

DEFI

DEMYSTIFIED

AN INTRODUCTION TO
DECENTRALIZED FINANCE

JAMES BACHINI

James Bachini

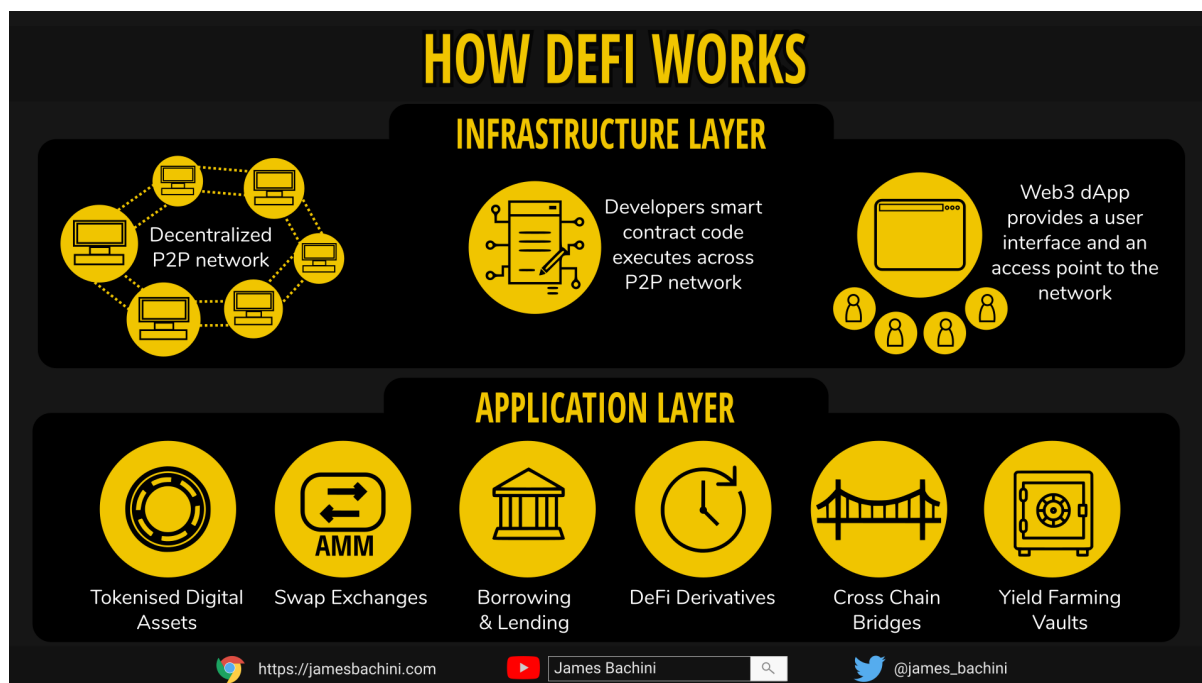
DEFI DEMYSTIFIED

An Introduction To Decentralized Finance

Introduction	7
History of Cryptocurrency	8
Smart Contracts	13
dApps & Web3	14
Automated Market Makers	20
Synthetic Assets	23
Stablecoins Compared	24
DeFi Borrowing & Lending	28
Crypto Oracles	30
Token Launches	31
DeFi Derivatives	34
Where Does Yield Come From	42
Impermanent Loss	46
DeFi Risk Framework	52
Setting Up A Wallet	60
Testnets	60
Block Explorers	61
Yield Farming	61
What Comes Next	62
Regulation	62
Central Bank Digital Currencies	63
Bridging Traditional Finance	63
Multichain	64
Further Reading	64
About The Author	65
DeFi Definitions & Terminology	65

Introduction

For a quick understanding of the DeFi sector we can break down the tech into two areas, infrastructure and application layers.



DeFi Infrastructure Layer

The infrastructure for DeFi runs on a peer to peer network much like torrent or napster (for want of a better example) networks where each computer connects to another computer on the network to share information.

On Bitcoin they share transactional information about who is sending who funds. On Ethereum each node runs a virtual machine which is an isolated computer program that executes 3rd party code. Developers can deploy their smart contract code to the network and all the computers on the peer to peer network will execute it. Small amounts of data can be stored on the network as well.

For non-developers a web based user interface is provided. They can simply connect a web browser to the platform's website. Then funds can be deployed from a digital wallet which is often a browser plugin. The wallet is connected to the website, the website connects to the smart contracts and transactions and functions can be executed at the click of a button.

DeFi Application Layer

The application layer is built on smart contract backends and web3 dapp frontends much like traditional web development is built on databases and user interfaces.

At this point everyone has heard of tokens and there are two main types to be aware of.

- Fungible tokens = All the same My Bitcoin = Your Bitcoin
- Non Fungible Tokens (NFT's) = Unique ownership rights, no one has the same NFT as me

Fungible tokens are swapped on automated market makers the most famous of which is Uniswap. These enable investors to deploy liquidity pools containing two digital assets and then traders can swap one for the other.

Borrowing and lending platforms enable users to take out over-collateralized loans and investors to gain a yield on their holdings.

DeFi derivatives are similar to traditional finance futures and options products except they use digital assets.

Ethereum isn't the only network to create a booming DeFi ecosystem and as we see new emerging blockchains compete, the ability to transfer funds between blockchains has become big business.

On top of all these building blocks developers can deploy yield farming strategies and vaults to programmatically move funds around to gain the best yield possible on their digital assets.

History of Cryptocurrency

The history of cryptocurrency starts long before Bitcoin. Blockchain's have been around since the 1980's and Bitcoin was built not as a totally novel concept but on top of other works like Nick Szabo's BitGold which predated it. However the explosion of Bitcoin, Ethereum and other cryptocurrencies created a trillion dollar asset class built on an elegantly simple idea. The decentralization of financial technology via a shared blockchain.

Bitcoin | Zero To One For Blockchain

31 October 2008

Hal Finney was at home in Temple City, California, reading a post about a peer-to-peer cash system. The [whitepaper](#) described blocks of data, stacked in numerical order and interlinked with cryptography known as a blockchain. The elegant beauty of a blockchain meant that to change any single block you would need to adjust all the blocks on top of it. This provided an immutable store of data that could be used to keep a record of transactions.

The paper described digital cash distributed to miners who interlink the blocks in a process known as proof of work. A miner on the peer-to-peer network takes all the waiting transactions, compiles them into a block of data and then repeats a hashing calculation over and over



again. Roughly every ten minutes one miner on the network will find a hash which meets a set target criteria and the block is finalized. The miner gets a block reward and the network moves on to the next block starting the process over.

Hal was intrigued by the concept of digital money and contacted the developer. Satoshi Nakamoto was obviously an anonymous pseudonym, perhaps for an individual or a small group, perhaps it was Hal himself, to this day the creator of Bitcoin is still a mystery.

Satoshi mined over 1,000,000 Bitcoin in the early days, worth billions and has never moved or used any of those funds. If Bitcoin reaches somewhere around \$200,000 Satoshi Nakamoto will become the wealthiest person in the world.

The first block on a blockchain is known as the genesis block. Bitcoin's genesis block famously included an encoded message saying *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*

22nd May 2010

In Bitcoin's early days it was used experimentally by cypherpunks and libertarians. The concept of digital money was novel and there was no value associated with the actual Bitcoin's themselves. If anyone could run a program on a home laptop to mine them how could they be digitally scarce?

This changed over time as demand grew and supply was constantly halved every four years due to the halvening schedule. Perhaps the most notable turning point was in May 2010, a time when the community gathered and discussed all things Bitcoin on the forum [BitcoinTalk](#).

Laszlo Hanyecz posted a message to the forum on the 18th May stating *"I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later ... If you're interested please let me know and we can work out a deal."*

Four days later a user called Jercos got the pizza delivered and collected his Bitcoin payment. It was the first time that Bitcoin had been used to make a purchase and today the 22nd May is still celebrated as *Bitcoin Pizza Day* by the blockchain community.

Bitcoin went on to become a trillion dollar asset and was seminal to what came next. It wasn't a smooth ride however and the protocol has faced many challenges along the way. Before DeFi decentralized services for decentralized money there were only centralized exchanges to buy and sell digital assets.

7th February 2014

In late 2013 and early 2014 if you wanted to buy Bitcoin you did it on Mt. Gox, a collectibles marketplace that pivoted to a Bitcoin exchange. Based in Tokyo the exchange handled more than 70% of the total Bitcoin trading volume at its peak.

Mt.Gox allegedly discovers missing funds in it's treasury of 744,408 BTC (3.5% of all Bitcoin) resulting from a bug that had been exploited for over two years. CEO Mark Karpeles held an

emergency investor meeting where he “outlined the extent of the Mt.Gox losses” but investors refused to bail out the company.

Withdrawals in Bitcoin and cash were suspended and within a week the website was closed down and the company filed for liquidation. Karpeles was charged with a suspended sentence in 2019 for falsifying data.

The Mt.Gox failure slowed Bitcoin down but it didn't stop the inevitable growth and powerful network effects. It was around this time that the original code for the Ethereum network was being developed.

“Make no mistake – Ethereum would never have existed without Bitcoin as a forerunner. That said, I think Ethereum is ahead of Bitcoin in many ways and represents the bleeding edge of digital currency.” – Vitalik Buterin

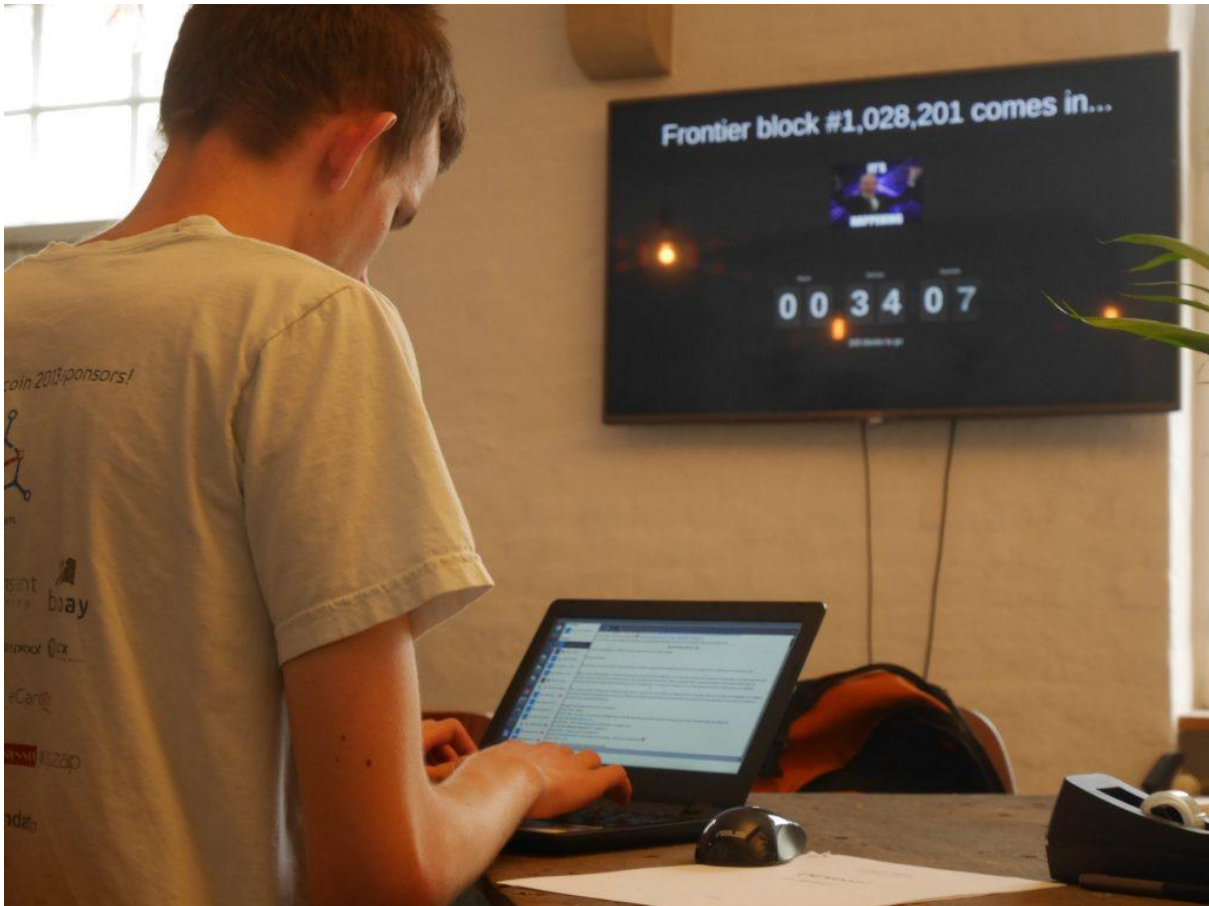
Ethereum | The Worlds Global Computer

30th July 2015

A monitor on the wall counted down as last minute checks were being anxiously executed. In 35 minutes the Ethereum frontier would launch to the public. The software had been in development for two years and the entire crypto community was watching.

