Dai by putting your ETH or BAT into the vault. Assuming ETH is currently worth $150, you can thus lock 1 ETH into the vault and receive a maximum of 100 DAI ($100) with a 150% collateral ratio.

You should not draw out the maximum of 100 DAI that you are allowed to but leave some buffer in the event that ETH price decreases. It is advisable to give a wider gap to ensure your collateral ratio always remains above 150%. This ensures that your vault will not be liquidated and charged the 13% liquidation penalty in the event that ETH falls in price and your collateral ratio falls below 150%.

2. Trading DAI

The above methods are all the ways DAI are created. Once DAI is created, you can send it anywhere you want. Some users may send their DAI to cryptocurrency exchanges and you may also buy DAI from these secondary markets without the need to mint them.

Buying DAI this way is easier as you don't have to lock up collateral and do not have to worry about the collateral ratio and stability fee.

Black Swan Event

A black swan event is an unpredictable and extreme event that may cause severe consequences. In the case where both ETH and BAT has a significant drop in price, Emergency Shutdown is triggered. It is a process used as a last resort to settle the Maker Platform by shutting the system down. The process is to ensure the holders of Dai holders and Vault users receive the net value of assets they are entitled to.

Why use Maker?

As previously mentioned in Section 2: Stablecoins, there are many stablecoins out there and the core distinctions of these coins lie in their protocol. Unlike most stablecoin platforms, Maker isfullyoperating on the distributed ledger. Thus, Maker inherently possesses the characteristics of the blockchain: secured, immutable and most importantly, transparent. Additionally, Maker's infrastructures have strengthened the security of the system with comprehensive risk protocols and mechanisms via real-time information.

And that's it for Makers' Stablecoin, Dai.

DECENTRALIZED LENDING AND BORROWING

One of the most common services offered by the financial industry is the lending and borrowing of funds, which was made possible by the concept of credit and collateralization.

> *It can be argued that the invention of commercial-scale lending and borrowing was what brought about the Renaissance age as the possibility for the less wealthy to acquire startup funds led to a flurry of economic activity. Thus, the economy began to grow at an unprecedented pace.*

Entrepreneurs can borrow the upfront capital needed to establish a business by collateralizing the business while families can get a mortgage for a house that would otherwise be too costly to buy in cash, whilst using the house as collateral. On the other hand, the wealth accumulated can be lent off as capital to lenders. This system reduces the risk of borrowers absconding with the borrowed funds.

However, this system requires some form of trust and an intermediary. The role of an intermediary is taken up by banks and trust is maintained via a convoluted system of credit, whereby the borrower must exhibit the ability to repay the loan in order to be qualified to borrow, among a laundry list of other qualifications and requirements by the banks.

This has led to various challenges and shortfalls of the current lending and borrowing system, such as restrictive funding criteria, geographical or legal restriction to access banks, high barriers to loan acceptance, and the exclusivity of only the wealthy to enjoy the benefits of low-risk high-returns lending.

In the DeFi landscape, such barriers do not exist as banks are no longer necessary. With enough collateral, anyone can have access to capital to do whatever they want. Capital lending is also something that is no longer enjoyed only by the wealthy, everyone can contribute to a decentralized liquidity pool of which borrowers can take from and pay back at an algorithmically-determined interest rate. In contrast to applying for a loan from the bank where there are stringent Know-your-customer (KYC) and Anti-money laundering (AML) policies, one only needs to provide collateral to take a loan in DeFi.

We will explore just how such bankless lending and borrowing mechanism is possible with Compound Finance, a Defi lending and borrowing protocol.

Compound

Compound Finance is an Ethereum-based open-source money market protocol where anyone can supply or borrow cryptocurrenciesfrictionlessly. As of Feb 2020, 7 different tokens—Basic Attention Token (BAT), Dai (DAI), Ether (ETH), Augur (REP), USD Coin (USDC), Wrapped Bitcoin (WBTC)and 0x (ZRX)—can be supplied or used as collateral on the Compound Platform.

Compound operates as a liquidity pool that is built on the Ethereum blockchain. Suppliers supply assets to the pool and earn interest, while borrowers take a loan from the pool and pay interest on their debt. In essence, Compound bridges the gaps between lenders who wish to accrue interest from idle funds and borrowers who wish to borrow funds for productive or investment use.

In Compound, interest rates are denoted in Annual Percentage Yield (APY) and differ between assets. Compound derives the interest rates for different assets through algorithms which account for supply and demand of the asset.

Essentially, Compound lowers the friction for lending/borrowing by allowing suppliers/ borrowers to interact directly with the protocol for interest rates without needing to negotiate loan terms (eg. maturity, interest rate, counterparty, collaterals), thereby creating a more efficient money market.

How much interest will you receive, or pay?

The Annual Percentage Yield (APY) differs between assets as it is algorithmically set based on the supply and demand of the asset. Generally, the higher the borrowing demand, the higher the interest rate (APY) and vice versa.

Using the DAI stablecoin as an example, a lender would earn 7.58% (as of Feb 2020) in a year while a borrower would be paying 8.00% interest after a year.

Do I need to register for an account to start using Compound?

No, you do not need to register for an account and that's the beauty of Decentralized Finance applications! Unlike traditional financial applications where users are required to go through lengthy processes to get started, Compound users do not need to register for anything.

Anyone with a supported cryptocurrency wallet such as Argent and Metamask can start using Compound immediately.

Start earning interest on Compound

To earn interest, you will have to supply assets to the protocol. As of February 2020, Compound accepts 7 types of tokens.

Once you have deposited your asset into Compound, you will immediately begin to earn interest on the assets you have put in! Interest accrued on the amount that you have supplied and is calculated after each Ethereum block (average ~13 seconds).

Upon deposit, you will receive corresponding amounts of cTokens. If you supply DAI, you will receive cDAI, if you supply Ether, you will receive cETH, and so on). Interest is not immediately distributed to you, but rather accrues on the cTokens which you now hold and are redeemable for the underlying asset and interest it represents.

cTokens?

cTokens represent your balance in the protocol and accrue interest over time. In Compound, interest earned is not distributed immediately but is instead accrued in cTokens.

Let's go through this with an example.Assume that you have supplied 1,000 DAI on 1 January 2019 and APY has been constant at 10.00% throughout 2019.

On 1 January 2019, after you have deposited 1,000 DAI, you will be given 1,000 cDAI. In this case, the exchange rate between DAI and cDAI is 1:1.

On 1 January 2020, after 1 year, your 1,000 cDAI will now increase in value by 10%. The

new exchange rate between DAI and cDAI is 1:1.1. Your 1,000 cDAI is now redeemable for 1,100 DAI.

