

THE WALL STREET ERA

IS OVER



**THE INVESTOR'S GUIDE TO CRYPTOCURRENCY AND
DEFI, THE DECENTRALIZED FINANCE REVOLUTION**



WRITTEN BY THE INDUSTRY EXPERTS AT [DEFIYIELD.APP](https://defiyield.app)

THE WALL STREET ERA IS OVER

THE INVESTOR'S GUIDE TO
CRYPTOCURRENCY AND DEFI,
THE DECENTRALIZED FINANCE
REVOLUTION

Written by the industry experts at **DeFiYield.App**

Copyright © 2021 DEFIYIELD

1st edition May 2021

www.defiyield.app

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any forms or by any means, electronic, mechanical, photocopying, recording or otherwise, except brief extracts for the purpose of review without the prior permission in writing of the publisher and copyright owners. It is also advisable to consult the publisher in any doubts as to legality of any copying which is to be undertaken.

PREFACE

On December 1st 2020, I lost \$1,200,000.

This amount was just some of the \$12,000,000 total that was lost in one of the biggest scams to hit the Yield Farming industry.

Since then, I have worked tirelessly to track down the scammer(s). I've employed the help of a blockchain investigation agency, built a community of over 600 victims, and filed claims in major finance jurisdictions around the world, including New York and London.

So why, you might ask, am I writing a book that encourages you to take part in an industry where a scammer can run off with other people's money?

The answer is simple. My losses only tell one small part of the story.

That's because Yield Farming is one of the most exciting trends to appear in the world of Decentralized Finance, or DeFi, which itself is revolutionising the entire global financial system.

It is an amazing industry, one that is made up of a community-driven ecosystem that has rewarded early adopters like Synthetix Spartan and YFI liquidity providers with 100x returns. It is an opportunity that is open to everyone and one that, I am sure, you can benefit from, if you go about it in the right way.

After all, DeFi is the place where you can make 100x or you can lose your life savings.

While the loss I suffered looks significant to many, there is every likelihood the scammer will be caught because of clues he/they left behind and resources I have put towards finding him/them.

Furthermore, these losses pale into insignificance when compared to the wealth I have created through Yield Farming. The opportunity to create that wealth for yourself is far from over.

While Yield Farming has grown exponentially in recent months, it is still a small niche within the wider world of cryptocurrencies. For anyone that

feels to have missed out on the rise of Bitcoin or other established digital assets, Yield Farming is without doubt the place to be.

When I started my journey in crypto in 2013, I was trading Bitcoin on the handful of exchanges where it was possible to do so. As the industry grew, I took the opportunity to dive into Initial Coin Offerings (ICOs) from 2015 onwards. When I did, I often FOMOed into them without doing the necessary due diligence. Unsurprisingly, this resulted in my first experiences of scams.

This is something I've had to get used to over the years but I wish I'd been able to access the knowledge and guidance of experienced investors back then so I could have avoided many obvious pitfalls.

This book is my chance to help others do exactly that.

Even though I began Yield Farming having amassed years of crypto experience, I found it confusing. There is a lack of clear and structured information about the industry. It is not regulated by any authority and is akin to the Wild West in terms of a secure investment. Furthermore, its exponential growth turned anonymous developers into crypto hedge fund managers almost overnight. While they were happy to take and hold investors' funds, some feel no responsibility to do what's right.

Scams are frequent. Events that may mean nothing to you right now - such as arbitrage attacks, rug pulls, infinite minting, minting exploits, pulled liquidity and owner tampering - happen regularly and can result in Yield farmers losing millions.

I want Yield Farming to be safe for everyone.

This is why I have translated complex concepts of Yield Farming into simple and clear explanations that anyone can follow. This book empowers you to skip months of painful experience with scams and fake projects, by helping you to learn what to pay attention to when assessing different ones. The stories inside provide my personal insights about various real-world cases, collating all the information you need in one place.

Mark Cuban, a billionaire entrepreneur who is famous for building and investing in internet companies before many believed the technology would transform the world, says this of DeFi:

“DeFi is really straightforward if you try it and you understand the principles behind it.” [1]

I totally agree with this statement. To understand DeFi and to benefit from Yield Farming, you need to try it for yourself. This book will help you to understand the principles behind it, while the tools and resources we make available through DeFiYield.App will help you step into this industry with confidence.

This book aims to lower the barriers of entry to the industry, so more people can engage in DeFiYield Farming. It can help everyone from absolute beginners to adept farmers. If you want to understand the industry, to succeed at Yield Farming and to remain safe while you do, this is the book for you.

INTRODUCTION

Who is The Wall Street Era is Over for?

This book has been written for anyone who wants to take advantage of the enormous opportunity that DeFi provides but is wary of the financial risks that come with it. As we delve deeper, in the book's second half we will thoroughly explore the DeFi's yield farming sector (also known as liquidity mining).

You might be a complete novice who has never bought any cryptocurrencies before. Or you may be a fledgling yield farmer who wants to learn from an established player who has seen it all. Perhaps you're somewhere in between.

Wherever you're starting from, this book has been written to give you all the background knowledge and basic principles you need to understand DeFi. From there, we will provide you with the necessary tools to start yield farming as soon as possible.

One thing you will require is some basic understanding of financial fundamentals and an existing interest in cryptocurrencies. It's OK if your knowledge in these areas is not very advanced, however. The very fact that you want to understand DeFi more fully is a sure sign that this book is for you.

How The Wall Street Era is Over will help you

The aim of this book is to bring clarity and confidence to anyone who wants to enter the DeFi industry. By reading it, you will significantly reduce the risk you are exposed to in this innovative new industry. This is particularly true if you want to progress to yield farming.

As I explained, I have been scammed in this industry—and also earned an even greater amount from it. I want to share my stories, experiences, and the lessons I've learned along the way, so you can be successful in DeFi yourself.

I'll walk you through the history of DeFi, the forces at play within the market, the participants who are involved, and the metrics you need to track. Then I'll introduce you to the primary DeFi projects that you should start with for yield farming.

Most importantly, I'll explain how my colleagues and I at DeFiYield have used our smart contract auditing experience to select the safest projects, and to warn yield farmers away from scams. In the process, I'll also reveal some exclusive information about the investigation into the scam I mentioned. This information has never been made public before—it will reveal how the scammer will be caught.

Finally, we'll look beyond the here and now. We will identify the most important trends to keep an eye out for, so you're empowered to continue your DeFi journey long into the future.

The crypto backstory

If the whole world of crypto is relatively new to you, it's important to understand some of DeFi's main narratives before you dive in.

Let's begin with a short description of where DeFi fits into the wider crypto environment industry. Then we'll work through the details of what this means:

“DeFi occurs on smart contract platforms. Smart contracts use programmable money to exchange value between entities in a trustless manner. This process can trace its evolution back to the original cryptocurrency, Bitcoin.”

This statement may not make complete sense to you if you are new to crypto, but it contains important basic concepts. Some of these concepts are firmly established, while others continue to be the subject of intense debate. All of them should be more clear by the end of this introduction, and provide you with a foundation that allows you to really dig into DeFi.

Of course, if you want to learn more about these key topics, we encourage you to continue on with your own research. The world of cryptocurrency and DeFi moves very fast! While we believe DeFi fundamentals will remain consistent, you can expect new innovations to build on each other and constantly reshape the game.

Bitcoin is Digital Gold

Even though Bitcoin was introduced to the world as “as a peer-to-peer electronic cash system”, most people now think of it as more akin to “digital gold.” Why is that?

There are many reasons, but probably the most important is the fact that it has a digitally provable limited supply. This makes it a good store of value over the long-term—the same way that many people view investing in precious metals such as gold and silver.

The Bitcoin codebase is open source and can be checked and verified by anyone. While they take some experience to understand, “block explorers”

are online tools that provide this very public view of blockchains (such as this one at <https://www.blockchain.com/explorer>).

Bitcoin's code states that there will only ever be 21 million bitcoins in the total circulating supply (Bitcoin trades as BTC on crypto exchanges). Another element of the supply is the number of bitcoins that will be mined, which essentially means the rate at which new bitcoins are added to the total circulating supply of the currency. This is also established in the code and is reduced every four years.

It's important to contrast the fixed supply of bitcoin with the considerably more fluid supply of a regular fiat currency. Let's look at the US dollar as an example: The total number of dollars in circulation has increased massively in recent years and will likely do so into the future as well. This is possible simply because the US Federal Reserve can choose to print more money at will, without any technical constraints or limits on its ability to do so.

The starkly different supply dynamics of Bitcoin and the US dollar is one reason people think of Bitcoin as more like gold than like a central bank fiat currency. Bitcoin's finite supply, and the fixed rate at which new assets are produced, gives Bitcoin and gold some key similarities. Like Bitcoin, gold is limited in supply and can only be mined (from the Earth) at a fairly consistent rate.

These characteristics have resulted in gold being classified as a Store of Value for centuries, if not millennia. The term "store of value" refers to assets, commodities, or currencies that can be saved, retrieved, and exchanged with the expectation that they will maintain their value into the future. (Contrast this with avocados, for example, which are tasty and desirable but have a short shelf life before they spoil).

Many people now view Bitcoin as a Store of Value and therefore refer to it as digital gold. When you consider that Bitcoin's market cap is just 5-10% of gold's market cap at the time of this writing, you can see why these same people also believe there is still plenty of room for the cryptocurrency's price to grow.

Financial Asset Market Cap

As of 11 April 2021

#	Name	Market Capitalization (\$ millions)
1	 Financial Assets	\$266,917,000
2	 Cash	\$39,000,000
3	 Gold	\$11,938,404
4	 Bitcoin	\$1,124,145



They both represent a Store of Value, but Bitcoin has several advantages over gold. These include:

- Bitcoin can be transferred over the Internet, whereas gold requires trucks, planes, and armored personnel to move it securely.
- Gold is very expensive to move and store, while transferring and storing Bitcoin is much cheaper.
- Verifying gold's authenticity prior to purchase requires handling, weighing, and testing it (or paying someone else to do this for you). Bitcoin's authenticity can be verified simply by checking the globally available ledger—the blockchain—to confirm your seller's crypto ownership claims.

Cryptocurrencies are programmable money

The Bitcoin narrative is an extremely powerful one in the crypto community. It has an amazing origin story, springing into the world from a [2008 white paper](#) written by the pseudonymous software developer Satoshi Nakamoto. Officially launched in 2009, Bitcoin was the first-ever cryptocurrency, in that it relied on cryptography to control money's creation and transfer in a secure way.

Bitcoin is an incredible achievement in so many ways. As open source software, it was envisioned by Satoshi as “A Peer-to-Peer Electronic Cash System.” Bitcoin represents the first practical application of blockchain, which was brilliantly combined with cryptography to unlock completely unprecedented powers.

Despite its many breakthroughs, it’s also fair to say that there are limitations to Bitcoin. The Bitcoin community has chosen to keep this monetary network as secure as possible. However, it is clear now that this security has come at the expense of other key considerations, including scalability and extendability .

Bitcoin is programmable money. It is code, with a set of rules embedded within it — such as the 21 million cap on how many bitcoins can be minted. All of this code comes together into a monetary system existing purely on a computer a network. Working together 24/7, this global computer network reaches consensus (or agreement) on a shared ledger of transactions—this is the Bitcoin blockchain in action.

However, even in the early days, many developers saw the potential for expanding the foundational technologies at the heart of Bitcoin. They saw how blockchain, digital assets, and consensus could be harnessed to do much more than just transfer value in the form of bitcoins.

This is where the second-most valuable cryptocurrency by market cap, Ethereum (trading as ETH), [began in 2015](#). Its co-founder Vitalik Buterin and other early Bitcoin advocates admired what Bitcoin had achieved and wanted to develop something different. With Ethereum, the vision was a cryptocurrency that could be more than just a payment system or a Store of Value. With Ethereum, Buterin and his colleagues saw the opportunity to create a crypto that could execute “smart contracts,” and therefore empower the creation of decentralized applications.

Now, Ethereum has over a million developers working on it and the vast majority of the DeFi ecosystem is built on it. NFTs, or non-fungible tokens, which certify the uniqueness of digital art, music, and much more are also built on the Ethereum blockchain.

This evolutionary process, which involves blockchain developers taking what has come before and using it to start a new project, is constantly unfolding. It works because most decentralized technologies are open source and available for anyone to see and build on. As a result, we now

have many different blockchain networks with their own cryptocurrencies, each with their own objectives.

There are wildly different variations in the quality of cryptocurrency projects, but one common principle they share is a basis in programmable money. This means they do not use the physical money we have been accustomed to for centuries (fiat currency such as coins and bills, or their digital equivalents). Instead, they can be programmed to have specific characteristics such as supply limits, transaction recording, and transfer protocols chosen by their developers and written into the codebase.

Smart contracts enable Trustless relationships

One of the main differences between Bitcoin and Ethereum, apart from monetary characteristics such as the supply of coins, is that Ethereum is far more extendable than Bitcoin.

With its extendable qualities, Ethereum moves well beyond simply being a Store of Value asset like Bitcoin. It also represents a platform for a whole new digital economy. Ethereum allows developers to build smart contracts that:

- interact with the network, and
- automate interactions between different parties
- in a trustless way.

A smart contract is simply code that lays out what will happen if certain criteria are met. The relationships they enable almost always involve the transfer of value, in the form of digital assets. These relationships and transfers play out based purely on what is programmed in the code.

This is what is meant by a trustless relationship. These occur when two entities—which could be two individuals but might just as well be two smart contracts—exchange value via a smart contract.

They do not exchange this value on the basis of the established social norm: trusting the person or organization on the other side of the transaction. Instead, the value exchange is governed solely by the smart contract code.

This may sound a little theoretical, but it's a fundamental function of DeFi. At their best, smart contracts remove personal judgment from the process, which eliminates human error. That's why smart contracts can run in an extremely efficient, frictionless manner. This is already vastly

reducing the cost and complexity of many industries—from decentralized finance to insurance to digital art.

Many DeFi concepts have proven to be vastly profitable. DeFi provides the best example of how smart contracts successfully interact. They form a dynamic marketplace that is growing every day.

DeFi is Finance 3.0

At DeFiYield, we see DeFi as Finance 3.0. It combines the elements of:

- programmable money,
- smart contracts, and
- trustless relationships.

Together, they have formed a new, open financial system that will replace traditional finance. Here's how we got to this point.

Finance 1.0 can be thought of as the world of gold and central banks, which most people see as the foundation of today's traditional financial system. For roughly 400 years from the mid-17th Century, we used money, in the form of coins and bills, that was backed by gold and issued by nation states. In the 20th century, the link between the coins and bills we use and the gold that backed them disappeared. In the United States, for example the U.S. dollar ceased to be connected to gold in 1971, the end of the "[gold standard](#)."

Next was **Finance 2.0**, which has evolved with the Internet and has enabled the digitization of money. Now, fintech applications like Stripe, Revolut, Robinhood and eToro leverage the Internet. They have added an additional communications layer to Finance 1.0.

This was a huge step forward, but there is a limit to how much more Finance 2.0 can expand. It's a sector primarily focused on allowing users to manage their money more easily with mobile apps. However, Finance 2.0 remains fundamentally centralized around nation states, commercial banks, and established institutions. Its outdated payment rails move assets and wealth with inefficient systems.

Finance 3.0 is totally different. It uses programmable money, not fiat currencies issued by a state. It uses open decentralized networks, not closed payment rails. It does not need commercial banks to operate as gatekeepers, because anyone can be their own bank.

Crucially, Finance 3.0 is permissionless and peer-to-peer. This means that anyone, anywhere can take part, regardless of their race, religion, gender, ethnicity, or country of birth. It is a truly egalitarian system that opens finance up to the whole world, not just a few big economies.

In Finance 3.0:

- there are no middlemen acting as central points of control
- You do not need to deposit your assets in a bank,
- It is a noncustodial system where you can be your own bank.

This also means that you own all your data. You do not need to hand it over to large, centralized institutions in order to gain access to the system. Finally, it is permissionless and uninterrupted, so you can transact at any time with who you want. Regulatory changes in DeFi are always a possibility, however—we will update the book as often as possible.

This is Finance 3.0. It's a revolution. It's DeFi.

The DeFiYield story

DeFiYield is your entry point into DeFi. We offer everything you need to access the wide world of DeFi. It's a place to participate in Yield Farming as safely as possible.

We also offer many community tools, supporting DeFi experts and newcomers alike. We provide how-to DeFi guides, and the largest Telegram group for advanced yield farmers. We'd love to hear from you! to Stay up to date with the latest Finance 3.0 tools, news, and insights by visiting us at <https://DeFiYield.App/>

Highlights of the intro

In case you are getting overwhelmed with all the info presented above, let's have a fast recap. You can find highlights at the end of each chapter, helping you to summarize your reading experience.

Bitcoin

Bitcoin is programmable money with limited supply

It performs all the classic functions of money: store of value, means of exchange, unit of account).

Bitcoin is now considered "digital gold".

Similarly to gold, the only way to bring new bitcoins into circulation is by mining them.

Bitcoin's circulating supply cannot be controlled by any centralized body.

Currently, Bitcoin's market cap is over 90% smaller than gold's - yet it has many advantages over gold:

- Users can safely self-custody it;
- Safe transfers performed digitally;
- Bitcoin can't be faked.

Smart contracts

Smart contracts are lines of code that allow to automatically execute terms of certain agreements and processes on a blockchain.

They automate interactions between different entities and make them 'trustless', meaning there is no need to rely on a third party to make sure that conditions of the interactions are met.

DeFi is Finance 3.0

Finance 1.0 was a financial system fully relying on regulations of central banks, commercial banks and fiat currency backed by actual gold reserves.

Finance 2.0 featured digitalization of commerce, payments, banking services and intermediaries being a part of each element of the financial system.

Fiance 3.0 is based on the concepts of programmable money, smart contracts and trustless peer-to-peer operations to form the entirely new, open and decentralized financial system.

WHAT IS DEFI?

To understand what DeFi is, let's start with another short description of this term. Then we'll use a practical example of how traditional finance markets work, so we can compare the similarities and contrast the differences.

Decentralized finance, a.k.a. DeFi, is an ecosystem of protocols, applications, investors, and traders that use smart contracts to perform financial transactions in an open, permissionless, and transparent way.

A good way to understand this concept is through your previous experience of traditional financial markets. If you think of any marketplace, whether it is a financial exchange like the New York Stock Exchange or a consumer app like eBay, you have three main entities working together: the buyer, the seller, and the marketplace itself.

- The buyer accesses the exchange in order to find a seller,
- the seller accesses the exchange to find a buyer, and
- the exchange works in the middle to facilitate these requirements.

As a buyer or seller, there are reasons you might want the exchange to know and hold information about you and the entity on the other side of your trade. However, the fundamental innovation at the heart of smart contracts is that you don't need them to know and hold this information, as long as you are able to make the trade on the terms you want.

With a smart contract, you (or anyone or anything) can make a trade without knowing who you are trading with, and without the smart contract holding or using any information about you. It is a trustless relationship, because all that it relies on is the smart contract's code performing as designed.

This trustless relationship is the key dynamic at the heart of the decentralized finance, or DeFi, industry right now.

How does DeFi differ from traditional finance?

In DeFi, smart contracts are facilitating relationships in the same way that banks, payment providers, financial exchanges and other intermediaries

have for centuries in traditional finance. For example, a DeFi protocol Compound Finance does this for lending and borrowing, as well as receiving digital assets from one entity and lending them to another, while an interest payment incentivizes the process.

There are countless other examples of smart contracts that replicate other areas of traditional finance, with more and more arriving every day. You only have to think of the size, power, and influence of traditional finance markets to see why there is such excitement about DeFi's potential.

Let's compare some key components of traditional finance (Finance 1.0) versus DeFi (Finance 3.0) to see how they differ:

Traditional Finance vs. Decentralized Finance

	Traditional 1.0		Decentralized 3.0
Type of money	Fiat For example: dollars, euros, yuan and yen.	→	Cryptocurrency For example: Bitcoin (BTC), Ethereum (ETH), stablecoins and tokens.
Money issuance	Controlled by the state Central banks decide how much new money to print, based on senior bankers' decisions.	→	Auditable in the code The amount of tokens/coins that are minted is specified in each crypto's code for anyone to assess and understand.
Money transfer	Closed payment rails Payment networks, such as SWIFT, are controlled by commercial banks and used to transfer funds between agreed-upon entities.	→	Open payment networks Crypto is transferred quickly and cheaply to anyone you choose, without prejudice and without any requirement for middlemen.
Lending and borrowing	Controlled by banks Restricted to the customers of major commercial banks, like HSBC, who the bank deems "credit-worthy."	→	Enabled by smart contracts Any individual can lend or borrow in DeFi using their crypto, without the need for a bank to approve them.
Exchanges	Require middlemen To trade stocks, you need to access brokerages, like Charles Schwab, and exchanges, like the Nasdaq.	→	Automated and P2P (Peer-to-Peer) Decentralized exchanges enable buyers to interact directly with sellers (peer-to-peer) and remain in control of their funds.

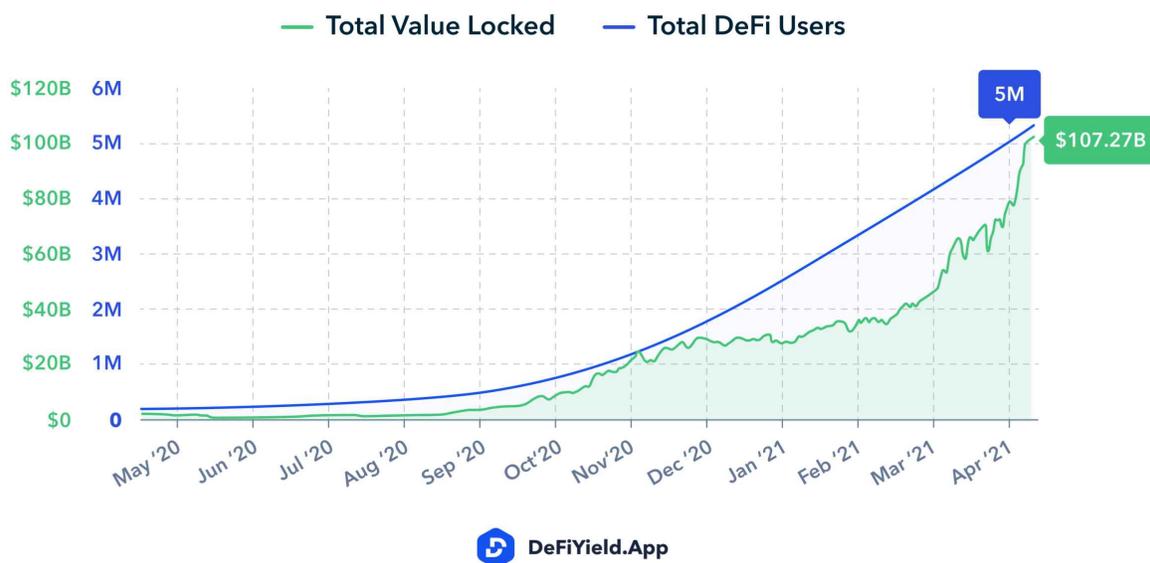


It's not just early adopters and tech aficionados who are getting excited about DeFi.

Many of the world's biggest banks dismissed Bitcoin as a sham in 2017 and actively discouraged their clients from investing in cryptocurrencies. Now they are rushing to hold (or "custody") digital assets on their clients' behalf so they can be saved, traded and transacted. For example, Jamie Dimon, CEO of JP Morgan, [called bitcoin a "fraud" in 2017](#), yet the bank is launching [a debt instrument of bitcoin proxy stocks in 2021](#).

By every measure, DeFi usage is increasing. As the table below shows, both the Total Value Locked (or TVL, which shows the total dollar amount of all coins and tokens that have been deposited in DeFi protocols) and the number of DeFi users has grown rapidly starting in the mid-2020.

Total value locked & users in DeFi



Even though DeFi usage is increasing, the total number of users around the world in March 2021 was just 1.5 million users. Therefore, if you are reading this book to become a DeFi user, you will definitely be part of the first 1% of early adopters in this innovative and disruptive new industry.

Key concepts to understand

Custody and self-sovereign money

Do you *really* own the money in your bank account?

You might think that you do. But in reality, you rely on your bank to give you access to that money, as per the agreement you signed when you deposited your funds. That may seem to be same as owning it, however that's probably because you are lucky enough to live in a country where you haven't experienced the shock of being able to access your money on one day but not the next.

The reality is that a commercial bank can and does stop individuals from accessing their money for all kinds of reasons. One of the most concerning scenarios for a customer is when a country's central bank directs its banks to block people's access to their funds.

If banks don't stop people from outright accessing their money, they might instead put restrictions on what they can do with it. You only need to search for terms like "bank run" or "capital controls" to see many examples from the last 50 years where countries have put arbitrary controls on what their citizens can do with their own money. This disturbing scene played out in Cyprus in 2013, for example, when lenders warned that emergency liquid assistance (ELA) authorized by the European Central Bank was about to be cut, causing a potential run on the banks. Cypriot banks went into a two-week shutdown to head off a bank run that would drain them of their capital, while pension funds and other large depositors lost uninsured savings.

Cryptocurrencies are very different. They are the financial manifestation of the concept of self-sovereignty, also known as self-ownership, which means the right and ability to have exclusive control over your own life. Cryptocurrency represents self-sovereign money because only you control your crypto through an increasingly easy-to-use process of cryptographic signatures.

Because of its decentralized nature, and the fact that it is not issued by a government authority, there is no need for intermediaries such as banks in order to buy, sell, and transact with crypto. This is the essence of the peer-to-peer electronic cash system that Satoshi Nakamoto pioneered when he created the first-ever cryptocurrency, Bitcoin. . This is also why

crypto is a life-saving resource for dissidents in totalitarian regimes, as well as for ordinary citizens who do not trust how their country's finances are run, since it allows these people to transact with a currency that is borderless and valued globally.

Of course, you could choose to use centralized crypto exchange and custody services, such as Coinbase, to buy and store your cryptocurrencies. However, the drawback is that this not only leaves your funds under the control of a centralized institution that is regulated in much the same way that a bank is. It also doesn't allow you to enjoy benefits of DeFi projects, which are built on highly decentralized platforms and protocols and have limited compatibility with centralized crypto exchanges.

Crypto Wallets

Crypto wallets are virtually as old as crypto itself. Satoshi Nakamoto himself released the very first wallet protocol in 2009, Bitcoin-Qt, later rebranded as Bitcoin Core. Nostalgists will be pleased that it is still available for download at the Bitcoin.org website.

Broadly speaking, wallets are either "Hot" or "Cold":

- [Hot wallets](#) connect to the Internet (Web3.0 wallets like MetaMask).
- Cold wallets use secure physical devices to store crypto and private keys locally - but no internet connection (hardware wallets)

Hardware wallets are considered the safest way to store cryptocurrencies but there are still vulnerabilities to keep in mind.

How to access DeFi

In order to access DeFi, you will need three things:

1. The internet
2. A PC or smartphone
3. A DeFi wallet (also referred to as a crypto wallet or Web3 wallet)

Once you have all three, the final thing you'll need is some amount of a blockchain network's native token in your wallet, in order to pay for the transaction fees involved in DeFi.

These fees are also referred to as gas fees as they require some energy to be expended in order for the transaction to be recorded on the underlying blockchain. On the Ethereum network, the gas fees are charged in 'gwei', which is the fractional unit of 'Ether', the Ethereum network's native token.

Understanding wallets

The wallet you use to access DeFi might be described as a crypto, DeFi or Web3 wallet in different situations but this is just because these are emerging industries that are closely intertwined and not clearly separated.

Wallets are virtually as old as crypto itself. Satoshi Nakamoto released the Bitcoin-Qt, first wallet protocol, in 2009. It was later rebranded as Bitcoin Core and is still available for download at the Bitcoin.org website.

However you describe your wallet, the important thing to realise is that it is the main tool you use to interact with the decentralized applications (or dapps) built on blockchain networks that characterize the new Web3 paradigm.

The wallet you use is also referred to as a self-custody wallet because you are the only one that controls access to it. This is unlike a bank account, where you have access but only because the bank gives you access. In this way, wallets give you full control and responsibility.

More specifically, using a wallet ensures that:

- Your identity is not required
- Your personal data is never requested
- Your transactions are not restricted
- Your wallet can only be accessed by you [\[2\]](#)

Buying crypto for the first time

Although DeFi provides an autonomous, decentralized financial ecosystem, the reality is that most people still need to make their first step into it by converting the fiat currency they hold (such as dollars, euros or pounds) into a cryptocurrency or token (like bitcoin or ether).

Some readers will understand this process and will have taken the steps involved already. For those who have not, it will more than likely involve sending some of the fiat currency you hold in your bank account to an account you have with a centralized cryptocurrency exchange, such as Coinbase or Binance.

In this situation, crypto exchanges are referred to as on/off ramps because they are the mechanism you use to go onto the crypto ecosystem or off it back into the fiat one.