Ethereum was revolutionary, it expanded Bitcoin's blockchain technology to provide a peer to peer network of interconnected computers operating as one. Developers could execute code and store information on this network which no one had full control over.

In a small crowded office in Berlin Vitalik Buterin was nervously tapping away on a laptop. He was surrounded by colleagues who supported his vision for a decentralized virtual machine. But at this moment he was alone in his thoughts, it was down to him to launch the network and change the financial world forever.



Before DeFi there was Ethereum. It is the foundation network and protocol layer that decentralized finance is built on. Understanding Ethereum's "*world computer*" is key to understanding what makes DeFi applications so disruptive.

If we think of a collection of computers on a peer-to-peer network all talking to each other in a group. There is no central server or data provider and data is communicated by whispers between the peers. Examples of peer-to-peer networks outside of the blockchain sector include Napster and Torrent networks where files are shared across peers. Each computer interlinks with multiple other computers on the network and broadcasts and relays messages to them. No single computer or central server is in charge of the network.

Transactions coming into the network are processed by the nodes and a consensus mechanism states that more than 50% of the nodes on the network have to agree on the results or state after the transactions are processed. Once the network reaches consensus it moves on to the next block of transactions.

Ethereum was born out of the idea that miners could process code as well as transactions. 3rd party code executing in a secure environment across a global network of machines to store and distribute data.

Whereas Bitcoin could only store transaction data relating to who sent who BTC, Ethereum could store anything you wanted.

This works by including a virtual machine in the code which executes user code in a secure, isolated environment. This code known as a smart contract has been used by developers to create the protocols that form today's DeFi ecosystem.

A virtual machine is like a version of windows running in a window on your laptop. Think of it as an operating system running as an application on top of the main operating system. Ethereum's virtual machine is designed to run across a network of nodes that agree on the persistent state of data on the network. It's not just Ethereum that uses EVM, it's also used by alternate chains like Binance smart chain, Polygon and HECO.

Ethereum still operates a blockchain which stores the transactions which execute interactions with smart contracts. These are hashed in much the same way as the Bitcoin network although block times are much faster and a new block is written approximately every 13 seconds.

The process of hashing is a cryptographic method used to verify data. All data can be broken down into binary ones and zeros. A hashing algorithm can be used to calculate a representative value for that data. The algorithm is one way meaning you can calculate the hash from the data multiple times but can not calculate the data from the hash. If just one byte of the data changes the hash will change completely. The most common hashing algorithm is known as SHA256, a 256-bit (32 bytes) hash usually printed out as a hexadecimal number of 64 digits.

Transactions need to be signed before they are sent to the nodes that form the Ethereum network. This is achieved via a private key, public key pair and is usually done in the background via a digital wallet such as [metamask](#).

A private key is a random set of one's and zero's, you could create one by tossing a coin 256 times although more often it is managed by the wallet. Private keys, as the name suggests, should be kept private as anyone who knows the key can sign transactions and take any funds in the account. A public key is the same thing as your address. On ethereum both private keys and public keys will start with 0x... to show it's a hexadecimal formatted address.

The public key is derived from an accounts private key however it is not possible to find the private key from a public key. When we want another user to send us funds we will share our public key and they will send funds to that address. When they send funds the transaction will be hashed and then signed using their private key and elliptic curve cryptography. This will then be sent to nodes along with their public key to prove the sender approves the transaction. The nodes have a cryptographic function to check if the signature matches the public key for the account.

The persistent storage or state of the network has limited capacity and is expensive to write. A gas fee is charged for transactions that store or modify data however there is no fee to read data. To pay the gas fee a developer needs some Ether or ETH which is the native asset of Ethereum. The fee varies widely depending on network congestion and usage. At times of peak demand it can cost in excess of \$100 to make a simple token swap.

Two years after launch the Ethereum network was at a standstill, congested and unusable due to a new blockchain game. CryptoKitties were virtual pets, each one a unique graphical representation of underlying Ethereum code.



Cute cats on the internet are a thing and it took off in a big way highlighting the dire need for increased capacity on the Ethereum network.

Today that bottleneck in capacity is still an issue and Ethereum is gearing up for the long awaited release of version 2.0.

Smart Contracts

Decentralized finance is built on smart contracts. The code that enables users to lend, borrow and swap tokens is all run on Ethereum's virtual machine.

Smart contracts are written (*mainly*) in the language of Ethereum known as Solidity. It's a statically typed language designed around the Javascript syntax making it familiar for web developers.

Smart contracts can't be changed or fixed after they have been deployed to the Ethereum network. This means there is no room for bugs making it more like hardware development than traditional software coding.

For this reason they tend to be *as simple as possible* with existing audited code being imported and reused where possible. You can create a standard token in less than 10 lines for example by importing an existing template and providing some variables for the name, ticker and minted supply.

Here is a very simple hello world Solidity smart contract.

```
contract MyContract {  
    string public myStateVariable = 'Hello World';  
}
```

This can be deployed to store any string of text on a public blockchain. When deployed the contract will be given an address which can then be used by anyone to access that data.

A smart contract address is like the post code of a smart contract on a decentralized network. It maps to the memory address of the executable code on the virtual machine. When we want to interact with a contract we often need the contract address. A common example of this is a token address which describes where to find that token contract.

Those four lines of code alone have some powerful use cases. Once deployed no one can remove the text, no one can change it, it will live in the Ethereum blockchain for eternity.

DeFi smart contracts build on this concept to create applications to provide financial services. Imagine if instead of storing text in our contract we stored a ledger of funds of who owned what, who owed who and stored funds for collateral within the contract itself.

Smart contracts quickly became interconnected within the Ethereum ecosystem. They have been described as the lego bricks of internet money.



In DeFi terms composability is the potential for smart contracts that form the DeFi protocols to interact with each other. A contract might connect to a lending platform to take out a flash loan and then use those funds to interact with an automated market maker to swap tokens for example. This interoperability between contracts has helped DeFi evolve to a complex interconnected network of financial applications.

“The next killer app is not the notes, it’s the links – Uniswap, Decentralized finance, etc. Every application is a component the future ecosystem can gain from.” Vitalik Buterin

If you would like to know more about building smart contracts then check out the [Blockchain Developer Roadmap](#)

dApps & Web3

If smart contracts form the back end brains of a DeFi platform then dApps or decentralized applications form the front-end that we interact with as users.

In theory dApps can be compiled from source code and run locally without needing a central point of access. In practice the compiled code is uploaded to a website which serves as the access point for the DeFi application for the vast majority of users.

The Evolution Of Web3

The web was built as a publishing portal based on print media which was considered Web version 1.0. After the dot com boom and bust the web evolved to web 2.0 where social media networks revolutionized the space. Users create, share and consume their own content.

Social media giants emerged providing services in exchange for our personal data to improve their advertising targeting. Web 3.0 according to Ethereum “*refers to decentralized apps that run on the blockchain*”. The concept promises social networks with no central entity in charge, there is no one to profit or monetize our personal data.

Web3 has come under some criticism recently, most notably from Twitter founder and Bitcoin maximalist

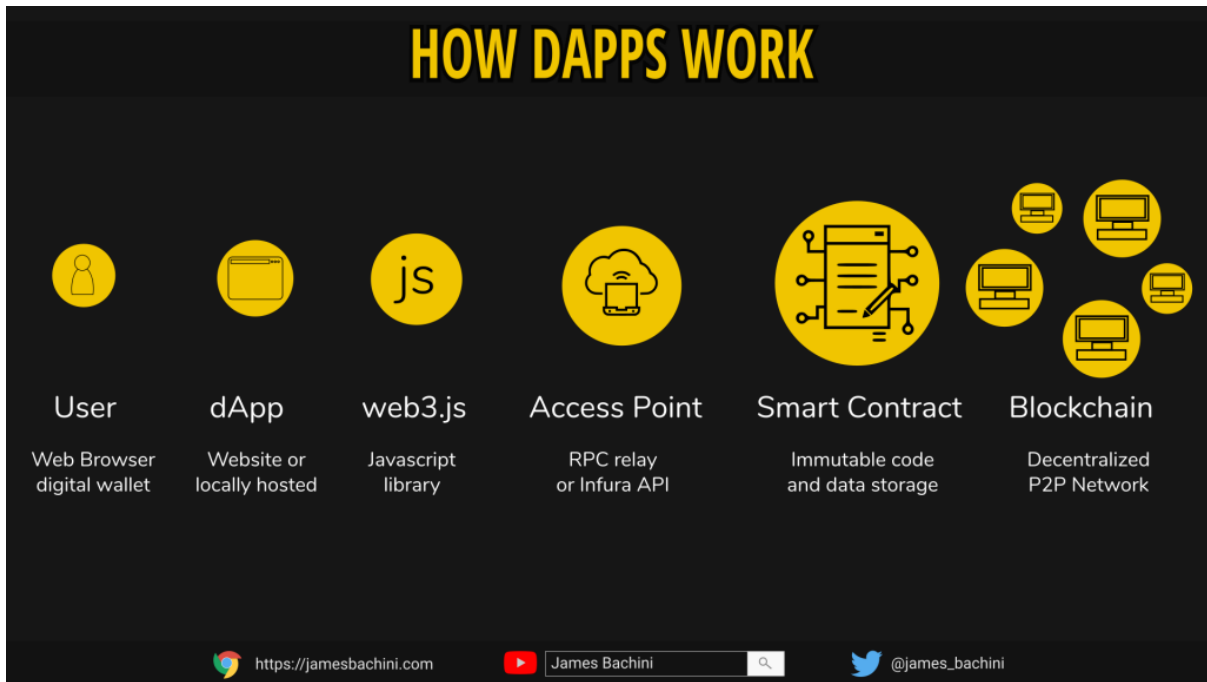
[Jack Dorsey](#). He highlighted the impact of VC funding rounds on early stage blockchain projects and the negating effect it had on decentralization.



How dApps Are Built

Decentralized applications are built using the same frameworks as existing websites. A web or app developer will import a Javascript module such as web3.js or ethers.js which will provide a library of tools to build on. The module will connect to a node on the Ethereum network, often via a service provider called Infura.

The developer will provide a mechanism to connect a wallet to the application which the end user will need to confirm. They can then execute complex smart contract functions at the click of a button.



The entire blockchain sector is built around the concept of decentralization. This means that a network has no central point of failure and is instead built around equal peers. Decentralization is not a binary concept and networks can become more or less decentralized over time.

Often blockchain technologies start very centralized with a developer as the central point of failure. Over time the network builds and momentum dissipates control.

"It's clear to me now that Ethereum is the new currency of the Internet. It's way ahead of where Paypal was in its day, and it's much more exciting to its customers than Paypal ever was." Gil Penchina

An Existential Threat To DeFi

I am as guilty as anyone of using centralized web interfaces instead of compiling front ends from source.

It's so much easier to go to Uniswap's website and interact with smart contracts via a nice web interface running on AWS.

However there are multiple concerns over centralisation here. The vast majority of users keep their funds in Metamask which is a ConsenSys owned product. The wallet connects to the Ethereum network via an API provider called Infura which is also owned by ConsenSys. Infura is a single point of failure where if there was a denial of service attack on their infrastructure it would make DeFi almost unusable for the vast majority of market participants.

Probably more of a threat than denial of service attacks is regulation. ConsenSys is a large corporation that has to oblige with any regulations law makers can come up with. The SEC is

being particularly aggressive with regulation through enforcement policy and large companies in the industry are easy targets.