1 Jan 2019:
Deposit 1,000 DAI. Receive 1,000 cDAI. Exchange Rate: 1 cDAI = 1 DAI

1 Jan 2020:
Redeem 1,000 cDAI. Receive 1,100 DAI. Exchange Rate: 1 cDAI = 1.1 DAI (cDAI value increased by 10%)

To account for the interest accrued, cTokens become convertible into an increasing amount of the underlying asset it represents over time. cTokens are also ERC-20 tokens, meaning you can easily transfer the "ownership" of supplied assets if someone wants to take over your position as a supplier.

Start borrowing on Compound

Before borrowing, you have to supply assets into the system as collateral for your loan. Each asset has a different collateral factor. The more assets you supply, the greater is your borrowing power.

Borrowed assets are sent directly to your Ethereum wallet and from there, you can use them as you would anycryptoasset—anything you want to! Do note that that borrowing incurs a small fee of 0.025% to avoid spams and misuse of the Compound protocol.

Price movement of collateral asset

If you're thinking about putting in collateral to take a loan, you may be wondering -what happens if the value of the collateral changes? Let's see:

1.Collateral value moves up
If the value of the asset you used as collateral goes up, your collateral ratio also goes up, which is fine -nothing will happen and you can draw a bigger loan if you'd like to.

2.Collateral value moves down
On the other hand, if the collateral goes down such that your collateral ratio is now below the required collateral ratio, your collateral will be partially sold off along with a 5% liquidation fee. The process of selling off your collateral so that you achieve the minimum collateral ratio is known as liquidation.

Liquidation

Liquidation occurs when the value of the collateral provided is less than the borrowed funds.

This is to ensure that there is always excess liquidity for withdrawal and borrowing of funds, meanwhile protect lenders against default risk. The current liquidation fee is 5%.

And that’s it for Compound.

DECENTRALIZED EXCHANGES (DEX)

While Centralized Exchanges (CEXs) allow for large trades to happen with plenty of liquidity, it still carries a lot of risks because users do not have ownership of their assets in exchanges. In 2019, over $290 million worth of cryptocurrencies were stolen and over 500,000 login information were leaked from exchanges.

> ***More people are realizing these risks and are turning to Decentralized Exchanges (DEXs). DEXs work by using smart contracts and on-chain transactions to reduce or eliminate the need for an intermediary. Some popular Decentralized Exchanges include projects like Kyber Network, Uniswap, Dex Blue and dYdX.***

There are two kinds of DEXs -order book-based DEXs and liquidity pool-based DEXs. Order book DEXs like dYdX and dex.blue operate similarly to CEXs where users can place buy and sell orders at either their chosen limit prices or at market prices. The main difference between the two is that for CEXs, assets for the trade would be held on the exchange wallet whereas for DEXs, assets for trade can be held on users' own wallets.

However, one of the biggest problems facing order book-based DEXs is liquidity. Users may have to wait a long time for their orders to be filled in the order book. To solve this issue, liquidity pools-based DEXs were introduced. Liquidity pools are essentially reserves of tokens in smart contracts and users can buy or sell tokens instantly from the available tokens in the liquidity pool. The price of the token is determined algorithmically and increases for large trades. DEXs liquidity pools can be shared across multiple DEX platforms and this pushes up the available liquidity on any single platform. Examples of liquidity pools-based DEXs are Kyber Network, Bancor, and Uniswap.

We will be going through the Uniswap example in this book.

One of the features offered by CEXs is the margin trading function. Margin trading enables an investor to trade leveraged positions, boosting one's purchasing power to gain potentially higher returns. Innovations to bring margin trading on DEXs have appeared as well.Examples of DEXs offering decentralized margin trading are dYdX, NUO Network and DDEX. In this book, we will be exploring dYdX which combines both decentralized lending and borrowing markets with margin trading on their exchange.

Uniswap  Uniswap

Uniswap Exchange is a decentralized token exchange protocol built on Ethereum that allows direct swapping of tokens without the need to use a centralized exchange. When using a centralized exchange, you will need to deposit tokens to an exchange, place an order on the order book, and then withdraw the swapped tokens.

On Uniswap, you can simply swap your tokens directly from your wallet without having to go through the three steps above. All you need to do is send your tokens from your wallet to Uniswap's smart contract address and you will receive your desired token in return inyour wallet. There is no order book and the token exchange rate is determined algorithmically. All this is achieved via liquidity pools and the automated market maker mechanism.

Liquidity Pools

Liquidity pools are token reserves that sit on Uniswap's smart contracts and are available for users to exchange tokens with. For example, using ETH-DAI trading pair with 100 ETH and 20,000 DAI in the liquidity reserves, a user that wants to buy ETH using DAI may send 202.02 DAI to the Uniswap smart contract to get1 ETH in return. Once the swap has taken place, the liquidity pool is left with 99 ETH and 20,202.02 DAI.

Liquidity pools reserves are provided by liquidity providers who are incentivized to obtain a proportionate fee of Uniswap's 0.3% transaction fee. This fee is charged for every token swap on Uniswap.

There are no restrictions and anyone can be a liquidity provider -the only requirement is that one needs to provide ETH and the quoted trading token to be swapped to at the current Uniswap exchange rate. As of Feb 2020, over 125,000 ETH have been lockedinto Uniswap. The amount of reserves held by a pool plays a huge role in determining how prices are set by the Automated Market Maker Mechanism.

Automated Market Maker

MechanismPrices of assets in the pool are algorithmically determined using the

Automated Market Maker (AMM) algorithm. AMM works by maintaining a Constant Product based on the amount of liquidity in both sides of the pool.

Let's continue the ETH-DAI liquidity pool example which has 100 ETH and 20,000 DAI. To calculate the Constant Product, Uniswap will multiply both these amounts together.

ETH liquidity (x)	*	DAI liquidity (y)	=	Constant Product (k)
100	*	20,000	=	2,000,000

The price for this ETH will be determined asymptotically. The larger the order, the larger the premium that is charged. Premium refers to the additional amount of DAI required in order to purchase 1 ETH compared to the original price of 200 DAI per ETH.

How to get a token added on Uniswap?

Unlike centralized exchanges, Uniswapas a decentralized exchange does not have a team or gatekeepers to evaluate and decide on which tokens to list. Instead, any ERC-20 token can be listed on Uniswap by anyone and be traded as long as liquidity exists for the given pair. All a user needs to do is to interact with the platform to register the new token and a new market will be initialized for this token.

And that's it for Uniswap.

dYdX

$\delta Y / \delta X$

dYdX is a decentralized exchange protocol for lending, borrowing and margin/leveraged trading. It currently supports 3 assets—ETH, USDC, and DAI. Through the use of off-chain order books with on-chain settlements, the dYdX protocolaims to create efficient, fair and trustless financial markets not governed by any central authority.At first glance, dYdX appears to have some similarities to Compound -users can supply assets (lend) to earn interest and also loan assets (borrow) after depositing collateral. However, dYdX takes it one step further by incorporating a margin and leveraged exchange with ETH margin trading up to 5X leverage using either DAI or USDC.