Using your bank to buy crypto

Before you try to transfer funds from your bank account to an exchange account in order to make your first purchase, you should be aware that many banks across the world do not allow transfers to cryptocurrency exchanges.

Furthermore, in 2021, there were reports that banks which had not previously restricted transfers were changing their policies without warning. In some cases, these banks were also restricting other transactions and even closing accounts altogether. Therefore, to avoid any issues, always check whether your bank has any such restrictions.

Many of the digital or neo banks advertise themselves as 'crypto-friendly'. What this actually means depends on the individual bank but, by doing some research, you may find one in your country that allows you to make transfers of this kind.

Banks' and regulators' view of crypto

Keep in mind that the regulatory situation is fluid, with many countries urgently reviewing their regulatory frameworks in order to keep pace with the crypto industry's staggering growth.

In the US, there have been some positive regulatory signs of late regarding the use of blockchain networks by banks. In January 2021, the US Office of the Comptroller of Currency said the following:

“A bank may use stablecoins to facilitate payment transactions..., including by issuing a stablecoin, and by exchanging that stablecoin for fiat currency. In this context, stablecoins function as a mechanism of payment, in the same way that debit cards, checks, and electronically stored value (ESV) systems convey payment instructions. Banks have long used cashiers’ checks, travelers’ checks, and other bearer instruments as a means of facilitating cashless payments.”

This matters because of the leading position of the US economy, the US dollar and the US banks within the global financial system, as it could have a knock on effect on regulators in other jurisdictions.

‘Hot’ wallets vs ‘cold’ wallets

As interest in crypto markets and different blockchain networks has increased in recent years, a number of different wallet solutions have been developed to meet the needs of users.

Broadly speaking, wallets are classed as ‘hot’ or ‘cold’. A hot wallet is one that connects to the internet and makes it easy to interact with DeFi and other Web3 applications. A cold wallet is a physical device (often referred to as a hardware wallet) that stores private keys locally on the device and are generally considered to be the safest option.

This is because hardware wallets are rarely connected to the internet, in order to reduce the potential for attacks. They use random number generation to create public/private keys and let you set your own PIN code and recovery phrase.

No verifiable hacks to hardware wallets have yet been confirmed but there are still vulnerabilities to keep in mind. For example, vulnerabilities can occur if devices have been tampered with or compromised, so make sure to only use trusted brands and to buy directly from the manufacturer.

Finally, you should also consider the risk of a hardware wallet being damaged or lost.

Wallet security

Wallet security is achieved through a private key and/or seed phrase. You alone are responsible for their safekeeping so, if you lose them, you lose your crypto.

To ensure this doesn't happen, you should follow some security best practice:

- Keep your private keys in a non-digital/manual record
- Keep a non-digital/manual record of your seed phrases
- Use multiple wallets to distribute your tokens and diversify your risk
- When connecting to a DeFi dapp for the first time, use a test wallet that holds only small amounts of tokens (just enough for gas).
- Be aware of and avoid phishing attacks - where scammers make fake versions of legitimate websites - by double checking you are only clicking on official links.

Finally, you should keep in mind that blockchain networks are public, so transactions and wallet addresses can be viewed and monitored (using etherscan.io, for example).

This doesn't mean anyone can see the tokens you hold as they would need to connect your personal information to a particular wallet or transaction. However, the fact that this is possible with the right kind of forensic analysis should tell you why it's important to be careful who you share your wallet and transaction data with.

Popular wallets you can use

Below are a few examples of well-known hot and cold wallets that you may want to consider. Keep in mind that it's good security practice to use multiple wallets and therefore, as you progress in DeFi, you can and should use more than one of the examples provided.

MetaMask

MetaMask was launched in 2016 by ConsenSys as a web browser plug-in and later added mobile app functionality in 2020.

In October 2020, Consensus also added the Swaps functionality to MetaMask that allows users to trade crypto tokens directly in the wallet. In April 2021, ConsenSys reported that MetaMask had 5 million active monthly users, representing 5x growth during the previous six months.

MetaMask is compatible with ERC20 and ERC721 tokens, which are tokens designed for the Ethereum network. MetaMask is not compatible with Bitcoin but users can access some other popular DeFi chains, such as Binance Smart Chain (BSC). That's because these chains were

specifically developed to be compatible with the Ethereum Virtual Machine (EVM) in order to easily migrate Ethereum DeFi users and developers.

DeFiYield has published a number of online tutorials that provide Metamask users with step-by-step instructions on how to add EVM-compliant chains, such as BSC, to their MetaMask wallets.

Trust Wallet

Trust Wallet is Binance-owned and has become the most widely-used mobile DeFi wallet. It is multi-chain compatible (including Bitcoin) and also features a built-in Web3 browser, as well as staking functionality.

Trezor

Trezor, which means vault in Czech, released the world's first hardware wallet and introduced the important seed recovery and passphrase protection (BIP39 and BIP44) processes.

Ledger

Ledger introduced the [BOLOS operating system](#) and was the first hardware wallet to incorporate two-factor authentication (2FA).

Game Theory

Game Theory is a process of mathematical modelling. It is used to study and predict human behavior based on the rational decisions each person would be expected to make in a “game” scenario. Game theory can play out in a wide range of contexts including social interactions, business, war, biology, and many more.

It is certainly not exclusive to cryptocurrencies, but Game theory does play an important role in various areas of the crypto market. For example, many aspects of the Bitcoin protocol's design were influenced by game theory to predict what might constitute the most secure network, if nefarious actors began to participate.

The use of game theory has influenced the design of virtually all cryptocurrencies and blockchain projects ever since, so it's always worth understanding this concept at a basic level. In terms of Yield Farming, this can be translated to:

- Always trying to understand the various entities involved in a project,

- the incentives that are attracting them to it, and
- the rational or probable decisions they might make based on these factors.

Incentives

Incentives and incentive design play a very important role across blockchain and crypto technology. You should always have them in mind when making an assessment of a new project or the entities involved in it.

Incentives are designed into systems to direct behaviors in a certain way. For example, Proof of Work (PoW) is the process used in the Bitcoin network to keep it as secure as possible and the incentive that leads miners to expend energy in PoW consensus - is the coins that miners receive as a reward.

Another example of incentives is how decentralized exchanges, like Uniswap, or lending/borrowing projects, like Compound, require liquidity to function. Therefore, they incentivize asset holders to lock up assets in a smart contract by rewarding them with an interest rate and governance tokens.

Different market participants have different objectives. Many of the best incentive designs in crypto networks or protocols manage to balance these objectives so that everyone benefits. That said, you should always take time to assess the incentives in any project you are considering for Yield Farming, in order to identify incentives that are skewed towards one participant at the expense of the others. For example, with a fixed amount of reward tokens in a Farming pool, the more liquidity is locked, the less rewards per dollar invested the participants receive. In other words, by investing more you would be diluting those who already invested.

Memes

Your friends send you memes—funny pictures, videos, gifs, or phrases—all the time for a laugh, right? But memes are more than just a bit of fun when it comes to crypto markets. They actually play a sometimes surprisingly important role in how the market functions. That's because they can have a greater effect on driving the success or failure of a project than might first be expected.

For example, Elon Musk has heavily promoted Dogecoin and the memes that surround it through his Twitter account. As one of the richest people in

the world, his attention to Dogecoin has had a dramatic effect on the asset's price.

This is just one simple example of the effect of memes and there are too many in crypto to name them all. However, it's worth looking at a couple more examples to demonstrate their power.

Bitcoin, as the original and most established cryptocurrency, has plenty of memes. "Digital gold," which has been mentioned already, is a powerful meme because it relates to the asset's store of value characteristic and the advantages it has over actual gold. "Hodl" (which is the intentional repetition of the misspelling of "hold" that first appeared in a post on bitcoin.org in 2013) is another important meme you should know. It relates to the idea that, once you hold cryptocurrency you should never sell it., That's because, regardless of volatility in the short-term, it is expected to be worth much more in the long run as cryptocurrencies rise and fiat currencies decline.

An important meme to understand in the world of DeFi is 'ETH is money'. This relates to the idea that, as Ethereum-based projects (particularly DeFi projects) continue to grow, ether is becoming synonymous with money in the same way that bitcoin is synonymous with gold.

All of these examples are important narratives to understand because more and more participants are aligning with them every day, consciously and unconsciously. Subsequently, memes play an increasingly important role in how the markets move.

FUD (Fear, Uncertainty and Doubt)

With the memes comes the FUD—and there's almost as much of this as there are memes!. FUD covers conspiracy theory-style topics such as whether cryptocurrencies will be banned, how markets are manipulated by whales, and whether the whole idea of crypto is one big Ponzi scheme that is ready to collapse at any moment.

Essentially, the best way to deal with FUD concepts as a Yield Farmer is the same way you should deal with memes. You should know about them, do enough research to understand them, assess whether you think they are likely to have a big effect on the market, and plan your strategies accordingly.

Understanding memes and FUD as much as possible puts you in a strong position. You'll be able to take advantage of volatility when you sense that these important dynamics are wielding undue influence over market behavior.

Cycles

While many mainstream commentators describe cryptocurrency markets as volatile, this view is often skewed. That's because they look at snapshots of the markets on days when things are particularly volatile, which is what leads them to decide that cryptocurrency markets are worth commenting on.

However, seasoned cryptocurrency investors see far less volatility over the long-term and generally agree that cryptocurrencies increase in value when viewed on a logarithmic scale (which is a way of compactly displaying numerical data over a very wide value range). They also recognize how, historically, the market has moved in roughly four-year cycles that are based on Bitcoin halvings or "halvenings" (i.e. Pre-programmed events when the number of bitcoins a miner can receive as a reward for mining a new block is cut in half. This is done to help keep Bitcoin's inflation rate in check).

This cycle may or may not continue in the future as bitcoin dominance waxes and wanes, but what's really important for you to understand is where market participants generally agree we are in any cycle. This matters to Yield Farming for a number of reasons, but some examples include:

- paying lower fees during a bear market (as fewer transactions are occurring), or
- seeing greater asset returns from a less proactive strategy in a bull market (as everything rallies regardless).

The most important DeFi protocols

Hopefully you are starting to get excited about the opportunity that Yield Farming provides, and confident enough to get started! Learning is an ongoing process for everyone in this industry, and reading this book is a great start. Most important of all, however, is learning by doing—that is what will truly take your comprehension to the next level.

With that in mind, it's time to look at some of the best and most well-known DeFi projects that you can use to get started. You may well recognize the names of many projects because their profiles are rapidly increasing a lot over the last year. This section is intended to give you a better idea of the fundamentals behind them.

Having looked at some specific projects, I'll also go on to explain the important area of seigniorage coins, which is one of the most profitable areas of my strategy.

	2.0 FINANCE			3.0 FINANCE		
STORE OF VALUE:		Gold	→		Bitcoin	
MONEY:		USD	→		DAI	
BANKS:		HSBC	→		Compound	
						AAVE
BROKERAGE:		Robinhood	→		DeFiYield.app	
						
EXCHANGE:		NYSE	→		Uniswap.org	
						Balancer
ASSET MANAGEMENT:		BlackRock	→		Curve.fi	
						Yearn Finance
INSURANCE:		AXA	→		Nexus Mutual	
						



Lending and borrowing protocols

As with traditional finance, lending and borrowing is a key part of the decentralized financial system. Many of the earliest and most established DeFi protocols are focused on this area.

There are many diverse DeFi protocols that incorporate some element of lending and borrowing in their user services, even if it is not their core offering. Let's look at the key differences between lending and borrowing in traditional finance via a bank, like HSBC, and in decentralized finance via a protocol, like Compound or Aave.

These are highlighted in the table below.

Traditional Finance vs. Decentralized Finance

Lending and borrowing comparison

	Traditional 1.0		Decentralized 3.0
Banks	 HSBC	 Revolut	→  Compound  AAVE
Application time	Several Weeks Even if you already have a bank account, it can take weeks for a credit department to agree to terms. Without a bank account in place, the whole process might take months.	→	A few minutes To access a DeFi loan, all you need to do is deposit funds as collateral with a protocol like Aave or Compound. You can borrow what's needed in just a few clicks, as no middlemen are involved.
Control of funds	Custodial Any funds lent are provided by the lender and held in an account in the client's name, which the bank allows the client to access.	→	Non-custodial The lending and borrowing takes place via decentralised smart contracts. The user holds funds in a wallet only they can access.
Availability	Limited and restricted Only available to the borrowers who a credit department approves. This usually restricts access to the upper and middle classes within leading economies.	→	Trustless and borderless Totally open and available to anyone, anywhere who chooses DeFi. It is accessible to all races, religions, genders, and nationalities, without prejudice.
Minimum amount	Roughly \$1,000 Traditional finance institutions have cut their costs and optimised their business models to suit large lending and borrowing, not ordinary people with small needs.	→	Just a few cents Because DeFi runs on smart contracts, human interaction costs are non-existent and users can access loans of any size to suit their needs.



[MakerDAO](#) is one of the core protocols within DeFi.

It offers a hybrid model of services for lending and borrowing that are built around the DAI stablecoin, which is one of the most trusted stablecoins used in the DeFi ecosystem.

Token holders can deposit various tokens into Maker vaults, where their deposits are used as collateral for loans. The collateral in the vaults is used to determine how many DAI tokens can be minted by the owner of the collateral and the applicable fees. DAI is a debt / loan extended by the MakerDAO to a user, and secured by the tokens such user deposited to the vaults.

The most important point to remember about MakerDAO is that the DAI stablecoin it issues is decentralized. This is unlike other stablecoin issuers, such as Tether, where users simply wire fiat currency to a centralized entity, where the stablecoins are minted by the entity that now controls their collateral. DAI is different, issued in a noncustodial fashion that involves only smart contract interactions.

Compound Finance

[Compound](#) is a DeFi pioneer that enables anonymous lending and borrowing. It was founded by CEO Robert Leshner and CTO Geoffrey Hayes in 2017 to create a better crypto credit market.

Compound has introduced many innovations into the industry, including peer-to-peer lending, tokenized balances and algorithmic interest rates, and has been highly rated by almost every Yield farmer as a result. It has also helped to make DeFi into a composable toolbox via integration with other DeFi projects—that's why DeFi is often referred to as "Money Legos," since protocols can easily connect with each other in endless combinations. This makes the industry more flexible and enables better returns for users.

It hasn't all been plain sailing for Compound though, as its team have had to overcome many of the most significant issues to hit DeFi. These included the exponentially growing network/transaction fees (aka 'gas costs') sometimes exceeding the value of relatively small transactions, and making the platform (and, to be fair, the platform's competitors on Ethereum Network) unattractive to anyone but the biggest investors. As an

Ethereum-based protocol, it also didn't support non-Ethereum assets that were growing in popularity.

For these reasons, Compound has decided to develop Compound Chain, which is intended to be an autonomous distributed ledger that can support digital assets from a variety of different blockchains. This newly developed platform will support its own native token, called CASH, which is created through a borrowing process. Its holders and validators are rewarded with a compounded interest rate, which is now 3%.

The token is designed to be used to pay fees for transactions on Compound Chain. Users can borrow CASH after supplying any asset supported for collateral purposes and use it to pay fees.

When CASH is downloaded and held on peer blockchains, interest accumulates on Compound Chain by synchronizing with the interest index.

Currently, CASH is arbitrarily pegged to USD but this can be adjusted in the future through governance. The governance of Compound Chain occurs through the initial Compound Governance system, according to which holders of the COMP governance token determine the network parameters through a voting process.

Asset management protocols

Protocols that manage digital assets within DeFi, such as [Yearn Finance](#), play a similar role to that which asset managers, like [BlackRock](#), do in traditional finance.

In both cases, the role of these entities is to help the user invest their assets in a risk adjusted manner to generate the appropriate Yield from these assets over time. The key difference is that asset management in DeFi is trustless, permissionless and executed via smart contracts, rather than through middlemen in traditional finance.

The key differences between the two approaches is summarized in the following table:

Traditional Finance vs. Decentralized Finance

Asset management comparison

	Traditional 1.0		Decentralized 3.0
Asset Management	 BlackRock	 Vanguard	→  Curve.fi  Yearn Finance
Application time	Several Weeks Even if you are applying to a bank where you have an account, approval from its compliance team could take several weeks.	→	A few minutes All it takes is a few clicks and a few minutes of your time to deposit the funds you control in protocols such as Yearn Finance.
Control of funds	Custodial You hand over full control of your funds to an asset manager, who decides how and where to invest your money.	→	Non-custodial You choose which protocols to deposit your assets into and can decide based on fully transparent investment strategies.
Availability	Limited and restricted Only the wealthiest citizens within leading economies have the funds required to access traditional asset managers.	→	Trustless and borderless Totally open and available to anyone. It is accessible to all races, religions, genders or nationalities, without prejudice.
Minimum amount	Roughly \$1,000 Asset managers and hedge funds only want to work with clients who can deposit a minimum of several thousand dollars.	→	Just a few cents DeFi users can access asset management protocols like Yearn Finance with just a few dollars.



Yearn Finance

[Yearn Finance](#) is a project I began farming from the start and it remains one of the main sources of my capital gains. Previously known as iEarn, it is a decentralized platform for asset management that provides a range of

Yield Farming opportunities via liquidity provision, insuring DeFi risk and lending assets. However, its central product is [Vaults](#), which allow users to maximize their Yield Farming returns through a combination of strategies.

Yearn was founded by Andre Cronje, who has since become one of the best-known people in Yield Farming. He came up with the idea because he wanted to manage his own stablecoin portfolio in a way that would make it into his traditional bank savings account.

He also wanted to tackle what he believed was a big issue with how token economies worked, namely that playing with tokens sucked up energy and was generally a waste of capital. Therefore, he designed Yearn Finance as a Yield optimizer mainly for stablecoins, in order to manage assets and automate profit maximization.

Yearn Finance's growth has been immense since it introduced its native YFI token, with the project's assets reaching over \$400M within the first week of the token being introduced. At this point, the project drew a lot of attention through its interaction with the Ethereum-based exchange liquidity pool Curve.

Users that provided liquidity to yPool and the YFI Balancer pool on Curve were eligible to claim the YFI token. The pools were developed to be:

- used as Yield aggregators,
- automatically sending staked funds to Compound and Aave for lending, and
- receiving additional returns from this operation.

Apart from optimizing Yields though, one of the most revolutionary approaches taken by Yearn was how it ensured the full decentralization of the project. It was the first DeFi project to introduce the concept of a "fair launch," with no premine of tokens and no developer rewards. Instead, they took what is seen to be the most decentralized route. Instead of Cronje and his colleagues receiving tokens for building Yearn, there was a transparent and equitable distribution of its YFI token.

This is important because digital assets gain value when there is balance between distribution, acknowledgement, and acceptance. Initially, it was settled that the total amount of tokens minted at the time would not be inflated and that 100% of these tokens would be distributed in Farming rewards.

In this respect, Yearn Finance introduced the very concept of Yield Farming.

While Andre Cronje initially had the exclusive right to mint tokens, he didn't use this to his own advantage. Instead, he transferred the right to mint tokens to nine multisig (multi-signature) owners, who were all active members of the DeFi community.

He notably left himself off this list. In accordance with the fair launch strategy, six signatures were required to submit the token minting, and Andre decided to not distribute any tokens to himself.

Such a favorable and community-oriented token distribution had never occurred in DeFi before. But with Yearn, all project participants got equal rights, equal risks, and were able to make decisions based on the same information.

This approach contrasts markedly with centralized crypto projects. In most cases, centralized crypto firms cooperate with influential and financially strong institutions, such as venture capitalists, in order to help the project gain momentum. But Yearn was financed from the ground up with its fair launch. To many, this is why DeFi also represents an extremely important evolution of how startups and innovators are being funded.

The personality of Andre Cronje deserves special mention here, as he now has a strong influence on how crypto events are perceived by the community. He is a talented DeFi architect who has revolutionized Yield Farming. Andre also has a legal background and knowledge of various key areas of traditional finance, including banking and insurance.

His crypto involvement started in the ICO era circa 2017 when he worked for large-scale blockchain projects, such as [Fusion](#) and [Fantom](#), in technical advisory and leadership roles. In these roles, he reviewed the codebases of various ICOs, discovering their strengths and weaknesses. This eventually enabled him to develop the vision of an automated smart saving account that was fulfilled with Yearn Finance.

Multiple copycats were created very quickly following YFI's success, including YFII, YFIII, and many more. Some of these were obvious scams that were just trying to ride the hype of the original project, which goes to show how significant it was.

Exchange protocols

Decentralized exchanges, including aggregators, liquidity protocols and automated market maker (AMMs), have become the DeFi protocols with the most users, the most total value locked (TVL), and the most value exchanged.

For this reason, they are very important and increasingly abundant. There are also key differences between exchanges in traditional finance, such as the Nasdaq or the New York Stock Exchange, which are summarized on the table below.

Traditional Finance vs. Decentralized Finance

Exchanges comparison

	Traditional 1.0		Decentralized 3.0	
Exchanges	 NYSE	 Nasdaq	→  Uniswap.org	 Balancer
Listing Process	Complicated and restricted For an asset to be listed at the NYSE or Nasdaq, a huge amount of time, effort and money is required.	→	Totally accessible Anyone can list a token on Uniswap and create a market, no matter who they are or where they come from.	
Listing timeframe	Many months The complex legal and regulatory process means an initial public offering can take many months to navigate.	→	A matter of minutes Anyone can list a token on a decentralized exchange in minutes.	
Availability	Limited to big corporations Companies can only go public after a long and expensive legal process, which restricts it to an elite group of corporations.	→	Open to any project Any token can be listed, without restriction. It is then up to the market to decide whether the token is popular and worth trading.	



Bancor

[Bancor](#) is considered an important DeFi protocol because it was the first to introduce the concept of an AMM (see the upcoming chapter, “How DeFi Protocols Earn Revenue for a full explanation of AMMs). While other protocols, such as Uniswap, have come to dominate the AMM space over time, the Bancor protocol continues to innovate.

In 2021, Bancor introduced the idea of single-sided exposure for liquidity pools as a solution to the problem of “impermanent loss.” Impermanent loss is a frequently-heard term in DeFi — what follows is a brief explanation, and if you want to learn more visit our Medium post [here](#).

The problem of impermanent loss may occur when a token holder lends two separate tokens and locks up their assets in a DeFi protocol’s smart contract, in order to provide liquidity for exchange pairs of the two tokens.

If prices for the locked tokens shift too much in external markets, liquidity providers might experience a temporary loss on the value of tokens they have locked up. This loss becomes permanent if they remove their tokens from the liquidity pool at the wrong time.

Bancor has suggested a solution to the issue of impermanent loss in the form of single-sided exposure., This involves Bancor’s BNT token providing the other side of a token pool’s liquidity and thereby reducing the risk of impermanent loss. In addition, Bancor has suggested it will also insure liquidity providers against impermanent loss. However, it should be remembered that these single-sided exposure and insurance-related solutions are in their early days of development.

Uniswap

As mentioned, [Uniswap](#) followed Bancor into the AMM space. Since then it has grown to become the largest and most well-known Decentralized Exchange (DEX) in the Ethereum DeFi ecosystem.

Uniswap is radically different from any sort of exchange that has been seen in the traditional finance world before. In many ways it is a standard bearer for the whole DeFi ecosystem.

The key thing to what differentiates Uniswap from exchange competitors like Binance, Coinbase and Kraken is decentralization. While these competitors all complete huge volumes of transactions every day, they all require users to go through a centralized intermediary to do so. That means depositing funds into a centralized exchange’s accounts and passing over control of your funds to them. It also means going through the Know-Your-Customer (KYC) process that these centralized exchanges require.

None of that is necessary with Uniswap. You can instantly exchange one asset for another without your funds going through an intermediary,

meaning you are in full control of your assets right up until the moment you choose to exchange them. In this way, custody remains with you throughout—you are acting as your own bank.

To exchange digital assets via Uniswap, you need to have your assets stored in a digital crypto wallet. You can then send the desired amount of funds to [MetaMask](#), which is a popular cryptocurrency wallet that allows users to interact with Ethereum-based DeFi protocols like Uniswap. From there, it's a simple process of buying or selling tokens in an instant.

It's generally agreed that Uniswap has risen to the top of the DEX rankings because it is the easiest DeFi AMM to use. In addition, users of Uniswap can earn passive income by depositing their tokens into fixed liquidity pools that contain 50% of one token and 50% of the other. Finally, it's worth noting that Uniswap is frequently used by new protocols to establish a liquid marketplace for their native token. Since Uniswap is widely used, this can help to speed up growth of the new protocol's user base.

SushiSwap

[SushiSwap](#) is a decentralized cryptocurrency exchange and AMM created from a “fork” of the Uniswap protocol. Forks, or forking, is a temporary or permanent change that diverges a blockchain into different paths. Even though these two forks share the same genesis code, moving forward they exist as separate networks with different rules and governance.

SushiSwap has a fairly controversial history, due to a couple of high-profile incidents. The first involved what came to be referred to as a “vampire attack,” where SushiSwap's initial launch incentives for its [SUSHI](#) token designed to drain liquidity from Uniswap in order to boost SushiSwap's market position (see more about vampire attacks in this book's section “Additional concepts to understand”).

The second event saw one of SushiSwap's main developers, the pseudonymous Chef Nomi, suddenly liquidate \$14M of SUSHI tokens that were stored as a development fund. He decided to return the funds six days later. However, the overall effect of this unexpected event—which raised red flags that SushiSwap may be an exit scam—weakened the entire DeFi market for a period.

Credit to SushiSwap for surviving this rocky start and continuing to move forward. SushiSwap evolved from there to become a community-driven protocol, and has retained a leading position in DeFi. This is mainly

because of the attractive terms and incentives it has offered. Here are three highlights:

1. Sushiswap offered new terms for passive income. Liquidity providers on SushiSwap lock their funds into a pool and receive returns for this in the form of SUSHI. However, unlike Uniswap, the SUSHI tokens received also allow liquidity providers to continue earning trading fees, paid in SUSHI, even when they unstack the deposited funds.
2. SushiSwap improved on an issue that Uniswap had when it came to diluting the rewards of smaller liquidity providers. Because staking larger amounts into Uniswap liquidity pools resulted in larger fees being paid to these providers, smaller liquidity providers became diluted as the total value of the Uniswap pools grew. SushiSwap solved this issue by distributing SUSHI tokens in a different way: They allowed early adopters to gain ten times more SUSHI than those who brought liquidity to the pools later on.
3. Sushiswap has also enabled limit orders. This is an important exchange feature that will attract traders, and therefore should result in more fees for liquidity providers.

Curve Finance

[Curve Finance](#) is a decentralized exchange (DEX) and AMM designed to enable efficient token swaps. It focuses on stablecoins, such as [DAI](#), [USDC](#), [USDT](#), [TUSD](#), [BUSD](#) and [sUSD](#), and enables users to enjoy low impermanent losses and little slippage. Stablecoins are cryptocurrencies designed to peg their value to something external such as fiat currencies, other cryptos, or exchange-traded commodities.

The idea for Curve was developed by Russian physicist Michael Egorov [in a whitepaper](#) at the end of 2019 and launched as a protocol in early 2020.

Even though Uniswap is the most well-known AMM, Curve Finance has managed to stand out because of the unique advantages it offers. First, Curve enabled lower transaction fees by swapping stablecoins directly with one another, rather than routing through the Ethereum blockchain and incurring the gas costs and slippage this can cause (slippage is the difference between a trade's expected price and its actual price once it's executed—it's most prevalent when markets are volatile). Later on, Uniswap applied this same improvement in its own updated second version.

Next, Curve has managed to reduce slippage when swapping tokens. This was achieved through advanced mathematical formulas that define the relationship between token prices and their supply.

From there, Curve allows liquidity providers to interact with Compound, allowing them to earn extra interest on top of fees by sharing liquidity. This means that users can increase their earnings without holding more volatile tokens. A similar interaction was made possible with Yearn, which allowed stablecoin holders to benefit from high interest, which was enabled by the automated rebalancing of the underlying tokens.

Several months after its initial success, Curve Finance issued its own governance token, [Curve DAO \(CRV\)](#). People who had invested in the project prior to the token launch were eligible to receive CRV in the token distribution. As a result, Yield farmers are attracted to Curve because they could receive Yield on their staked stablecoins and receive CRV rewards for providing liquidity.

Some pools offer even higher returns. These so-called incentivized pools include, for example, the sUSD pool that provides additional rewards in the form of [Synthetix](#) tokens (SNX).

The Yield Farming interest that is available from Curve pools fluctuates constantly, with the biggest return on stablecoins currently at around 5%. A process you can use to users compare liquidity pools:

1. Gauge the total return for each one, by
2. taking into account all additional interest paid in CRV and the pool's specific tokens.
3. You must also consider the high gas fees that come from interacting with Curve's smart contracts on Ethereum, and
4. decide how your frequency of withdrawing Yield could eat into any profit gained.

Balancer

[Balancer](#) is another AMM worth knowing about, mainly because of the unequal liquidity pools it enables.

The less intuitive UX of Balancer is generally thought to hold back its growth alternatives like Uniswap that are easier to use. However, Balancer's "unequal liquidity pools" can provide good Yield opportunities for advanced users.