This is in no way a criticism of ConsenSys themselves who have done more than anyone to bring DeFi to the masses. At some point though it may be worth thinking about why we are all here in the first place and how we can build better decentralized infrastructure either on top of existing web technologies or as a separate entity.

The token economy is the accelerating migration of assets into the digital world. One of the first breakthroughs for Ethereum was a smart contract that facilitated the creation and transfer of tokens. Anyone who has ever run a startup will know the quest to reach product market fit. *For Ethereum the token economy gave them their zero to one moment.*

The Token Economy

Token contracts could be broken down into two categories:

- **Fungible tokens** where any one token was equal to another held by someone else on the same smart contract ledger.
- **Non-Fungible Tokens (NFT's)** where the token was unique, a one of a kind digital asset.

From then on the majority of new projects in the blockchain space launched with their own token. In the future we might see **everything tokenized into a digital asset**, stocks, bonds, real estate. Any contractual stake in a real world entity may eventually end up on-chain.

5th April 2017

I had followed Bitcoin's development for some time however in 2017 something changed. It wasn't just a single use electronic cash system any more. New projects were launching on a day to day basis. Blockchain technology seemed to be on the verge of disrupting every industry on the planet.

There was a boom in initial coin offerings or ICO's to sell tokens to the public. Some of these tokens would double, quadruple or more overnight. Speculation ran rife and I was drawn into expanding my portfolio of digital assets into more and more risky investments.

The ICO boom ended in disaster around the start of 2018 as the booming crypto markets came crashing back down to reality. Bitcoin went from \$20k in December 2017 to \$6k in February 2018. More risky altcoins and ICO tokens lost the vast majority of their value, some being wiped out completely.

An altcoin is any cryptocurrency other than Bitcoin. It stands for alternative coin and stems from when Bitcoin completely dominated the markets.

There are currently over 10,000 individual tokens and coins listed on the industry tracking platform CoinMarketCap. Of these over half use a variation on an Ethereum smart contract known as an ERC20 token. All of these tokens are controlled and powered by Ethereum's

global network of mining nodes. The ERC20 token template contains functions to create, transfer, approve spend and check balances.

Developers can take an ERC20 template code, change the name, ticker and total supply of tokens and deploy it to the blockchain in under an hour. It gave digital businesses a new way to raise funds and gain early traction building communities.

NFT's – Non-Fungible Tokens

NFT's are unique tokens deployed via a smart contract. Whereas a normal token is exchangeable for another just like it, **a non-fungible token is a one off**. NFTs are used to represent and transfer ownership of metadata often linked to digital art and collectibles.

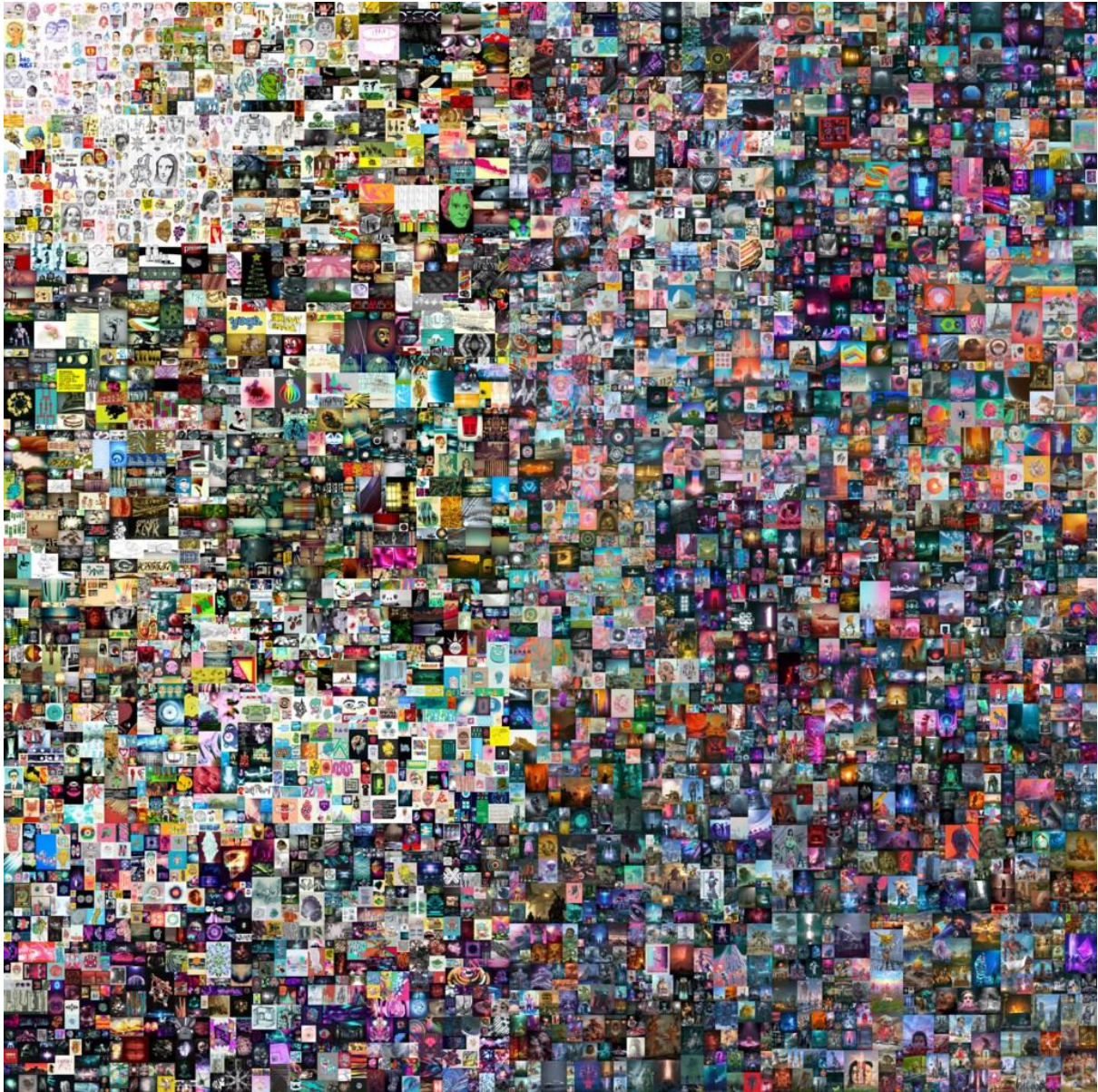
Many market places and NFT portals provide web based applications for creators to easily mint NFT artworks without ever interacting with the underlying code. A creator may take a jpg image, upload it to [Opensea](#) or [Rarible](#) and mint an NFT.

A creator must pay the transaction fee to mint an NFT because it deploys a smart contract requiring a gas fee to be paid. Lower cost alternative chains and layer 2 solutions do exist but the majority of valuable NFT works are currently stored on Ethereum.

1st May 2007

It was a warm May morning in Wisconsin when the artist Mike Winkelmann started work on what would become the most valuable NFT ever created. Every day for over 13 years he created a new piece of art and posted it online using the nickname Beeple.

The works were collaged together and minted in an NFT smart contract which became known as *"The First 5000 Days"*. It was auctioned at Christies in New York on the 11th March 2021 for \$69,346,250 US dollars.



This wasn't the first indication that something was happening in the NFT space. Months earlier some early Ethereum developers and supporters had started buying up a series of *crypto punk* NFT's to use as avatars on social media. These were already rising rapidly in value when the Beeple auction took place.

The ERC721 token is the industry standard token used for NFT's. It contains many of the standard ERC20 token functions alongside additional functions to declare and modify ownership and store metadata. Metadata contains the data which the NFT represents; it is often a hash of the data rather than the data itself.

"An NFT has more utility than cryptocurrency because you're getting an asset that you want as a collectible, which is a status symbol." Gary Vaynerchuk

There is more information on NFT's here: [NFT's | Non Fungible Tokens](#)

Governance Tokens

A decentralized autonomous organization or DAO is a smart contract built to manage voting and governance for a new type of organization. There are no CEO's, no managers, no hierarchy of control. Instead token holders propose updates which then go to a demographic vote.

Governance tokens are used to control the development and direction of an organization. A DAO is an extreme example of a fully decentralized organization, however governance tokens can also be used to implement a voting system in more traditional equity formed companies.

Token holders and conglomerates can get together to post a proposal which is then voted on by the governance community.

Protocols often require funds to operate. For example a lending and borrowing platform needs a float and lenders before they can start lending. DeFi protocols will often bootstrap initial funding through liquidity mining. This is the incentivisation to get users to deposit funds to the platform. This may take the form of distributing governance tokens to early adopters or providing high APY returns for staking LP tokens for the ETH/GovToken pair providing a liquid market for the governance token.

For a token to go up in value the **demand must outweigh the supply** on exchange. The economics of the token ecosystem are known as tokenomics. There are various methods to try and increase demand and reduce supply such as staking, fee burning and holder benefits.

30th April 2016

The original DAO project raised \$150m via an initial coin offering or ICO. The tokens were distributed to 11,000 contributors in late May. Then disaster struck.

On the 12th June 2016 Stephan Tual posts to the DAO blog *"No DAO funds at risk following the Ethereum smart contract 'recursive call' bug discovery"*

Four days later, while DAO developers are working on a fix, a hacker drains 3.6m ETH from the DAO's treasury. At the time this was 15% of the entire circulating supply of Ether and would be worth billions today.

A solution was proposed by Vitalik to fork and update the code being run by miners blacklisting the hackers funds. This went through but raised a number of questions whether the Ethereum network was truly decentralized.

A fork is when code is split or duplicated to a new repository. A hard fork creates a new duplicated blockchain and nodes must update their software to participate. A soft fork is seen as a more minor alteration to existing code and continues on the existing chain. When major changes are pushed out a subset of the nodes may not accept them continuing with alternate or pre-existing code. This division of nodes is known as a hard fork. An example of this took place on Bitcoin where Bitcoin Cash split off due to a debate over block sizes.

The blockchain sector prides itself in being transparent which includes the vast majority of code being open source. This means that it can be forked by anyone and developers can create replicas of their favorite DeFi protocols quite easily.

“With DeFi, we are building the finance system of tomorrow that is more efficient, faster, more rewarding, and levels the playing field for everyone.” – Olawale Daniel

Automated Market Makers

In late 2017 all the tokens were on Ethereum and it made sense that someone would eventually build a decentralized digital asset exchange. The first popular one was called IDEX and it followed the principles of a standard exchange order book and matching engine. In 2018 the game changed, perhaps forever, with the release of Uniswap. Uniswap’s automated market maker grew quickly to become one of the backbones of DeFi.

How Automated Market Makers Work

An automated market maker works differently to an orderbook based exchange. It uses a pair of assets in a pool which are deposited by a liquidity provider. A trader can then trade one asset within the pool for the other paying a fee. The price will fluctuate with demand along a liquidity curve.

For example a liquidity pool might have ETH as the base asset and an ERC20 Token as the traded asset. Price is calculated along a curve dependent on the quantity of assets in the pool. If someone starts buying the ERC20 token with ETH it pushes the price up as more ETH is added and the ERC20 tokens are removed from the pool.