Lending

If you are a crypto holder who would like to generate some passive income on your otherwise unproductive cryptoassets, you may consider lending it out on dYdX for some yield. It is relatively low risk and by depositing it into dYdX, interest accrues every second without any additional maintenance or management needed. As a lender on dYdX, you only need to be mindful of the earned Interest Rate (APR) -this represents how

much you will earn from lending out your assets.

Who pays the interest for my deposit?
The interest you earn is paid by other users who are borrowing the same asset. dYdX only allows for over-collateralized loans. This means that borrowers must always have enough collateral to pay back their loaned amount. If a borrower's collateralfalls below the 115% collateral ratio threshold (i.e < $115 of ETH for $100 DAI loan), their collateral is automatically sold until they fully cover their position.

Interest rates are dynamic and change over time based on supply and demand, ensuring that users will always earn market rates. Additionally, both the initial capital and interest earned can be deposited and withdrawn at any time.

Borrowing

You can use dYdX to borrow any of the supported assets (ETH, DAI and USDC) as long as a 1.25x initial / 1.15x minimum collateral ratio is maintained. Borrowed funds are deposited directly to your wallet and can be freely transferred, exchanged or traded.

As a borrower on dYdX, the two numbers you need to look out for are:

(i) Interest Rate (APR) -how much you pay to loan the money
(ii) Account collateralization ratio -This is the ratio of your asset/loan amount. You can borrow until this ratio is 125%, and you will be liquidated once it falls below 115%.

Margin & Leveraged Trading

In dYdX you can enter either short or long positions with leverages up to 5x. When margin trading on dYdX, funds are automatically borrowed from lenders on the platform.

Consider a scenario where you start with 300 DAI & 0 ETH in your dYdX account. If you are going to short ETH (assume ETH is now $150), you will:

1. Take a loan of 1 ETH ($150)
2. Sell loaned ETH for 150 DAI, balance in dYdX is now 450 DAI & -1 ETH
3. Assuming ETH price goes to $100, you can now rebuy 1 ETH for $100 to repay your debt.
4. Your final balance is 350 DAI—you profit 50 DAI ($50)

With dYdX, you don't need to actually own ETH to enter a short position. You can borrow it and enter a short position it all in one place.

Pro Tip:
Collateral used to secure margin trades continuously earns interest, meaning you don't have to worry about losing out on interest when waiting for an order to fill. This feature is unique to dYdX as far as we know as of the time of writing.

What is leverage?
Consider two different leveraged positions scenarios (numbers approximated) for a trader who has 10 ETH ($150 per ETH), or $1500. In the first scenario, the trader enters a **5x long position with 1 ETH ($150):**

1. The position size would be 5 ETH ($750)
2. 10% of the Portfolio is at risk (1/10 ETH used)
3. A price movement of ~10% ($15 on ETH) downwards will liquidate the trader's position, meaning there is very little buffer for price spikes.

On the other hand, if the trader enters a **2x long position with 1 ETH($150):**

1. The position size would be 2 ETH ($300)
2. 10% of the portfolio is at risk (1/10 ETH used)
3. A price movement of ~45% ($65 on ETH) downwards will liquidate the trader's position.

Essentially, leverage is really just a factor of how much risk a traderwants to take (in terms of exposure to price movements), which in turn determines a trader's distance to liquidation. High risk, high rewards!

Note:
Margin positions for trades made from the US are limited to 28 daysas of Feb 2020.

What is liquidation?
On dYdX, whenever a position falls below the collateral threshold of 115%, any existing borrows will be deemed as risky and in order to protect lenders, risky positions are liquidated. Collaterals backing the borrows will be sold until negative balances are 0, along with a liquidation fee of 5%.

How are Profits/losses calculated?
For example, you open a 5x long with a 3 ETH deposit with an open price of $220.

You'll need to borrow $220*12 = 2640 DAI to buy 12 additional ETH (Total of 15 ETH locked in your position)

If you close the position at 250, you'll need to pay back your loan of 2640 DAI with= 2640/250 ETH= 10.56 ETH

This will leave you with 15 -10.56 = 4.44 ETH. So your profit would be 4.44-3 = 1.44 ETH

Steps to calculate profit:

1. Determine initial leverage and deposit amount to get position size (Leverage*Deposit)
2. Loan Amount = (Position Size -Deposit) * Open Price
3. Loan topay back = Loan Amount/Closing Price
4. Balance = Position Size -Loan to Pay back
5. Profit = Balance -Initial Deposit

And that's it for dYdX.

DECENTRALIZED DERIVATIVES

A derivative is a contract whose value is derived from another underlying asset such as stocks, commodities, currencies, indexes, bonds, or interest rates. There are several types of derivatives such as futures, options, and swaps. Each type of derivative serves a different purpose and different investors buy or sell them for different reasons.

> ***Some of the reasons investors trade derivatives are: to hedge themself against the volatility of the underlying asset, speculate on the directional movement of theunderlying asset or leverage their holdings. Derivatives are extremely risky in nature and one must be equipped with strong financial knowledge and strategies when trading them.***

The Total Value Locked in DeFi derivatives Dapps is $114.3 million or 12% ofthe DeFi ecosystem. Though the figure is relatively low compared to other DeFi markets such as the lending market ($745.6 million), it is worth noting the decentralized derivative market has only been around for one year and it has grown significantly. Some of the major DeFi derivatives Protocols are Synthetix and bZx.

In this book, we will deep dive into Synthetix, the biggest DeFi derivative protocol.

Synthetix

SYNTHETIX

Synthetixis exactly as the name sounds, a protocol for Synthetic Assets (called Synths) on Ethereum. There are two parts to Synthetix -Synthetic Assets (Synths) and its exchange, **Synthetix. Exchange.** Synthetix allows for the issuance and trading of Synths.

What are Synthetic Assets (Synths)?

Synths are assets or a mixture of assets that have the same value or effect as another asset. Synths track the value of underlying assets and allow exposure to the assets without the need to hold the actual asset.

There are currently two different types of Synths -Normal Synths and Inverse Synths. Normal Synths are positively correlated with the underlying assets while Inverse Synths are negatively correlated to the underlying assets.

An example of a Synthetic Asset is Synthetic Gold (sXAU) which tracks the price performance of gold. Synthetix tracks real-world asset prices by utilizing the services of Chainlink, a smart contract oracle that obtains price feed from several trusted third party sources to prevent tampering.

An example of an Inverse Synthetic Asset is Inverse Bitcoin (iBTC) which tracks the inverse price performance of Bitcoin. There are 3 key values related to each Inverse Synths -the entry price, lower limit, and upper limit.

Let's consider Inverse Synthetic Bitcoin (iBTC) as an example. Assume that at the time of creation, Bitcoin (BTC) is priced at $10,600 -this will be the entry price. If Bitcoin moves down $400 to $10,200, the iBTC Synth will now be worth an additional $400 and will be priced at $11,000. The opposite will also be true. If Bitcoin moves up to $11,000, the iBTC Synth will now be worth $10,200.