Unequal liquidity pools are ones that deviate from the starting 50:50 split that some AMMs use., The user might choose different correlations, such as 80:20. They do this because they see an opportunity to generate more Yield from the assets they deposit. However, this should be considered an advanced strategy, as these Yield farmers also expose themselves to increased impermanent loss risk.

dYdX

[dYdX](#) is a decentralized exchange built to meet the needs of traders used to centralized exchanges' high quality user interface and feature-rich experience.

Users of dYdX benefit from derivatives, perpetual and leveraged trading via a decentralized order book. This can be particularly useful if a trader wants to trade an asset that doesn't have a huge amount of liquidity on a decentralized market. dYdX users can create a derivative that doesn't require volume in the underlying asset, and trade the risk instead.

dYdX Layer 2 cross-margined Perpetuals are available on mainnet Ethereum with the [integration of Starware](#). With the L2 integration, dYdX aims at becoming a trustless, noncustodial version of Bitmex/Binance Futures.

Like many other protocols, dYdX offers lending and borrowing services as well.

Injective Protocol

[Injective Protocol](#) is another decentralized exchange that has emphasized an intuitive UI, appealing to everyone from new DeFi users to experienced traders. It operates as a cross-chain, interoperable relay chain, allowing users to trade spot and future derivatives.

Ox

[Ox](#) plays a significant role within DeFi. It is an open protocol that enables peer-to-peer asset exchange, making it useful to a number of other protocols when they are creating their own decentralized exchanges.

Ox enables them to build order books for their exchanges using the Ox protocol as an oracle for pricing. Oracles are verified data feeds, such as price feeds for traditional financial assets, that can be used to price assets.

See more about them in this book's section "Other Important Protocols and Projects."

As a result, 0x has become a major source of bid and ask prices for a variety of DEXes. In addition, DEX aggregator protocols use 0x to find the best price among a range of DEXes. Examples of this type of protocol include [1inch](#), [Paraswap](#) and [Matcha](#). The latter was built by 0x itself.

PancakeSwap

[PancakeSwap](#) is a decentralized exchange that runs on [Binance Smart Chain](#) rather than Ethereum. It is also the largest project on Binance Smart Chain at the time of this writing, in terms of Total Value Locked (TVL).

It enables efficient swapping of BEP20 tokens, BEP20 being the token standard on Binance Smart Chain that extends Ethereum ERC-20 and is compatible with it. This swapping takes place via the AMM model and offers attractive Farming opportunities.

There are some key advantages that a decentralized exchange running on Binance Smart Chain has. These include transactions only costing a few cents, with transaction speeds of approximately 2,000 per second. Both metrics are much more attractive than their equivalents on Ethereum.

PancakeSwap offers Farming of its [CAKE token](#). This is possible when users deposit and lock up liquidity pool (LP) tokens, known as FLIP tokens. LP tokens act like share certificates for the funds you have deposited, giving you the right to withdraw your funds according to your share of the whole liquidity pool. (See more about them in this book's section "Additional concepts to understand.")

Yield farmers can then also stake CAKE tokens to get additional rewards, which are paid in SYRUP tokens. The SYRUP token was developed as governance and a lottery token. However, SYRUP tokens are discontinued at the time of this writing due to a smart contract flaw., with the project team migrating all distributed and future SYRUP tokens to CAKE-based pools.

Brokerage and account services

Brokerage and account services in DeFi involve managing and deploying assets across a variety of DeFi protocols and blockchain networks to generate Yield. The best brokerage and account services enable this,

while also protecting their users from scams. They do this by auditing DeFi smart contracts and only listing safe protocols for them to use.

There are many differences between a brokerage provider in traditional finance, such as Robinhood, and a DeFi brokerage protocol, such as DeFiYield, which are outlined in the table below.

Traditional Finance vs. Decentralized Finance

Brokerage & account services

	Traditional 1.0		Decentralized 3.0
Banks	 	→	
	Robinhood Interactive Brokers		DeFiYield.App
Application time	Several Weeks Even if you already have a bank account, it can take weeks for a credit department to agree to terms. Without a bank account in place, the whole process might take months.	→	A few minutes To access a DeFi loan, all you need to do is deposit funds as collateral with a protocol like Aave or Compound. You can borrow what's needed in just a few clicks, as no middlemen are involved.
Control of funds	Custodial Any funds lent are provided by the lender and held in an account in the client's name, which the bank allows the client to access.	→	Non-custodial The lending and borrowing takes place via decentralised smart contracts. The user holds funds in a wallet only they can access.
Availability	Limited and restricted Only available to the borrowers who a credit department approves. This usually restricts access to the upper and middle classes within leading economies.	→	Trustless and borderless Totally open and available to anyone, anywhere who chooses DeFi. It is accessible to all races, religions, genders, and nationalities, without prejudice.
Minimum amount	Roughly \$1,000 Traditional finance institutions have cut their costs and optimised their business models to suit large lending and borrowing, not ordinary people with small needs.	→	Just a few cents Because DeFi runs on smart contracts, human interaction costs are non-existent and users can access loans of any size to suit their needs.



DeFiYield is a decentralized protocol for cross-chain asset management. It includes an all-in-one dashboard that allows users to manage their digital asset investments in one place, as well as a range of additional security products that keep users safe and protected from scams.

Cross-chain Asset Management Dashboard

The DeFiYield Dashboard allows users to manage their funds staked in liquidity pools and Yield Farming vaults . You can also use it to exchange tokens at the best rates and swap fiat currencies for cryptocurrencies.

Crucially, because DeFiYield is a cross-chain solution, it allows users to relocate funds across multiple blockchains. These currently include Ethereum, Binance Smart Chain and Huobi ECO Chain, with new ones constantly being evaluated for potential inclusion.

One of DeFiYield's unique features is its presentation of precise calculations for Yield Farming rewards. The platform allows users to see detailed metrics about their portfolio's performance, including:

- P&L chart with hourly, daily, monthly, and yearly overview
- P&L value for selected timeframe
- Accrued expenses
- Earned value
- Gas costs
- Impermanent loss
- Claimable rewards
- Fees earned

As well as helping users to track investments, DeFiYield also makes it easier to develop DeFi investment strategies. The platform provides detailed information about DeFi protocols and in-depth audits of the smart contracts they use.

These are just some of the DeFiYield tools that help users deposit their funds in the safest DeFi protocols, while generating the maximum Yield. Please visit us at [DeFiYield](#) to see the latest ways that we're improving DeFi!

Derivative protocols

Derivatives are financial instruments that derive their value from an underlying asset—examples from the traditional finance world include futures, options, and credit default swaps. In the case of DeFi, this underlying asset might be a digital or traditional asset.

As a result, some of the best-known derivative protocols in DeFi were established to enable the trading of products from traditional finance, by “wrapping” them in a digital asset derivative. Wrapping in this context means creating compatibility with a particular blockchain, like Ethereum.

Synthetix

[Synthetix](#) is a very important DeFi project that may well play a significant role in the industry for years to come. It provides what’s known as a synthetic market for every asset imaginable.

Synthetic assets replicate other assets. They do this by using smart contract-based derivatives that derive value from an underlying asset. These underlying assets could include commodities, fiat or crypto currencies, stocks, interest rates, bonds, indexes and more. Stablecoins, which peg their value to fiat or crypto currencies, are an example of a synthetic asset.

The platform, which was founded by Kain Warwick, was launched in December 2018. It is a borderless and limitless marketplace, that essentially wraps every asset into something that can be traded. This is a welcome development because trading certain assets can be difficult for some investors. For example, you might want to trade gold, cobalt or Tesla stocks but be restricted from doing so. That could be because of where you live in the world, or because those markets are not open to anyone but specialist investors, among other reasons.

In Synthetix, however, these restrictions go away. On this platform, you can trade a synthetic derivative that represents the underlying asset. From there, you can implement your chosen strategy to take advantage of the price changes you expect, without ever having to trade the actual underlying asset. Being able to trade via Synthetics opens up numerous benefits for all participants that reduce friction and costs, while encouraging market innovation.

Synthetix also allows traders to use leverage in their trades. Leverage is the use of borrowed funds to increase a user’s trade position beyond their available cash balance, which can amplify profits as well as losses. These

features combine to make it a vast derivative liquidity project, one that may well expand in size and influence.

Also notable is Synthetix' "Spartan Council"., This is a delegated council with seven seats that was voted for in December 2020 to govern the Synthetix protocol. It is an example of one of the many approaches to protocol governance, which aim for varying ratios of centralization to decentralization.

Other important protocols and projects

DeFi is only in its early days of development but, even at this early stage, there are some potentially huge and transformational projects being developed right now.

The following examples are projects you should DeFinitely be aware of as you start your Yield Farming journey, as they are not only important within this immature industry right now but could also grow into huge and truly fundamental projects in future.

The Graph

The Graph is an indexing protocol for querying decentralised networks. It has been labelled the Google of DeFi and, more widely, Web3. It was founded in 2018 by Yaniv Tal and Brandon Ramirez, and the mainnet was launched in December 2020.

The problem that The Graph solves is being able to search through the huge amounts of data available on public blockchain networks in a fast, efficient and decentralized way. You may already be aware of blockchain analytics services that already search and index blockchain data. However, most of these are centralized services that extract the publicly available information, index and store it on their own databases, and then make it available for others (usually for a fee).

The Graph is different because it enables this indexing of information in a totally decentralized way. That is why The Graph is used by most DeFi projects to display data about blockchain networks that users need to make financial decisions.

It is becoming the standard for big data analysis within DeFi because it is a trustless and open sourced way of finding out what's the best data source. This process is enabled within The Graph network by validators, indexers

and curators being incentivised to work in tandem to search for and organise data from blockchain networks.

It is a hugely significant service that is worth knowing about now as it will likely be used by most Ethereum-based projects and probably also across many other smart contract platforms.

Oracles

While The Graph is an example of a protocol that allows DeFi projects to use the data from public blockchain networks to enrich the services they offer their users, these same projects may also need to use data that comes from other sources.

In DeFi, and Web 3.0 more generally, the best way of doing this is through oracles. Essentially, these are verified data feeds, such as price feeds for traditional financial assets that can be used to price synthetic derivatives.

Trustless DeFi is enabled by trustless oracles and truly decentralised applications will aim to use decentralised oracles. These networks act as the antennae for data that is relevant to DeFi, collecting it from all sorts of sources and feeding it through to the projects that need it.

Oracles can help DeFi projects to avoid the disruption that might be caused by an asset's price crashing on a single exchange, as prices gathered from multiple decentralised oracles would mitigate any damage done. Not all DeFi projects use decentralised oracles though, with Compound's use of Coinbase price data feeds being a well-known example of a closed data source.

Chainlink

Chainlink is the most well known decentralised oracle network, with a market cap that puts it in or around the top 10 cryptocurrencies. It was first conceived as far back as 2014 by CEO Sergey Naxarov, raised funds via an ICO in 2017 and went live with its mainnet in June 2019.

It is made up of a network of decentralized nodes that connect off chain data sources to smart contracts on the blockchain. It is used by a whole range of DeFi protocols for this reason but is also used by a whole range of other decentralized applications.

Apart from the fact that it has been around for a long time, Chainlink's growth has also benefited from the support of LINK Marines, the early

adopters of the coin who have a strong presence across social media.

Decentralized insurance

Decentralized insurance protocols are a growing niche within decentralized finance but they currently relate to insurance cover for a set of specific risks, rather than mirroring the wide range of events that can be insured in traditional markets.

So, for example, one of the key decentralised insurance products that is available covers breaches or exploits of smart contracts. Nexus Mutual and other decentralized insurance protocols offer for cover for this type of incident.

One key similarity with the traditional insurance world is that there is usually an element of discretion involved in the claims these protocols payout for. For Nexus Mutual, the governance of these decisions revolves around holders of the native token, with these participants deciding to vote for or against a claim.

Seigniorage coins

Seigniorage coins are algorithmic stablecoins that form the basis of a number of projects. This means their value is not collateralized with any asset and is instead adjusted algorithmically through certain supply dynamics.

One of the main reasons they are so important is because they may provide a solution to the problems of using cryptocurrencies as a medium of exchange.

Empty Set Dollar

Empty Set Dollar was first introduced to us by Mervyn Chng, Co-Founder of stakewithus. The project's ESD token was designed to become the reserve currency of DeFi and you need to purchase ESD tokens for bonding to get started.

From here, you can generate Yield by taking advantage of the expansion and contraction cycles that the token goes through. The expansion cycle occurs when the price of ESD is above the \$1 peg and the supply of ESD tokens is being raised.

Dynamic Set Dollar

Dynamic Set Dollar (DSD) is very similar to ESD but it utilizes a more reactive mechanism of supply adjustments and includes improved terms for users. It's important to point out that DSD is not based on a rebase system, so holders won't experience changes in the token balance within their wallet. Instead, the price stability is reached by giving holders a financial incentive to sell or burn tokens, which is referred to as Voluntary Elastic Supply.

When the price of DSD rises above the \$1 peg, the protocol activates the expansion phase and new DSD tokens are minted. The token supply can increase by a maximum of 10% every 2 hours, with the total expansion limited to 35%. These newly minted tokens are then distributed to reward DAO stakers and liquidity providers.

Why the seigniorage coin hype is over (for now)

The seigniorage and algorithmic stablecoin opportunity peaked around December 2020, since when some protocol values have dipped as much as 90%. Surfing the token supply cycles of seigniorage coins provided high and stable incomes for a period and the market is still young some imperfections should be expected.

One of the protocols that has emerged from the hype cycle with a positive image is Frax, which did not lose its peg even after several tests. This segment of DeFi is working on perfecting its toenomics and it is worth watching as one that might catch on again in future.

How DeFi protocols earn revenue

Before we dive into how individual farmers can profit from opportunities that DeFi projects provide, let's examine how these DeFi projects earn revenue for themselves.

In DeFi, there are many different business models that projects can employ. Innovation occurs at breakneck speed in this industry. New projects can employ and integrate elements from different models in order to earn revenue, in endlessly varying combinations—the composability or “money legos” we discussed earlier.

To get started with Yield Farming however, you only really need to understand the main DeFi protocol revenue models. We explain them below.

But first, dev rewards

Before looking at the specifics, let's discuss the important concept of dev rewards.

Here's a good starting point: each DeFi protocol operates as its own central bank and digital asset issuer. The majority of projects function this way during initial coin offerings (ICOs) or initial exchange offerings (IEOs) to allocate a specific portion of tokens towards internal funding. This allocation to developers is usually referred to as dev rewards. It represents financing required for ongoing development.

Why does this matter? Because even though a protocol's ecosystem might be considered sufficiently decentralized at an early stage, the initial brainpower and development capacity come from a centralized entity.

It is understood that this entity needs to be rewarded for the significant value it provides early on and dev rewards are the solution. These are normally structured to avoid any substantial downward pressure on the native token's price, which otherwise could occur if the team was able to sell its dev rewards without restrictions.

Now, following are the primary ways that DeFi protocols earn revenue:

DeFi Protocol Revenue Streams

Part 1

Type of Revenue	Type of protocol	Examples
Credit margin The difference between rates for borrowing and lending.	Lending and borrowing.	 Aave  Compound  Cream  Venus
Asset rehypothecation Using spare or under-utilized assets to generate yield.	Lending and borrowing, exchanges and others.	 Celsius  yEarn ... others
Fees Either service fees or additional gas charges.	Asset management, aggregators and relayers.	 yEarn (2% Management, 20% Performance fees on Vaults)  Pickle (0.5% exit, 3% subsidized gas fees on Jars/Vaults)  Harvest  1inch  Paraswap

DeFi Protocol Revenue Streams

Part 2

Type of Revenue	Type of protocol	Examples
<p>Exchange spreads</p> <p>Finding arbitrage opportunities between exchanges.</p>	Aggregators.	 Kyberswap
<p>DevRewards</p> <p>Benefitting from a price increase in the native token.</p>	Almost all DeFi projects.	 1inch token (1INCH) allocations: <ul style="list-style-type: none">• 22.5% core team and future employees;• 19.5% to investors and shareholders.  Harvest Finance token (FARM) allocations: <ul style="list-style-type: none">• 10% of the FARM tokens will vest to the Operational Treasury;• 20% of the FARM tokens will vest to the Development Team.
<p>Yield Farming</p> <p>Early adoption of the protocol's incentive mechanisms.</p>	Used by almost every project with farming tools but not always made public.	As an example, a project team providing liquidity at an early stage using its funds from development reserve or otherwise, would have high chances to capital gains in the case of an increase in the project token price.



Here are the specific ways we see these mechanisms play out in DeFi.

Credit monetization

Well-known examples of projects in this category include Compound, Aave, Cream and Venus. Think of them as decentralizing the way

traditional banks use deposits and loans to generate revenue.

In a credit monetization model,:

- A project attracts liquidity from the market by providing interest rates on the deposits made.
- These rates may be fixed or variable.
- The liquidity that has been attracted from lenders is then provided to borrowers, with a margin added to deposit rates.
- These loans are also available at fixed and variable rates, with the fixed rates normally higher than the variable ones.

An additional feature of credit monetization DeFi projects that's different from traditional banks is that they usually incentivize customers to deposit or borrow funds. They do this by distributing rewards to users in the form of platform tokens.

Sometimes there is excessive liquidity in a particular asset, because more funds have been lent by depositors than have been loaned to borrowers., That's when projects might choose to put these assets to work in a different way.

For example, they might lend these deposits to other projects, in a process that mirrors interbank (bank-to-bank) loans in traditional finance. Alternatively, they might invest funds in automated asset management projects, which are detailed below.

In addition, whenever a project chooses to distribute a token and the token becomes freely tradeable, the project might also sell tokens to generate additional revenue. However, this will depend on how the token was distributed and its utility characteristics.

Automated Market Maker (AMMs)

The Automated Market Maker (AMM) market started initially with the Bancor Network. Other well-known examples of platforms in this category include Uniswap, Balancer, Curve and SushiSwap.

Think of AMMs as an open-air marketplace. Essentially, anyone can use these projects to set up shop in a trading market (except for Curve among the projects mentioned above).

An AMM user would:

- Set up a trading market to facilitate the exchange of any tokens that are acceptable to the network.
- and earn revenue on the trading fees.
- They might also set up a trading market to connect and exchange one token for another, provided there is sufficient liquidity.

The host protocol earns revenue by charging fees for trading. It may also introduce wider spreads between the buy and sell prices of certain token pairs, and subsequently benefit from arbitrage opportunities.

As with other DeFi projects, these AMM projects may also choose to distribute a native token. That token might be retained by the platform. It may also be sold for profit on the open market at times of price appreciation.

Automated Asset Management

Well-known examples of projects in this category include yEarn, Pickle and Harvest.

Think of these projects as asset managers in traditional finance. The service they provide is based around routing customer funds to various parts of the DeFi market. Then they can take advantage of various DeFi instruments and achieve the highest possible Yield.

These projects usually offer single asset vaults, each one holding only USDC or DAI, for example, or a specific liquidity pool share token. They use these to collect customer funds and accumulate revenues, for instance by selling rewards/incentives. These revenues are then redeemable by customers, in return for paying a fee to the project that provided the vault.

These projects attract users and generate revenue by providing the most profitable strategies across volatile markets, in parallel with the cheapest transaction costs. The cost-effectiveness of the platform is particularly important if users are seeking Yield as part of a strategy that involves multi-layer transactions.

That's because these multi-layer interactions with multiple smart contracts can potentially generate a lot of network fees., Automated asset management projects try to reduce these costs and generate revenue for themselves via the transaction savings they enable.

Once again, these projects can also generate additional income from a native token. It may be partially retained by the platform, or sold for profit

on the open market at times of price appreciation.

Aggregators, routers & relayers

Well-known examples of aggregator, router, and relayer platforms include 1inch, Paraswap and Matcha.

Their business model is built around finding and providing the best exchange rates for traders. They do this by:

- Integrating with and connecting to multiple liquidity sources,
- then routing buy and sell orders,
- in order to find the optimal balance of FX rate and network fees.

Some of these projects also use off-chain order book management to substantially reduce the related network fees. This matters because network fees can jump to extremely high levels.

Projects can also use “slippage surplus” to generate revenue, which is the case with 1inch. In this model, the platform generates revenue by collecting the positive difference between the order price when the transaction was confirmed, and the actual settlement price.

These platforms can also generate revenue from a native token. This native token may be partially retained by the platform, or sold for profit on the open market..

Additional concepts to understand

Before you take your first steps into Yield Farming, it's worth detailing some related concepts that will help you to understand how the industry works and some of the dangers that exist within it.

Decentralized governance and DAOs

One of the most important benefits of decentralized finance is that you are able to take advantage of the decentralized governance that DeFi projects offer. As mentioned previously, decentralization is at the heart of the innovation that cryptocurrencies and blockchain technology provide.

In its truest form, decentralized governance is embodied by a Decentralized Autonomous Organisation or DAO, which is a totally new form of organizational structure enabled by blockchain technology. Unlike a limited company, which exists within the legal frameworks of a particular state, a DAO exists only on the internet. The rules that govern a DAO are encoded in a series of smart contracts, in much the same way the rules that govern a limited company are written down in legal documents.

However, DAOs can be much more open, transparent and easy for anyone in the world to interact or take part in. The specific benefits of decentralized governance within a DAO as compared to centralized governance in a limited company can be seen in the table below.

Traditional Governance vs. Decentralized Governance

Limited Company vs Decentralized Autonomous Organisation (DAO)

	Centralized	Decentralized
Decision Making	Limited Directors and management only.	Unlimited Any stakeholder can have their say.
Proposing changes	Restricted Restricted to those with executive powers as defined by a legal structure.	Open Open to any community member within a truly decentralized structure.
Quorum and approval thresholds	Fixed in legal documents The legal documents define the	Defined by smart contract This can remain as initially

	The legal documents define the minimum thresholds for votes to be valid.	This can remain as initially deployed or adjusted via community vote.
Influence on decisions	Controlled by elites Normally limited to majority shareholders and management.	Available to anyone All community members are listened to as defi protocols are open to innovation.
Barriers to entry	High difficulty Specific legal procedures cover how members can withdraw, depending on the entity setup.	Easy access Any stakeholder can withdraw at any time by disposing of governance tokens.
Transferability	Complicated Specific procedures exist for the transferring of rights, depending on the entity setup.	Simple Usually any stakeholder can freely transfer their governance tokens to any other person or wallet.
Understanding dilution	Effort intensive It may require substantial effort and legal costs to fully understand how one's influence on decision making can be reduced.	Clear and transparent By evaluating smart contracts, one can understand any perspective dilution scenarios or related risks.



How DeFi uses decentralized governance and DAOs

Just as DeFi is an emerging industry, so is decentralized governance an emerging concept. Therefore, not all DeFi protocols can be said to embrace fully decentralized governance. While full decentralization should be any protocol's ultimate goal, there are various reasons why individual DeFi protocols have adopted their own approach.

Founder control: The least decentralized projects, these have a similar governance structure to private companies, with founders guiding the project strategy, controlling the execution of the technical roadmap and DeFining the project's future.

Some projects will claim that they lean towards this form of governance temporarily because they are at an early-stage and the mechanics

required for the project to function correctly are not launched yet.

This can be a reasonable position but, unfortunately, some projects fail to prove they are moving towards decentralization by making the necessary code changes in the protocol. For example, they will not design steps to transfer governance to or share governance with users, so we flag this lack of open governance to the community.

Council model: This approach is sometimes used by immature projects and it involves selecting a group of experts to help make decisions about the product, roadmap and any issues that must be resolved. Councils are usually made up of core developers and established crypto founders, such as Andre Cronje or Stani Kulechov. This partnership style approach is usually in high demand because of the industry influence these individuals wield.

Representative democracy: Users are able to elect individuals to represent them and this group of representatives is assigned to making decisions concerning project development on the behalf of users.

Full decentralization: This is what open governance looks like and it is something we have never seen before in traditional finance. This approach is enabled by governance tokens, with projects distributing governance tokens to users so they are put in direct control of a project's future. A project may choose to use a Decentralised Autonomous Organisation (DAO) platform, such as Aragon, to manage this process.

The primary goal of governance tokens within DeFi is to give users of a project the right to influence strategic decisions about how the project develops and how to solve any issues. Holders of governance tokens are able to influence the direction of the project by:

- Proposing a change and initiating a vote to decide whether it goes ahead
- Voting for or against a change that they or another user has proposed

The growing demand for governance tokens indicates how crypto market participants want to take control of how their assets are used by DeFi projects. Furthermore, as the weight of a user's vote is directly correlated with the amount of governance tokens they hold or stake, many believe this is a good reason to acquire as many governance tokens as they can.

This innovative approach to governance has definitely raised the standards of how all crypto projects are designed and run.

	 DELAWARE, LLC	 ETHEREUM, DAO
Structure	Legal shares	Token share
Medium	Analog	Digital
Database	Registered to a Nation State	Registered to the Internet
Access Control	Nation State Identity (SSN)	Private Key
Requirements	Citizenship or U.S. Status	Internet connection
Financial System	Traditional Finance	Decentralized Finance
Bank Account	BOA, JPMorgan, WellsFargo	Ethereum Address
Registration Costs	\$90 one-time +\$300 annual	\$20 one-time gas fee
Credit	Robust credit system	Not currently available
Protocol Taxes	State & Federal Taxes (20 to 40% of profits)	None
Jurisdiction	United States	Global
System Cost	Entire U.S. Government (Double digit trillions annually)	Ethereum Protocol (Single digital billions annually)
<u>BANKLESS</u>		

When governance tokens don't work: It's worth noting that governance tokens are not a panacea for all issues related to governance and they can lead to undesirable consequences.

For example, if governance rights are tokenized but no vesting period is put in place for the tokens, a malicious founder could dump their tokens onto the open market, causing a supply shock that undermines the price of the token as well as the project's credibility.

Another potential issue might arise if an already well-established project uses its position to acquire a significant portion of a new project's governance token, resulting in parts of the DeFi ecosystem becoming centralized in the hands of the larger project's token holders.

Benefits of decentralized governance for DeFi users

To understand how an individual defi user can benefit from decentralized governance, let's refer to the example of a bank account in traditional finance. Even if you are a citizen within one of the world's leading economies and do not fear government seizure of your funds, there are plenty of other reasons why you should look at the money sitting in your bank account and consider whether it might be put to better use in DeFi. Firstly, that's because of Yields. Interest rates in major fiat economies are at historic lows and likely to remain so for the foreseeable future. You could receive an interest rate of under 1% in a traditional bank account or at least 10% in DeFi.

Furthermore, if you are interested in seeking Yield on your investments, DeFi provides far greater potential for you to take control of that process than is possible in traditional finance. This is possible because of decentralized governance and DAOs. If, for example, you decided to seek better Yield than a standard bank account provides and instead opened your funds up to the bank's wealth management department, you might achieve better Yields (although it's likely these still won't be as good as in DeFi).

But what happens in this scenario if the 'advice' you receive isn't very good? Can you go to the wealth manager and start to dictate terms? Maybe that's possible if you're investing millions but not if you're the average investor.

With DeFi, if you don't think a project is offering the best investment opportunities and strategies, you can change them by using your governance tokens to vote for the ones you like. This is the real power of open and decentralized governance.

Stablecoins

Stablecoin Categories

Type	Description	Examples
Fiat-backed	An Ethereum stablecoin can represent a U.S. dollar, with each token issued backed by a corresponding U.S. dollar in a treasury.	USDC USDT
Crypto collateralized	An Ethereum stablecoin can be issued when collateralized by other digital assets like ETH, BAT, or USDC.	DAI
Interest-bearing stablecoin	An Ethereum token can be created to represent a stablecoin deposit earning interest, also known as an interest-bearing stablecoin.	cUSDC aUSDC aUSDT
Synthetic	An Ethereum token can be synthetic, introduced by synthetix where sUSD is backed by SNX holders, who are rewarded for providing collateral and stability with fees generated by Synth transactions.	sUSD
Algorithmic	An Ethereum token can be programmed to optimize in search of the highest yield opportunities, or have its treasury managed through the minting and burning of existing supply.	AMPL yUSDC

Source: [Consensys](#)



Stablecoins are tokens designed to maintain a stable price that is pegged to another asset. In most cases the asset is the US dollar but there are stablecoins that track other fiat currencies, as well as gold and stock market indices.

In recent years, stablecoins have become much more prominent in crypto. That's mainly because they allow traders and investors to monitor and denominate gains and losses in a currency whose value has remained far more stable over time than most cryptocurrencies have.

As a result, stablecoins have replaced bitcoin and ether as the primary medium of exchange for crypto trading pairs. They have also become a core component of DeFi, with the supply of stablecoins increasing in line with the rise of DeFi. According to Consensys, stablecoin total supply on

Ethereum increased almost 7x from \$5.5 billion in Q1 2020 to [\\$37.4 billion in Q1 2021](#).

Different types of stablecoin

As mentioned, the most common peg used in stablecoins is the US dollar. Different stablecoin projects use different mechanisms for maintaining this peg and experience different levels of success in doing so.