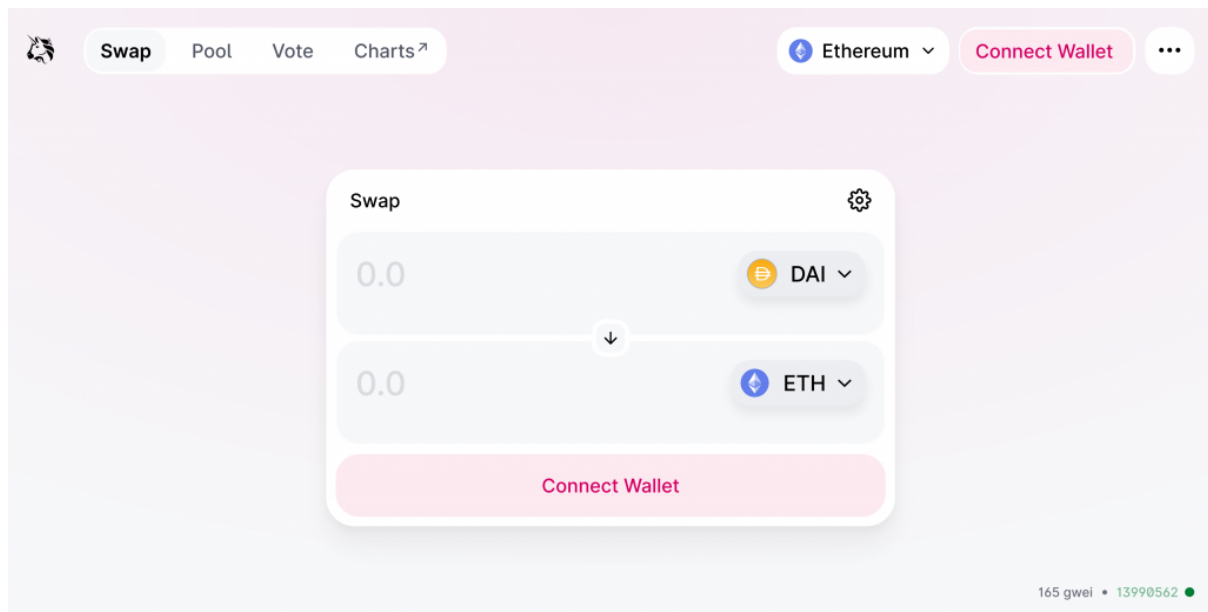
Liquidity provider (LP) tokens act like a receipt for the funds deposited and they will automatically be sent to the same address that deposited the funds. LP tokens can be transferred and can often be staked on DeFi platforms in return for staking rewards.

2nd November 2018

Every now and again someone comes along that just simplifies things down to their fundamentals. This is what Haden Adams did when he launched the Uniswap platform. Rather than rely on a clunky order book Hayden had devised a swapping protocol where investors would send equal values of assets to a smart contract. The assets were put into a liquidity pool where users could then trade between them paying a fee to the liquidity provider.

If someone swapped some ETH for a new token then the price would go up along a predefined curve. If they sold some of the token back to ETH the price would drop back down again to balance the pool.

It was ingenious in its simplicity and enabled investors in ETH and ERC20 tokens to gain a yield on their holdings.



<https://app.uniswap.org/#/swap>

It wasn't all roses though as Uniswap liquidity providers flirted with the risk of impermanent loss. This was the effect of one asset increasing in value beyond the other which would mean the liquidity providers would be left with more of the lower value asset in the pool. Impermanent loss was very much a permanent problem if the asset never returned to its previous valuation. When a liquidity provider deposits funds to an automated market maker they receive fees in exchange for accepting the risk of impermanent loss.

In theory there's no reason for the price in a liquidity pool to follow the price on a centralized exchange; however in practice any differences are quickly arbitrated away. In crypto markets arbitrage is big business. Networks of bots will scour centralized and decentralized exchanges looking for mispricings between assets. Arbitrage can be as simple as buying an asset on one exchange and hedging the position by selling on another or it can be more complex such as when triangular arbitrage exposes three way price discrepancies.

Arbitrage bots play an important role for automated market makers to keep their prices in line with centralized exchanges.

The Sushi Saga

5th September 2020

Uniswap liquidity providers send their tokens to a smart contract and in return get LP tokens as a kind of receipt and IOU for the liquidity position.

A developer going by the pseudonym Chef Nomi had forked Uniswap's open source code and created a copycat version of it called Sushiswap. Sushi tokens were distributed to users who staked Uniswap LP tokens on the platform. Chef Nomi used the LP tokens in a vampire attack to drain liquidity from Uniswap and put it on Sushiswap.

The plan worked and Sushiswap grew in what became known as the first billion dollar heist. At one point it held more liquidity in terms of TVL than Uniswap.

Smart contracts can contain funds locked within the contract itself. The smart contract address owns the funds until a user redeems them. The TVL or total value locked within a smart contract or protocol is often expressed in USD terms.

Chef Nomi wasn't satisfied with his success and in a moment of madness dumped the entire development fund of SUSHI tokens on the open market through centralized exchanges such as Binance and FTX. The token value instantly dropped 70% and claims of carrying out what would later be referred to as a rug pull "for the good of the community" were met with disdain from the community.

The following day, perhaps after sobering up and a few death threats, Chef Nomi transferred funds and ownership control to the CEO of [FTX Sam Bankman-Fried](#) who set up multisignature wallets for the funds.

Multisignature wallets enable multiple entities to safely control access to funds. A multisig is another form of smart contract that states how many signatures are required to distribute funds and which accounts have signatory rights.

Sushiswap recovered and while it still played No.2 to Uniswap on May 19th 2021 it had a record day with trading volumes nearly hitting three billion US dollars.

Today the vast majority of decentralized trading now takes place on automated market makers like Uniswap and Sushiswap.

DEX Aggregators

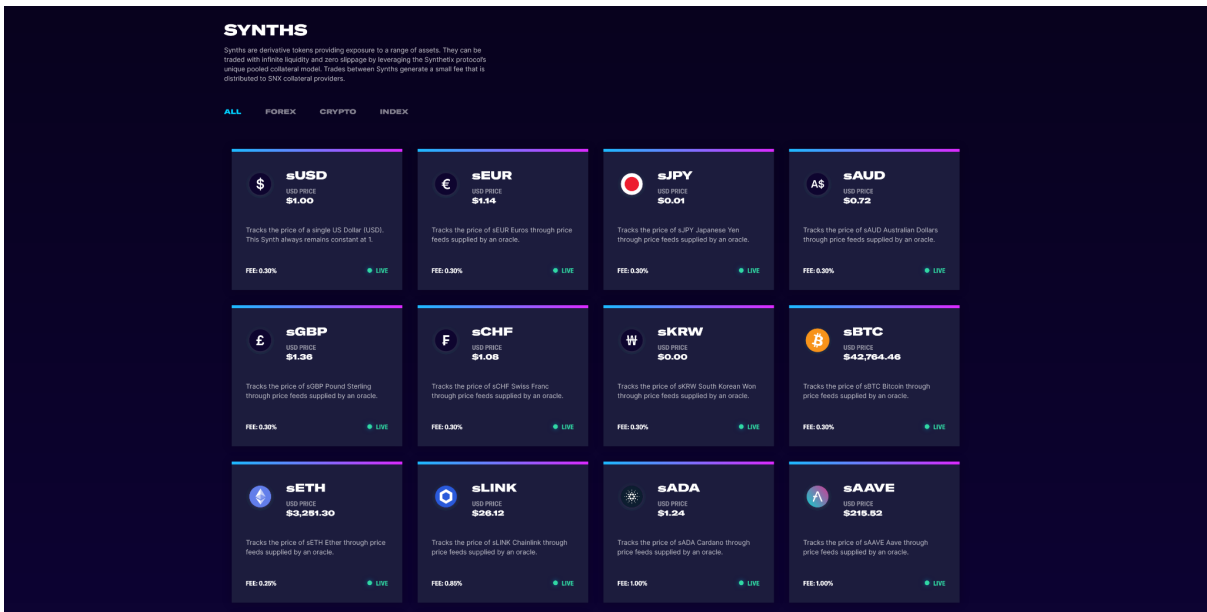
With multiple decentralized exchanges to choose from, how can a user be sure they are getting the best price for their token swap on any one single exchange? This is where decentralized exchange aggregators such as 1inch exchange come in.

A user will connect to a DEX aggregator and put in the details of the transaction they want to carry out. The aggregator will then scan all available markets and more complex triangular transaction routes to calculate the optimal strategy for carrying out the swap. This can on occasion provide a better price for the trade.

Synthetic Assets

Synthetic assets are a form of derivative product in decentralized finance. Synths are created which follow the price of an underlying asset. For example sTSLA will follow the stock price of Tesla and can be traded on decentralized exchanges.

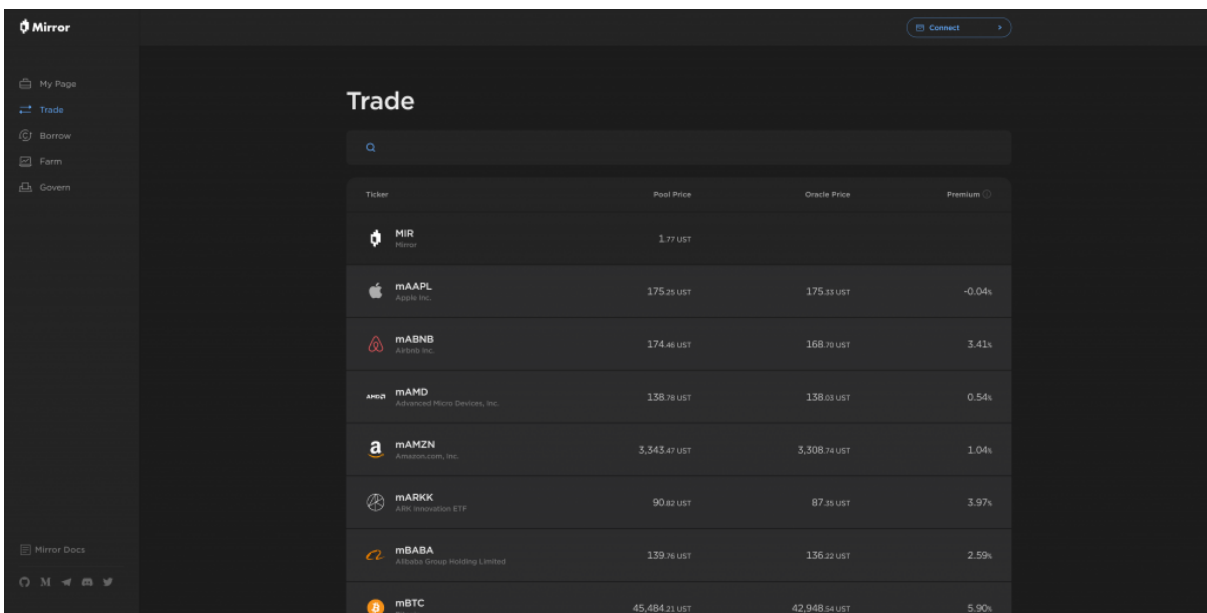
Synths are tokens minted via a DeFi protocol such as Synthetix. Liquidity providers contribute to an underlying asset pool in return for fees and native tokens.



When a trader purchases a synth they are effectively trading against the underlying asset pool as any gains will be taken from it. If all the synthetic assets go up at the same time then the liquidity pool diminishes in value. In practice the diversified nature of the assets works well to keep things in balance.

Not everyone is happy about the move to digital assets including US & UK regulators. The SEC & FCA are currently imposing regulations to prevent the trading of securities on DeFi. Uniswap was forced to conform by blocking a number of synthetic assets on their frontend in July 2021.

Mirror protocol is also under active investigation by the SEC. Mirror provides the ability to take long and short positions on synthetic stocks like Tesla or commodities like gold.



A concern for regulators is the ability of these protocols to hold their pegs to the underlying assets. DeFi has only been around a couple of years and we haven't seen a deep bear market where token prices depreciate and pressure is put on protocol economics.

Synthetic assets are an interesting addition to the DeFi landscape. If they can overcome the regulatory hurdles then it could provide a short cut to the eventual tokenization of all assets.

Currently there aren't high volumes being traded in Synthetic tokens however if the benefits do start to attract trading volumes away from the big stock exchanges around the world then we will likely see further crackdowns from regulators.

Stablecoins Compared

USD stablecoins have become big business with over \$100 billion of collateral locked in USDT and USDC alone.

How Stablecoins Work

Stablecoins are a form of ERC20 token which aims to match the price of an underlying asset. Usually they are pegged loosely to the USD and provide a critical role in the DeFi ecosystem.

- Traders will hold stablecoins when they want to remain neutral in uncertain markets.
- Yield farmers will deposit stablecoins to gain a yield on a low risk asset.
- Automated market makers often use stablecoins as a base asset instead of ETH.

Collateralised Stablecoins

Collateralised stablecoins have a simple business model. Take payment and hold collateral then issue a token to represent the value of that collateral on chain.

Examples of collateralised stablecoins include USDT and USDC. A company will issue new tokens when receiving payments via bank wires. They will also accept tokens in return, burn them and issue a payment as part of a withdrawal process.

The issue with this business model is that it is centralized around a single corporation that is responsible for managing the collateral. Enter algorithmic stablecoins which aimed to decentralize the issuance of stablecoins.