Inverse Synths trade in a range with a 50% upper and lower limit from the entry price. This places a cap to the maximum profit or loss you can obtain on Inverse Synths. Once either of the limits is reached, the tokens' exchange rates are frozen and the positions liquidated. Once disabled and liquidated, these Inverse Synths can only be exchanged at Synthetix. Exchange at those fixed values. They arethen reset with different limits.

Why Synthetic Assets?

As mentioned above, Synths give traders price exposure to the asset without the need to actually hold the underlying asset. Compared to traditional gold brokerages, Synthetic Gold (sXAU) allows traders to participate in the market with much less hassle (no sign-ups, no traveling, no middleman etc.).Synths have another utility -they can be traded frictionlessly between one another, meaning Synthetic Gold can be switched for Synthetic

JPY, SyntheticSilver or Synthetic Bitcoin easily on Synthetix.Exchange. This also means that anyone with an Ethereum wallet now has open access to any real-world asset!

How are Synths Created?

The idea behind the creation of Synths is similar to the creation of DAI on Maker. You have to first stake ETH as collateral on Maker's smart contract before being allowed to create DAI based on the collateral posted.

For Synths, you first need to stake the Synthetix Network Token (SNX), which acts as the collateral backing the entire system. SNX is less liquid compared to ETH and its price is generally more volatile. To counter that, a large minimum initial collateral of 750% is needed on Synthetic compared to the minimum 150% initial collateral needed on Maker.

This means that to mint $100 worth of Synthetic USD (sUSD), you will need a minimum of $750 worth of SNX as collateral.

Note:
As of 27 November 2019, the only Synth that can be minted by users is sUSD.

Minting of Synths is a fairly intricate system. It entails the staker taking on debt, the levels of which are dynamically changed depending on the total value of Synths in the global debt pool, causing the debt owed by the staker to fluctuate with changing values. For example, if 100% of the Synths in the system were synthetic Ethereum (sETH), and the price doubles, everyone's debt would double including the staker's own debt as well.

Once minted, these Synths tokens can be traded on Synthetix Exchange or on Decentralized Exchanges like Uniswap.

If you want to trade Synths but don't want to take on Debt or mint your own Synths, you can actually buy it on the sETH Uniswap Pool. The sETH pool on Uniswap is currently the largest Pool on Uniswap with over 35,000 ETH (~$80mm @ $200 ETH) in liquidity).

What Assets do Synths Support?

At the point of writing, Synths support the following 4 major asset classes:

1. **Cryptocurrencies:** Ethereum (ETH), Bitcoin (BTC), Binance Coin (BNB), Tezos (XTZ), Maker (MKR), Tron (TRX), Litecoin (LTC), and Chainlink (LINK)
2. **Commodities:** Gold (XAU) and Silver (XAG)
3. **Fiat Currencies:** USD, AUD, CHF, JPY, EUR, and GBP
4. **Indexes:** CEX and DEFI

Index Synths

One of the interesting Synths available on Synthetix is the Index Synths. At the time of writing, there are 2 different Index Synths, namely sCEX and sDEFI.

Index Synths provide traders with exposure to a basket of tokens without the need to purchase all the tokens. The index will mirror the overall performance of the underlying tokens. Index Synths allow for exposure to particular segments of the industry as well as diversification of risks withoutthe need to actually hold and manage various tokens.

sCEX
sCEXis an Index Synth designed to give traders exposure to a basket of Centralized Exchange (CEX) tokens roughly approximating their weighted market capitalization. The current sCEX index consists of Binance Coin (BNB), Bitfinex's LEO Token (LEO), Huobi Token(HT), OKEx Token (OKB) and KuCoin Shares (KCS).

There is also the Inverse Synth called iCEX which is an inverse of the sCEX Index Synth and works like other Inverse Synths.

sDEFI
With the growing interest in DeFi, the sDEFI Index Synth was introduced to provide traders with an index exposure to a basket of DeFi utility tokens in the ecosystem. The current sDEFI index consists of the following tokens: Chainlink (LINK), Maker (MKR), 0x (ZRX), Synthetix Network Token (SNX), REN (REN), Loopring (LRC), Kyber Network (KNC), Bancor Network Token (BNT), and Melon (MLN).

The inverse of this Index Synth is called iDEFI.

Fun fact:
These Index Synths were created through a series of Twitter polls. The weight of each token was determined using the proportionate market capitalization of each token, before being amended as per community feedback.

Synthetix Exchange

Synthetix.Exchange is a decentralized exchange platform designed for the trading of SNX and Synths without orders books employed by most DEXs. That is, rather than a peer-to-peer system (Uniswap or dYdX) which relies on users to supply liquidity, Synthetix. Exchange allows users to trade directly against a contract that maintains constantly adequate liquidity, thus theoretically reducing risks of slippage or lack of liquidity.

Since users are purchasing a synthetic contract rather than trading the underlying asset, users are able to buy up to the total amountof collateral in the system without having any effect on the contract's price. For example, a $10,000,000 BTC buy/sell order would likely

result in considerable slippage in traditional exchanges, but not in Synthetix Exchange as users trade against the Synthetix contract directly.

The other thing to know about Synthetix is that over 2020 they'll be launching a range of new trading features, including such new assets as synthetic indices and equities, leveraged trading, binary options, synthetic futures, and triggered orders.

And that's it for Synthetix.

DECENTRALIZED FUND MANAGEMENT

Fund management is the process of overseeing your assets and managing its cash flow to generate a return on your investments. We have started seeing innovative DeFi teams like starting to build ways for users to better manage their funds in a decentralizedmanner.

> *In DeFi, fund management is conducted in a manner where it removes the investment manager and lets you choose the asset management strategy that best suits your financial need. The decentralized fund management also reduces the fees paid.*

The Dapp will have algorithms to conduct trades for you automatically instead of doing it yourself. To understand how fund management can work in the decentralized ledger, we will introduce you to Token Sets.

TokenSets

TokenSetsis a platform that allows crypto users to buy Strategy Enabled Tokens (SET). These tokens have automated asset management strategies that allow you to easily manage your cryptocurrency portfolio without the need to manually execute the trading strategy. With an automated trading strategy, you will not need to manually monitor the market 24/7, thus reducing missed opportunities and risks from emotional trading.

Each Set is an ERC20 token consisting of a basket of cryptocurrencies that automatically rebalances its holdings based on the strategy that you choose. In other words, SET essentially implements cryptocurrency trading strategies in the form of tokens.

What kinds of Sets are there?

There are two kinds of Sets: (i) Robo Sets and (ii) Social Trading Sets.