Some stablecoins support a huge amount of transactional trading while retaining a value that is extremely close to the \$1 peg. However, others completely fail to retain this peg as a result of poor design or insufficient dollar reserves.

To use stablecoins successfully in DeFi, it is therefore crucial that you understand how these mechanisms work and whether the \$1 peg stability is likely to be maintained.

Fiat-backed stablecoins

This is generally considered to be the most reliable mechanism for retaining a peg but this reliability comes at the expense of decentralization. Every stablecoin issued is backed 1:1 by a corresponding dollar deposited in a bank account controlled by the entity that mints the stablecoin.

Tether USDT is the dominant stablecoin of this kind, with a market size of \$52 billion as of Q2 2021. It is also the most liquid and heavily traded token among all cryptocurrencies. However, the true extent of the dollar reserves backing USDT has been questioned, with the New York State Attorney General concluding in February 2021 that the stablecoin was not fully backed.

USDC is the second-largest fiat pegged stablecoin and is owned by the Coinbase exchange and Circle Inc., under the CENTRE consortium. USDC dollar reserves are regularly audited and publicly reported. In 2021, Visa announced it will allow for transaction settlement with USDC on Ethereum, representing a giant leap towards mainstream adoption.

It is important to note that all major centralized stablecoin issuers retain the power to blacklist wallet addresses and have blocked wallets from using the stablecoin in the past when requested by law enforcement.

Crypto-collateralized stablecoins

These stablecoins are backed by the collateral of other digital assets.

DAI is the most well-known example and it was introduced in 2017 by the MakerDAO protocol. As per the rules of the MakerDAO smart contracts, DAI is backed by a basket of tokens, which includes ETH, LINK, YFI, UNI and fiat-backed stablecoins like USDC.

These stablecoins are usually highly over-collateralized, meaning the collateral value of the MakerDAO crypto reserves far exceeds the value of DAI that is issued. Unlike USDT and USDC, no central authority is able to blacklist DAI wallets.

Synthetic stablecoins

This category specifically refers to sUSD, a US dollar-pegged token introduced by Synthetix and backed by SNX holders. Platform users can mint sUSD tokens by staking SNX tokens and trading them against other synthetic assets.

The sUSD pegging mechanism is complex but essentially correlates the supply of sUSD with demand for the Synthetix platform. As with DAI, it is operated by smart contracts and cannot be centrally determined or blacklisted.

Interest-bearing stablecoins

These are stablecoin deposits which are earning interest.

Examples include cUSDC or aUSDC, which represent USDC deposited in the Compound or Aave protocols respectively in order to earn interest from lending. This category includes tokens with complex algorithmic components, such as yUSDC, which represents USDC deposited in the Yearn protocol and programmed to continuously reallocate assets to optimize yield.

Algorithmic stablecoins

This is a broad category of stablecoins that are not backed by an underlying asset. Instead they aim to maintain a peg through complex mechanisms of token minting and burning that are based on game theory.

Although algorithmic stablecoins may seem appealing because they can be established without the need for a collateral reserve, none have proven successful over the long term.

Seigniorage tokens like ESD, DSD and BAC have tended to lose their peg within weeks. Elastic supply algorithmic tokens like AMPL have managed to oscillate around their intended peg but have also suffered huge volatility.

Fractional-algorithmic stablecoins like FRAX have been relatively successful in maintaining their peg. However, this model is still partially dollar collateralized and therefore can't be labelled as a truly algorithmic stablecoin, even though it does still expose holders to algorithmic risk.

Token Standards

Token Standards

	ERC-20	ERC-721	ERC-1155
Proposed	November 2015	January 2018	June 2018
Officially Recognized	September 2017	June 2018	June 2019
What it does	Defines a common list of rules that all fungible Ethereum tokens should follow rules that all fungible Ethereum tokens should follow.	Allows the implementation of non-fungible assets within a smart contract.	Allows the implementation of various fungible tokens, non-fungible tokens, and semi-fungible tokens in a smart contract.
Token Creation	Create assets that have value and can be sent and received.	Create only one token in a single contract.	Create multiple tokens in a single contract.
Example	DAI, ETH, UNI	CryptoPunk, Sorare, Axie Infinity	Euler Beats

Source: [Consensys](#)



Token standards are the rules defining a token's properties and how it interacts with other tokens. The standards are important because they ensure compatibility, so that independently issued tokens and smart contracts can interact consistently and predictably.

The most common token standards on the Ethereum network are ERC-20 and ERC-721.

ERC-20

This is the most common standard and is the one used by the most well-known tokens on the Ethereum network, including USDT, DAI, UNI, SNX, LINK and YFI. ERC-20 provides a standard interface for fungible tokens, meaning the same sort of ERC-20 tokens are equally exchangeable with one another (i.e. 1 DAI token is exchangeable with another DAI token). Core DeFi tasks, such as staking and governance, follow the ERC-20 standard.

ERC-721

This is the standard for non-fungible tokens (NFTs), which are unique digital assets that are not equally exchangeable with one another. Digital art in the form of NFTs are the most well-known examples of ERC-721 tokens but the standard can be adopted for many other use cases. ERC-721 is also used for collectibles like trading cards, for characters or costumes in gaming and also to represent real world assets like lottery tickets or seats at events. Some well-known examples of ERC-721 tokens are Hashmasks, CryptoPunks and Axie Infinity.

ERC-1155

This standard enables the creation of assets in a smart contract, including fungible, non-fungible and semi-fungible tokens. It is sometimes known as a multi-token because it allows the creation of multiple tokens within the same contract. The main benefits of this standard are to reduce the fragmentation of tokens and to ensure better integration of fungible and non-fungible tokens, which are normally incompatible.

Liquidity pool (LP) tokens

As mentioned, many DeFi projects want to attract liquidity from cryptocurrency holders in order to enable the financial transactions at the heart of their business model. Therefore, when you start Yield Farming, you will start to deposit funds into liquidity pools in order to generate Yield.

Liquidity pool (LP) tokens act like share certificates for the funds you have deposited, giving you the right to withdraw your funds according to your share of the whole liquidity pool. This can be a disconcerting process when you do it for the first time, as you will confirm the deposit of funds and see your account has been debited for this amount. What is not immediately clear though is what you hold in return for this deposit. This is where LP tokens come in, as these are included in the same transaction.

In order to see the LP tokens you hold and therefore what share of the total liquidity pool you can redeem, you will need to inspect the transaction with a blockchain explorer. When you do, you will see the amount debited from your account and the LP tokens you hold. For example, if you were depositing into a Uniswap liquidity pool, you would hold UNI LP tokens that represent your share of the liquidity pool and therefore the proportion of trading fees from this liquidity pool that you are entitled to.

Most of the time, you can use these LP tokens to withdraw your funds whenever you want. However, some projects may limit withdrawals or add a fee for withdrawing funds outside of certain set parameters. Finally, it's worth remembering that each pool's tokens are unique, even if the assets within the pools are the same. Therefore, you couldn't exchange Uniswap LP tokens for SushiSwap LP tokens, even if both tokens represented a share of an underlying ETH: USDC liquidity pool.

Finally, it's worth noting that DeFiYield allows users to trade their LP tokens.

Vampire attacks

A vampire attack is specifically designed to drain liquidity from a DeFi project and is usually performed by a rival project in order to attract users during the early stages of development. This is possible because most DeFi protocols are developed as open source and permissionless projects.

While some projects try to attract users by offering better services, some well known DeFi projects have used vampire attacks where they simply replicated the functionality of a competitor and attracted users of the latter by offering better Yield Farming terms.

The well known examples include SushiSwap, which established itself as an Ethereum-based DeFi project by attacking Uniswap in this way, and PancakeSwap, which made a similar manoeuvre by attracting DeFi users on to Binance Smart Chain and away from Ethereum when the network's fees were very high.

DeFiYield Farmers need to be aware of vampire attacks because they can provide great opportunities that may only be short-term, if the terms that enable the attack are changed.

Black swan events

You may recognise the notion of a black swan event from your understanding of traditional finance. It is a metaphor used to describe an unexpected and often catastrophe event that few people predicted.

It is a theory developed by Nassim Taleb to explain the significant role that unexpected events have played in history. Essentially, the metaphor was used because black swans were not unexpected to exist and is often used to describe situations where humans' psychological biases make them unable to see rare events.

In the context of DeFi, a black swan event occurred on March 12 2020, when the price of Bitcoin crashed by roughly 50%. You need to understand the potential harm that a black swan event can cause and always ensure you have a margin of safety that will protect you from them, at least to some extent. Degens, who are high risk traders and investors who operate in crypto markets with little or no safety cushion, leave themselves open to being destroyed by black swan events.

Flashbots

In April 2021, following months of spiralling network gas fees on Ethereum, that even led many to question its longer term viability, some then argued that an important innovation by the Flashbots research organization was responsible for achieving a stunning recent reduction of gas fees.

The MEV Problem

Flashbots offer a solution to the critical inefficiencies of “miner extractable value” (MEV). MEV is sometimes referred to as crypto’s version of Wall Street frontrunning, and also a, “systemic risk to consensus-layer security and a realistic threat to Ethereum today.”

Specifically, MEV measures the profit a miner can make by the process of including, excluding, or reordering transactions in the network blocks they produce.

That process was previously operated by Priority Gas Auctions (PGAs), which have been described as a kind of “all-pay open auction”. Miners naturally prioritize the transactions offering the highest gas price, however the open nature of PGAs made them gameable by arbitrage bots, which constantly bid up gas fees in an attempt to frontrun other pending transactions.

That had the effect of spamming the entire Ethereum network, which in turn, raised gas costs for all network users. That mass frontrunning effort was also responsible for creating key inefficiencies of blockspace usage and network congestion.

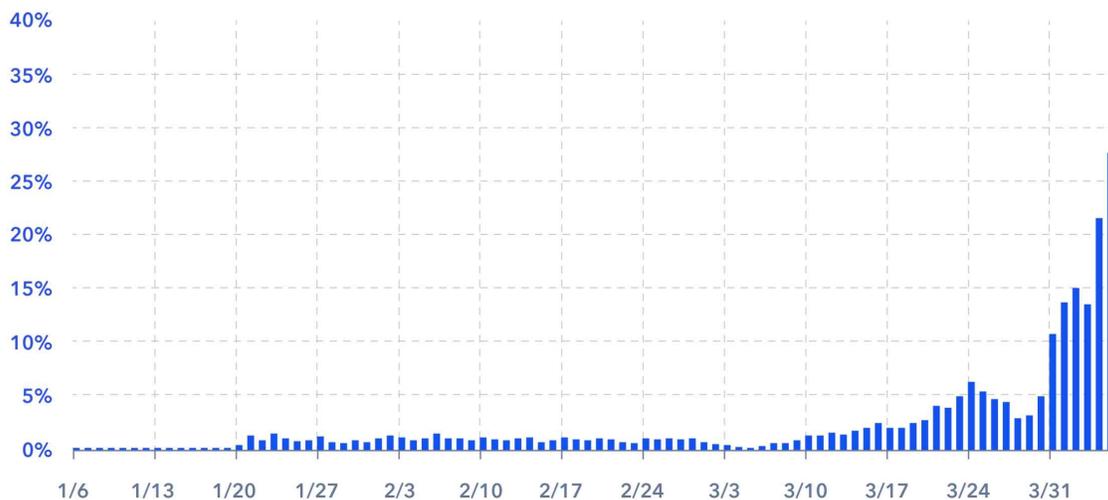
According to Flashbots, “MEV risks becoming an insiders’ game,” whereas they aim to, “Ensure both small and large participants have equal access to low-level financial primitives and that core Ethereum properties are preserved.”

The Flashbots Solution?

Instead of an open, all-pay auction, Flashbots introduces more of a ‘sealed-bid’ model that enables zero gas transactions - but requires a separate fee sent directly to miners upon transaction completion. Flashbots provides a communication channel between traders and miners to allow those inefficient gas bidding wars to occur off-chain now instead.

As of March 2021, at least 58% of Ethereum network hashrate was reported to have become accountable to flashbots. Arguably, this innovation may prove more impactful on gas fees than the more highly anticipated Ethereum EIP-1559 updates.

% Ethereum blocks with flashbots bundles included



Source: [Consensys](#)

THE DEFI INVESTOR RULEBOOK

How do different investors assess DeFi opportunities?

That's the question that will be answered in the following section, as we set out definitive rules for DeFi investing. Whether you want to gradually and carefully increase your exposure to a new class of assets or boldly seek out the most rewarding opportunities for yield generation, this guide will cover all you need to know about DeFi investing.

Before we look at various investment rules that different investors should stick to though, we need to be clear about what are three main types of DeFi investors.

Three types of DeFi investors

Some investors are comfortable with a small amount of risk exposure in order to generate some returns, others are ready to take on a huge amount of risk in order to potentially increase their returns by an enormous margin. Depending on the risk level taken, all investors can be classified into three main investor types.

The cautious investor

The cautious investor wants exposure to DeFi because they see there is an opportunity to generate yield and they realise that this new industry has a lot of growth potential. At the same time, they are very conscious of the risks that are inherent to any emerging market and do not want to over expose themselves.

They see the best way of doing this is by investing in the most 'blue chip' projects, which have been around the longest, have the most users and are the most battle tested. They also believe they need to move cautiously, doing as much primary research as they can before they invest in any opportunities.

In general, they will only a minority of their overall digital asset holdings to defi and expect steady but not spectacular returns as a result

The risk-on investor

The risk-on investor is more excited about the potential returns that DeFi offers than the cautious investor and wants to dive deeper into this new industry. They are not comfortable with just dipping their toe in and want to investigate the opportunities for Yield Farming (which is explained later) that DeFi offers.

In this respect, they are far more open to a wider range of smaller projects than the cautious investor. At the same time though, they will definitely go through a research process for everything they invest in and they remain wary of the most risky projects.

In general, they are likely to be willing to put at least half of their digital asset holdings to work and are keen to generate healthy returns for doing so.

The degen investor

As the name suggests, a degen or degenerate investor is totally enamoured by the potential returns available in defi and is willing to risk it all in order to return life-changing amounts.

They do not restrict their potential investments in any way and are willing to go all in (or “ape into”) even the newest and most unknown protocols. Speed is of the essence for this investor, so they don’t have time to do lots of upfront research on the team behind a protocol or the risks that a smart contract might pose. All they care about is APY.

In general, a degen investor is not only willing but feels it is imperative to dedicate all their digital asset holdings to Yield Farming, even if they risk losing it all. One important thing to remember about operating in degen mode is that it is only really possible during the bull run part of a cycle.

Approaches for investing in DeFi

The following table provides a quick overview of the three main types of DeFi investors and approaches they take when assessing various investment indicators.

		Investor Behaviour		Part 1
Investment indicator	Cautious	Risk-on	Degen	
Size and capitalization	Only considers the top 100 protocols by market cap and the top 15 by Total Value Locked.	Only considers the top 300 protocols by market cap and the top 25 by Total Value Locked.	Will consider any protocol with a Total Value Locked that allows them to ape into it.	
Sufficient volumes	Wants to see minimum daily volumes of \$1 million, so that large positions of over \$100k can be disposed of.	Wants to see average daily trading volumes during the previous 20-30 days of \$200k, so a \$20k position can be liquidated without slippage.	Does not consider this to be an important indicator.	
Platform stability	Will undertake a comprehensive check of the protocol's social media and website.	Will undertake a check of the protocol's social media and website.	Will skim through a protocol's social media and website.	
Cyber security record	Will read the auditor's report from back to front.	Will perform a basic search for suspect functions.	Generally doesn't care much about this.	



		Investor Behaviour		Part 2
Investment	Cautious	Risk-on	Degen	

indicator	Cautious	Risk-on	Rege
Team record	Will perform a comprehensive check of each team members' record.	Will perform a quick check of the key members of the team to see if they've been involved in previous projects.	Doesn't know or recognise any of the team and doesn't care.
Impermanent loss	Will perform a deep review of the impermanent loss risk and use tools within DefiYield to forecast various scenarios.	Will use their basic understanding of Impermanent loss to assess what effect it might have on yield farming returns.	May not understand impermanent loss and doesn't care about it.
Investment timeline	Likely to remain involved in any single investment for over a year.	Likely to remain involved in any single investment for a few months.	Likely to remain involved in any single investment for a few weeks.
Calculations	Undertakes accurate calculations, such as those to measure the real APY that includes gas fee deductions.	Makes some basic calculations to assess whether the advertised APY makes sense.	Focuses on the advertised APY and rarely considers further calculations.
Budgeting	Will not deposit more than 5% of their net worth in a single platform.	Will not deposit more than 17% of their net worth in a single platform.	Keen to deposit 100% of their net worth in a single platform.
Expected APR	On average, 5-15% return on stablecoins.	15-25%+	Over 150% APY.

Investor Behaviour

Part 3

Investment indicator	Cautious	Risk-on	Degen
Likely investments	Tier 1 lending and borrowing platforms and protocols. For example, Aave or Compound Finance (decentralized) or Blockfi (centralized).	Tier 2 lending, borrowing, exchange and money market protocols and platforms, such as Cream Finance or Venus Finance.	Mostly new and emerging markets, including newly generated tokens and newly created platforms or protocols.
Cost considerations	Transaction costs, including network fees and platform fees, need to be considered. This is particularly true when interacting with the Ethereum network.	Transaction costs, including network fees and platform fees, need to be considered. This is particularly true when interacting with the Ethereum network.	Smaller investments over shorter time frames mean it is essential to keep track of the transaction costs, which can cause expenses to override potential returns.
Risk considerations	Depends on an individual's risk appetite, however it is not recommended to go over 30% of a digital asset portfolio.	Depends on an individual's risk appetite but an entrepreneurial DeFi user may not want to allocate more than 50% of their digital assets to this approach.	Degens go all in during a bull run but even then they should only risk what they can painlessly afford to lose. Alternatively, degen 'mode' can be used for 5% of a portfolio.



This summary is a useful reference point to return but, if you are uncertain about the areas called investment indicators, there are fuller descriptions available below.

DeFi investment indicators explained

There are many ways to assess a DeFi investment opportunity. In this chapter, we will consider the most fundamental ones. Some of the terminology used for these investment indicators may be new to you, so they have been described in more detail below.

Size and capitalization

While there is no guarantee that a large project will not crack, top projects by market cap and Total Value Locked (TVL) might be worth attention. A project with \$1 billion TVL has clearly earned a significant amount of trust amongst market participants already and investors can use this fact to assess the risk involved.

Platform stability

Passive income products in DeFi usually come with a warning that the rates are unstable, that high returns should not be expected over the long term and that funds should not be left unattended. Therefore, it's advisable to research the historical performance of such products, as well as the levels of TVL in specific vaults or pools and the reward token's performance in the market.

Cyber security record

It is vitally important to assess the safety of locking funds in a specific product. To do this, you can assess:

- Existing audits of the platform and the smart contracts it uses
- Any exploits identified, including external attacks or internal project vulnerabilities
- Responses of the project team to such attacks, such as patches or code updates
- Code reviewers' and auditors' background, to assess their reputation

Team record

Reviewing the background of the team is important because some team members could be involved in scam projects in the past. Most probably, they would use their fraud experience and previously stolen funds to create hype around the new project in order to steal again.

In addition, it's a good idea to stay away from anonymous projects, which have had their smart contracts deployed with a wallet funded via a mixer like Tornado Cash.

Terms of liquidity pools

Before adding liquidity to any pool, you should make sure to understand all major risks involved, especially how impermanent loss can affect your funds. DeFi AMMs are truly innovative in the way they make it possible for anyone to create their own market and set out the rules of trading within it. Therefore, if you are providing liquidity for a market, you should review its terms, including the transferability of pooled assets.

Impermanent loss

If you provide liquidity to a pool with at least one volatile token, it is smart to research what can happen if its price spikes or collapses. Newly created liquidity pools and the investors who provide liquidity for them are vulnerable to arbitrage and trading bots. The latters are usually set up to buy a token when a pool is created in order to dump it later.

The risk of impermanent loss is covered in detail further in the book.

Investment timeline

Rewards, risk and time - the three fundamental features of investing. The importance of selecting the right timeline for investment strategies in Defi is even bigger than in traditional finance, as DeFi is highly volatile and unpredictable due to its immaturity.

When choosing an investment timeline, it's important to understand industry-specific developments and cycles. With DeFi in a rapid growth and innovation cycle that involves massive inflows of development capability, a project may be considered well established even if it has a positive track record of just six months.

Annual Percentage Yield (APY)

In DeFi, the most common way to evaluate returns of an investment opportunity is by looking at its APY - annual percentage yield. This metric shouldn't be confused with APR - annual percentage yield that reflects the simple interest rate, while APY stands for the rate impacted by compounding of the interest. To put it simply, when calculating APY, the

interest is applied not only to the investment amount, but also to all previously accumulated interests.

It should be remembered that APYs declared by DeFi projects can be highly volatile, depending on a range of supply and demand conditions within the crypto markets.

Additional areas of DeFi investment research

Once you have understood the general principles behind how yield can be farmed from different projects, it's time to start assessing individual projects to see where the best opportunities exist.

Essentially, this is a process of comparing different projects by weighing the yield that can be obtained against the risks that they might pose. To do this, you should assess the following features.

Product value

The most important thing to consider when assessing a project is the nature of its token and whether the token adds value to the project or is just a speculative asset that isn't really necessary.

Another thing to consider is whether the project's launch has contributed or could contribute to the growth of the DeFi market, or whether it introduces new features that improve the user experience for Yield farmers.

To assess a product's value, you should therefore consider:

- The problems that the project solves
- What differentiates the project from existing solutions
- The attractiveness of its reward system
- The transaction speeds involved
- The amount of fees paid to the platform
- The availability of voting rights
- The variety of token pairs
- The offered asset staking ratios

One example of how you might assess product value based on some of these areas is by comparing a project that utilises the faster transactions and lower fees available on Binance Smart Chain as compared to the Ethereum blockchain.

Opportunity cost

Yield farmers always need to be aware of the opportunity cost of either taking or passing on a particular Yield Farming opportunity.

Factors that are worth considering are things like how much you have to invest in the first place. For example, if you have \$10,000 to invest, you might find that the opportunity cost of implementing a complex or diverse

strategy that incorporates many smart contract interactions and levies the related fees just isn't worthwhile.

The same might be true when you are considering utilizing an automated asset manager in order to generate Yield. In this situation, it would make sense to consider the opportunity cost of doing so on the Ethereum blockchain vs an alternative blockchain.

Smart contract security

I discuss smart contract security at length later on in the section on 'how to stay safe while Yield Farming' but it's worth mentioning some key principles that are worth understanding here.

Firstly, it's crucial that you do not let a project's extraordinary APY distract you from what might be clear security holes or code weaknesses in the smart contract. You must always ensure that there are no suspicious functions in the code that allow project founders or development teams to exert too much control over user funds or to influence token prices.

Team credibility and public profile

While all projects probably should aspire to decentralized governance where individual founders, developers or investors don't matter and all you need to trust is the code, the reality is that these details within a project's structure still must be assessed.

Building a Yield Farming platform requires a lot of skill and deep technical knowledge, not only of blockchain technology but also of financial markets. Therefore, you should be looking at whatever evidence is available that demonstrates the project you are weighing up has experience in all these areas.

Moreover, it's important to understand what the project is doing in terms of its marketing, public relations and communications strategies and whether these suggest it is one that can be trusted. You should try to see how it behaves in public, what its team has done before and whether it is sticking to a roadmap, in order to decide whether its actions support its ambitions.

WHAT IS YIELD FARMING?

Let's begin with a short description of what Yield Farming is and then work through different topics within this description, in order to build a better picture of this important trend.

Yield Farming is the process of staking digital assets for a period of time to a variety of DeFi contracts they utilize in order to receive returns (or 'yield') in the form of additional digital assets.

Depending on your crypto experience, this statement will either make a lot of sense to you or not much at all. If you're in the latter camp, the first thing to do is reference the glossary at the back of the book for some descriptions of specific terms. This is a good habit to get into when you come across any terms you don't understand or can't remember throughout this book.

In addition, this chapter is focused on explaining what Yield Farming and related terms mean, so you start your journey with some solid foundational knowledge. We'll look at the specifics of what DeFi is and what Yield Farming is. We'll also look at where this exciting trend came from and how it has evolved in its relatively short existence so far.

To start off though, let's look at how Yield Farming fits into the wider crypto industry that has developed over the last ten years, so we can build understanding of why this trend matters.

How does Yield Farming fit into DeFi?

Yield Farming, which is also sometimes referred to as liquidity mining, is a small but growing trend within the DeFi industry. It really took off during 2020 but we can trace its origin back to September 2018 when Compound, a decentralized lending and borrowing protocol on the Ethereum blockchain, released a smart contract that kicked off the whole Yield Farming concept.

Yield Farming is possible because of some key market dynamics that are present within DeFi. One of the most important is that projects, which operate decentralised applications (or Dapps) made up of various smart contracts, may want to hold quantities of a given cryptocurrency in a smart contract for a number of reasons, including to provide an exchange market for this cryptocurrency or to lend it out to borrowers.

Of course, cryptocurrency holders are unlikely to stake their funds by depositing them in a project's smart contract (particularly a very new one, which may not have been audited) without being incentivized to do so. This is where Yield comes into action.

In return for depositing their funds to smart contracts and having these funds 'locked up' in there for a set period of time, the original holders are rewarded with additional digital assets. This is the Yield they receive and the 'Farming' part comes from finding and utilising various opportunities that different projects offer.

One final point to remember about Yield Farming is that it's often a high risk/high reward activity to get involved in. There are many scammers out there who are looking to entice cryptocurrency holders into depositing their funds, only to steal what's been invested and disappear without a trace. It's therefore important to be aware of these dangers and to access the knowledge of Yield Farming experts to stay safe.

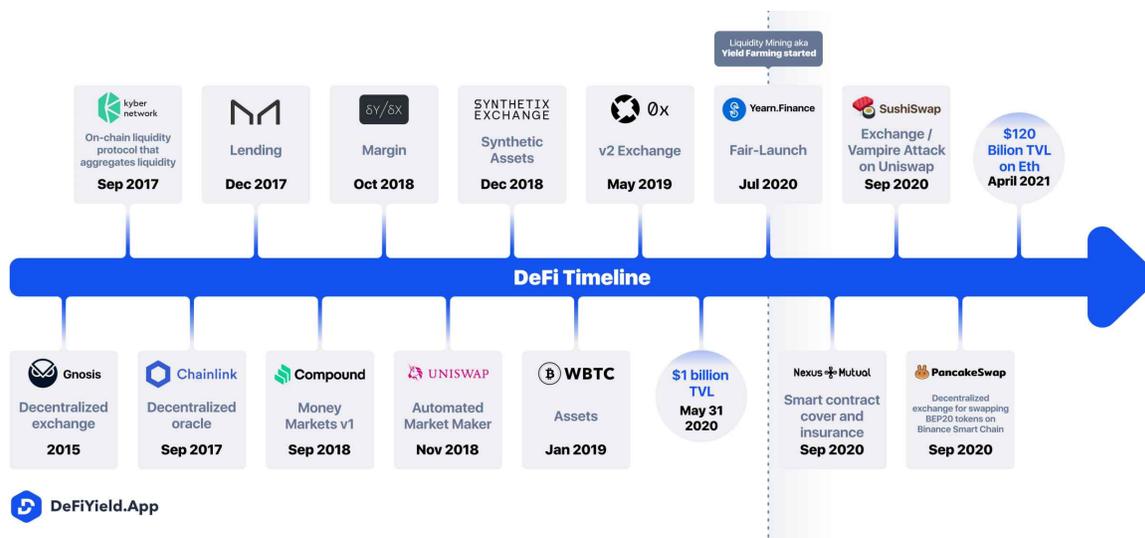
This is the DeFiYield way.

Where did Yield Farming come from?

Yield Farming really came onto the crypto community's radar during 2020, with the introduction of governance tokens. However, this momentum had been building since September 2018, when Compound Finance released its protocol that enabled the Yield Farming industry to spawn.

A lot of innovation had happened in the wider crypto and blockchain industry to enable the release of this important protocol. We will turn to these significant stages later but first, it's worth understanding why Compound's work matters and what happened afterwards to get us to where we are today.

The Compound Finance protocol that was released in September 2018 enabled what traditional finance might refer to as a money market fund. Cryptocurrency holders would put funds into the protocol in order to lend them out or borrow cryptocurrencies.



Depositors would then be rewarded for lending their funds. This would come from the interest that borrowers paid the smart contract in return for the loans that were lent out. This interest that cryptocurrency holders could earn from lending their funds is the first form of 'Yield' that can be said to have been 'farmed'.

Yield Farming has moved on a long way from purely earning interest by lending your funds to liquidity provision, and I'll discuss these in detail later in the book. Also, Compound is not the only DeFi protocol that plays a role in Yield Farming (not by a long shot). However, it is a very important one to

understand because it has played a significant role in the development of the industry and been at the heart of some key milestones.