Algorithmic Stablecoins

The issues with centralized custodial stablecoins led naturally to the concept of a decentralized alternative. Algorithmic stablecoins are smart contracts which aim to track the price of an underlying asset such as the USD.

These often work with two pools of capital: a high volatility native token and the stablecoin token. The aim is to smooth out price swings in the stablecoin via incentive mechanisms using the high volatility asset.

Issues arise if confidence is lost in the protocol as there is no guarantee the asset will always be valued and traded at \$1. Shortly after the launch of FEI the valuation dropped to below \$0.8 due to unprecedented supply hitting exchanges and a rush to exit.

Stablecoins Compared

Obviously no stablecoin is perfect and most have derived from their peg to some degree at some point in their history. The following are all currently traded at \$1 and this document outlines some of the key and unique features that have made these stablecoins so popular.

USDT

The most widely used stablecoin has always been USDT. US Dollar Tether isn't decentralized at all, it's a token backed and managed by centralized exchange Bitfinex. A company will send a bank wire to *Tether Holdings Limited* and they will mint and send USDT tokens in return. The tokens can be withdrawn by sending them back, where they'll be destroyed in a process known as burning, and the funds will be sent back in real US dollars.

15 October 2018

The value of USDT dropped to \$0.90 after growing concern over the ability of Bitfinex to pay back more than two billion USDT in circulation. In theory it should be a simple business model, hold the funds until they want redeeming. However federal prosecutors were investigating Bitfinex for using the funds to provide liquidity for their other business operations and manipulate the price of Bitcoin.

Today there is more than 70 billion US dollars of tether in circulation. It is still a controversial and concerning issue for the industry although tether has gone some way to providing audits on their reserves and holdings.

USDC

USDC is a direct competitor to USDT which has grown in popularity, partly due to the legal issues Bitfinex faced. USDC or *USD Coin* is managed by Circle and [Coinbase](#).

INTRODUCING USD COIN

A stablecoin brought to you by Circle and Coinbase



An open source, smart contract-based stablecoin

True financial interoperability requires a price stable means of value exchange. Centre's technology for fiat-backed stablecoins brings stability to crypto. The initial implementation is USD Coin (USDC), available as an Ethereum ERC-20, Algorand ASA, Avalanche ERC-20, Hedera SDK, Solana SPL, Stellar asset, and TRON TRC-20, and creating possibilities in payments, lending, investing, trading and trade finance — and the ecosystem will grow as other fiat currency tokens are added.

UST

UST is the stablecoin of the Terra/Luna ecosystem. It has become a \$10 billion dollar asset thanks to great lending rates available on Anchor Protocol.

The current APY for lenders of UST is 19.46% which far outweighs anything available in traditional finance.

Note that the SEC is currently investigating the Terra protocol. It's believed this is mainly focused on Mirror protocols [synthetic assets](#) but that investigation will possibly cover Anchor and UST as well.

MIM

MIM stands for *magic internet money* and is the creation of blockchain developer Daniel Sestagalli. It's another high yielding stablecoin on lending platforms like [abracadabra.money](#)

ABRACADABRA.MONEY IS A SPELL BOOK THAT ALLOWS USERS TO PRODUCE MAGIC INTERNET MONEY.

You, the Spellcaster, can provide collateral in the form of various interest bearing crypto assets such as yvYFI, yvUSDT, yvUSDC, xSUSHI and more.

With this, you can borrow magic internet money (MIM) which is a stable coin that you can swap for any other traditional stable coin.

MIM is one of the big players in the [Curve Wars](#) where protocols are fighting for voting rights to create liquidity.

DAI

DAI was launched in late 2017 by MakerDAO and immediately underwent a stress test as the crypto markets crashed. It was perhaps the first decentralized finance protocol to gain attention and adoption.

Today DAI has lost much of its market share to new entrants in the markets but it was seminal for stablecoin and general DeFi technology.

FRAX

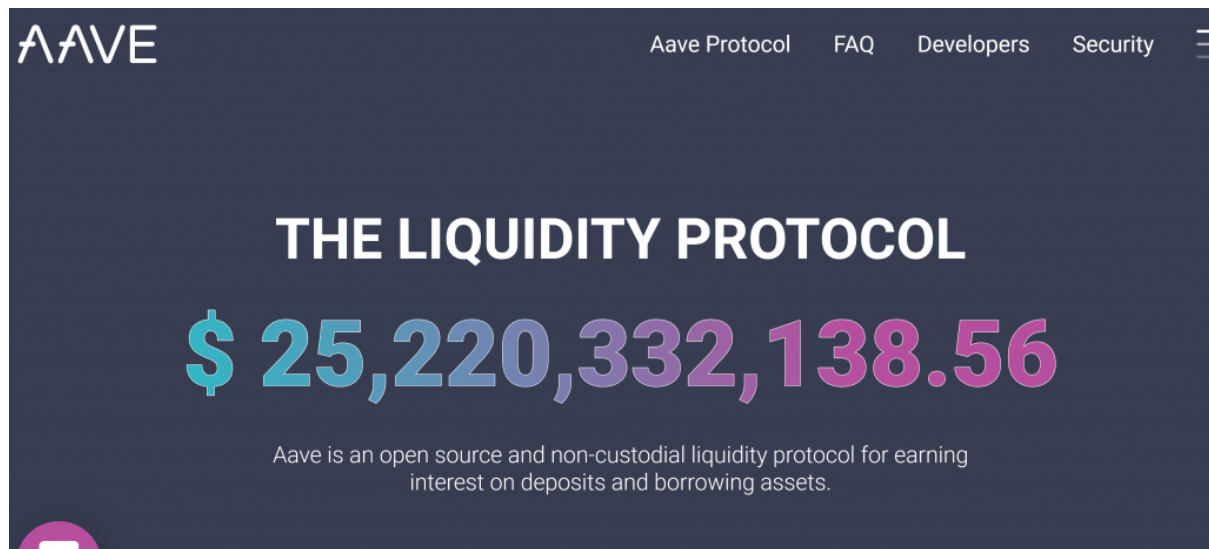
Frax pioneered a fractional reserve system which combines collateral and algorithmic stablecoin technology. It is community governed via a DAO and uses oracle price feeds to maintain its peg to the US dollar.

The project has two tokens the FRAX stablecoin and a FXS governance token which receives fees, seigniorage revenue and excess collateral value. FXS is a speculatively traded DeFi token and is highly volatile in terms of price. FRAX is the stablecoin pegged to the USD and should always trade at \$1 in theory.

DeFi Borrowing & Lending

DeFi borrowing and lending differs from traditional finance where institutions will lend funds based on credit ratings. In DeFi accounts are anonymous, there are no credit ratings to assess risk. Borrowing and lending is more often carried out using over-collateralized loans.

A user will deposit digital assets to a DeFi Lending smart contract and will receive a yield for lending those assets. Currently lending USD stablecoins on various DeFi protocols can get between 5-20% APY far exceeding the interest paid in traditional finance.

The image shows a screenshot of the Aave website. At the top left is the 'AAVE' logo. To the right are navigation links: 'Aave Protocol', 'FAQ', 'Developers', and 'Security'. The main heading is 'THE LIQUIDITY PROTOCOL' in white. Below it is a large number '\$ 25,220,332,138.56' where the '\$' is blue and the rest is purple. Underneath is a subtitle: 'Aave is an open source and non-custodial liquidity protocol for earning interest on deposits and borrowing assets.'

AAVE

Aave Protocol FAQ Developers Security

THE LIQUIDITY PROTOCOL

\$ 25,220,332,138.56

Aave is an open source and non-custodial liquidity protocol for earning interest on deposits and borrowing assets.

Aave has a cool \$25 Billion USD in Total Value Locked

A second user will deposit ETH as collateral to the smart contract and can then borrow up to a specified percentage of around 80% of the value of the ETH in stablecoins. If the value of ETH goes down below a liquidation threshold the collateral is liquidated to pay back the lender.

So what is the point in borrowing funds less funds than you deposit as collateral. The key here is that you can deposit a range of different tokens as collateral and still receive any gains while they are being held. If the ETH used as collateral doubles in price then the borrower still gets back the same amount of ETH when they pay back the loan with interest.

One common use is for tax planning as borrowed funds aren't applicable to capital gains tax in some jurisdictions. A user can deposit cryptocurrency they are holding and borrow on those funds for material purchases without exposing themselves to a large tax bill.

The Summer Of DeFi

16th June 2020

If there was one moment that kickstarted the DeFi movement this was it. Compound was already a very successful decentralized borrowing and lending platform. It was facing tough competition from similar platforms like Aave and MakerDAO. To differentiate themselves and incentivise the use of their platform they started distributing a governance token to borrowers and lenders.

For a time you could literally get paid to borrow funds because the governance tokens earned were worth more than the interest due. The funds borrowed could then be recycled back into the lending platform or put into more aggressive yield farming strategies.



The original summer of DeFi, what a time to be alive

Flash Loans

Most borrowers will pay back their loan and release their collateral after a few months or years. However DeFi introduced a new type of borrowing where the loan only lasts a few seconds. A flash loan can be taken out to fund a smart contract with huge amounts of capital as long as the loan is repaid in the same block of transactions. If the loan isn't paid back the entire transaction simply fails. This can be used to execute highly leveraged trades and manipulate prices on decentralized exchanges and liquidity pools.

Flash loans are possible because smart contract transactions can be batched to process in order. Time stands still while the transactions are processed and failed batches of transactions are reverted atomically. When transactions fail a gas fee is still charged.

Lending protocols like [Aave](#) and [dYdX](#) currently offer flash loans from a billion dollar asset pool giving everyone access to huge amounts of capital on demand. You too can be a billionaire for at least a few seconds.

This capital can be used for good and bad.

An arbitrage trader can take out a flash loan for a stablecoin and then use these funds to swap for token A, in the same block they will swap token A for token B and then token B back to stablecoins. If the triangular arbitrage trade resulted in more stablecoins being received they will pay back the loan in the same block and profit the remaining funds.

Most famously flash loan attacks have been used to manipulate price tracking on liquidity pools to drain assets from them and steal the funds. These types of attacks are hard to prevent however users can insure against them and oracles can provide external price feeds to keep liquidity pool mechanisms in check.

Crypto Oracles

Crypto oracles provide an essential bridge between off-chain and on-chain data. If a smart contract needs access to price feeds, random numbers or external data they will need to use an oracle because the smart contract can not make outgoing connections past the boundaries of on-chain data.

In traditional web development, an API (application programming interface) provides a web address for developers to connect to so they can gain access to data and execute functions programmatically. Centralized exchanges such as [Binance](#) will provide API access and API keys for their users so they can trade programmatically using trading bots and scripts for example.

Smart contracts can only read data provided to them via user transactions and can't connect to anything externally posing a problem for developers that need external data. This problem is being solved by oracles who upload data such as price feeds to the blockchain.

Oracles take real world data and upload it to the blockchain so it can be used within smart contracts. The most famous oracle service is [Chainlink](#) which itself has a market cap of ten billion US dollars.

The market cap or capitalisation of a cryptocurrency is calculated by multiplying the circulating supply by the token price. This is usually a debatable issue with leading websites not including vested tokens and treasury wallets in the circulating supply.

Smart contracts can use price feeds supplied by oracles to help prevent smart contract attacks that manipulate prices such as flash loan attacks.

Flash loans enable the instant deployment of massive amounts of capital which can be used to manipulate the value of assets within a liquidity pool. Pools that use oracle price feeds can reject transactions which are out of line with the current off chain price provided by the oracle.

Token Launches

When a new project launches a token it is quite common that they create an initial distribution through a token launch.

Token sales became very popular in the **ICO (Initial coin offering)** boom of 2017. This led to ICO's getting a bad reputation and the standard token launch rebranded to either an **IEO (Initial exchange offering)** on a centralized exchange or an **IDO (Initial dex offering)** on a decentralized exchange.

The principles of token swaps haven't changed however and the general idea is for teams to raise the funds required to launch a protocol by selling off either all or a percentage of the supply of a new token.

With an **airdrop** tokens are not sold but are distributed for free to users that meet certain requirements. These may be promotional in nature or simply to users who have previously interacted with their services. In September 2020 Uniswap distributed 400 UNI tokens via an airdrop to anyone that had previously used the platform.