Robo Sets

Robo Sets are algorithmic trading strategies that buys and sells tokens based on predefined rules encoded in smart contracts. There are currently 4 main types of algorithmic strategies, namely:

1. **Buy and Hold:** This strategy realigns the portfolio to its target allocation to prevent overexposure to any one token and spreads the risk over other tokens.
2. **Trend Trading:** This strategy uses Technical Analysis indicators to shift from target asset to stablecoins based on the implemented strategy.
3. **Range-Bound:** This strategy automates buying and selling within a designated range and is only intended for bearish or neutral markets.
4. **Inverse:** This strategy is meant for those who wish to “short” a benchmark. Traders can purchase this when they think a benchmark is due for a correction.

Social Trading Sets

Social Trading Sets enable users to follow top trading strategies by some featured traders on TokenSets. By buying this Social Trading Set, you can copy the trades performed by these featured traders automatically. Social Trading Sets are also algorithmic-based, but instead of it being written by the TokenSets team such as those found in Robo Sets, they are written by prominent traders.

How are Sets helpful?

Sets essentially tokenize trading strategies. If you are keen to try out any of the selected trading strategies or follow professional traders’ footsteps, Set is likely the easiest way to go about it.

That being said, always do your due diligence. Just because a Set has been performing

well historically does not mean that it will continue to do so. The cryptocurrency market is highly volatile and the old saying of “past performance is not an indicator of future results” is especially truehere. Instead, research and compare the available strategies to see which one makes the most sense to you and then use TokenSets to get started in no time.

We will be going through one of the best performing Robo Set as an example—the ETH/BTC RSI Ratio Trading Set. In this case, the Robo Set follows the Trend Trading Strategy which uses the Relative Strength Index (RSI) technical indicator. This trading strategy saw the value increase of 102.33% versus 41.29% for holding BTC or 94.17% for holding ETH. Since Token Set is relatively new, there is only performance data for the past 3 months as of writing time.

That’s it for TokenSets.

DECENTRALIZED LOTTERY

Thus far, we have gone through various protocols for stablecoins, decentralized exchanges, swaps, and derivatives -all of them serious stuff. In this section we will introduce you to something light and fun -a decentralized, no-loss lottery.

> ***Earlier in February 2020, a user who had deposited only $10 won $1,648 in PoolTogether'sweekly Dai Prize Pool, a 1 in 69,738 chance of winning.***

The best part of PoolTogether's lottery is that participants are able to get a refund of the $10 deposit if he or she did not actually win. There is no loser in this game, but only opportunity cost involved. Read on to find out more.

PoolTogether

What is PoolTogether?

Pool Together is a decentralized no-loss lottery or decentralized prize savings application where users get to keep their initial deposit amount after the lottery prize is drawn. Instead of funding the prize money using the lottery tickets purchased, the prize money isfunded using the interest earned on Compound by the pooled user deposits. For each round of PoolTogether, all the user deposits will be sent to Compound to earn an interest and one lucky winner will be selected at random at the end of each interval to winthe entire interest prize money.

Participating in PoolTogether is fairly straightforward—simply "purchase" PoolTogether tickets using DAI or USDC. Each ticket represents 1 entry and the chance of winning increases proportionately with the number of tickets purchased. PoolTogether currently supports 2 different lotteries -a weekly DAI pool (launched December 2019) anda daily USDC pool (launched February 2020).

A portion of the money currently earning interest in PoolTogether is sponsored. Currently, this amounts to roughly $250,000 in the Dai pool and $200,000 in the USDC pool. This is provided by sponsors to increase the interest earned on Compound each week to make the prize pool larger. The sponsored tickets are not eligible to be a winner on PoolTogether.

This concept is not new and it is similar to Prize-Linked Savings Account (PLSA) where it incentivizes people to save more in their bank's savings account by providing sweepstakes for lucky winners. PLSA is a popular concept with banks and credit unions from many countries around the world offering such programs. One of the known PLSA programs is "Save to Win" by Michigan Credit Union League.

Why bother with Decentralized Lotteries?

One of the attractions of decentralized lotteries in the contextof PoolTogether is that funds do not go through middleman or brokers, but are instead held by smart contracts that have been audited. There is also no lock-up period on funds, meaning that they can bewithdrawn at any moment.

Traditionally, the jurisdiction and protection laws of the gambling industry have made real-world no-loss lottery, such as PLSA programs, restrictive to users from certain geographical areas to join. This is where Decentralized Applications truly shine as well—anyone from anywhere can participate if they have the funds to do so.

What's the Catch?

Surely there can't be free money? Spot on! There's a small catch -the opportunity cost of

putting your funds into PoolTogether. If you put your funds into Compound to supply liquidity, you will be able to earn interest from it but if you put it into PoolTogether, you will lose the interest that can be earned from Compound but instead now have the opportunity to win the lottery. Your "fee" to enter the lottery is effectively whatever interest you would have earned by lending it out on Compound.

So, Lendingon Compound vs. participating in PoolTogether?

Naturally, the next question we asked ourselves -would it be better to put our money in Compound or in PoolTogether? We geeked out on some numbers -check out the table below for a comparison:

Weekly PoolTogether (DAI)	
Currently in PoolTogether	
Total Amount	999,000.00
Where	
Eligible Tickets	749,000.00
Sponsored	250,000.00
Open tickets	-
Additional 1,000 Dai	
+ Additional Deposit (Dai)	1,000.00
Compound Supply APR^	8.81%
Weekly Interest Rate	0.17%
Weekly Interest Earned (Dai)	1.69
Updated Figure PoolTogether	
New Total Amount	1,000,000.00
where	
New Eligible Tickets	750,000.00
Sponsored	250,000.00
Open Tickets	-
Prize Pool	1,694.23
Analysis	
Chances of Winning Each Time	0.13%
Expected PT Interest in a week	2.26
Annualised Compound Return	88.10
Annualised PT Return	117.47
Annualised PT Expected Return Ratio	11.75%
ALPHA	1.33

Daily PoolTogether (USDC)	
Currently in PoolTogether	
Total Amount	299,000.00
Where	
Eligible Tickets	99,000.00
Sponsored	200,000.00
Open tickets	-
Additional 1,000 USDC	
+ Additional Deposit (USDC)	1,000.00
Compound Supply APR^	4.84%
Daily Interest Rate	0.01%
Weekly Interest Earned (Dai)	0.13
Updated Figure PoolTogether	
New Total Amount	300,000.00
where	
New Eligible Tickets	100,000.00
Sponsored	200,000.00
Open Tickets	-
Prize Pool	39.78
Analysis	
Chances of Winning Each Time	1.00%
Expected PT Interest in a Day	0.40
Annualised Compound Return	48.40
Annualised PT Return	145.20
Annualised PT Expected Return Ratio	14.52%
ALPHA	3.00

tl;dr —
at the time of writing PoolTogether seems likelier to have better returns than saving in Compound due to the presence of sponsored tickets that are not eligible to win. But then again, you may not want to compare lotteries with savings so do take our findings with a grain of salt!