Apart from the protocol launch in September 2018, another of these milestones came in June 2020, when the COMP governance token was launched. Governance is an important concept to understand in Yield Farming and is another topic I will discuss in detail later.

For now it is worth understanding two important points about it. Firstly, why a project launches and distributes a governance token and, secondly, what it means for the evolution of Yield Farming.

The main reason projects give away governance tokens is to become more decentralized. It allows them to distribute their decision making power to a wide range of different entities. The reason this matters to Yield Farming is because the distribution of governance tokens became a new form of Yield to farm.

Why would a farmer consider it useful to receive Yield in the form of governance tokens? Essentially because they view owning a share of the governance of a project (which is what a governance token represents) as valuable, either now or in the future.

A simple way to understand these benefits is to make the link between how a cryptocurrency investor might see value in holding a governance token and how a traditional investor might see value in holding shares in a company. One reason why traditional investors see shares as valuable because they represent a share in the governance of the company, just as a governance token represents a share in the governance of a project.

While I'll explain governance in more detail later, it's worth layering on a little more detail to this simple analogy by looking at another noteworthy Yield Farming project, Yearn Finance. Even though Compound introduced a governance token first, Yearn Finance took the distribution of its governance token to a whole new level by instigating a 'fair launch'.

This meant that all tokens were made available to buyers and participants in the project, rather than being held back for founders, team members and privileged investors. The aim was for full transparency, full decentralization and open governance. This not only had a short-term positive effect on Yield Farming opportunities but also on how DeFi projects have either developed or stalled ever since.

Many of the best known Yield Farming projects we will cover later in the book launched and distributed their own governance tokens and I'll explain what you need to know about these later on.

What's most important to note at this point is that the introduction of the governance tokens provided a new form of Yield and was an important milestone in the progress of Yield Farming because it kicked off a lot of 2020 hype. Now, the hype cycle has turned towards algorithmic stablecoins, which I'll explain in more detail alongside the other essential elements of Yield Farming.

Developing an in-depth knowledge of every aspect of DeFi and wider crypto markets is both unrealistic and unnecessary if your aim is to start Yield Farming as soon as possible.

At the same time though, jumping in before you have at least understood some key concepts and market dynamics is likely to leave you more open to scams than you need to be. In the following section, I want to build on the backstory I've already provided about where Yield Farming fits into DeFi and crypto by briefly introducing some topics you need at least a basic understanding of.

As with all areas of crypto, we encourage you to do more research on any areas that you find difficult to grasp and to continue building your knowledge on an ongoing basis.

Types of Yield Farming

Keep in mind that Yield Farming is essentially a process of finding the best returns for your assets from a range of different projects. The returns are the 'Yield' and the finding is the 'Farming'.

There are four main types of Yield Farming you need to understand, which are explained in detail below. They involve locking your assets up for a period of time in a smart contract, so it can use them for whatever it needs before passing them back to you. It's therefore a good idea to have some understanding of why a project would incentivise you to lock your assets in one of its smart contracts and what it will do with them once it has.

You should also be aware that these types of Yield Farming are often interconnected in a way that makes them far more attractive than traditional financial products. A Yield farmer might assess a potential opportunity and conclude that it can provide Yield from lending fees, liquidity provision, governance tokens and other types of token distributions.

This can be seen in examples such as Compound on Ethereum and Venus on Binance Smart Chain, where lending and borrowing may be incentivised by the protocols' token distribution.

Yield from lending

Lending and borrowing is a simple concept to understand when it comes to gaining a return on your assets. Throughout history, people have lent money to others in order to generate Yield. The Yield comes from the interest rate borrowers pay for getting the money.

This concept is no different in DeFi, it just doesn't require the lender and borrower to have a direct relationship. In DeFi lending protocols, such as Compound and Aave, you can view the interest rates you will be offered for lending or borrowing money by simply visiting their websites. Then it's just a matter of allowing the DeFi protocol to interact with your metamask account and agreeing to the terms.

There are some key differences between DeFi lending and the same process in traditional markets. DeFi loans are generally heavily collateralized on the borrower's side, meaning the borrower needs to put down quite a lot of collateral in order to borrow funds themselves. This

makes the transaction safer for the lender. Moreover rates for borrowing and lending are set automatically by smart contracts, based on how many assets are demanded to be borrowed and are available to be lent at one time.

This demonstrates the automated and trustless nature of these lending markets, which are based almost entirely on smart contract code interactions rather than individuals risk assessing other individuals.

Yield from providing liquidity

Providing liquidity to a project is a slightly more complex use case to understand than lending and borrowing, but it does have some similarities and should be fairly easy to grasp once you understand players involved.

Essentially, projects like Decentralised Exchanges (DEXes) need to be able to access enough liquidity in a variety of assets for users to be able to trade and exchange these assets. As decentralized projects, they probably wouldn't want to hold these assets themselves and, even if they did, they probably couldn't hold vast quantities of assets required to provide these liquidity pools.

Therefore, they borrow a concept from the traditional finance world and tweak it to the needs of the decentralized one. A market maker in a traditional finance market does as the name suggests, they 'make' a 'market' for a pair of assets (for example, USDT and ETH) by holding enough of these assets and always being available to trade them when a user wants to.

In the decentralized finance world, these market makers become automated market makers (AMMs), which are large pools of asset pairs orchestrated and adjusted by smart contracts to reflect a mid-market price for the asset pair. This automated price discovery process is essentially brought about by arbitrageurs identifying a discrepancy between the price offered by a pool and the price offered by another exchange, and then buying or selling the assets in the liquidity pool to take advantage of this opportunity.

However, this relatively technical process doesn't need to be understood in depth to understand liquidity provision within Yield Farming. More important is the question of where these automated pools of liquidity come from?

This is where the individual asset holders, such as Yield farmers, come in. Projects incentivise individuals to deposit and lock up their assets into liquidity pools for the specific purpose of providing liquidity. In return, the depositors receive a portion of fees that are paid out to this liquidity pool by traders wanting to buy or sell the assets in them.

Yield from governance token distributions

As mentioned previously, governance tokens are a unique innovation that has developed within decentralised finance. They provide different rights, privileges and advantages depending on which project they relate to but, in terms of Yield Farming, they all provide the potential for additional returns.

That's because many projects, in deciding to decentralize their governance, have chosen to distribute governance tokens to their users. In some cases, this means to anyone that has ever used the project for borrowing, trading or whatever services offered. But, in many cases, distribution of governance tokens is specifically attached to liquidity provision or asset lending and borrowing.

Therefore, Yield farmers can and should consider distribution of governance tokens when defining the overall Yield that a project offers. One thing that's important to note here is that governance tokens are very much in their infancy and therefore can be difficult to value in terms of returns they provide. While some governance tokens give holders the right for fees accumulated by the projects, others are less clear about the real returns that will be provided.

In this respect, many should be thought of as speculative. For example, holding the governance token for Uniswap - UNI - does not currently entitle the holders to any fees from the platform. However, they do provide voting rights on governance issues and treasury distribution, so it's conceivable that holders could accumulate them through Yield Farming and play a role in deciding to add a specific fee collecting feature to the token in future.

Yield from other token distributions

There is one more notable type of Yield Farming worth mentioning and that involves the returns you can generate from project tokens that do not hold any governance value.

Tokens might be issued for all sorts of reasons that do not relate to governance, including enabling transactions within a project ecosystem or

representing synthetic value of an off-chain asset. You might decide these tokens hold some intrinsic value, either now or in the future, and decide to farm them to generate Yield.

Alternatively, you might not see much intrinsic value in a token at all but still decide that its price will rise and decide to farm it so you can sell it at a future date. All of these potential outcomes should be considered when assessing different Yield Farming opportunities.

Advantages of Yield Farming

By this point, you're probably sold on the idea of Yield Farming but it's worth recapping why this new industry offers such a great opportunity, particularly against the wider macroeconomic backdrop that is overshadowing traditional financial markets.

Yield Farming with DeFi projects provides advantages over traditional investments now, but it also gets you involved in the industry that has plenty of room to grow.

Higher returns than in traditional finance

While APY that you access through Yield Farming depends entirely on DeFi platforms you choose to engage with, all opportunities compare extremely favourably to APY available in traditional investments.

As a rule of thumb, token pairs that feature the highest price volatility offer the highest potential returns. The APY range of liquidity pools that are present on the top 10 DeFi platforms can reach up to 900%, but this is mainly when we are experiencing a bull run. In comparison, APY offered by traditional investments starts from around 0.1% and rarely goes higher than 5%, even when invested in the riskiest venture capital projects.

When you consider that the average inflation rate is around 2%, most traditional investments are losing value over time. This makes Yield Farming a great opportunity for anyone looking to increase value of their assets in the short, medium and long term. For up-to-date information on the latest APYs of various Yield Farming projects, check out [DeFiYield.App](#).

Different risk levels for different risk appetites

Yield Farming liquidity providers can choose liquidity pools that reflect their risk appetite and profit expectations.

For example, if you are more comfortable with achieving moderate profits that are lower risk, you can deposit money into less volatile token pairs involving stablecoins, such as USDT, USDC and DAI.

Of course, you could avoid all Yield Farming and smart contract risk by custodying your crypto with a company like BlockFi, a licensed business under the New York regulator, and gain some limited Yield from doing so.

Coinbase Custody or Genesis Trading provide similar solutions for institutional investors too.

However, this isn't the DeFiYield way. If you're ready to take the highest risks for spectacular returns, your requirements can be met by liquidity pools that contain volatile or heavily hyped tokens.

Furthermore, investors can maximize their passive income by using automated solutions that rotate funds in search of higher returns. They can also set different strategies that reflect their short-term or long-term goals, rather than be tied into low Yielding traditional assets with set minimum terms.

No intermediaries

Yield Farming proceeds in accordance with terms encoded in smart contracts that run on a blockchain, meaning it allows for noncustodial financial activity with no intermediaries involved.

There is no need for a third party to control acceptance of funds, to choose where these funds are invested, to conduct transactions or to ensure investment terms are followed. This absence of intermediaries reduces the cost of making investments, meaning returns can be more evenly weighted towards the investor rather than service providers that proliferate traditional financial markets.

In Yield Farming, liquidity providers only pay transaction fees in the form of gas to the blockchain where a project exists.

No suits

Most ordinary people are completely excluded from interacting with traditional financial markets and institutions that control them. This world can seem like an impenetrable playground for wealthy bankers in their flashy suits and ivory tower skyscrapers. DeFi is the complete opposite.

Whereas someone with \$1,000 to \$10,000 would be given short shrift by asset managers in his bank and told to join the queue of regular customers, that same person is empowered by the gamification and community-driven atmosphere of DeFi to manage the funds on his own.

By interacting with DeFi projects and smart contracts they are based on, investors can not only feel they are independent from intermediaries, but

also engage in an enriching experience with like-minded peers rather than aloof and dismissive elites.

Accessibility

For individuals who may have found the range of traditional finance products they can invest in restricted by regulations or a lack of financial institutions where they are based, Yield Farming opens up a unique opportunity to make meaningful returns in freely accessible markets.

The only things these investors need are internet access and funds. Even as a liquidity provider, they can start with any small amount of funds and add to their investments as they become confident from learning more. In this way, Yield Farming is making investing much more accessible for many people around the world.

Diversity of platforms

The variety of Yield Farming protocols means that investors can select and adjust investment strategies so they are based on the most up-to-date information about the global financial market or cycles within the cryptocurrency industry.

Although Yield Farming is at an early stage of its development, it already includes an impressively diverse array of DeFi platforms that are all striving to provide innovative reward strategies and optimized user experience. For example, new liquidity pools are constantly being added with varied token ratios to optimise against impermanent loss and increase customization of risk strategies.

Furthermore, we are seeing the spread and diversification of DeFi and Yield Farming onto other blockchains than Ethereum, with Binance Smart Chain being a notable example.

Composability

One of the greatest steps forward that decentralised applications have made in the last couple of years is becoming composable elements of a hugely enriched blockchain ecosystem.

DeFi protocols are often compared to Lego pieces, and a shared settlement layer like Ethereum allows these protocols and applications to interconnect. Therefore, automated asset management projects can make

use of decentralized exchange projects or achieve leveraged positions through credit monetization projects.

Two or more pieces can be combined or forked in so many different directions to create a mesmerising petri dish of financial innovation that reveals something new on an almost daily basis. Anything that has been created before can be used by any entity, and this flexibility allows for an ever-expanding range of possibilities.

Fast growth

Even though some investors have benefited from Yield Farming already, the industry has plenty of growth potential due to the fact that it provides a great alternative to traditional savings accounts and lending services.

The foundations that have already been laid will serve as a base for further innovation and infrastructure improvements in the coming months and years. These might include:

- The emergence of advanced Yield DeFi platforms, which utilize multi-chain mechanisms and follow higher security standards
- The demand for code security stimulating more auditing agents coming to the market
- More complex investment strategies being invented and spread across the Yield Farming community
- Further development of multi-chain platforms, which operate using less gas
- Better communication with project teams, including them giving detailed instructions on smart contract operations and the steps involved in staking funds

Collectively, the work of the close knit Yield Farming community will result in better security and higher returns for all its members.

Disadvantages of Yield Farming

Nobody said that Yield Farming is easy.

The reality is that big rewards come with big risks and anyone that ignores the latter part of this balancing act is likely to get burnt. The market is constantly being flooded with new projects and new information, the sheer weight of which is almost impossible to track single-handedly. Furthermore, Yield farmers have to simply accept that there are inefficiencies that must be dealt with in what is still a very immature industry.

Understanding disadvantages of Yield Farming will help you to ensure you maximise benefits that you reap.

UX Barrier

Even though one of the great advantages of DeFi Yield Farming is that it is open to anyone who wants to take part, there are still accessibility issues in terms of the user experience (UX).

This is an issue not only because many DeFi protocols employ poor UX design but also because users will often need to understand tools like Metamask to get started. In order to solve this problem, DeFiYield has developed a range of tools with simple and easy to follow UX that are perfect for new entrants to DeFi.

Volatility of cryptocurrency markets

One of the most obvious realities that every Yield farmer must accept is that cryptocurrencies remain highly volatile assets, the value of which can change quickly and violently. This is significant when your strategy is based around locking your assets in a smart contract for a finite amount of time, as you can be exposed and unable to respond to these changes. For example, if prices of tokens in the trading pairs you provided liquidity to shift significantly in secondary markets, you might well find that your investments drop dramatically in value.

Complexity of smart contracts

As mentioned previously and discussed in depth later, checking and understanding staking terms that are encoded in smart contracts is a crucial part of ensuring investment security. Unfortunately, a lot of Yield

farmers don't understand smart contracts they use and don't bother to find comprehensive reviews or audits about projects they select.

However, DeFiYield is the only platform that audits every single project before listing it. This approach allows to add an additional layer of security for DeFi users.

Reliance on gas prices

Although all Yield farmers can hopefully look forward to a much more benign gas price environment once Ethereum 2.0 is fully functioning, they still have to deal with high gas prices now and for some months ahead.

That's because most Yield Farming projects are using Ethereum 1.0, which is based on a proof-of-work concept called Ethash that involves miners validating new transaction blocks and being rewarded for this with fees paid by network users. Miners are of course interested in higher gas prices so, when the network becomes congested, miners decide to validate transactions that are paid with the highest gas prices first.

Put simply, liquidity providers have to pay higher and higher fees just like anyone else using the network, which can make the real returns of any liquidity provision a lot less appealing.

However, the benefit of using Binance Smart Chain or Huobi Chain in the meantime is that there is no need to deduct gas fees from the advertised APY. Also, the DeFiYield cross-chain asset management dashboard provides precise calculations of Farming rewards across chains, which includes gas fees as well as a range of other cost/return metrics.

FUD, rumors and outright lies

As you start to Yield farm, you'll notice how many other investors focus so much of their attention on the most hyped projects, even if they aren't really bringing a lot of value into the industry.

A lot of Yield Farming platforms are actively promoted and discussed by the community, even though those, doing the talking, haven't properly analyzed their economy, token utility, code security or project development plans.

From my own experience, I can tell you how hard it is to avoid getting wrapped up in a FOMO cycle, but you must remain logical in your analysis and conduct your own comprehensive research.

Scam projects abound

The Yield Farming industry is growing extremely fast and a lot of new projects are entering the market every day. Unfortunately, a lot of them are scam projects that use the FOMO mentioned to distract investors from doing proper due diligence before they put their funds in.

As a result, we see cases like Unicat, Compounder.finance, Groot, SuperMarioBros and others defrauding investors of millions of dollars worth of assets. Identifying scams is covered later in the 'how to stay safe while Yield Farming section' but you can also always refer back to our comprehensive database of scam projects and check whether something is too good to be true.

DeFiYield Safe is the one and only solution that is mitigating the risk of scams to keep Yield farmers safe.

The DeFiYield database of scams, which is the largest of its kind, has been developed to ensure our users and the wider community can avoid fraud projects. The scam database is available alongside the bug library, automated smart contract checker and audit database that exist in DeFiYield Safe, a unique machine learning tool that detects and alerts users to approvals of malicious smart contracts.

Hacker attacks

One of the main reasons that we advocate smart contract audits is because, when they are not performed, investors are not warned of possible hacker attacks or system errors that can result in rug pulls.

If a protocol stops running properly, the financial information encoded in it gets lost along with all the funds invested. But even if the code weakness is found by the dev team in time and an attack is prevented, the project tokens might well still dump because rumors about the risks spread and investors lose trust in the project.

Fraudsters might go unpunished

Cybercrimes are always extremely hard to control due to innovative ways that hackers attack and the absence of a single jurisdictional power that can find and punish them.

Yield farmers should always be aware of this risk, and proper due diligence will help to ensure they are not caught up in a hacker's schemes. You can also rest assured that DeFiYield is at the forefront of ensuring hackers are not able to get away with their attacks, as demonstrated by our investigation into Compunder.finance that we detail later.

In fact, with our publishing of deep research in this area, we are the only project that is truly busting the scammers.

Yield Farming risks and mitigation strategies

Risks are always evolving and emerging in Yield Farming, so the principle of “research in depth before taking action” must be followed at all times and used to constantly increase your knowledge base.

This foundational awareness of scams and other risky characteristics is what we have built up and continue to improve on at DeFiYield. This section looks at some of the most common risks we’ve seen and shows you how to avoid them.

Funds liquidation risk

You need to be particularly aware of this risk if tokens you are lending out or providing liquidity with were borrowed using other tokens as collateral. If the price of the collateralized tokens drops by a certain amount, this might mean the leverage threshold has been reached within the borrowing transaction and the collateral is liquidated.

A simple example might be borrowing BTC and collateralizing this loan agreement with ETH. If the price of ETH drops, the value of BTC in relation to ETH increases, which means the borrowed BTC amount becomes increasingly leveraged against the underlying ETH collateral. If the leverage threshold has been breached, the ETH will be liquidated to cover the value gap.

In most cases, this threshold is 75% and, if breached, collateralized funds are liquidated. Therefore, it’s crucial to monitor prices of collateralized tokens you use for any transaction.

One way to mitigate this risk is by using advanced price tracking technology, which allows you to remain informed about potential price changes and react to liquidation threats.

Another approach to controlling liquidation is using stablecoins as collateral. Depending on your appetite for risk and reward, you might also go further and use stablecoins for both the loan and the collateral. An example of this risk minimization approach might be borrowing USDC against DAI. As the value of both assets is pegged to fiat, the likelihood of funds being liquidated because price swings lead to leverage thresholds being breached is very small.

Impermanent loss turning permanent

[One of the most significant risks that Yield farmers](#) are exposed to is impermanent loss (IL). It can occur when they provide liquidity to DeFi projects such as decentralised exchanges (DEXes) by locking up funds for a certain amount of time in liquidity pools. If the price of one of the assets in a liquidity pool increases or drops on an external cryptocurrency market, traders will notice an arbitrage opportunity.

Arbitrageurs come to take profit from the price differences occurring between DEXes and other markets. They even out the DEX prices so that they reflect the global market fluctuations.

Before The Price Change

$$5\,000 \text{ ₮} + 8.33 \text{ ⬡} \times \$600 = \$10\,000$$

After The Price Change

$$5\,244.2 \text{ ₮} + 7.945 \text{ ⬡} \times \$660 = \$10\,488.45$$

Holding The Funds

$$5\,000 \text{ ₮} + 8.33 \text{ ⬡} \times \$660 = \$10\,497.8$$



DeFiYield.App

Let's assume you've provided \$10,000 liquidity into a 50:50 pool of ETH and USDT on a decentralized exchange. This means that you've equally split the deposit between these two assets. At the time of the tokens

staking ETH was worth \$600, so you've provided 5,000 USDT and 8.33 ETH.

Now, let's consider a situation when the ETH price goes up by 10% on an external market, such as Binance, reaching \$660. This creates an arbitrage opportunity for traders. Having noticed the price difference between the DEX and Binance, the arbitrageurs buy cheap ETH until its price is evened out with the price point on Binance.

The staked funds are adjusted as the AMM rebalances the pool. After the price hike, the total balance amounts to \$10 488.45, meaning there are 5,244.2 USDT and 7.94 ETH. This equates to an impermanent loss of \$9,35.

In order to mitigate the IL risk, you need to always check how price fluctuations can influence your Yield Farming results. This is not easy and can be particularly tricky for a novice Yield farmer. That's why I decided to develop an advanced impermanent loss calculator, which takes into account many factors influencing IL in order to maximize the result accuracy. It is based on a spiral calculation and reflects rebalancing steps that are executed at certain price changes in a liquidity pool.

Rising gas fees on Ethereum

Many Yield Farming projects are based on the Ethereum 1.0 blockchain and therefore face scalability issues when the network becomes congested. This congestion can result in a significant increase of gas fees, which are paid when interacting with the network.

The first point to note here is that a solution to rising gas fees is being implemented by Ethereum. Ethereum 2.0 has various updates scheduled that will improve scalability and reduce gas fees. The most important of these changes is moving from the Proof-of-Work consensus mechanism to the Proof-of-Stake mechanism.

As mentioned previously, the transaction fee situation is comparable to the issue of bandwidth on the internet during the mid-nineties. In time, it will be resolved. For now though, it is a barrier and a reason why Yield farmers might consider blockchains other than Ethereum in the short term.

This transition is happening gradually and will result in an even better ecosystem for DeFi and Yield Farming, but you don't need to wait until ETH 2.0 is fully launched to farm Yield with lower gas costs.

One option that is immediately available is to take up the opportunity of Yield Farming on an alternative blockchain, namely Binance Smart Chain (BSC). BSC is more centralized than Ethereum, which can turn Yield farmers away from using it. However, there are also benefits, with one of the main ones being low gas costs and higher transaction speed than on Ethereum.

Also, users can make big and small transactions on BSC while still only paying a few cents in fees. I expect more Ethereum alternatives to be introduced as the Yield Farming market grows and these will likely introduce other options for those looking to avoid rising gas prices.

Flash loan attacks

[Flash loans, which are uncollateralized loans](#) that users make use of to finance almost instant arbitrage transactions, are a significant innovation enabled by DeFi. However, they are also an important risk to be aware of.

Because they require no collateral to be put at risk, scammers use them to quickly benefit from flaws in smart contracts. These scams take a variety of different forms. But, essentially, scammers try to trick smart contracts into acting on the basis of incorrect asset valuations in needed transactions so that they can manipulate prices of related tokens.

To illustrate how these scams work, it's worth looking at some examples from the recent past.

The Top 17 DeFi Hacks Of 2020 **Part 1**

	Project name	Date	Value of the Loss
1	 Compound	26.11.2020	\$89,000,000
2	 Lendf.me & dForce	19.04.2020	\$25,000,000
3	 Harvest Finance	26.10.2020	\$24,000,000
4	 Pickle Finance	21.11.2020	\$19,700,000
5	 Eminence	28.09.2020	\$15,000,000
6	 SharkTron	09.11.2020	\$10,000,000
7	 bZx (2)	13.09.2020	\$8,000,000
8	 Maker	12.03.2020	\$8,000,000
9	 Warp Finance	18.12.2020	\$7,700,000

The Top 17 DeFi Hacks Of 2020 **Part 2**

	Project name	Date	Value of the Loss
10	 Origin Protocol	17.11.2020	\$7,000,000
11	 Value DeFi	14.11.2020	\$6,000,000
12	 Cheese Bank	16.11.2020	\$3,300,000
13	 Akropolis	12.11.2020	\$2,000,000
14	 Percent Finance	04.11.2020	\$1,000,000
15	 bZx	14.02.2020 & 18.02.2020	\$954,000
16	 YAM	22.09.2020	\$750,000
17	 Pluto	30.10.2020	\$700,000



The dYdX attacks

The first significant flash loan attack took place on the dYdX protocol. The scheme was based on leveraging five DeFi protocols within one transaction in order to manipulate token prices and bank profits within a few seconds.

The following steps were executed by the attacker:

- 10,000 ETH were borrowed as a flash loan

- The loan was split and forwarded to other lending platforms, such as Compound and Fulcrum
- The first tranche of ETH was collateralized in order to borrow WBTC on Compound
- Another tranche was sent to Fulcrum and used to open five short positions for ETH against WBTC
- This led to the Fulcrum smart contract buying WBTC
- Information about this transaction was then sent to Kyber, another DeFi protocol
- Kyber then executed the buy order on Uniswap
- At the time, liquidity on Uniswap was low and the price of WBTC was therefore inflated
- This meant that Fulcrum overpaid for the WBTC purchase
- As the price pumped on Uniswap, the attackers exchanged the WBTC loan taken on Compound to ETH using Uniswap
- They then banked the profit and repaid the flash loan on dYdX

To summarise, the problem was caused by a flaw in the bZx smart contract used by Fulcrum, which was tricked to overestimate the value of WBTC.

The second attack took place in the same week as the first one and also utilized flaws in the bZx protocol. However, this time the scammer was able to trick the smart contract by overestimating sUSD. After the flash loan was paid off, the attacker took the profit and the platform had to deal with under-collateralization.

The Value DeFi attack

A much bigger flash attack happened on Value DeFi in November 2020.

The platform was exploited for almost \$6,000,000, where the scammers used two flash loans to execute the scheme. They first took a flash loan of 80,000 ETH from Aave and borrowed additional 116,000,000 DAI on Uniswap through the flashswap.

These funds were then used to exploit the MultiStables vault on Value DeFi. The scammers executed a series of swaps between USDT, USDC and DAI to undermine the pricing logic applied by the vault's withdrawal method.

This resulted in a dump of the protocol's native token from \$2.76 to \$1.99.

Code weaknesses in smart contracts

Before I move onto explaining the risks that I class as clear scams, it's worth looking at how some projects can, whether intentionally or not, introduce code weaknesses that may put Yield farmers' funds at risk.

Even when a project has got a positive reputation throughout the Yield Farming community, code weaknesses can still present a problem that even the project's dev teams are not aware of. That's because, in the Wild West that is the emerging DeFi industry, it's often only a matter of time before hackers exploit these security flaws.

These are the sort of flaws that you wouldn't find unless you are experienced with smart contract audits, a topic I will go into later. However, protection from scams is one of the unique benefits you receive from using DeFiYield.

As mentioned previously, DeFiYield is the only team that performs audits for free and for the benefit of the community. We believe that the payment auditors receive for their work makes them biased. We don't receive payments because we want to remain independent so we can fight scammers for the DeFi community's benefit.

In doing so, we are supporting legitimate projects and their founders in building Finance 3.0 for everyone. There are many projects that do not fit into this category though and even more where smart contract vulnerabilities put users at risk.

Therefore, it's worth telling the story of some projects where our audits resulted in significant improvements.

The Deus Finance smart contracts

Deus Finance is a good example of the process DeFiYield goes through in analyzing smart contracts and communicating with project teams in order to make changes to their smart contracts that will protect the Yield Farming community from danger.

It was a positive example of a Yield Farming project being responsive and flexible.

[When I audited the project](#), I identified that the staking process was insufficiently decentralized. The staking smart contract owner had a lot of permissions, such as an opportunity to transfer all rewards and staked tokens to any address without any timelock. I therefore rated Deus as a

high risk opportunity for Yield farmers, based on the project's development being fully dependent on the smart contract owner's decisions.

In response to my analysis, one of the Deus team claimed that the highlighted code features were required as a temporary platform development step. Following this, he tweeted that the contract ownership had been transferred to a DAO on Aragon in order to decentralize governance. This new ownership model looked much more trustworthy, as crucial smart contract term changes could be implemented only through a voting process. However, there was still an issue, as 23% of DEA tokens were laid in an EOA. Again, I shared this fact with the public.

The changes that had been implemented led me to update the project risk level to medium, as a token price dump initiated by the team could still occur. Eventually though, this final 23% of DEA tokens were transferred to the Aragon DAO smart contract. With all the changes made and the compromising factors eliminated, I was able to change the smart contract risk level to low.

Deus had made clear steps towards decentralization as a result of the DeFiYield audit, and the affair demonstrated how we can help to keep the community safe.