The concept of a **fair launch** token was popularized by Yearn Finance when they released their governance token without any team allocation or VC interest. They simply gave it away to the people that were using the protocol. This created a strong community which benefits the project to this day.



Token launches are very high risk and just like most startups, many fail. Many projects will never find product market fit and the ones that do have to battle through hacking attempts, regulations and scaling issues.

The few projects that do go on to build ecosystems around their tokens and gain traction provide a high potential reward opportunity for investors who are willing to allocate capital during a token launch.



Planning A Token Launch

Token supply and distribution economics are very important in the initial period of a tokens existence. Sometimes venture capital firms will get discounted terms, founders and advisors will get large pre-mine allocations, vesting schedules release tokens at set periods and pump and dump groups will inflate and collapse prices of low liquidity assets.

When planning a token launch the first factor that comes into play is the type of token. There are either fungible (ERC20) tokens and non-fungible tokens (NFT's).

Token Sale or Liquidity Pool

One of the first decisions you'll have to make as a developer is whether to set up a token sale contract where users can purchase tokens directly from your website. Or to set up a 3rd party liquidity pool on an [automated market maker](#) like [Uniswap](#) or [Sushiswap](#).

There are pros and cons for both methods. Running your own token sale requires no initial capital to set up a liquidity pool whereas if you have some funds then users may be more familiar and trusting of buying tokens on Uniswap/Sushi.

There is some further information here about how to deploy a new token and set up a liquidity pool: <https://jamesbachini.com/new-token/>

Choosing A Blockchain

This really comes down to the cost impact of gas fees. On Ethereum mainnet users will be paying \$50-100+ to buy or sell your token via an AMM. There are a host of other options, these would be my current recommendations as of Q1 2022. All of these are EVM compatible so Solidity code can be easily deployed. Transaction costs are estimates.

Blockchain	Transaction Cost	Description
Ethereum Mainnet	\$50	Premium network with high fees. Highest level of decentralization and security. Exposure to largest L1 DeFi ecosystem
Polygon	\$0.20	Strong community, mature ecosystem, low fees and some support from Ethereum
Arbitrum	\$2	Layer 2 optimistic rollup, slow but steady growth
Binance Smart Chain	\$0.20	Centralized EVM chain run by Binance. Popular and mature ecosystem.
ZKsync	\$0.50	Not yet live on mainnet but one to watch for the future. Highly anticipated ZK rollup technology
Aurora (Near Protocol)	\$0.00	Zero cost high performance EVM chain from core team at Near protocol. I wrote about this here: https://jamesbachini.com/aurora-near-protocol-trisolaris/

Deployment Costs & Budgets

To deploy the contracts will cost roughly 10-50x the transaction cost above because there is more data that needs to be stored on chain when deploying contracts compared to a simple transaction.

Developers should also budget time and funds for:

- Code auditing (3rd party code audits are highly recommended)
- Domain name & hosting
- Social media management
- Marketing, branding, outreach
- Paid Advertising (Twitter ads recommend)
- Explainer videos, pdfs, whitepapers, docs
- Transaction fees (airdrops etc.)

Token Launch Process

The general process would be something along the lines of:

1. Deploy smart contracts on a testnet.
2. Have an auditor look over the contracts and run unit tests.
3. Then migrate the contracts to the mainnet of choice.
4. Carry out some mainnet tests and secure any treasury funds in a multisig wallet.
5. Deploy a liquidity pool or token sale contract
6. Announce token launch

DeFi Derivatives

DeFi derivatives are financial contracts which track or provide exposure to an underlying asset.

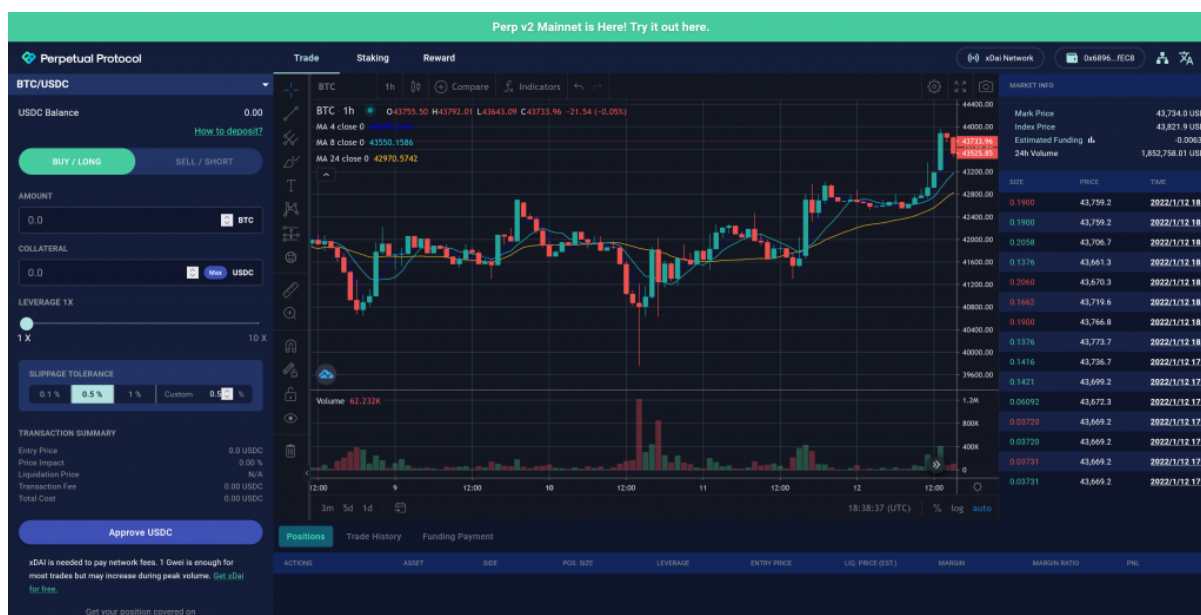
The most common derivatives products in crypto markets are futures and options. In crypto markets derivatives are traded at greater volumes than the underlying spot markets. This means there is more buying and selling of Bitcoin futures than there is of actual Bitcoin.

Futures

Futures are a form of derivative that tracks the price of an underlying asset. The contract allows traders to bet on the price going up (long) or to bet on it going down (short). In crypto markets perpetual futures products which don't expire are very popular and are traded at higher volumes than the underlying base assets.

Made popular by Bitmex and finessed by Binance and FTX these products are only just starting to be traded on DeFi trading platforms and volumes on centralized exchanges remains the bulk of the market.

Perp Protocol



<https://perp.exchange/>

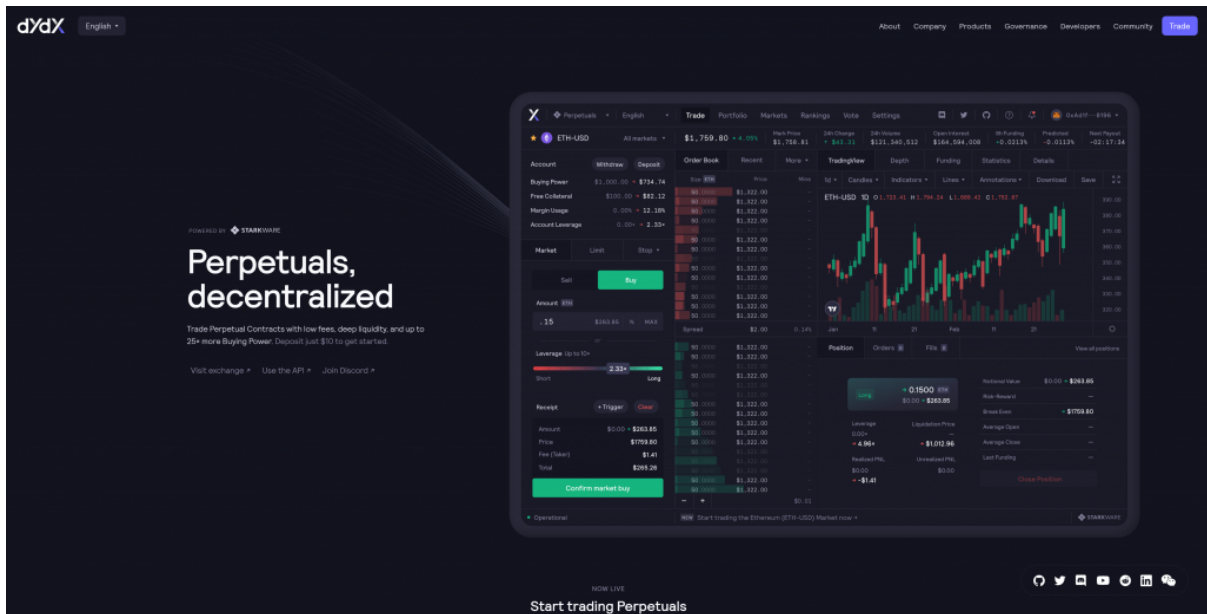
Perpetual Protocol offers a decentralized exchange and protocol to trade perpetual futures contracts with up to 10x leverage. It uses the xDai sub chain currently which reduces fees compared to Ethereum mainnet.

Perpetual futures contracts continuously track the price of an underlying asset. They do this by adjusting a funding fee inline with demand. If demand is high the protocol will charge

anyone that wants to go long (buying the asset) a fee which will be paid to anyone who holds a short position (short selling the asset).

When demand is very high it's possible for traders and DeFi yield aggregators to short sell the perpetual futures contract to gain a yield from the funding fee. Their position will be hedged by buying the underlying asset on spot markets, known as a cash and carry trade.

DyDx



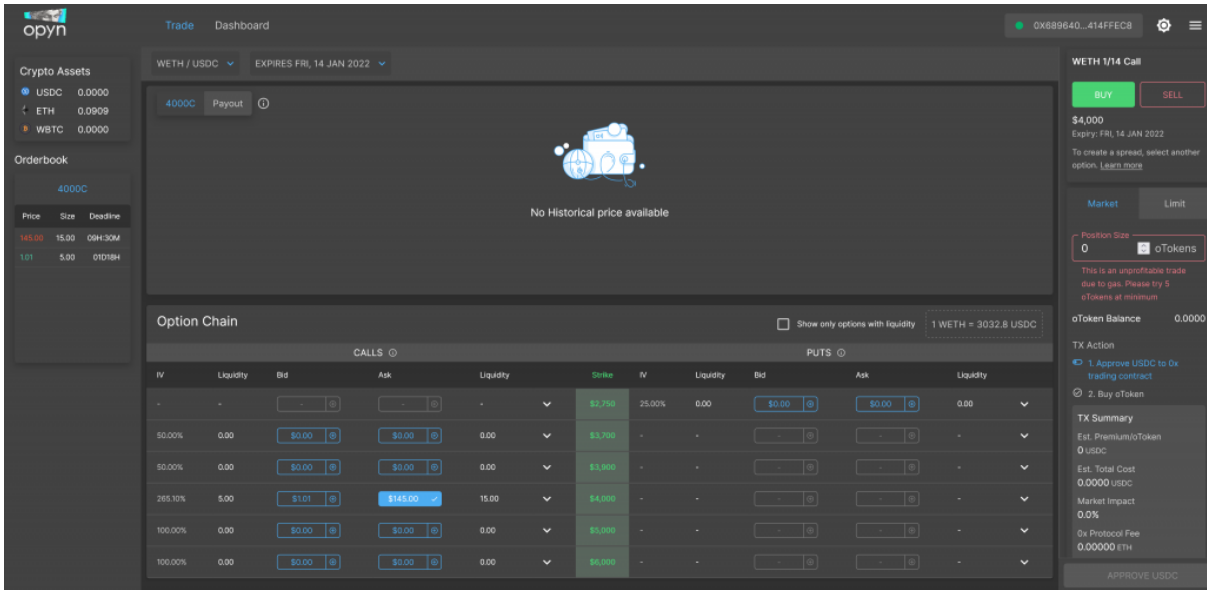
<https://dydx.exchange/>

DyDx is an open trading platform for perpetual futures. The protocol has \$1B in TVL as of January 2022 and provides one of the best DeFi trading experiences.