To make better sense of these numbers, we will walk through them line by line. We will start off by assuming that we will be depositing $1,000 worth of either DAI or USDC. Note that the figures given here are just for the purpose of this explanation. For the latest figures, please head over to:https://www.pooltogether.com/#stats

First we will see what the supply APR for Compound is, which you can find here: https://compound.finance/markets. From this rate, we simply divide it by 52 (for weekly) or 365 (for daily) to get the new periodic rates. This would give us the daily and weekly interest earned.

Daily Interest Earned = Compound Supply APR/365
Weekly Interest Earned = Compound Supply APR/52

Now, since we have the Compound interest amount (which is guaranteed), let's see how much we can expect to win from Pool Together. Let's say the DAI pool has 1,000,000 total tickets while the USDC pool has 300,000 total tickets.

As mentioned earlier, both sponsored and open ticketsWILL NOT win the lottery. However, they will both contribute to the interest earned for that period, making the prize pool much larger and attracting more people. We then calculate this prize pool amount by simply multiplying the total number of tickets by the weekly/daily interest rate that we calculated earlier.

USDC Prize Pool Amount = Total Ticket * Daily Interest Rate
DAI Prize Pool Amount = Total Ticket * Weekly Interest Rate

The chance of winning is proportional -the more tickets you buy, the higher the chance of winning. Multiply this with the new interest amount and you'll have Expected Returns for that time frame. Annualize this number and you can compare it to the earlier number from lending it directly to Compound.

$$\textbf{Expected Returns} = \frac{\textbf{number of tickets owned}}{\textbf{number of eligible tickets}} * \textbf{Prize Pool}$$

Annualized Pool Together Returns = Expected Returns * Number of Periods (52 or 365)

If this expectedreturn is more than good enough for you, do look into getting into it. The Alpha (Expected PoolTogether Returns over Compound lending returns) will decrease as more tickets come into play due to opportunity cost. While the numbers do seem to suggest that it's a good idea to consider PoolTogether, due note that you may be unlucky and not win a single lottery at all throughout a year.

In terms of security and funding, PoolTogether was funded by Makerand has gone through several security auditsto review their codes. PoolTogether also had a fundraising round which enabled them to increase the sponsored pool, and no longer takes fees from the winnings as initially planned, which means more money for the winner!

DECENTRALIZED PAYMENTS

While decentralized payments can already be done by sending ETH or DAI directly, it can still be made better—think cheaper & faster transactions, timed transfers, transfer by conditions as well as standardized invoicing formats and more.

> ***Some of the more well-known projects working on decentralized payments are Lighting Network, Request Network, xDai and Sablier.***

In this chapter, we will be exploring Sablier—a project which we find interesting and has the potential to solve some of the outstanding issues for people who are vulnerable in society.

Sablier

What is Sablier?

Sablier is a payment streaming application—meaning that it allows payment and withdrawals to be made in real time and in small increments (by the second!) between different parties. Think about payments for hourly consultation work, daily contract workers or monthly rent payment made in real time as work/progress is being made. Just like you can stream music on Spotify, so you can stream money on Sablier!

What Does Streaming Payment Mean?

Instead of having to wait for a fixed period of time (eg. monthly, bi-weekly) for pay, payments are sent in real time in periods defined and agreed upon by both parties. Through Sablier, payees can now receive their pay in real time and withdraw it whenever they want to.

Why is this important?

We think that Sablier has the potential to help those who live paycheckto paycheck. These people are those most vulnerable to delays in their income, where even a few days of delay would mean that they do not have the means to put food on the table.And when that happens, they often resort to payday loans—a short term, uncollateralized loans with very high interest rates (up to 500% APR). With astronomical interest rates and limited income, payday loan lenders are especially susceptible to debt spirals—one that has seen many arrested in the US for being unable to repay their loan.

Trust
Streamed payment can be especially useful for new, remote contract workers who prior to this had to trust their new employers to actually pay them for the work they do. When a contract is signed through Sablier, both parties know for sure that payments arebeing made and can verify it in real time.

Timing
Traditionally salary payments are made on a monthly or bi-weekly basis but there may be instances where funds are required immediately—and payment streaming can help with this. A salaried employee does not have to wait till payday to access his remuneration—he can withdraw as much as he has earned till date, which may resolve immediate concerns. Furthermore, this is also helpful to avoid delays. Even if a worker fully trusts their employer, streaming paychecks guarantees that the payout will be made in full at the end of the period!

Example of how it works

Imagine you provide online consultancy services for a fee of $60 per hour ($1 per minute), to begin with you'll likely have to think about whether to:

1. Collect payment upfront, however this may be off-putting to some new clients OR
2. Collect payment later, meaning you'll have to trust your client to pay you OR
3. Use an escrow service/platform to protect both sides for a commission.

With the advent of payment streaming however, you'll no longer need to trust either party to be honest. You can be paid on a minutely basis to ensure that you and your clients both get their money's worth, and that if they do try to run away from paying, you'll lose only 1 minute of your time. Essentially, the "trust" part of an online transaction has been shifted from a person to lines of immutable codes (the blockchain & smart contract).

It's already being used—this is exactly what Reuben, a cryptocurrency and blockchain consultant,did to charge his client for 30 minutes consultation.

And that's it for Sablier

DECENTRALIZED INSURANCE

To participate in DeFi, one has to lock tokens in smart contracts. Tokens locked in smart contracts are potentially vulnerable to smart contract exploits due to the large potential payout. While most projects have gotten their codebases audited, one will never know if the smart contracts are truly safe and there is always a possibility of a hack which may result in a loss.

> *There have been two high-profile DeFi exploits that took place recently involving a DeFi Dapp called bZx. Both exploits happened on the 15th and 18th February 2020 amounting to a total loss of 3,649 ETH or roughly $1 million. The first exploit resulted in a loss of 1,271 ETH and the second exploit resulted in a loss of 2,378 ETH. Both exploits are highly complex transactions that involve multiple DeFi Dapps.*

The potential for such massive losses highlights the risks inherent in DeFi and it is something which many people are not paying close attention to. Here are some of the risks that are faced by DeFi users:

1. **Technical Risks:** where smart contracts could be hacked or bugs could be exploited;
2. **Liquidity Risks:** where protocols like Compound could run out of liquidity;
3. **Admin Key Risks:** where the master private key for the protocol could be compromised.

The risks highlight the need for purchasing insurance if one is dealing with large amounts on DeFi. In this section, we will be covering 2 major providers of decentralized insurance to help you protect your DeFi transactions, namely **Nexus Mutual** and **Opyn**.

Nexus Mutual

What is Nexus Mutual?