The Bundles Finance smart contracts

Another way that code weaknesses can be identified is through attentiveness and proactive actions of the DeFi community. [This was the case with Bundles Finance.](#)

The story began with a warning from a member of the DeFiYield team, indicating that the project's smart contract code contained high risk issues. Specifically, the drain function was revealed, which could be executed allowing the contract owner (an EOA) to drain liquidity pools at any time.

The Bundles Finance team noticed this warning and admitted the code must be corrected. In fact, the project's founder published a video with a detailed explanation on the situation. He explained that the smart contracts had been audited by SolidityFinance prior to the platform being deployed. However, after that, a member of the project's external development team decided to add the drain function as a code security enhancement. The idea was that if something happened to the smart contract functionality, funds would not be locked in it and their withdrawal could be managed.

As the Bundles Finance founder pointed out, the fact that the developer had not communicated the addition of the drain function or the rationale for doing so to the project managers had been a failure of internal communications.

Eventually, Solidity was contacted with a request for new contracts deployment for Bundles Finance. As a result, funds staked with the insecure smart contract version were withdrawn to liquidity providers. Staking was paused until a new smart contract code could be deployed and externally audited.

It was another example of how we help DeFi projects to become more trustworthy, transparent and safe for the community.

The Alpha Homora case

Unfortunately, some projects don't react to warnings and recommendations regarding improvements that should be made to code of their smart contracts. While it would be wrong to say these projects could be high risk, the opportunity for a token price dump remains, and the community must be warned.

An example of this occurred in my auditing of Alpha Homora, which Alpha Finance Lab developed in December 2020. The process began when I revealed some unacceptable smart contract code details, as follows:

- The project conducted a premine of 1,000,000 ALPHA tokens to a wallet marked as Alpha Deployer
- The tokens were transferred to another EOA wallet
- 96% of the total token supply was under the control of the project deployer
- The project team was allowed to mint tokens anytime

The nature of Alpha Finance Lab posed a risk of centralization, and I informed the community about my findings. After a while, my communication with Alpha Finance Lab started and they initially tried to eliminate these concerns in the following way:

1. They said that all cross-chain platforms couldn't function in a fully decentralized manner. The fact that all user tokens were locked in one Ethereum EOA was absolutely fine, as they could only be unlocked when a requested transfer was performed to the same address on Binance Smart Chain. (This argument referenced some

famous projects, saying they had followed the same centralized principles.)

2. They said the infinite minting had been enabled for some potential protocol updates and the developers didn't intend to apply it.
3. They defended the fact that the project admin fully controls the smart contracts of Alpha Homora by mentioning other projects where the centralized control of smart contracts existed.
4. The team also pointed out that the Alpha Homora team was not anonymous.

It is certainly true that the project team is not anonymous and has a pretty active public facing team. However, none of the team's arguments are backed up by the smart contract code.

Moreover, transactions that can be tracked on Etherscan prove there are reasons to doubt the security of the user funds. Liquidity providers are supposed to just trust the project's intentions, which goes against the important crypto principle of "don't trust, verify".

Even though this project has gained a lot of traction, it is still the case that 98% of the user tokens are locked in the single EOA under the Gnosis Safe smart contract and that five project owners can perform any transactions with these funds without any timelock. The team can sell all the tokens at any time on any exchange and rug pull all liquidity currently available on the platform. All of [this was discussed with Tascha, the founder of Alpha](#), in the Lobster DAO telegram group.

Therefore, this is a good example of how DeFiYield is identifying potential issues in smart contracts so the community can make the best decisions about where to place funds, regardless of how big or well known projects get.

At the same time, it's worth noting that DeFiYield do not expect Alpha Finance to perform a rug pull or exit scam because it is backed by Multicoin Capital and Defiance Capital, who are major, high-profile VC firms. You can find out more in our [in-depth report on Alpha Lab infinite minting](#).

Scam projects

Some projects are scams, plain and simple.

I come across projects that are actively aiming to deceive users almost every week. They take advantage of the fact that high Yield Farming returns make some people less cautious about risks and only interested in rewards. They also take advantage of the avalanche of information about new projects that is generated every day and the difficulty most people have in sifting through it all to separate signals from a noise.

Furthermore, most of these scam projects are designed by highly technical individuals who take advantage of the average Yield farmer's inability to audit smart contracts. However, I cannot emphasise enough what an important element of scam identification smart contract audits are. Fortunately for you, this is exactly what DeFiYield's experts do everyday in order to keep the community safe and why we are building the biggest database of scams for you to avoid being deceived.

The methods we use for auditing smart contracts are explained a little later but it's worth starting with a brief look at some of the scams we have identified to show how they work.

The '1-click rugpool' scam

This type of scams has occurred across a number of projects, including the Unicat scam that involved a rug pull of \$200,000.

The Unicat scam wasn't noteworthy for the amount stolen, but because it highlighted a dangerous backdoor, which allowed the scammers to drain all Ether from users' Metamask wallets. All the users had to do was to approve a smart contract of the scam project once to expose their funds to the scammers and to potentially lose all of them.

The first thing to note about the Unicat scam was how it used a name similar to that of a famous project, Uniswap. It is common for scammers to try to attach their projects in the minds of their victims to some well known brands, even though these projects have absolutely no connection to scammers.

Victims of Unicat were duped into allocating their UNI tokens into Unicat's fake Yield Farming project in the expectation that they would be rewarded with MEOWs - the native token of Unicat. However, malicious code had been developed that allowed the scammers to withdraw the victims' UNI tokens.

This occurred once the victims had approved the Unicat contract. Instead of using these funds for staking, as had been outlined in the rewards incentive, the contract deployer was able to take the deposited tokens without limitations.

The specific backdoor used involved anyone with ownership of the smart contract being able to call the setGovernance function. This gave them the right to control any transactions, including transferring staked funds to any address:

```
// Set governance contract. Can only be called by the owner or governance contract.
function setGovernance(address _governance, bytes memory _setupData) public onlyOwnerOrGovernance {
    governance = _governance;
    (bool success, bytes memory returndata) = governance.call(_setupData);
    require(success, "setGovernance: failed");
}
```

Another important point to note about this scam was the fact that the funds stayed under the control of the scammers even after they were withdrawn from Unicat's smart contract. As a result, every user that had ever approved the smart contract had to revoke that approval or risk further fund losses.

It is important therefore to always use tools that check token allowance. Many other smart contracts utilize unlimited token approvals, as they claim it improves the user experience users don't have to validate all future transactions. The problem with this is twofold:

- The smart contract has unlimited control to transfer deposited funds wherever it likes
- The approval doesn't expire, so control over users' funds remains forever

The final aspect of the Unicat scam that is worth noting is the use of the Tornado cash smart contract, which was applied to remove all traces before the scam. The Tornado cash smart contract allows an EOA to be hidden, thereby allowing scammers to pay ETH for deployment of their smart contracts and stay untraceable.

Fortunately for DeFiYield users, one of our newest tools is specifically designed to check for these 1-click rugpull backdoors and help you ensure you have not approved any.

The YFFS Scam

Another rug pull that the Yield Farming community has had to deal with in recent months was that from YFFS. This time, users lost around 300 ETH, worth around \$130,000 at the time, that had been invested in a pre-sale phase which lasted no more than a minute.

Once again, you can see the pattern of mimicking a well known and well respected project in the way the scam was named. Once again, it's worth reiterating that YFI and YFFS have nothing to do with each other.

[When I first audited YFFS](#), I revealed various issues that made it highly likely to be a scam and DeFined it as very high risk. The fact that the contract owner could pause transactions and transfer staked tokens put user funds at risk. Furthermore, the funds staking contract was owned by an EOA, which could call the stop, start and deposit functions. The first one of these was probably the riskiest, as it allowed the dev team to stop the staking contract and transfer all deposited tokens into their wallet.

I immediately informed the Yield Farming community on my social media accounts. Initially, the team behind YFFS noted my warnings but did not make any improvements to rectify the issues highlighted. In fact, they disputed my assessment. However, I continued to insist that the centralized control over user funds had to be eliminated. Interestingly, I was accused by a lot of community members of spreading FUD.

While these debates were going on, the YFFS team pretended to be cooperative and then agreed to edit the problematic code.

I had suggested renouncing ownership of the token smart contract and adding a timelock to prevent the centralized execution of the aforementioned functions as soon as possible. In response, they decided to burn the admin key and called the transferOwnership and setGovernanceAddress functions, in order to set a 0x000 address as the ownership transfer parameter for the YFFS DeflationStake contract.

These might have been positive steps but they were actually part of the team's deception. Maybe they made these initial changes in order to buy themselves some time as, in the end, they managed to steal user funds.

[The Compounder Finance scam \(and how we will find the scammer\)](#)

[As mentioned previously, the biggest scam to hit the Yield Farming industry](#) so far was the one performed by Compounder.finance. It is one in

which I personally lost \$1,200,000, and users lost \$12,000,000 overall. [It is an important story to tell for a number of reasons.](#)

Firstly, it shows the sheer scale of possible Yield Farming losses and why you should always be on guard to risks this industry poses. Secondly, it demonstrates how even experienced yield farmers with smart contract auditing experience can be scammed and why you should always be aiming to deepen your knowledge of the industry.

Finally and most importantly, the story shows that by working together as a community to help make Yield Farming as safe as possible, we will all ensure that scammers do not get away with their criminal activity. That's because, as you will see in my explanation of this scam, I will reveal the exclusive information we have that will ensure the scammer will be caught.

How did the scam work?

The Compounder.finance scam involved the use of a backdoor in the smart contract that allowed the contract owner to drain all user funds. The scheme couldn't be traced on the public blockchain as a mixer was used to launder the loot.



DefiYield.info 🚗
@defiyield_info



Message to the scammer of [compounder.finance](#) just scammed approximately \$10,800,000

I have personally lost approx. 1m\$ and the rest of the crypto community lost approx. 10m\$ from your rug pull.

1:16 PM · Dec 1, 2020 · Twitter Web App



However, since the incident occurred we have been investigating and uncovered the mechanics of the scam.

We were able to identify the rug pull technique applied by Compounder.finance, which was based on introducing a special role into

the smart contract called Strategist, which belonged to the scam team. A list of exclusive terms were encoded that allowed Strategist to call specific functions for transactions with the platform tokens.

```
function inCaseTokensGetStuck(address _token, uint _amount) public {
    require(msg.sender == strategist || msg.sender == governance, "!governance");
    IERC20(_token).safeTransfer(msg.sender, _amount);
}

function inCaseStrategyTokenGetStuck(address _strategy, address _token) public {
    require(msg.sender == strategist || msg.sender == governance, "!governance");
    IStrategy(_strategy).withdraw(_token);
}
```

Strategist could call an 'inCaseTokenGetStuck' function, followed by a token withdrawal function, at any time and without any preventive mechanism for controlling the triggered processes.

We have also discovered that Compounder.finance used the Tornado cash smart contract for the same purpose as Unicat did in its scam.

What has the response been?

As soon as the scam occurred, the project's website and all related accounts were instantly removed from the web. Therefore, it initially looked like the scammers might have gotten away with an extremely sophisticated plot. However, as you will see, DeFiYield has been at the forefront of tracking them down and we are confident they will be caught.

Our investigation began by looking at the scam transactions that had occurred. We also looked into analysis that had been done by others. This included reading a report from SolidityFinance, which had audited Compounder.finance before the scam but not revealed any backdoors.

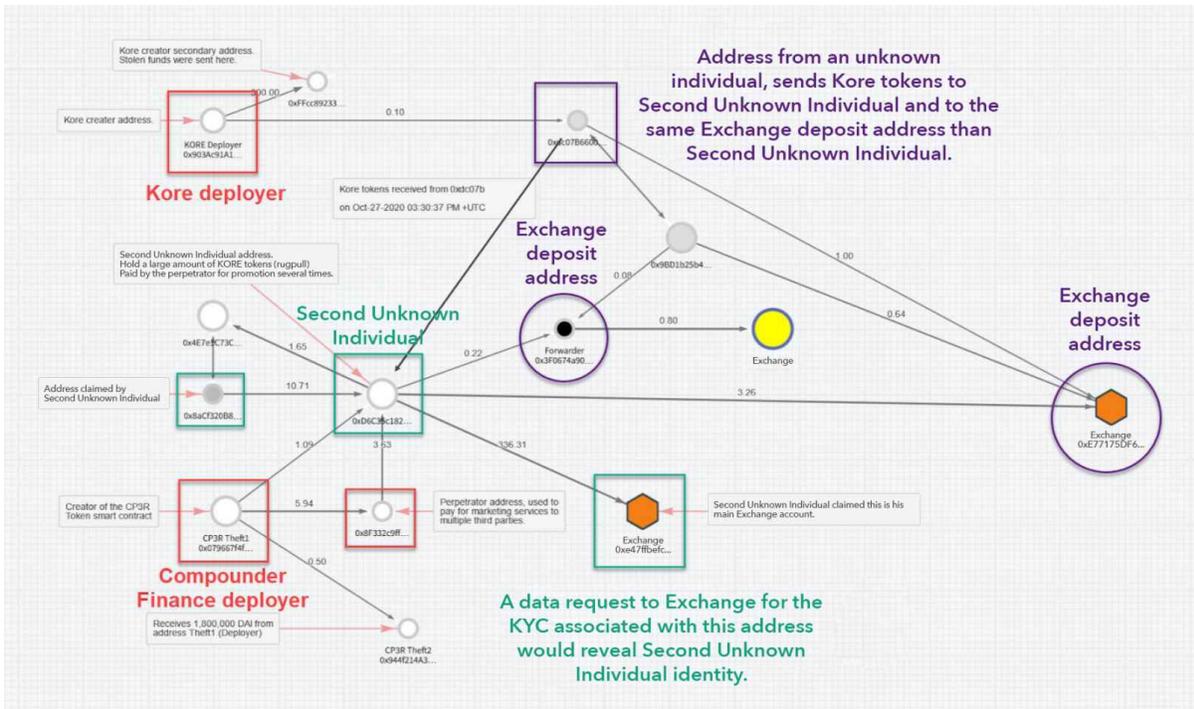
DeFiYield also became the coordinator of a victim group involving about 600 members from various countries. The investigation was building momentum, and we started a cooperation with a blockchain forensic agency to dig even more profoundly. Now, we have officially filed claims against the scammer(s) in three jurisdictions.

How will the scammer be caught?

Throughout our investigation, we have been sharing information with the public about how the scam occurred. This is to ensure yield farmers are aware of the techniques used and do not fall foul of them again.

It is also to show the community that the net is tightening on the scammer(s). We can now reveal exclusive information from our cooperation with the blockchain forensic agency, demonstrating how the scammer will be caught.

The key bits of new information are visualised in the following image and then explained below.



The blockchain forensic agency report that contains this visualization uncovered several leads, which are:

- The perpetrator used a famous international hosting provider, which is likely to possess information associated with the perpetrator or an accomplice.
- The perpetrator registered domain names on the registrar Public Domain Registry, which may possess the perpetrator or an accomplice's information.
- Compounder Finance used famous social media to communicate with investors so that this social media may possess information associated with the perpetrator's account on that platform.
- Specific addresses receiving payments from the perpetrator received ETH from a famous exchange, which may possess information regarding those addresses' ownership.

- The perpetrator also used a famous and widely used hosting provider in Russia, and obtaining the associated data could reveal his/their identity.
- An individual helped the perpetrator in several frauds. His identity and details of a potential second individual who could also be involved can be retrieved by contacting the exchange.

Now, the investigation started with these leads. It's only a matter of time before the authorities catch up with the scammer(s), and we will update the community with more information as and when it is available in the coming months. *(Names has been omitted)*

Highlights of the chapter

Yield Farming refers to staking funds into different DeFi platforms with the purpose of gaining returns.

All Yield Farming opportunities can be classified into four types: liquidity provision, lending, receiving governance token distributions and other token distributions.

The common practice is combining different types and strategies of Yield Farming for yield maximization.

Yield Farming is based on a range of DeFi innovations, such as:

- Automated market makers;
- Automated setting of interest rates and other terms by smart contracts;
- Ability to combine different DeFi opportunities to maximize returns;
- High collateralization of loans, which increases security for lenders;
- Flash loans - uncollateralized loans, where funds are borrowed, used and paid within one transaction.

The main advantages of yield farming include high returns, large variety of investment opportunities for different risk levels and yield expectations, composability, accessibility, absence of intermediaries and fast growth.

Despite the long list of the exciting benefits of Yield Farming, you should always be aware of all its disadvantages and risks: high market volatility, high gas prices when farming on Ethereum-based platforms, FUD and rumors, impermanent loss, UX barrier, complexity of smart contracts, large number of scam projects, high frequency of hacker attacks, flash loan attacks and low probability of fraudsters being chased and punished.

HOW TO SUCCEED AT YIELD FARMING?

Now you've got some foundational knowledge about the key concepts underpinning DeFi and Yield Farming, it's time to start getting into the detail of how you can actually start generating returns.

In this section, I will explain some general principles that you can use as a basis for all the strategies you employ. These are lessons learnt from many months of Yield Farming, not just by me but also the DeFiYield community of experienced farmers. These principles and the advice of the community should start to build your confidence and readiness to get started with Yield Farming.

Then, I'll move on to explaining details behind some of the best known projects in DeFi, which you can start to build into your first Yield Farming strategies. We'll look at mechanisms and incentives within these projects that allow farmers to generate yield. Finally, I'll describe simple steps you need to take to actually start investing while staying safe.

General principles for safe and profitable Yield Farming

Yield Farming is a game of big rewards and big risks. At DeFiYield, we have learned to try to grasp these rewards while mitigating these risks wherever possible.

In this chapter, I will describe some general principles every yield farmer should take to reduce risks and to get the most out of the market.

If you're already investing in traditional finance, some of these will sound familiar. Whether you have investment experience or not though, some will be new as they relate to specific idiosyncrasies that are unique to DeFi and Yield Farming.

Get in early

If a Yield Farming strategy becomes mainstream, you are probably too late. I always focus on the latest market offers and the hottest APY deals. This is true for all members of the DeFiYield DAO group too, who have all been able to 100x their returns by following this same principle for Yield Farming with various projects.

DeFi projects used to offer early adopter programs in order to create a liquidity pillow for an effective start. These included higher rates of return and a range of additional financial incentives. I have profited in the past from situations where platforms conducted token distributions amongst a small number of people.

As an early adopter, you might participate in some projects that go nowhere but, if you don't embrace this approach, you will DeFinitely miss out on the best opportunities. Also, it's worth remembering that these wins on early projects can help you to build a base of funds that can allow you to make even bigger moves for bigger rewards in a subsequent project.

Don't be scared by market inefficiencies

The crypto and DeFi markets are full of market inefficiencies because they are still relatively immature when compared to bigger and more liquid traditional financial markets.

You should not let this scare you. It's actually a benefit that you should take advantage of. That's because, if you're able to spot inefficiencies as

opportunities, you'll be able to farm them and generate massive yields before anyone else.

So, instead of worrying about market inefficiencies, do research to understand them and develop a strategy that allows you to benefit from them.

Diversify your investments

This is a classic investment rule and it is relevant for Yield Farming.

Just as you'll spot market inefficiencies all around DeFi markets, you'll also see a range of different risks. Rather than dismissing every opportunity as too risky to jump into, you should tailor your portfolio of Yield Farming investments following the principle of diversification to balance out risks.

For example, if you start to assess DeFi projects that exist on other chains than Ethereum, you could decide that these projects are too risky because the underlying blockchains have not been battle tested to the same degree as Ethereum. Rather than miss out on outstanding APYs that might be available though, it's probably better to take the risk while also keeping most of your funds in Ethereum's DeFi ecosystem, just in case your worst fears are realized.

Do your own research

As mentioned previously, it really is imperative that you always research projects you intend to farm as deeply as you possibly can.

I never skip this step, no matter how hyped an opportunity is. It's crucial to dedicate time to a rounded analysis of the whole project and continually monitor all potential changes. APY benchmarks, smart contract security, the team's credibility and the project's unique features are areas that must be covered.

Fortunately, you'll be able to access the deep research that is gathered from our own DeFiYield audits and fed into the tools we provide. However, this isn't a substitute for doing your own research, which really must become a habit that you never skip.

Think independently

Part of the deep research habits you must practice is to never blindly follow what DeFi influencers say or rumors that swirl around the community on an

ongoing basis.

Having covered crypto communications for a long time now, it's clear that certain influencers have far too much power over how their followers act, even though they are far from being experts themselves.

This is why I always take time to check if a promoted investment opportunity has objectively provable benefits that make it worth taking seriously and I never blindly follow DeFi market influencers or rumors inside the community.

Farm with a large budget

Yield Farming can be attempted with any budget but it's generally more suited to one of a few thousand dollars. However, this is only true if you want to stick to the Ethereum network, as yield farmers who use Binance Smart Chain and Huobi ECO Chain can do so with smaller budgets.

There are two main reasons for this. Firstly, Ethereum transaction fees are very high at the moment. This is likely to be the case until eth2.0 is fully rolled out, which is expected to happen in 2022. Therefore, when you invest a relatively small amount, the gas costs you pay for making farming-related transactions can easily exceed your projected returns. This is because every action that involves staking tokens or withdrawing tokens requires submissions on the blockchain, which require network payments in the form of gas.

It's worth noting that the transaction fee situation is comparable to the issue of bandwidth on the internet during the mid-nineties. In time, it will be resolved. For now though, it is a barrier and a reason why yield farmers might consider blockchains other than Ethereum in the short term.

Secondly, as mentioned previously, I recommend diversifying your investments in order to mitigate risks. This strategy means your budget will be split across various projects and you'll have to pay staking and withdrawal-related gas fees across all of them. As a result, any yield you generate will quickly be swallowed up by fees.

Impermanent loss, slippage and other Yield Farming risks must also be considered when defining how much to invest in each project.

Avoid high-volatility times

While you should always try to 'be early' on projects, there's DeFinitely a case for being too early. What I mean by this is I never join any project during the first three days after it has launched. It is almost impossible to find an optimal entry price point this early, mainly because of the high price volatility that tokens exhibit in these early days.

Monitor whale activity

I frequently monitor wallets of known whales in order to check which pools they farm. This helps me to define optimal entry points for certain projects, as the movement of whale funds provides a signal of the way the market is moving and of projects that have the highest potential. Two on-chain analysis tools that are worth using for whale monitoring are Glassnode and Nansen.

Learning from experienced yield farmers

It's really important to use experience of others to speed getting into the best strategies as soon as possible. Even though the Yield Farming industry has a small minority of scammers in it, the vast majority of participants are happy to help their peers succeed and stay safe.

This knowledge sharing is exactly why we have set up the public DeFiYield Telegram group, where you can discuss ideas and learn from other farmers. We encourage you to join this popular group, which is the most advanced Yield Farming group available on Telegram. We also run an exclusive DeFiYield DAO group, which is the most advanced Yield Farming group in the industry.

In the next section, I will provide some stories from experienced yield farmers, including myself, that demonstrate why the general principles of safe and effective Yield Farming are important. By sharing my story, and those of my closest associates, I am aiming to demonstrate how strategies we used resulted in us learning the industry and benefiting from Yield Farming so far.

Overview of the DeFiYield team strategy

We, the DeFiYield team, employ a mixed strategy of market buying and Yield Farming that is based around diversification. ETH and BTC make up the majority of our assets but we also have portfolio portions reserved for DeFi index buying and for active Yield Farming.

The DeFi index buying involves market-buying blue chip DeFi tokens. It is not complex to do and is focused on buying and holding the most popular and important for the industry projects. We were in touch with some DeFi projects about participating in their pre-sales or partially acquiring them, but a lack of time didn't allow us to close some deals.

In terms of blue chip DeFi, we have a basket of tokens that includes Uniswap, Synthetix, Aave and Yearn Finance. We bought some of these at their peak during the DeFi Summer of 2020 and therefore were hit by the bear market at the end of 2020. However we didn't sell and only sell these tokens when the price goes up a lot. For example, we sold about 40% of our positions in February 2021 after seeing them 3x but we still hold more than 50% of our DeFi blue chip basket because we believe in them as projects for the long term.

Yield Farming is more complex. It requires skill and calculations to get it right. The less complex part of my Yield Farming strategy involves depositing stablecoins in Compound and Aave, the two major lending platforms, to achieve lower APYs that are more secure and lower risk. However, Yield Farming with higher APYs is a short term strategy and much more complex.

For example, the early auditing of Binance Smart Chain projects that we did, allowed us to get in early on projects like Pancake Swap and Beefy. We joined Pancake Swap in December 2020 when the TVL was very low but it went parabolic later on. This allowed me to make 20x on this project, after which I sold 80% of my position. We achieved similar returns on Beefy as well.

More stories from our Yield Farming journey so far

When we began Yield Farming, we preferred to stake funds in stablecoin pools or pools with a 98:2 asset ratio, where 98% was taken by coins with a stable value, in order to minimize impermanent loss.

In the first few weeks, we focused on Farming with YFV and YFII, which involved depositing funds into DAI pools. The results were impressive, with an APY that reached up to 2000% at the time, as a result of Farming the YFI token through YFII. This opportunity is a great example of why it's important to get in early, as the distribution of tokens to users started off as 10,000 per week but this number halved with every week that passed.

This strategy paid off for us in such a dramatic fashion because we started Farming YFI when it was worth \$800. Having researched the project in some depth, we could see that Yearn Finance was a truly unique idea and that its governance token had real value. Therefore, in addition to our YFI Farming strategy, we also chose to purchase a significant amount of YFI tokens on an exchange, as we expected the token price to increase. This certainly paid off, as the token hit an all time high price of over \$43,000 in September 2020.

Soon afterwards, our success was interrupted by a significant loss we absorbed from Farming with ULU finance. We lost several thousand dollars by staking funds in a 95:5 USDC/ULU pool because the price of the ULU token collapsed by 70% in just one day, turning my impermanent loss into a permanent one.

Having also started testing the Balancer 95:5 liquidity pools, we came to the conclusion that they are much riskier than the 98:2 pools we had started out using. Therefore, our next step was to return to this previous strategy by depositing funds into the 98:2 SAFE/DAI pool.

A couple of other projects that are worth noting because we got in early with them are CREAM and Harvest. We liked that these projects presented clear roadmaps, market vision, innovative ideas and good explanations of the utility of their tokens.

After suffering from the compounder.finance hack, which we describe in much more detail in the next section of the book, our next success came from joining Empty Set Dollar (ESD) and Dynamic Set Dollar (DSD) early on. Again, the lesson you can learn from this success is to be always early and there will be many more of these opportunities to look out for.

Just as we succeeded with YFI and Spartan (another well known Yield farmer) did the same with SNX, you will be able to find your own stand out project. In fact, one area that is worth watching is other blockchains than Ethereum, such as Binance Smart Chain, where the next YFI or SNX is likely to occur.

The other point to make about my ESD and DSD success is that they came from seigniorage coins, which is an area that has been extremely profitable for us and one that we'll explain in more detail later on.

Finally, it is worth noting that getting in early on some defi protocols built on Binance Smart Chain, such as Bifi and Autofarm, was also highly

rewarding.

Ask the community for help

While there are many untrustworthy entities within DeFi, who are just looking to scam you or use some insider knowledge to ensure you get rekt, there are many many more with good intentions who can help. [The DeFiYield Telegram channel](#) is a great example of a group where novices can ask questions and source genuine assistance from more experienced farmers.

It really is important to find a like-minded group of Yield farmers who can help you to stay safe and succeed. There's so much to think about in this industry and so much can change that it can be really overwhelming to keep up. For all these reasons, you need to be accessing these nuggets of information on an ongoing basis.

That's exactly why we set up the Telegram channels and, as you can see from the following user comment, the community recognises this value too:

“I was hoping to find a serious group of members because I really believe we can help each other a lot. We can win if we are all hard working, vetting projects and having good discussions with substance. I'm looking forward to bringing value to the group.”

What the DeFiYield community says about Yield Farming

The DeFiYield Telegram community is a truly unique resource that includes both the main public group for everyone to discuss new and existing projects, as well as the exclusive DAO group for the top level of Yield Farming experts. The DAO group is a collection of Yield Farming OGs that includes the founders of many successful DeFi projects.

As a new or relatively inexperienced Yield farmer, you can access the main channel and it will become one of your most useful resources for learning about the best projects and strategies. As you develop your knowledge, you might be invited to join the DAO group and discuss these topics with a group of expert peers.

However, rather than wait to be able to access this exclusive knowledge, I want to share the thoughts of some of our experienced DAO members on lessons they have learnt so far. The comments below come from the DeFiYield Telegram channel and our private group. Some of it tallies with the lessons and general principles I have already outlined but some will contain completely new insights for you.

“Get in early and make sure to harvest and sell. Don’t hang on waiting with your crops too long. They all go bad.”

“Don’t go chasing every new project. Look at the utility of any project or token over the hype. Look for teams with goals and ones that already have the development to back it up.”

“I have learned to not FOMO in before I understood what I was getting into. I’m also starting to do better due diligence, like evaluating front end code for errors in APY calculations.”

“I generally avoid high Yield farms these days. Seigniorage is an exception because I know I can play it well. Otherwise, I pick projects that I like and, if they Yield 100%+ APY, then it’s a bonus.”