Options

Options provide the purchaser the option (but not obligation) to purchase an asset at a set price at a set expiry date. Options trading has gained a lot of traction with the Wall Street Bets movement in stocks and shares but we haven't seen the same influx of retail driven options trading in crypto as of yet. Centralized exchange [Deribit](#) is the market leader but we are starting to see some DeFi competitors emerge.

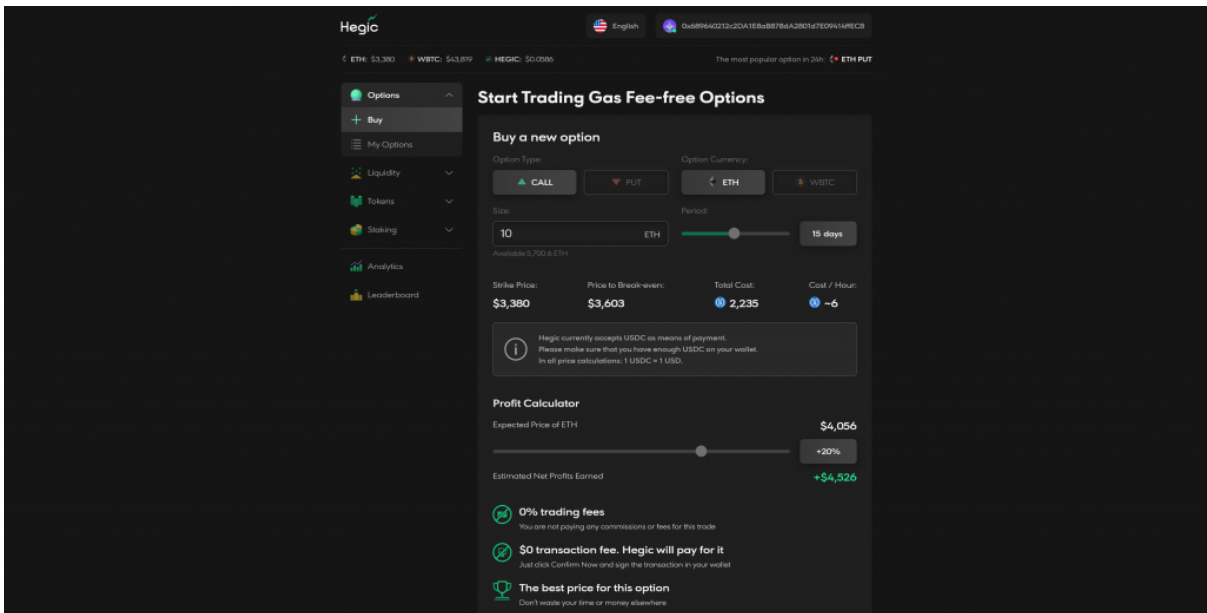
Opyn



Opyn is an options trading platform with weekly expiries. The team also collaborated with Paradigm in the release of Squeeth which is a tokenized perpetual options product.

More info on Squeeth here: <https://jamesbachini.com/squeeth/>

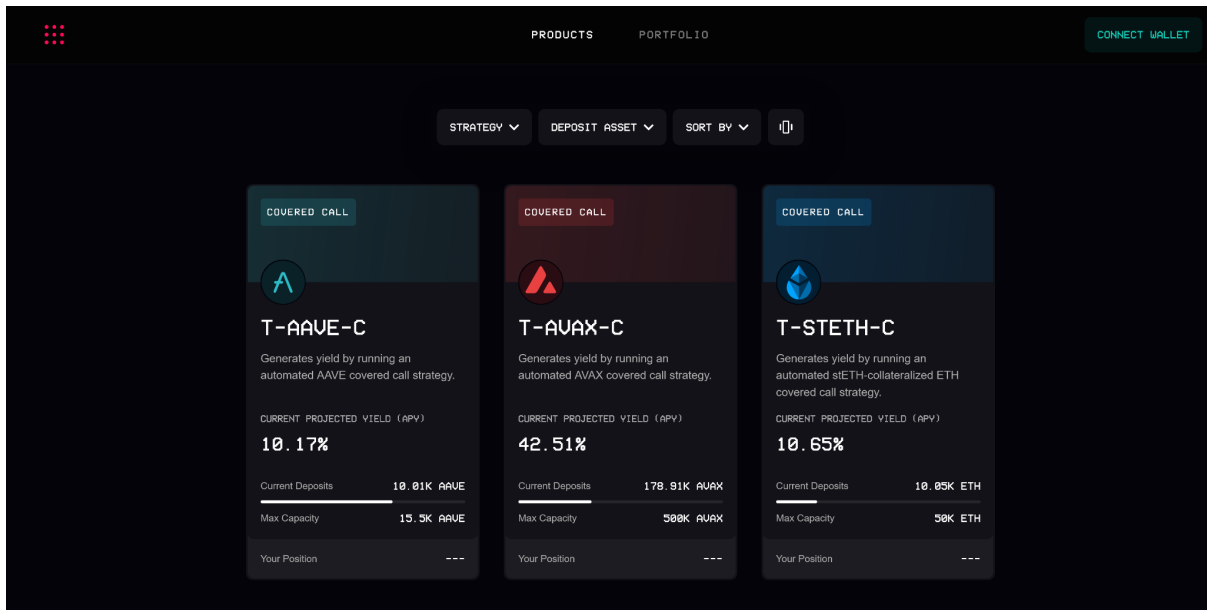
Hegic



<https://www.hegic.co>

Hegic was the undisputed market leader in decentralized options for a long time before Opyn came along and stole the mantle. The platform boasts 0% trading fees and \$0 transaction fees.

Ribbon Finance



<https://app.ribbon.finance/>

Ribbon finance builds options strategies on top of decentralized options protocols. They run strategies like covered calls to generate yield on selected assets.

Synthetic Assets

Synthetic assets are tokenized versions of stocks, indexes and commodities. Basically anything with a price feed can be tokenized on a synthetic asset platform because traders trade against a shared liquidity pool. These DeFi derivatives have unique advantages over traditional markets because they can be traded 24/7, moved and transferred at ease. In the future we may see tokenized stocks used as collateral in other areas of DeFi.

Mirror Protocol

Symbol	Asset Name	Pool Price	Oracle Price	Premium
MIR	Mirror	1.80 UST		
mAAPL	Apple Inc.	176.39 UST	175.62 UST	0.44%
mABNB	Airbnb Inc.	176.29 UST	169.99 UST	4.07%
mAMD	Advanced Micro Devices, Inc.	139.04 UST	137.66 UST	1.00%
mAMZN	Amazon.com, Inc.	3,346.98 UST	3,313.61 UST	1.00%
mARKK	ARK Innovation ETF	89.26 UST	85.44 UST	4.47%
mBABA	Alibaba Group Holding Limited	141.96 UST	136.90 UST	3.40%
mBTC	Bitcoin	45,875.97 UST	43,622.72 UST	5.16%
mCOIN	Coinbase Global, Inc.	247.99 UST	238.11 UST	4.06%
mDOT	Polkadot	28.80 UST	27.21 UST	5.84%

<https://mirrorprotocol.app>

Mirror protocol incentivises trading on both long and short sides of synthetic assets including:

- Stocks
- Indexes
- Cryptocurrencies
- Commodities

Synthetix

SYNTHS

Synths are derivative tokens providing exposure to a range of assets. They can be traded with little liquidity and price slippage by leveraging the Synth's proprietary unique pooled collateral model. Trades between Synths generate a small fee that is distributed to SNX collateral providers.

ALL FOREX CRYPTO INDEX

sUSD USD PRICE \$1.00 Tracks the price of a single US Dollar (USD). This Synth always remains constant at 1. FEE: 0.30% LIVE	sEUR USD PRICE \$1.14 Tracks the price of sEUR Euro through price feeds supplied by an oracle. FEE: 0.30% LIVE	sJPY USD PRICE \$0.01 Tracks the price of sJPY Japanese Yen through price feeds supplied by an oracle. FEE: 0.30% LIVE	sAUD USD PRICE \$0.72 Tracks the price of sAUD Australian Dollars through price feeds supplied by an oracle. FEE: 0.30% LIVE
sGBP USD PRICE \$1.36 Tracks the price of sGBP Pound Sterling through price feeds supplied by an oracle. FEE: 0.30% LIVE	sCHF USD PRICE \$1.08 Tracks the price of sCHF Swiss Franc through price feeds supplied by an oracle. FEE: 0.30% LIVE	sKRW USD PRICE \$0.00 Tracks the price of sKRW South Korean Won through price feeds supplied by an oracle. FEE: 0.30% LIVE	sBTC USD PRICE \$42,764.46 Tracks the price of sBTC Bitcoin through price feeds supplied by an oracle. FEE: 0.30% LIVE
sETH USD PRICE \$3,261.30 Tracks the price of sETH Ether through price feeds supplied by an oracle. FEE: 0.30% LIVE	sLINK USD PRICE \$26.12 Tracks the price of sLINK Chainlink through price feeds supplied by an oracle. FEE: 0.30% LIVE	sADA USD PRICE \$1.24 Tracks the price of sADA Cardano through price feeds supplied by an oracle. FEE: 1.00% LIVE	sAAVE USD PRICE \$216.82 Tracks the price of sAAVE Aave through price feeds supplied by an oracle. FEE: 1.00% LIVE

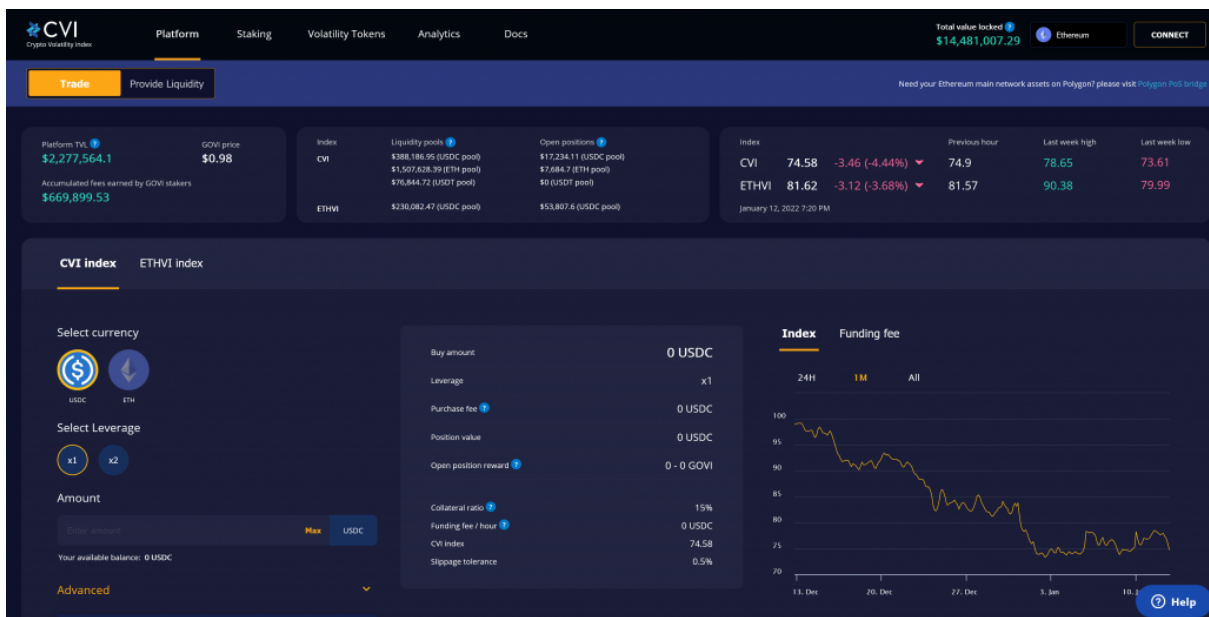
<https://synthetix.io>

Synthetix was the original synthetic product which has struggled to gain traction due to high gas fees on Ethereum.

Indexes

Over the last 30 years we have seen a migration from managed funds to passive index funds in stock markets. In crypto it's been much easier to "beat the market" but at some point this will likely change and we will see more Top100Coins type index products. Currently there are volatility products and token funds which aren't gaining huge amounts of traction. As markets mature I would expect to see more market trackers gain traction as DeFi derivatives.