Nexus Mutual is a decentralized insurance protocol built on Ethereum that currently offers cover on any smart contract on the Ethereum blockchain. Here's a list of some of the DeFi smart contracts that can be covered by Nexus Mutual:

Nexus Mutual Supported DeFi Smart Contracts (Feb 2020)			
No.	DeFi Smart Contract	No.	DeFi Smart Contract
1	MakerDAO	10	Set Protocol
2	Moloch DAO	11	Fulcrum
3	Nuo	12	Aave
4	Gnosis	13	Compound
5	0x	14	Edgeware
6	Tornado Cash	15	IDEX
7	Uniswap	16	Instadapp
8	Argent	17	DDEX
9	dYdX	18	Pool Together

What event is covered by Nexus Mutual?

Currently, Nexus Mutual offers coverage against smart contract failures, which protects against potential bugs in smart contract code. The coverage may result in protection against financial losses that may be incurred due to hacks or exploits in the smartcontract code. Note that smart contract cover only protects against "unintended uses" of smart contracts, so security events such as the loss of private keys or centralized exchange hacks are not covered.

How does coverage work?

To get started you will first need to choose the Cover Period and the Cover Amount. The Cover Amount is the amount that you would like to purchase cover for and will be the amount that will be paid out in case there are smart contract failures. Upon a smart contract failure incident, a Claims Assessment process will take place that will be evaluated by Claims Assessors. Once it has been approved, the Cover Amount will be paid to you.

How is the coverage priced?

While all smart contracts can be covered by Nexus Mutual, the price of Smart Contract Cover is based on several criteria such as:

1. The characteristics of the smart contract that requires coverage. Examples include

value held in contract, transactions processed etc.
2. Cover Amount
3. Cover Period
4. Value staked by Risk Assessors against the smart contract

A smart contract that does not have sufficient value staked against it or has not been battle-tested enough will return a quote which is un-coverable, meaning that the smart contract cannot be covered at the time.

For example, let's say you buy 5 ETH worth of cover for the Compound smart contract when ETH is $200. Assuming the coverage is 0.013 ETH per 1 ETH of coverage for a year, this would cost you a total of 0.065ETH for a year of coverage. If Compound gets hacked during this period of time, you will be able to get back 5 ETH regardless of the price of ETH during the time of hack. If ETH has risen to $300 during the hack, you would still receive back 5 ETH as long as your claim is approved.

Note that anyone can buy cover on any smart contract and submit a claim once there is an unintended use of the smart contract. You do not need proof that you had funds invested in the smart contract and suffered a loss.

How to Purchase Cover?

1. Specify which smart contract address you want Cover for.
2. Specify the Cover Amount, currency (ETH or DAI) and Cover Period.
3. Generate a quote and make the transaction using Metamask.
4. You are now covered!

NXM Token

Nexus Mutual has its own native token known as NXM. The NXM token is used to buy cover, participate in Risk Assessment and Claims Assessment. It is also used to encourage capital provision and represents ownership to the mutual's capital. As the mutual's capital pool increases, the value of NXM will increase as well.

Through the platform, users can do two things -purchase cover for their capital or become a Risk Assessor by staking NXM.

It uses a token bonding curve which is affected by both the amount of capital the mutual has and the amount of capital it needs to meet all claims with a certain probability.

Currently the NXM token is not traded on any exchange and is only used as an internal token for Nexus Mutual.

What is a Risk Assessor?

A Risk Assessor is someone who stakes value against smart contracts (essentially vouching that the smart contract is safe) and is incentivized to do so by earning rewards in NXM, as users take cover on their staked smart contracts. A Risk Assessor would besomeone who understands the risks in solidity smart contracts and either:

(1) assesses individual Dapps themselves, or
(2) trusts someone who says the contract is secure (like an auditor or other staker)

Has NXM ever paid out claims before?

Yes! In thecase of the recent bZx flash loan event, there were 6 members who had cover on the smart contract for a total cover of roughly $87,000. As of the time of writing, three claims have been accepted so far, receiving their payouts immediately after the Risk Assessors voted to approve their claims.

Opyn

What is Opyn?

Opyn is another DeFi app that provides insurance for smart contracts. Currently, Opyn has protection for USDC and DAI deposits on Compound and stablecoin deposits on another DeFi dapp, Curve.

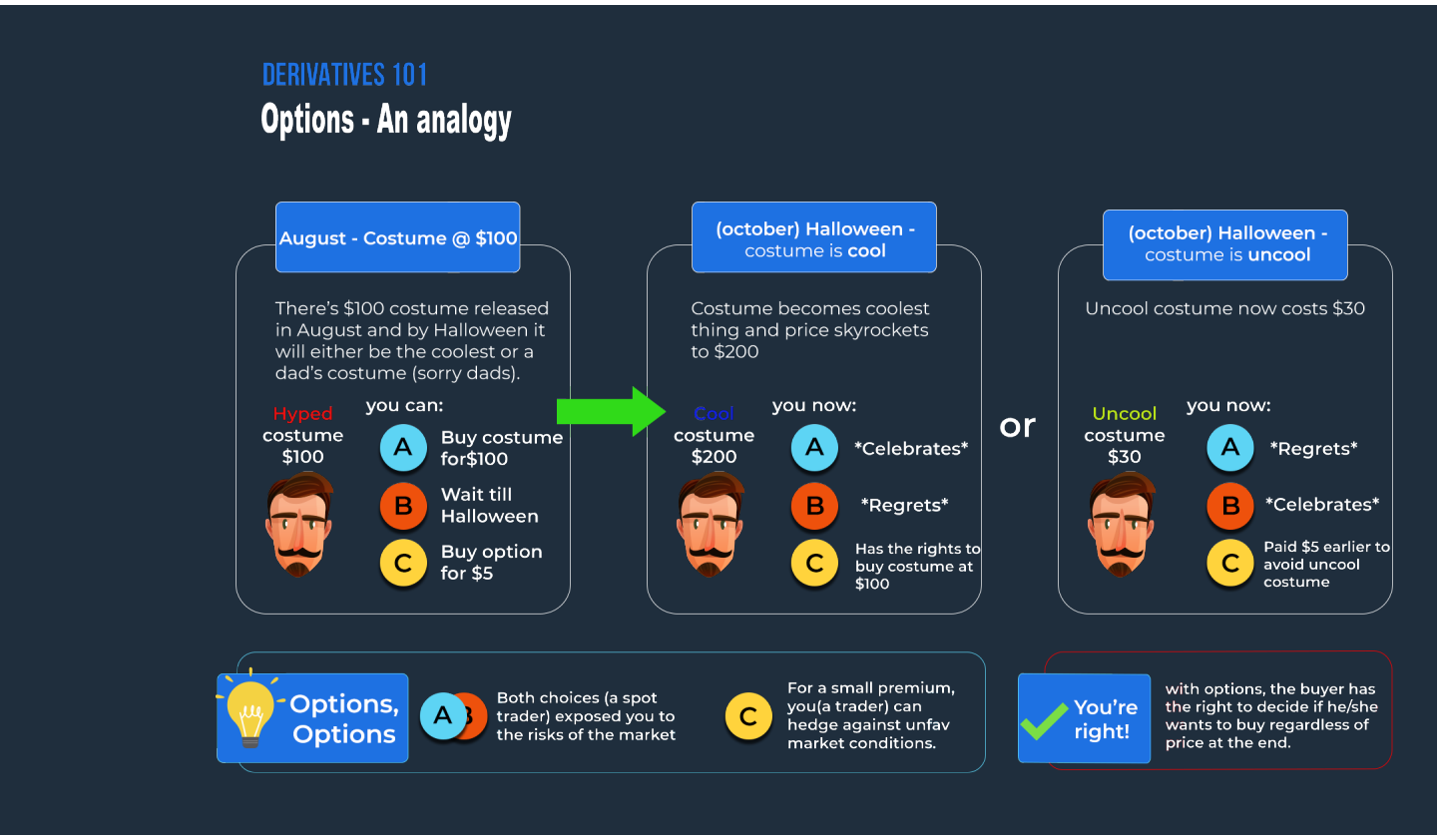
Opyn provides protection against a number of risks beyond smart contract failures such as financial risks and admin risks. Opyn does this by making use of financial derivatives, namely options.