“Decisions based on extreme fear or euphoria are both likely to get you rekt very quickly. It’s tough to be rational during FOMO fever, especially as there have been some cases where it really hurts to miss out, but one mistake is enough to be totally rekt. It’s better be careful and suck it up if the lost opportunity moons later.”

“My biggest mistake was probably overselling mining rewards during dips. Sometimes it’s better to hold clearly oversold coins. However, it’s hard to know whether something will death spiral vs whether it will recover.”

“In a bull run don’t take 100% of profits, leave some for the home run. In a bear market, no low is too low, so it’s best to cut your losses.”

“Keep records so you can learn from your successes and mistakes.”

“[A paid] audit means nothing. They don’t test for outside attack vectors. DeFiYield technical review is way more comprehensive. Risk doesn’t go away just because it got audited.”

“If you wanna Yield farm, don’t become the Yield.”

Use the full suite of DeFiYield tools

Apart from our community, there are many tools you can use to avoid scams and get a fuller picture of any projects you are interested in. For example, we are making the biggest database of scams to avoid and also alerting you to scam projects that are linked to your metamask.

Auditing smart contracts

Auditing smart contracts is an absolutely crucial part of staying safe while Yield Farming.

However, it's worth remembering that an audit that a project pays for is only valid at the point when it is published because the project's developers could make changes to the code. You need to ensure you are tracking changes and always remember that Yield Farming is risky. Invest only part of the capital you have available and always do your own research.

DeFiYield's Safety Commitment to Smart Contract Audits

1. We are not paid for audits. We perform an agnostic technical review for the benefit of the DeFi community.
2. We do not sell audits and we do not respond to requests for paid reviews. We only do independent research, which differentiates us from paid smart contract auditors.
3. We only audit projects that the DeFiYield community wants. You can [submit a request for an audit](#) and, if this request is upvoted by the community, we will audit the project.
4. DeFiYield is the market leader in free and independent audits. We are the only team with the unique ability to perform free audits for the benefit of the community.
5. We believe that paid auditors are biased because of the financial incentives involved in their business model. This is why we will never accept payment for our audits.
6. DeFiYield's free auditing helps the DeFi community to fight scammers. We support legitimate projects and their founders in building Finance 3.0 for everyone.
7. We will continue to pursue scammers until the last one has been defeated.

8. The search for scammers and the ongoing need to protect the DeFi community motivated us to write “The Wall Street Era is Over” and offer DeFiYield Safe.

Our approach to auditing

At DeFiYield, we always interrogate the security of a project’s smart contract code and the specific investment terms involved. Over the past four months, we have independently audited more than 40 Yield Farming projects and we continue to publish more and more on an ongoing basis. Our work has resulted in the identification of scam projects before they could dupe investors as well as the introduction of security improvements in several projects.

The independent audits we undertake are very different to those of an auditor who is paid by the project. These paid auditors are usually there to tick boxes. We are independent and are not paid by the project.

Furthermore, we do not seek payment for audits or accept them when projects ask to pay us. Our audits are a contribution to the community, with the aim of holding scam projects to account and keeping Yield farmers safe.

Some sites, like Coingecko and CMC, display Yield Farming opportunities but they do not scrutinise the projects with the same attention to due diligence and auditing as DeFiYield, as their main focus is listing tokens.

In contrast, our work results in tangible security changes, such as the introduction of timelocks. In fact, we can point out 8-10 projects where our audits have led to specific security upgrades. We are also confident that the work we do in highlighting security issues is leading to many more early stage DeFi projects implementing better security from the start.

In this chapter, I will break down the main areas that need to be investigated in a smart contract and the order in which it makes sense to do so. Essentially though, the audits assess five key areas:

- Features of a smart contract system
- Token distribution
- Token location(s)
- Access to staked funds

We also look at security issues that do not specifically relate to the smart contract but do relate to the project’s external positioning and its reputation

within the DeFi community.

Understanding ownership

Before anything else, I check a project's ownership structure as the level of decentralization is an important feature that needs attention.

Ownership is important because it usually plays a role in the functions that can be called by a smart contract. Certain functions can directly affect the funds that users have staked, the tokens that can be minted and the distribution of both.

Many projects use external data sources and a special admin key to manage their system, conduct smart contract upgrades and perform emergency shutdowns. While these aren't necessarily an issue, users should be aware of these features, as they involve trusting the project owners to do the right thing.

If a contract is owned by an Externally Owned Account (EOA) belonging to the project owner and its team, they have the opportunity to call functions in order to conduct an unfair token distribution. This could result in either a token price dump or a steadily worsening value for the project.

Alpha Homora is an example of where this EOA contract ownership occurs. Alpha Finance Labs controls 96% of the token supply in an EOA wallet. Therefore they manage the admin keys without any governance in place.

However, centralized contracts can be even more risky if they give project owners the right to access users' locked funds. The owners could transfer funds into their own accounts and exchange them for other assets on secondary markets without any restrictions. In this way, they would suck all liquidity from the project and thereby perform a rug pull.

Auditing specific functions

Each smart contract has its own set of functions and a unique way in which they are controlled. Understanding these interactions is crucial for understanding a smart contract's security risk.

A function should only be considered suspicious when it's applied in combination with terms and parameters endangering user funds, such as centralized ownership and ability to set specific addresses as transaction

beneficiaries. Therefore, it's important to remember that a function's security depends on the context in which it operates.

The following section should give you a good idea of the main functions I check, the order that I work through these checks and the way I assess whether certain smart contract features pose a security risk.

The mint function

I always check whether the mint function or another function created for token generation is available, who can call it and who is the owner of the contract where it can be called. If no hard cap is specified for a token and minting can be called anytime without any restrictions, there is a risk of infinite token generation. This means tokens could be issued in unlimited amounts, which causes their inflation.

Another risk associated with minting can occur if the function can be called by the dev team at any time and an EOA controlled by the devs can be set as the receiver of the minted tokens. This is a very popular rug pull scheme in DeFi that is easy to perform.

For example, the owner of the project token smart contract might mint a million of tokens to his wallet address and then sell them out on a DEX for stablecoins, ETH or other crypto assets with real value, sucking out all liquidity out of the trading pairs used and killing the token price. Investors are then left out with the project tokens that don't have any value and can't be exchanged for real assets.

Alpha Homora is a project example, which has reached \$1.2 billion in total value locked, containing the smart contract flaw mentioned. Following our audit of December 2020, we consider the project as a high risk one.

The pause function

The pause function can be risky because, when it is called, users don't have access to their staked funds.

If a contract vulnerability is revealed and there is a need to transfer funds to a safer place, users won't be able to relocate the endangered funds. Scam projects introduce the pause contract function layered with other conditions in order to transfer funds to their own wallets. In fact, this trick was used by YFFS, a scam that was mentioned earlier.

At first, the YFFS smart contracts looked safe. However, a loophole they introduced was hidden under the pause function. The staking contract,

which could invoke the stop function, was owned by an EOA belonging to the project's developers. Therefore, they could stop the staking and transfer all staked tokens to their EOA wallet, what they eventually did.

The migrate function

Smart contract migration functionality can be used for a variety of purposes and is not dangerous itself. As with other functions, the risk it poses depends on encoded conditions it is combined with.

To understand how this works, you need to understand that smart contracts remain on a public blockchain forever and their code cannot be changed. On the one hand, this guarantees that embedded logic for execution of transaction conditions will remain the same.

On the other hand, this situation introduces issues for developers if they need to make functional improvements or security updates. In order to mitigate the inconvenience of this limitation, developers attempt to make it possible to make changes to smart contracts, and one of the ways they do this is by introducing the migration function.

One of the most common and legitimate use cases for the migration function is replacing an old token with a new one, where the latter will be managed according to the rules that have been coded into the project's smart contract system. In this case, availability of the opportunity to make migrations doesn't bring any risks to users.

However, if smart contract developers retain the opportunity to make changes to the code, there is a risk they will use it to scam users. For example, if developers introduce the migration function into a staking contract, they can add new functionality to the code, such as transferring staked tokens to any EOA they want, at any time and without the permission of users.

Proxy patterns

As code of already deployed smart contracts can't be upgraded, some projects choose proxy contract patterns: A proxy contract stores variables. Receiving message calls, it redirects them to a contract containing the logic. This architecture allows projects to bind newly deployed contracts with new logic to already existing dependencies as if the main logic gets upgraded.

This exposes users to the risk of losing funds as malicious logic can be introduced with a newly deployed contract anytime

The transferOwnership function

I always pay attention to whether there is a possibility to transfer ownership of a smart contract using the transferOwnership function alongside certain parameters.

If this possibility is present, I check limitations on what addresses can be set as new smart contract owners. I also check the availability of some preventive mechanisms for transferring ownership, such as timelocks or approving decisions to execute this type of transactions through governance voting.

If ownership of a staking or a token smart contracts can be transferred to any EOA at any time and the new owner is eligible to control all funds controlled by the vulnerable contract, this should be considered as a red flag that makes the project high risk for yield farmers.

I immediately warn users about this danger and suggest that developers renounce the ownership in public. If they insist on the presence of the transferOwnership function or ignore my warnings, this only confirms my suspicions. That's because, even if no direct danger can be detected, the functionality can be used in a cross-function reentrancy attack, which involves combining the vulnerable function with one that is controlled by an attacker.

Timelocks

Projects often introduce timelocks for execution of certain functions in order to convince liquidity providers and other users that the functions are safe. However, this never gives a full guarantee for user safety and I'll explain why. First though, it's worth looking at what a timelock is in more detail.

The Timelock contract or timelock conditions added to certain functions are used to delay a certain process or transaction being performed on a blockchain. There are a few reasons why contract deployers utilize them and one of the main ones is controlling token sales on the open market.

For example, a project might want to allow its developers to hold a big share of tokens granted to them as a reward. It might also want to allow

investors to purchase a large amount of tokens at an advantageous price at the start of a project's life.

If the project owners want to limit how and when these tokens are sold on the open market in order to avoid a price dump, they can introduce a timelock that does exactly that. This allows them to adjust incentives of token holders to be inline with the project's roadmap and strategy.

A timelock might also be applied in order to reassure users. This can be effective if the timelock lasts long enough for users to notice, understand it and properly react to smart contract changes and transactions that affect their funds. However, in my experience, timelocks usually don't exceed 24 hours and this is not enough time to consider them a good safety valve.

Furthermore, when a timelock is the only safety measure imposed on suspicious functions, yield farmers should use special Telegram bots to track the changes and perform necessary procedures to secure their funds in time. Moreover, it's important to understand that some timelock conditions can be bypassed.

Scammers often find ways of moving funds before timelocks expire, even when the Timelock contract or timelock conditions have no code vulnerabilities and prevent funds from being transferred for a given period. This trick usually involves transferring future ownership of the locked funds instead of getting a direct permission to move the tokens.

The bypassing mechanism is different for each type of timelock contract and there are many different ways allowing timelocks to be bypassed. For most readers, all you need to understand is that timelocks are DeFinitely not a one size fits all solution for improving smart contract security.

How DeFiYield keeps you safe

As you can tell from the in-depth details provided in this chapter, DeFiYield does a lot to keep yield farmers safe. That's because we want to make Yield Farming a safe opportunity for everyone and to provide the safest route for anyone entering the DeFi ecosystem.

The DeFiYield Safe solution was designed for exactly this user need. It is a machine learning tool that automatically detects and alerts users to instances where they have approved token allowances for malicious smart contracts. This is possible because DeFiYield Safe incorporates a range of tools including the open source Yield Farming scam database, bug library, automated smart contract check and audit database.

In addition to our unique products, here's a brief summary of the steps we take to keep DeFi users safe.

Auditing smart contracts so you don't have to

Some yield farmers have the technical knowledge to audit smart contracts themselves. If you're one of them, we encourage you to use your skills and share what you find with the community.

However, for those who do not have the necessary skills, DeFiYield is constantly auditing smart contracts of any projects that look like they might provide exceptional yield. We've audited 36 projects in 3 months and we share all our findings to help keep you safe.

Furthermore, the DeFiYield smart notification system provides an automated warning system for users that significantly reduces the risk of being scammed.

Notifying the community when we find issues

The reason we audit projects and do not take payments for this is to keep the community safe. We do this as a gift for the community so we can always remain independent and unbiased. In this way, ours is a totally different approach to auditors who receive around \$50,000 per audit from project teams.

When we do find an issue in a smart contract, we immediately notify the community and provide as much information as possible as quickly as

possible. This is important because it ensures yield farmers can act if any of their funds are at risk.

It also matters because we believe in transparency. We want the community to know what we have found out so everyone can stay safe. This strategy also means users can see what conclusions we have come to and discuss them in the open.

Crucially, we have also developed the DeFiYield Safe tool to automatically scan any DeFi project so that users are informed about dangers and can stay away from them.

Helping responsible projects to fix code weaknesses

As we have discussed in the chapter on auditing smart contracts, the existence of a suspicious function in a project's smart contract does not necessarily mean that the project is a scam. All code issues and vulnerabilities found must be considered in relation to other circumstances, in order to make a proper risk assessment of the project.

That's why we're also transparent about changes we suggest projects should make to reduce risks we identify. We understand that some projects may miss code weaknesses or have explanations for them, so we give them the chance to make changes.

Recording scams in the biggest database of its kind

When we know that a project is a scam, we make sure everyone in the community knows about it. To aid awareness, we are building the biggest database of scams that has ever been assembled and making it available for everyone to see.

Furthermore, we don't just leave it at that. As the example of Compounder.finance demonstrates, we are willing and able to pursue scammers on the community's behalf, using our blockchain forensic partnerships to investigate and filing claims around the world.

Providing a suite of tools to keep you safe

[DeFiYield](#) is the safest way for anyone to access Yield Farming opportunities that DeFi offers for all the reasons mentioned above. We are also building new tools everyday to keep you safe and help you make the most of the opportunity.

This includes a tool that monitors your Metamask account and ensures it is not exposed to liquidity drains from projects you have previously permitted. We are also in the process of developing a tool to monitor timelocks, which are introduced to functions influencing security of user funds.

Building a community of reliable Yield farmers

The final way we help you to stay safe is by giving you access to a ready made community of reliable and responsible yield farmers via our popular Telegram channel. This is not a place full of rockets and moons. In fact, anyone with that agenda is quickly excluded.

Instead, it is there for experienced farmers to share ideas, question new projects and generally help one another with Yield Farming. For those who are new to the industry, it's a great place to watch and learn from others who've been doing farming for a while.

Highlights of the chapter

In order to succeed in Yield Farming and make sure your funds are safe, you should follow the classical investment principles along with taking into consideration the nature of the DeFi market:

- Doing deep research prior to investing funds into a project. Besides APY evaluations, you should analyse the project's security, team and value of its products and services.
- Getting in early, before the investment idea becomes mainstream. But, volatility of the first 1-3 days after project launches should be avoided
- Selecting investment scale depending on farmings costs. Currently, transaction costs on Ethereum are high. Make sure they don't take a significant percentage of your returns. In order to see notable results, you should invest at least a few thousand dollars. Alternatively, stick to DeFi projects based on BSC or HECO
- Being flexible in terms of market inefficiencies: don't be scared of them. Use them.
- Independent thinking: don't follow rumors and opinion of market influencers blindly
- Watch what whales do
- Diversify your investments
- Ask the community for help
- Learn from experienced farmers

When you are skilled enough to check smart contract code of DeFi project, the features you should pay attention to are:

- ownership system of smart contracts, defining how decentralized the project is and what privileges the dev team has;
- governance system of the project;
- availability of token minting and its terms;
- migration;
- proxy patterns;
- timelocks.

THE FUTURE OF DEFI

So far, we have looked at the key components of Yield Farming, including the main dynamics that affect the market, the most important DeFi projects you need to know and the steps you must take to stay safe.

In this final section of the book, we will look at what the future holds for Yield Farming. What we see now is Yield Farming in its early development phase. A lot can and will change. It is likely that Yield Farming will grow as a result of many small subsectors blossoming into more substantial sectors in their own right. These sectors will cover new innovative financial services and technically sophisticated solutions for higher returns.

Therefore you need to be aware of some of the most important emerging trends, so you can be ready to take advantage as early as possible.

Governance-enabled growth

The growth in DeFi Yield Farming will undoubtedly be driven by unique governance systems that are developed within the most innovative projects. These are designed so that users can participate in decision making processes of the DeFi platforms through voting rights. In this way, users are empowered to define improvements that are aligned to their needs and requirements. Some areas of improvement where we expect to see further development in the short and medium term are ones like transaction cost optimization, Yield Farming reward enhancements and measures related to security of staked funds.

A great example of where this developing trend for user-enabled governance can already be seen is the way users made update proposals for Uniswap's reward system before its expiration. They wanted to restart the Yield Farming program with more attractive rules, as the old incentives had become weak in comparison to those offered by newly launched projects. As a result, the project's team reacted by updating its smart contracts in accordance with the user requirements.

Avoiding whale manipulation

Another reason why more and more market participants may be driven towards Yield Farming in DeFi is to counter the price instability of cryptocurrencies on the open markets. Earning through cryptocurrency trading is becoming more risky and complicated by the day for smaller players. That's mainly because the largest players, who are often referred to as whales, can manipulate market prices due to their massive trading power.

Their typical manipulation strategy consists of placing large sell orders for selected crypto assets, which causes the price to spiral downwards. After finishing the price attack, whales then place a large number of buy orders in order to scoop up the assets at the lowered price.

DeFi offers a variety of profit opportunities for market participants even when the whole cryptocurrency market is down, and this is likely to lead more people into Yield Farming.

Cross-chain solutions

As the popularity of DeFi increases, projects are becoming increasingly aware of the need to flex their protocols in order to optimize gas costs and transaction speeds for users.

This is leading traders to demand that they are able to perform transactions across multiple blockchains. Yield farmers need DeFi projects to increase the complexity of their architectures so assets can be managed across multiple platforms with different technical features. All of these things can be achieved by implementing cross-chain mechanisms.

Cross-chain solutions have emerged to tackle the issue of interoperability and thereby increase DeFi adoption. This has already transformed the technological landscape of the industry so that two or more blockchains can interact and exchange value. This value exchange mechanism is called the atomic swap and it will be an area that continues to grow.

An example lives of Cross-Chain Bridge with decent liquidity is [Anyswap Exchange](#) build by the Fusion Blockchain team.

Atomic swaps are based on a set of Hashed TimeLock Contracts (HTLC). No actual computation occurs between the blockchains used, with the two parties involved in a transaction confirming the movement of funds. If there is no submission by one of the parties within a limited timeframe, the transaction fails. In this way, HTLCs are used as a temporary escrow for the assets and the transaction is only completed when both parties confirm the swap. Decred is working on atomic swaps for Bitcoin.

Aside from atomic swaps, DeFi projects are constantly innovating in order to combine advantages of different blockchains and diversify yield opportunities by using strengths of several protocols at once. Therefore blockchain interoperability and cross-chain solutions are key areas to watch as they will be major drivers behind DeFi's rise above traditional finance.

For this reason, DeFiYield already allows users to manage assets cross-chain.

Binance Smart Chain

At the end of August 2020, Binance introduced its Binance Smart Chain to facilitate smart contracts and become the main alternative for Ethereum in the DeFi space. By the end of February 2021, the total value locked in projects built on Binance Smart Chain had grown to \$9 billion, with Pancake Swap and Venus becoming two of the top projects.

Binance Smart Chain Ecosystem

Part 1

Algorithmic Stablecoins

-  DITTO MONEY
-  BDOLLAR PROTOCOL
-  MONSTERSLAYER FINANCE
-  IRON.FINANCE
-  MIDAS DOLLAR

Crosschain token swap/bridge

-  ANYSWAP
-  BINANCE BRIDGE
-  JELLYSWAP
-  NERVENETWORK
-  REN PROTOCOL

Lending & Borrowing

-  CREAM.FINANCE
-  FORTUBE
-  VENUS
-  ALPHA FINANCE

Entertainment

-  BOUNCE
-  DEGO
-  JUGGERNAUT

Wallets

-  BINANCE CHAIN WALLET
-  MATH WALLET
-  MYETHERWALLET
-  ONTO WALLET
-  SAFEPAL WALLET
-  TRUST WALLET
-  TOKENPOCKET
-  COIN98 WALLET
-  DFOX WALLET
-  BITKEEP WALLET
-  MIDAS WALLET

Insurance

-  CERTIK
-  HELMET
-  SOTERIA

Aggregators

-  BSCEX
-  OPENOCEAN
-  1INCH

Derivative

-  HEDGET
-  METTALEX
-  INJECTIVE PROTOCOL

Ecosystem

-  BSCSCAN
-  MYWISH
-  NOWNODES
-  SNAPSHOT
-  YIELDWATCH.NET
-  LITENTRY
-  SWIRGE
-  PARSIO
-  MIRROR PROTOCOL
-  KEEP3R NETWORK
-  BERRY DATA
-  DXSALE
-  VFAT.TOOLS

NFT Marketplace

-  BAKERYSWAP
-  BCAEX
-  LOOTEX
-  PANCAKESWAP
-  GET PROTOCOL

DEXes

-  BAKERYSWAP
-  BURGERSWAP
-  PANCAKESWAP
-  SPARTAN PROTOCOL
-  STABLEXSWAP
-  UNIFI
-  NARWHALS
-  JULSWAP
-  ZEEDEX
-  DODO DEX
-  KEBAB FINANCE
-  CHEESESWAP
-  CAFESWAP
-  GOOSE FINANCE
-  CROW FINANCE
-  VALUE DEFI

Rankings and Market data

-  BITQUERY
-  COINMARKETCAP
-  COINGECKO
-  DAPPRADAR
-  DEFISTATION

Yield Optimizers

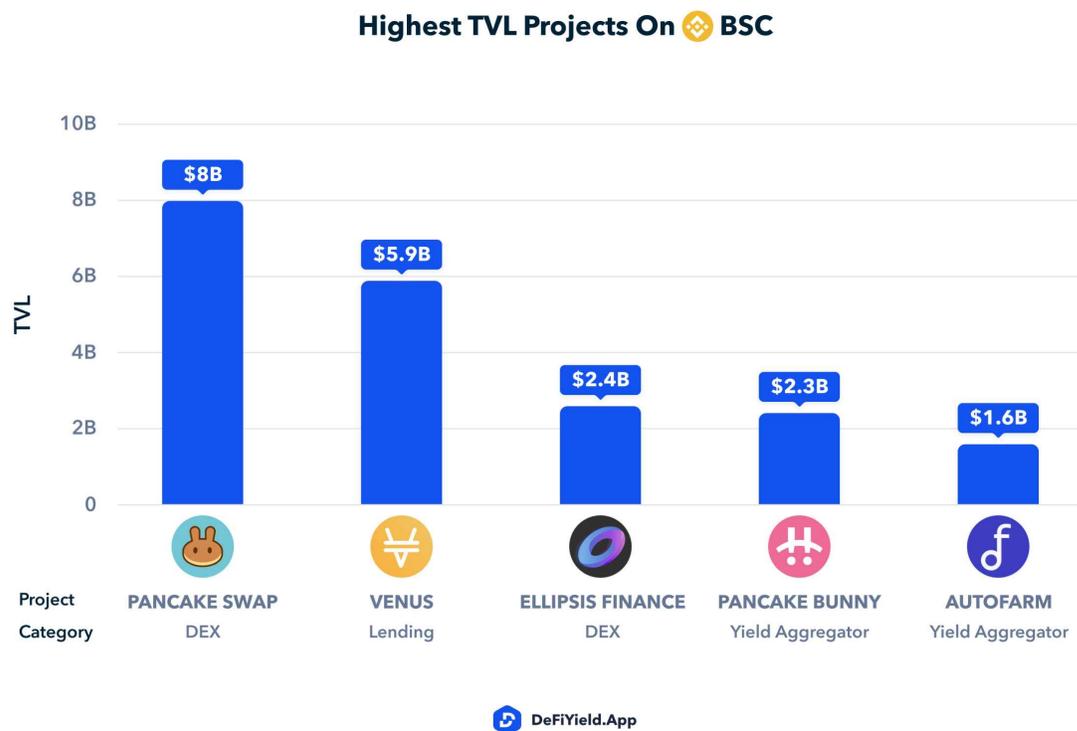
-  AUTO FARM
-  ACRYPTOS
-  BEEFY.FINANCE
-  FRY WORLD
-  JETFUEL
-  PANCAKEBUNNY
-  BEARN.FI

 DeFiYield.App

While Binance Chain, which had been launched in April 2019, did not support smart contract interactions and was designed to facilitate trading, BSC was developed to run smart contracts and enable compatibility with the Ethereum Virtual Machine.

With the deployment of BSC, a new token standard was introduced called BEP-20. It can be used by developers as a flexible format for issuing different tokens with different goals, such as the creation of peg versions of other blockchains' tokens, in order to make them applicable to BSC. Fees for all transactions with BEP-20 tokens are paid in BNB.

BSC can be DeFined as an extension to Binance Chain but it is not an off-chain scalability solution for Binance Chain. It functions independently and smart contracts can be run on it even if Binance Chain is disabled. By developing BSC, Binance's main aim was to enable DeFi projects to relocate from Ethereum, which is why it was also made sure that the network is compatible with popular user applications like Metamask. It's very easy to configure the wallet to work with BSC and only requires a couple of setting changes.



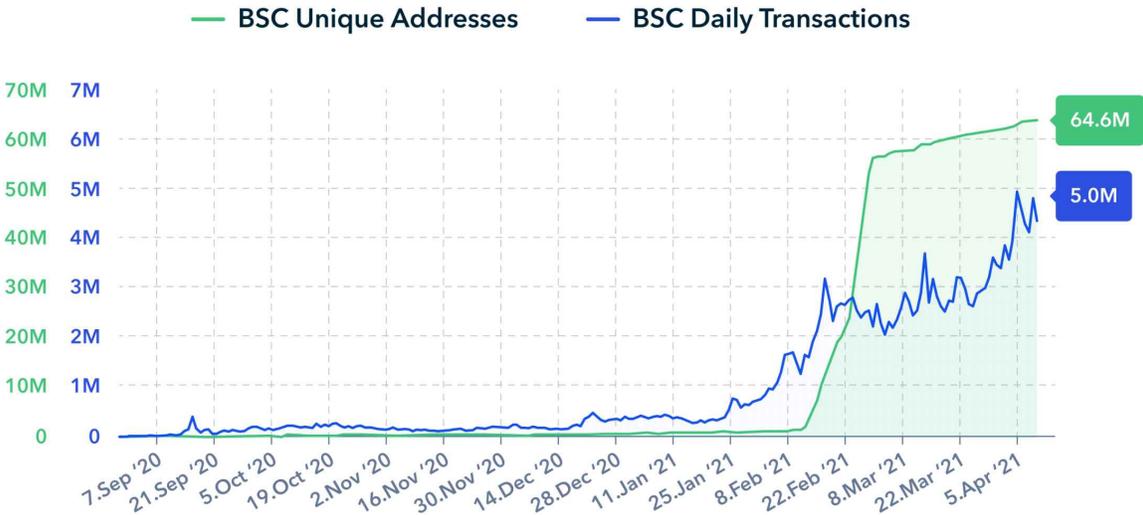
A number of effective DeFi apps are already built on BSC, with [PancakeSwap](#) standing out as a great Yield Farming opportunity. Projects with similar offers are Autofarm and BakerySwap. Spartan Protocol is another BSC-based project, which was developed as an efficient platform

for decentralized derivatives. It includes exchange services and money-market offers that are similar to the ETH-based Aave project.

This dual-chain system is important for users as it allows them to smoothly transfer assets used in DeFi from one chain to another. It is why the DeFiYield cross-chain app is also available for Binance Chain and Huobi ECO Chain.

The flexibility of Binance Smart Chain is already having a major effect on the growth of the entire DeFi space. This growth can be seen in the continuing adoption of Binance Smart Chain, with the increasing number of daily transactions on BSC demonstrating how the network is constantly gaining new users.

BSC adoption growth



Huobi ECO Chain

Another smart contract chain that is proving to be a good alternative for yield farmers who are put off by the high transaction fees experienced on Ethereum is [Huobi ECO Chain](#).

Huobi is an established cryptocurrency exchange with high transaction volumes and a large user base across the US, South Korea and other major cryptocurrency locations. Similarly to Binance Smart Chain, it has replicated the functionality of Ethereum in order to drain liquidity from it in what can be referred to as a vampire attack.

Huobi has a lot of customers across the globe and therefore may well succeed at draining liquidity from Ethereum because it can market to an established user base. Just as with Binance Smart Chain, it is likely that it has a good short-term advantage over Ethereum in 2021, at least until Ethereum transaction fees come down when new scalability solutions are introduced.

Interoperability

One of the most interesting developments of the bull run that has occurred from late 2020 into 2021 has been the way interoperability between blockchain has emerged. This topic has been on the radar of most people working in crypto for sometime but only recently has it become a really important reality for improving the experience with DeFi.

There are basically three ways that assets can switch between blockchains and therefore enable interoperability. These are atomic swaps, bridges and protocol interoperability.

The most well known interoperability protocols are Polkadot and Cosmos. Polkadot, which styles itself as a platform for Web3, was created by Ethereum's former CTO and co-founder Gavin Wood. Cosmos, which calls itself the internet of blockchains, was created by Jae Kwon, Zarko Milosevic and Ethan Buchman.

While it's not necessary to understand every technical detail behind these blockchain networks, it's worth understanding that interoperability will play a big part in how DeFi develops in the future.

We are already starting to see how DeFi projects are allowing their users to swap between blockchains without the need to understand the specifics of how this occurs. This trend will continue and accelerate over time, as interoperability becomes more and more established and cross-chain movements are abstracted away from the user experience.

Interoperability will allow users to hold collateral-type assets securely on one chain while also taking advantage of the transaction or user experience benefits of another chain, without needing to be technical at all. The [Compound CASH](#) system that is in development at the moment is a good example of early innovation in this space and something that we are likely to see a lot more of in future.

Layer 2 scalability

The question of scaling the Ethereum network to allow it to handle more transactions without gas fees spiking is not a new one. However, just as the DeFi bull run has increased the focus on cross chain solutions and interoperability, so has it meant that layer 2 solutions are increasingly being talked about.

Layer 2 solutions are chain-specific scaling solutions that use a sidechain of the main chain. Transactions can be calculated and batched on a sidechain before being completed in one go on the main chain, thereby reducing the cost of multiple transactions into just one.

A good way of thinking about this process is like how an accountant might create a ledger on a spreadsheet. While the main functions and formulae are incorporated into the spreadsheet, they will probably also use a pen to make small additions and subtractions on a piece of paper, which can then be added to the main spreadsheet in order to produce a finalised ledger. In this analogy, the spreadsheet is the main chain and the paper is the layer 2 sidechain.

Well known layer 2 solutions include [zkSync](#), which was created by Matter Labs, [Starkwave](#) and Optimism. Vitalik Buterin, the creator of Ethereum, has personally given his support to both zkSync and Optimism but all these solutions can be used to increase scalability. For example, traders might put limit orders on a sidechain, which can be made if someone else can be matched against the trade or released if no takers appear.

L2 Scalability Adoption

Project	Technology	Ecosystem Products		
 zkSync	zkRollup	 LOOPRING  linch  BINANCE  argent  flexa  StablePay  numio	 AAVE  coinbase  MoonPay  imToken  CoinGecko  golem  Curve	 Balancer  Huobi  ripio  MYKEY  STORJ  GITCOIN
 LOOPRING	zkRollup	 GITCOIN	 RAILS	 pNetwork
 STARKWARE	zk-STARK	 DeversiFi	 IMMUTABLE	 dYdX
 Aztec	zk-SNARK	 Zcash	 U S K	 MatterLabs
<i>Optimism</i>	Optimistic Rollup	 SYNTHETIX EXCHANGE	 coinbase	 Uniswap
 Hermes	zkRollup	—		

Increasing flexibility and functional updates of DeFi projects

As DeFi is a highly competitive and innovative environment, projects have to constantly update their functionality to satisfy as many user requirements as possible. Even if a project is well-known in the community and had a large influence on the industry in the past, it doesn't mean users will be loyal forever.

Uniswap is a great example of how a large, successful DeFi project follows market trends and pushes innovations to improve user experience and facilitate the overall DeFi adoption.

Uniswap V3

In order to keep its leading market positions, the project introduces Version 3. The two main advantages of the new version are concentrated liquidity and multiple fee tiers.

Concentrated liquidity is going to allow liquidity providers to control within what price ranges their funds can be allocated. This creates a set of individual positions combined in a single pool where users can trade.

Multiple fee tiers are introduced to compensate risks taken by LPs in accordance with degrees of the risks.

The updates enable:

- liquidity provision with up to 4000x investment efficiency compared to V2
- low-slippage trade execution
- lowering the downside risk of preferred assets
- improvement of the time weighted average price (TWAP) oracles, where any TWAP within the past ~9 days can be calculated in a single on-chain call
- decreasing gas costs through deployment of the L 2 Optimism solution

With introduction of these new features, the Uniswap team is striving to offer users the most flexible and advantageous AMM

Project partnerships

Increasingly, projects are partnering with one another where they see synergies between their stated aims and users they serve to.

There is a big difference between a DeFi partnership or merger and one that occurs in traditional finance. In traditional finance, such events usually require one dominant party to acquire the assets and rights of the other entity or they require the foundation of a new integrated entity, where stakeholders share rights and control. DeFi partnerships and mergers are usually based on a highly flexible set of terms for both parties.

Usually, a partnership in DeFi will seem advantageous if it can generate the following benefits:

- Greater economies of scale
- Acquisition of developer talent
- Increased promotion of the projects involved

Not all partnerships and mergers are the same though, so it's worth looking at a few early examples of how this has occurred in practice.

The Yearn Finance ecosystem

Yearn Finance is an outstanding example of this trend in DeFi, as the project has performed a range of strategic partnerships and structural transformations. The aim of its strategy has been to become a multi-purpose DeFi platform that offers a wide range of services. This diversification has already drawn the attention of yield farmers.

It could be said that Yearn Finance started the trend for partnerships as far back as its launch. The cooperation it enabled with Curve Finance on the development of its yPool and YFI Balancer pool resulted in a massive increase in awareness amongst the DeFi community and was covered at length by crypto media outlets and within forum discussions. Presumably, the success of this partnership led Yearn Finance to investigate how similar moves could positively affect the project too.

More recently, Yearn Finance extended its ecosystem with four other DeFi projects in the space of just one week. These involved mergers with Pickle Finance, C.R.E.A.M and Cover, plus a partnership with PowerPool.

Through the merger with CREAM, Yearn Finance wanted to develop and implement a more complex network of lending protocols to function as a

highly effective lending market. The Yearn Finance team will be involved in the development of CREAM V2, which is aimed at designing products for lending and leverage. Moreover, the flagship Yield Farming product of Pickle Finance, the pickle jars, will be integrated into the V2-vaults.

[Yearn Finance has also stepped into the field of smart contract coverage through the merger with Cover Protocol.](#) This project focuses on hedging against the risks inherent to farming and staking, and the Yearn Finance founder Andre Cronje was already advising the project before the merger was agreed.

Probably the most significant merger for the Yield Farming community though was the one Yearn Finance with SushiSwap initiated just after these announcements. This strategy was focused on putting together the best technical features of both platforms in order to offer a better infrastructure, combining total value locked into a single pool of assets and benefiting from common developer resources. Yearn is therefore clearly considering both horizontal and vertical approaches in its merger strategies.

Horizontal mergers are aimed at increasing market share and consolidating development resources. Vertical mergers are focused on incorporating different companies into single vertically integrated structures. Within these new structures, different entities can continue developing their regular products and services, but they also become integrated into one combined supply chain. The goal is to achieve synergies, and the Sushiswap, Cover and Cream mergers all fall into this latter category of vertical mergers.

DEXes extend their trading tools

Interest in decentralised exchanges has gradually increased over time amongst traders for a number of reasons, but one of the most important is that they fit more comfortably into the idea of decentralized finance than their centralized counterparts. That's because you do not have to give up custody of your assets to a centralized third party, which could lose them in an attack or seize them from you.

Trading volume on Ethereum-based DEXes



 DeFiYield.App

Although the number of users using DEXes has exploded, there are still a few UI-related obstacles that DEXes have to overcome to keep attracting new users. Various DeFi projects are innovating in this direction and user experience improvements are being made on an ongoing basis.

For example, most DEXes have added limit orders and decentralized order books recently, with one example being dYdX. These allow users to buy or sell assets at a specific price and remove the need to rely on market orders, which expose them to greater trading risks during volatile periods. If volatility is high or if a trade takes a long time to execute, users can experience large price slippages, affecting their investment strategies. Limit orders negate this and, when implemented on DEXes, are totally

noncustodial, which ensures users stay in control of their assets throughout.

Another feature that DEXes are adding is stop orders. These allow users to not have to wait for a certain price level to be reached in order to perform a desired transaction. Instead, they specify an exact price at which their buy or sell order will be automatically executed and are therefore able to manage risk.

Finally, a lot of DEXes are also working on enabling margin trading. Essentially, this allows traders to leverage funds in order to multiply their purchasing power. As with the other features mentioned, margin trading on DEXes is much more advantageous than on centralized exchanges firstly because users do not need to trust a third party and share personal information. Secondly, no hidden fees are present.

DeFiYield is also at the forefront of innovation in this space with a host of new relevant tools. These include the L2 Dex Aggregator, that allows for cross-chain crypto swaps at the best rates, and Cross-chain Spot Trading, which includes real-time trading charts, limit orders, asset leveraging, fast withdrawals and a potential for short positions.

Adoption of seigniorage coins

While the hype around these digital assets was temporary, the journey they are on is far from over as they represent a new way of optimizing monetary policies for cryptocurrencies.

If you're still uncertain about what differentiates these assets from others, one key feature to understand about them is that they are algorithmic stablecoins. This means their value is not collateralized with any asset and is instead adjusted algorithmically through certain supply dynamics. One of the main reasons they are so important is because they may provide a solution to the problems of using cryptocurrencies as a store of value and medium of exchange.

Seigniorage coins define the optimal coin supply and achieve this through the separation of the demand for a coin into speculative demand and transactional demand.

The benefits that seigniorage coins might provide to the DeFi ecosystem in future are as follows:

- Autonomy from outside markets
- Decentralization
- Stable value that protects against volatility
- No reliance on tangible assets
- Ability to integrate with any DeFi application

New seigniorage coin projects continue to emerge and this is leading to a distinct new DeFi sector that is worth keeping an eye on, even though the initial hype has passed.

NFTs

Non-fungible tokens (NFTs) are totally unique assets that cannot be duplicated or divided up.

They differ from other tokens, such as Bitcoin, which are fungible because each individual token is exactly the same. Just like one dollar can be swapped for one dollar, one bitcoin can be swapped for one bitcoin and this like-for-like exchangeability is key to a token being fungible.

NFTs have been around for some time and are the technology behind [CryptoKitties](#), which received a lot of coverage in the 2017 bull run. They have developed a lot since then though, and the strong belief behind the hype is that, because NFTs create digital scarcity, they can be used to revolutionise how music, art, content, collectables and many other unique goods are owned and paid for.

The majority of current activity is occurring across the most well known NFT marketplaces, which are [Rarible](#), [OpenSea](#), Mintbase and Nifty Gateway.

The 2021 NFT hype

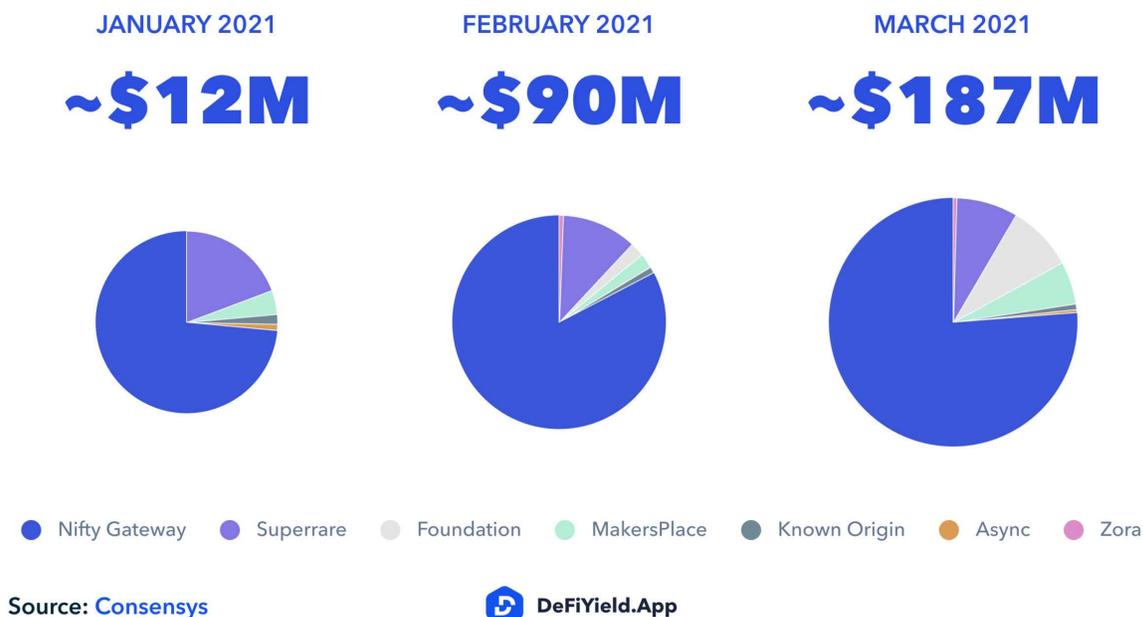
NFTs have caught the public's attention in a big way in 2021. This is mainly because of the celebrities, influencers and artists that have been promoting them. Such examples demonstrate that this trend for the future is already happening now.

Record NFT digital art sales

Even now, digital art is being sold at extraordinary prices. Beeple set a record price for a piece of NFT digital art, when his "[EVERYDAYS: THE FIRST 5000 DAYS](#)" sold for the equivalent of \$69.3m (40,652 ETH) through renowned auction house Christie's.

This followed other pieces of his art that he sold for large amounts, including CROSSROADS, which sold for \$6.6m (3,869 ETH), and THE COMPLETE MF COLLECTION, which sold for \$777,777 (456 ETH). Other artists that have managed to sell NFT digital art for significant amounts include pak, steveaoki and antonitudisco.

Crypto art volumes by marketplace in USD



Celebrity endorsements

Many of the richest people in the world who have already declared an interest in bitcoin, cryptocurrencies and DeFi, are also showing the same interest in NFTs.

These include [Jack Dorsey, who sold his first tweet as an NFT for over \\$2.9million](#), Elon Musk, who planned to sell a techno song as an NFT before withdrawing, and Mark Cuban, who has declared that he has invested in NFT platform Mintable. Grimes, the artist who is also the partner of Elon Musk, has sold off various images and videos for the equivalent of \$6 million.

Other social media influencers involved in NFTs include Logan Paul, who has sold over \$5million of NFTs, and Gary Vee, the investor and entrepreneur, has said he believes NFTs will be the gateway into crypto for the masses.

Brands getting in on NFTs

As well as the artists and celebrities selling rare pieces of art and music as NFTs, some well known brands are using their exclusive content licences to generate NFT digital collectibles.

Probably the best known of these is NBA Topshots, which are the officially licensed digital collectibles of the US National Basketball Association. The items being sold are short videos of significant shots or plays within games, which are “marked at creation with a unique serial number, with guaranteed scarcity and protected ownership guaranteed by the blockchain”.

The most expensive topshots, which include players such as LeBron James, Ja Morant and Zion Williamson, are trading for over \$200,000 on the platform’s marketplace.

The future of NFTs

While both the total potential value of the NFT market and the specific value of individual items is very difficult to assess right now, this is definitely a part of the crypto markets that you should keep an eye on. It’s also worth understanding a couple of dynamics that may result in the NFT industry operating in a slightly different way to many other areas of DeFi.

Firstly, there is the fact that the unique nature of an NFT means it is very unlikely that a regulatory body would see it as a security. They are more likely to be treated as a commodity, which means less potential difficulties for the issuer and therefore more likelihood that a greater number of issuers, including celebrities, artists and influencers, will be attracted to this space.

Secondly, you should also consider that the prices of NFTs will likely be uncorrelated to other crypto markets. Correlation has been a big part of crypto markets as they have grown over the last decade but NFTs are likely to be uncorrelated to other cryptocurrency and token prices, just as fine art is uncorrelated to gold or stocks.

Security concerns

For all of the positive trends that are emerging within Yield Farming, it should be noted that security concerns persist.

As the market innovates, some of this innovation will bring about more technologically complex projects that require more sophisticated investment strategies. Yield farmers should be aware of this complexity and make sure to research all opportunities thoroughly if they are to avoid opening themselves up to new security risks. Furthermore, they should be aware that, as DeFi grows, smart contract auditing cannot slip. The industry is currently lacking in qualified smart contract developers and auditors, so this is a real risk that users should be aware of.

Another issue to be aware of as DeFi and the wider crypto markets grow, is the threat that cyber attackers pose. Users need to stay alert to spot any scam projects these attackers might develop in order to steal funds, as well as always attempt to keep their identities hidden.

Of course, all of this should not stop you from taking advantage of the benefits that Yield Farming provides. It's a matter of being forewarned so that you are forearmed. The best way to remain up to date with any security issues you should avoid is through DeFiYield.App, which has all the tools and resources you need to succeed at Yield Farming while remaining safe.

Highlights of the chapter

DeFi is a highly innovative environment attracting users and investors from all over the world due to the wide range of advantages it has over traditional finance.

As new solutions are being constantly introduced by DeFi projects to improve user experience, offer higher returns to investors and mitigate security concerns, it's expected that the industry will keep its impressive growth pace in the long term.

The main current trends of the DeFi development are:

- enhancement of decentralized governance;
- further elaboration of cross-chain solutions;
- project partnerships;
- increasing adoption of Binance Smart Chain and Huobi ECO Chain;
- solutions enabling gas cost reduction on Ethereum, such as Layer 2 scalability;
- increasing flexibility and competitiveness of DeFi projects ;
- DEXes offering a bigger variety of services to attract more users from centralized exchanges;
- NFTs;
- Fighting security concerns through the community synergy, informing users about potential financial threats, auditing DeFi projects and introduction of automated tools for checking security of smart contracts.

WHY YOU SHOULD USE DEFIYIELD NOW

At the very start of this book, I included a quote from Mark Cuban, the billionaire internet entrepreneur. He said that DeFi is straightforward if you understand the principles and try it for yourself. In the same interview, he also gave the following message to the DeFi industry:

“If you don’t take care of the little guy, it’s going to backfire on the whole [DeFi] industry.”

Taking care of all of our users as they journey through the exciting world of DeFi is exactly what we are all about at DeFiYield.

Throughout “The Wall Street Era is Over”, we have outlined in detail the principles for succeeding at Yield Farming while staying safe. By reading this book, you have significantly reduced your risk exposure already.

The problems DeFiYield solves for DeFi users

There are still many issues that remain for Yield farmers, which can be summarised as follows:

- **Accessibility** - the poor user experience of many projects, coupled with the need to use and understand many different and unfamiliar tools, means it's still difficult to access DeFi.
- **Complexity** - you need to have a lot of foundational knowledge, and you must keep up with a large amount of new information, if you are going to succeed.
- **Security** - defects in smart contracts and the work of scammers mean that users must constantly be aware of DeFi's risks.

Solving these problems for users is at the heart of what we do. DeFiYield is a unique platform with many features designed to help you access, manage and secure your DeFi assets through a single, user-friendly portal. We are constantly updating and improving the solutions at DeFiYield, and new tools are always in development.

Please visit us at <https://DeFiYield.App/> to see the latest ways that we're improving DeFi. If you are finding "The Wall Street Era is Over" useful, we expect you'll feel the same way about DeFiYield!

CONCLUSION

Time for next steps

You've reached the end of *The Wall Street Era is Over*. But this is just the beginning of your journey.

Hopefully, you're excited about what's coming next for you in DeFi, and maybe you've already joined in. Since you've read this far, we assume you see the enormous potential of an informed approach to DeFi. It stands to make a positive impact on the finances of everyone who participates.

In turn, it's easy to see why DeFi is poised to create change for the better throughout the world economy. This is Finance 3.0 at its most advanced, an astonishing convergence of money and computer code, contracts that can execute on their own, and trustless environments where no central authority is needed. That means banking without middlemen, finance without friction. It truly is a revolution.

Throughout *The Wall Street Era is Over*, it's been our goal to empower you to take part. We've told you our own story—the good, the bad, and the ugly—and why DeFi is so important to us. You should have a firm grasp now of what makes DeFi different than anything, the protocols that form its foundation, and the projects that are propelling it. We've dealt with decentralized governance, and even lived through vampire attacks!

From there, we've tried to show you where you fit in. Are you a cautious investor, or are you risk-on or degen? And what do you need to know in order to properly size up a DeFi investment opportunity? From those generalities we zero in on the specifics, so you can apply these universal principles before you invest in particular projects.

That's when we draw back the curtain on the heart of DeFi for the individual investor: Yield Farming. Yield Farming is what we're really so excited about—it's where the opportunity in DeFi truly lies. And also the danger.

As you can see, we have not tried to give you a one-dimensional view of Yield Farming. Naturally, we are DeFi enthusiasts, but that doesn't mean

that we think it's for everybody. On the one hand, Yield Farming has the appeal of high returns, composable “money Legos” that form fascinating new financial structures, and much more growth to come. On the other hand, Yield Farming can be *hard*. Many of the tools are still in their infancy and difficult to use, there is extreme volatility, scams, and (for now) scant consequences for the scammers.

It's Your Turn

Once you made it that far, we shared what has made us successful: Our strategies. Our hope is that *The Wall Street Era is Over* is a playbook will not only enrich you financially, but also make you want to be a part of the larger DeFi community. At its best, the Yield Farming community are people who want to help each other learn and succeed.

Even the best investors, from traditional finance to DeFi, have days where they lose money. We certainly have! That's OK if those losses come as a result of the inevitable ups and downs of value changing hands via a level playing field.

Where it is definitely NOT OK, however, is if your losses come at the hands of scammers whose line of business is to trick you and steal your money. We've done everything we can to alert you to this possibility. As painful as it was, we've told you our own story of getting scammed so you'll understand our motivations. It was bad enough that it happened to us—we don't want it to happen to you.

This book outlines steps for you to stay safe, and DeFiYield's tools go even further. Please use them! Your safety in the DeFi space is paramount, because without security this vital financial sector cannot grow.

Things change fast in crypto, and NFTs are a great example of that. Although NFTs are not part of DeFi, strictly speaking, we included them because they're a perfect demonstration of how a crypto sector can suddenly explode in both attention and value, as they did in Q1 2021. Something that seemed like a fun diversion, as NFTs first did when they debuted as CryptoKitties in 2017, can suddenly become very serious business. That's true throughout crypto, and it's true in DeFi. Our point is, if something catches your eye, keep track of it—you never know when it might catch on.

The last section is all about DeFiYield's tools. We didn't want this book to be a veiled sales pitch for DeFiYield—it's first and foremost a guide for Yield Farmers to go deeper into the space and do so safely. We've told you about a wide range of tools, and we've even included "competing" platforms in these pages. You should choose the ones that feel best to you.

But when you try out what we've built at DeFiYield—such as the Cross-Chain Asset Management Dashboard, Yield Farming Optimizer, and especially DeFiYield Safe—we hope you'll feel the spiritual connection between our platform and this book. We created them to make DeFi a better place—not just profitable, but safe, stimulating, and exhilarating to explore. All we need now is YOU.

GLOSSARY OF TERMS

Arbitrage is benefiting from price differences of an asset between two markets. The profit is made from purchasing the asset on the exchange with the lower price and selling it for a higher price on the second exchange.

Backdoor is a deliberate security weakening of a smart contract aiming deceiving manipulations with user funds. This refers to situations when devs introduce functions and conditions of their execution to the code that allow them to control user assets, including transferring them to any wanted addresses seamlessly and at any time.

Collateralization is backing the value of one asset with the use of another asset. In the context of DeFi, this process is associated with locking of collateralized assets on a blockchain protocol. Usually, collateralization is used to secure loans or maintain value of stablecoins.

Crypto wallet is a software or a device that stores public and private keys and allows users to store, send, receive and monitor tokens of various blockchains.

Custodial and **noncustodial** are classifications of financial services provided to users for storage and management of their assets, where presence of the third party control over these assets is the main criterion of referring a service to one of the classes. In DeFi, noncustodial means that users can control their own crypto without being dependent on any external entity that would be responsible for management of the assets held, constantly exposing users to the risk of security issues, conflict of interests or betrayal.

DAO (decentralized autonomous organization) is a way of structuring an organization where it runs based on rules encoded on a blockchain. All decisions are made through voting of network participants. Transactions are executed automatically and only if all predefined required terms are met. No centralized guiding and control takes place in such a system.

Etherscan is a block explorer that allows analyzing transactions performed on Ethereum.

Epoch is a division of time used in a blockchain protocol.

DEX (Decentralized Exchange) is a digital platform designed to allow its users buying and selling cryptocurrency assets in the peer-to-peer way based on a set of conditions encoded on a blockchain. All offered services are provided automatically without participation of centralized intermediaries. Usually, DEXs are run by decentralized governance.

FOMO (Fear of missing out) is a form of anxiety experienced by participants of the cryptocurrency market that comes from a belief that peers might be benefiting from a possibly favorable event or a hyped project. The person experiencing FOMO feels an urgent need to repeat what everybody around is doing.

Gas is the fee that is required to conduct a transaction or a smart contract on a blockchain.

Gwei is the smallest unit of Ether (ETH) - the Ethereum network's cryptocurrency. 1 gwei is equal to 0.000000001 ETH

ICO (Initial Coin Offering) is a capital-raising process initiated by a crypto project.

Ledger is a system storing data about financial transactions. Blockchains function like distributed ledgers: they consist of a variety of nodes processing and verifying every transaction, generating records and creating a veracity consensus.

Leverage is a trading or investment tool that refers to borrowing funds in order to increase purchasing power and generate higher returns.

Liquidation is distributing assets of a borrower to a claimant when the required collateralization ratio is not maintained.

Liquidity pool is a pool of tokens locked in a smart contract and used as a source of liquidity for trading operations, lending, borrowing and other services, offered by decentralized Apps.

Liquidity is associated with the ease with which an asset can be converted to cash without having significant influence to its price on the selected market. In the crypto industry, liquidity usually refers to the trading volume in a market.

Margin trading is borrowing funds from a third party with a purpose of increase of the purchasing power in performing trading operations.

Metamask is a popular cryptocurrency wallet that allows users to interact with distributed applications based on the Ethereum blockchain.

Oracles are third-party services used by blockchain protocols as sources of external real-world data.

Order book is a list of buy and sell orders (bids and asks) for a specific asset placed by participants of a market at specific prices. Information about prices from order books is critical for investment and trading decisions.

Premining is a process that involves issuing a cryptocurrency asset before a project is launched and its blockchain protocol is deployed. As premining is controlled by project owners or core developers, it can be considered as a controversial step on the project's roadmap. Premined funds can not only be used as a reserve pool, ensuring financial soundness of the project, but also they can be distributed among small number of people that will have significant influence on development of the project and on market price of its tokens, if the receivers of the premined funds decide to sell them on the open market.

Private key is an algorithmic password, automatically generated by a blockchain wallet, that is required to access cryptocurrency assets and conduct transactions with them.

Rekt is a DeFi slang word derived from "wrecked" that describes a tremendous fund loss resulting from investment or trade. It may also refer to situations when the value of a crypto asset collapses.

Rug pull can be DeFined as an unexpected theft of token liquidity, provided by project investors, that is performed by scammers through malicious strategy contracts.

Scalability is the property of a blockchain to handle an increasing number of transactions without worsening the processing speed. The higher scalability of a network, the better it can react to the rising demand.

Slippage is the difference between an expected price of a trade execution and the actual price of the trade execution, which can occur as a result of the delay between the time points of the placing and its completion. This effect can be expected when a user places market orders during high

volatility on the market or when the size of a market order doesn't correspond to the demand for the traded asset.

Smart contract is a set of encoded terms of a transaction agreement that executes automatically through validation on a selected blockchain when the terms are met. Information about executed transactions is stored on the blockchain and can be tracked by users.

Stablecoin is a cryptocurrency whose value is linked to an outside, more stable asset, such as fiat, for stabilization of its price, which allows participants of the cryptocurrency market to use it as a store-of-value. Stablecoins can be backed with fiat, commodity, cryptocurrency or they can be algo-based, meaning its value is maintained automatically by an algorithm encoded on a blockchain protocol.

Store-of-Value is an asset whose value remains unaltered over time without being depreciated. Therefore, it can be used as a reliable means of saving purchasing power for future transactions.

Token is a crypto asset designed with a certain utility for accessing and using certain blockchain.

Volatility is a degree of the price change of an asset within an analyzed timeframe, which creates profit opportunities or can cause losses. The larger the price swing, the higher volatility.

Web 3.0 is the next step of the internet. Web 1.0 was the early, static web and Web 2.0 was the social but centralized web that big tech dominates. Web 3.0 is decentralized and powered by crypto.

Whale is an individual or an entity that possesses large enough funds to move prices for crypto assets, traded on a specific market. They can use their huge financial potential to make profits manipulating the prices.

White paper is a technical document issued by a blockchain project that explains its purpose, uniqueness, outlines its main features and presents the applied technology. This document may be updated at certain development stages of the project.

[1] Mark Cuban said this on the Bankless video and podcast show, when he was interviewed for the episode 'Why DeFi is the Future', which was released in February 2021.

[2] The important additional point to note here is that, if you start using your wallet to interact with DeFi, you will be giving the smart contracts that are

within these dapps access to your wallet.