Whatare Options?

There are two kinds of options, Call option and Put option. A Call option is a right, but not the obligation to purchase an asset at a specific strike price within a specific period of time. A Put option on the other hand is a right, but not the obligation to sell an asset at a specific strike price within a specific period of time.

For every purchaser of an option, there must be a seller of an option. A purchaser of an option will pay a premium to the seller of the option to get this right.

Here is a Halloween analogy of a Call option to better help your understanding of options:



There are two main options flavors, namely American and European options. The difference between the two is that for an American option, the buyer can exercise the option anytime before the expiry date whereas for an European option, the buyer can only exercise it only on the strike date.

How does Opyn work?

Opynallows users to hedge against the risk of a black swan event happening on Compound by allowing users to buy Put options on USDC and DAI stablecoin deposits.

As mentioned earlier in the Compound section, when someone loans DAI, they would get cDAI tokensin return. By using Opyn, a trader can buy oTokens which can be used as a right to sell cDAI and get back DAI in case there is a smart contract failure on Compound.

Purchasing 1 DAI worth of insurance on Opyn is essentially buying an American Put optionfor the cDAI asset with a strike price of $0.92. In the event that Compound fails, any DAI deposits on Compound will no longer be worth $1.00 but significantly less, say for example $0.10. With Opyn's ocDAI token, the insurance purchaser is able to redeem$0.92 back, payable in ETH. This protects the user against smart contract losses. No centralized entity is needed to verify the claim making this a truly decentralized insurance.

Important note:
Opyn covers only your principal deposit and not any interest that you may have accrued on Compound. When you deposit your DAI on Compound you get cDAI in return. To make a claim on Opyn, you send your cDAI and oDAI insurance tokens to Opyn and immediately receive your coverage amount.

How much does Insurance cost?

As of the time of writing, buying insurance on Compound using Opyn costs roughly the following Annual Percentage Rate: 1.22% on Dai deposits and 2.61% on USDC deposits. This means that if you are earning 5.41% uninsured yield on Dai deposits, after purchasing insurance on Opyn, you are guaranteed a 4.19% yield.

Do note that Opyn is still relatively new, having just launched in February 2020 and the cost of insurance may fluctuate as the market finds an optimal equilibrium.

Because the insurance is tokenized in the form of oTokens, they can be traded on DEXs like Uniswap which is why the price of the insurance would be dependent on the market price that is determined based on the supply and demand.

Why would anyone provide insurance on Opyn?

For every purchaser of insurance (purchaser of Put option) on Opyn, there must be a provider of insurance (seller of Put option) on Opyn. By being an insurance provider on Opyn, an ETH holder can earn a yield on their ETH.

To do so, one starts by supplying ETH as collateral to Opyn's smart contract at a minimum collateralization ratio of 160% to mint oTokens. Insurance providers can mint oTokens for either USDC or DAI on Compound.

Once oTokens have been minted, there are two exciting ways to earn premium:

1. **Being a Liquidity Provider on Uniswap**
   As a Liquidity Provider on Uniswap, one can earn transaction fees from individuals buying and selling on the Opyn platform through Uniswap. Liquidity Providers have the opportunity to make a large but variable return from providing liquidity on Uniswap. Liquidity Providers are allowed to remove funds at any time. Our section on Uniswap shows you the steps to provide liquidity on Uniswap.

2. **Selling oTokens on Uniswap**
   The oTokens that have been minted can be sold on Uniswap. To calculate the Annual Percentage Rate for selling oTokens on Uniswap, you can look at Opyn's main dashboard and calculate the difference between the uninsured yield and insured yield since this is what a user would give up to get insured. As of the time of writing, the Annual

Percentage Rate that can be obtained is 1.22% on DAI and 2.61% on USDC.

The premiums that can be earned on the ETH collateral is higher than anywhere else in DeFi. However, earning this yield does not come without risk. By selling the Put option for a yield, the option seller assumes the risk that there will not be a disaster event (e.g. technical risk like a hack, financial risk like DAI breaking its peg or a run on Compound). One must also maintain a collateral ratio above 160% so as not to be liquidated.

Is Opyn safe?

Opyn has a publicly verifiable smart contract and its smart contract has been audited by OpenZeppelin, a smart contract auditing firm. The full report is available here: https://blog.openzeppelin.com/opyn-contracts-audit/.

Opyn is also noncustodial and trustless, with a reliance on incentives for it to work.

	Nexus Mutual	Opyn
Covers Against	Smart Contract Hacks	Technical, financial, admin key risks
Claims Approval	Yes –Voting	No –immediate withdrawal upon claim
Coverage	Any Smart Contract on mainnet(Wider coverage)	Compound and Curve(Limited coverage)
Liquidity	Coverage Pools	Two-Sided Market
Fully Collateralized	No	Yes
Common Capital Pool	Yes	No
Pricing	Nexus pricing algorithm & Risk Assessors	Depends on the supply and demand of the market, mainly via Uniswap

Conclusion

One thing to note is that because the pricing of oTokens is determined by demand and supply, one can use this as a signaling mechanism to check if there is something wrong with Compound. If people believe that a black swan event is going to happen on Compound, they would start purchasing more oTokens and the oTokens would increase in price.

At the end of the day, the choice to insure or not to insure is ultimately up to you, the user. However, we at Finstreet definitely recommend purchasing insurance as we never know what could happen especially in the still nascent DeFi markets.

FIN.STREET

WWW.FINSTREET.IN

8968232722

@bandhulbansal

@finstreet.in

/bandhul-bansal
-09b0a14

Our Platform Sponsor

wazirx

Our Merchandise Sponsor

QuadB™