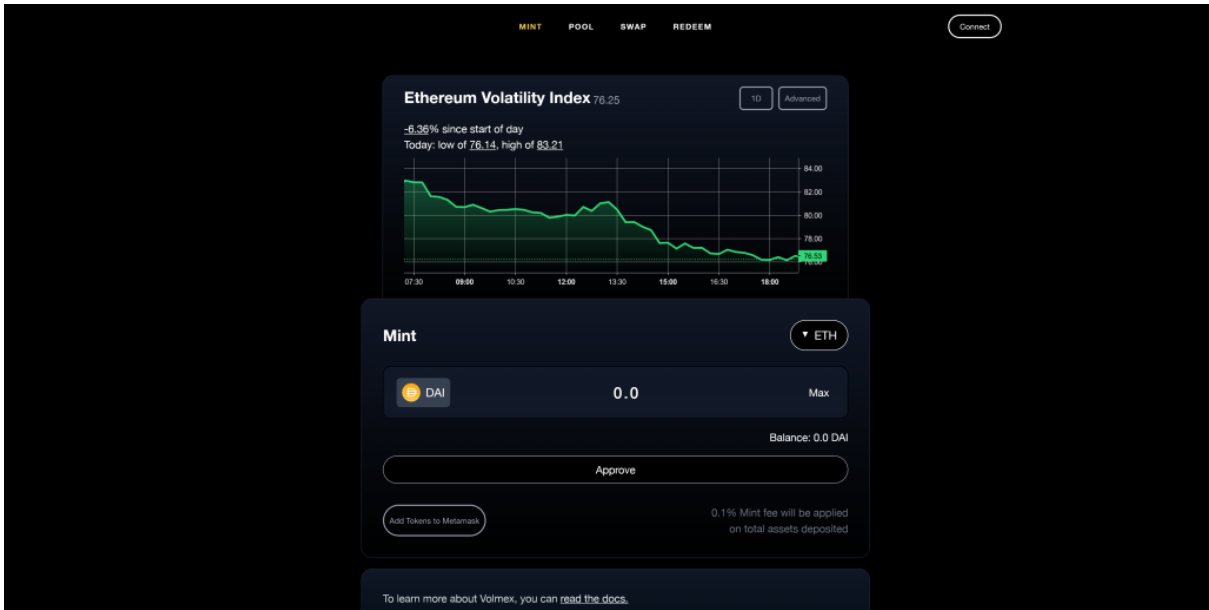
Crypto Volatility Index



<https://cvi.finance>

CVI aims to be the VIX of crypto. It's a DeFi protocol with a trading platform running on Ethereum that tracks the volatility of the crypto markets.

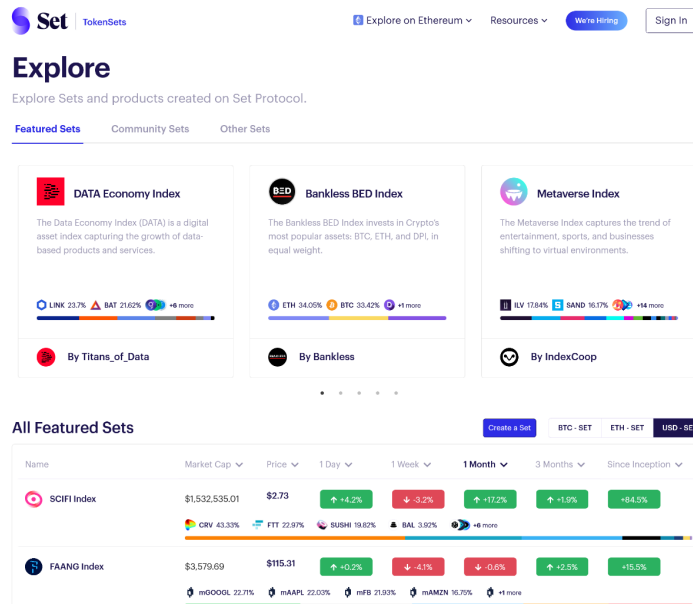
Volmex



<https://app.volmex.finance>

Volmex is another volatility index which offers tokenized volatility products that trade on Uniswap

Set Protocol



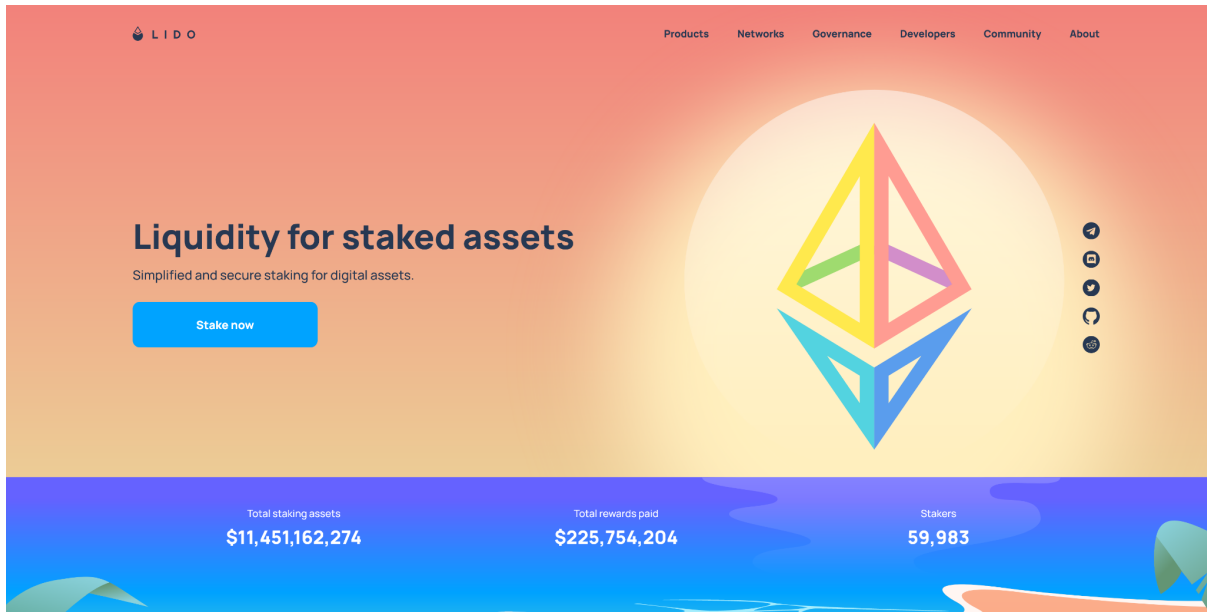
<https://www.tokensets.com/>

Set protocol provides user managed indexes or sets as they are known. These contain a portfolio of digital assets which are managed by a fund manager.

Liquid Staking

Liquid staking enables holders to deposit their native assets on a platform which will then stake them and return the rewards to a tokenized version of the base asset. It makes staking easy and with the rollout of Ethereum 2.0 this year I think it's going to gain a lot of attention.

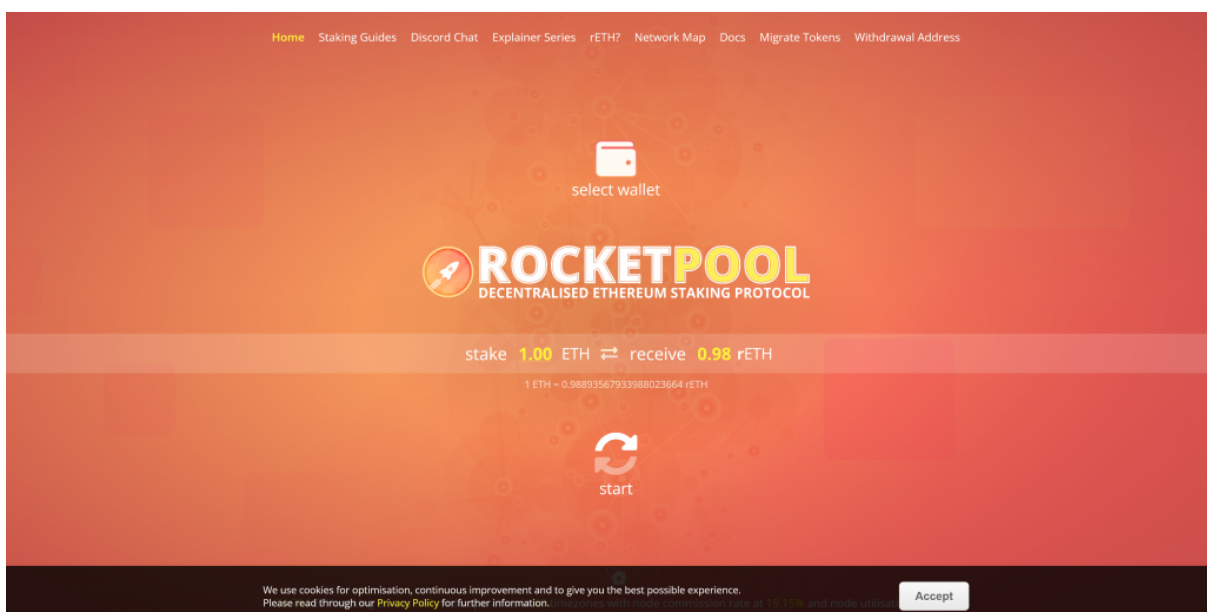
Lido



<https://lido.fi>

Lido is the leading liquid staking protocol on Ethereum, Solana and Terra. It provides tokenized assets that represent an underlying base asset + staking yield. For example stETH is staked Ethereum and holders see their balance increase every day as rewards from staking are distributed.

RocketPool



<https://stake.rocketpool.net/>

Rocket pool is a direct competitor to Lido with their rETH staked Ethereum token which is currently trading below the base asset.

Where Does Yield Come From

Interest rates in traditional banks are 0.1%, have you ever wondered how DeFi yield farmers are getting 20-100% yields on their digital assets? Is it sustainable wealth creation or a giant ponzi that risks collapsing in on itself.

Borrowers

There is always a demand for borrowing and in DeFi this is most often seen in the form of over-collateralized loans. Because no one has a credit rating in DeFi (yet) the only way to borrow funds is to provide more collateral than you want to borrow. But why would you want to do that? Well there are a few use cases in yield farming, short trading and tax planning.

Borrowers will pay a fee to lenders and lending protocols which generates yield for the lender.

Yield Farming Stables

Yield farmers will often deposit volatile digital assets such as native tokens like ETH or SOL. They will then take a loan out in USD stable coins and use this for yield farming strategies or to gain a leveraged position. As long as the value of ETH doesn't drop below or near the value of the USD they can use the stablecoins to do whatever and **still get the gains from price appreciation on the ETH** which is locked as collateral.

A borrower can normally borrow up to 80% of the value of their assets. This means they can purchase 80% more ETH then provide that as collateral to buy more ETH etc. If ETH goes up forever the value of their collateral increases allowing them to borrow more stablecoins. If the price of ETH drops sharply the borrower risks having their collateral assets liquidated and losing them.

Short Traders

A short trader will do a similar thing but they'll provide USD as collateral and borrow ETH if they expect the price to drop. They can then sell ETH on exchange to hold USD and buy it back at a lower price later if they are right to pay off the loan.

Tax Planning

Because I'm always net long, in these market conditions it doesn't matter, but in up only markets tax planning comes into play. In many jurisdictions there is **no capital gains tax on loans** or money borrowed on assets. It's still unclear whether this counts for crypto and to my knowledge we haven't seen any legal disputes arise to date. However many users are

holding their Bitcoin and Ether as collateral and borrowing stablecoins on that as a way to avoid capital gains tax.

Lenders & Lending Protocols

If borrowers are paying fees to borrow assets then lenders and **lending protocols can earn a yield by providing those assets**. DeFi protocols such as AAVE use this economy to generate yield for users that deposit and lend out their funds.

Trading Fees

Another source of yield is **trading fees from decentralized exchanges and trading platforms**. When someone trades one digital asset for another they will generally pay a fee. Uniswap for example has a standard fee of 0.3%. These fees form some of the most important revenue streams for DeFi protocols.

Liquidity Providers

Liquidity providers deposit funds to decentralized exchanges for traders to buy and sell against. Often this will be in the form of a liquidity pair such as ETH-USDT. Equal values of ETH and USDT will be provided to the liquidity pool and a trader can then swap some ETH and take out some USDT or visa versa. The trading fees are paid to liquidity providers to compensate them for lending their assets and to offset [impermanent loss](#).

These **trading fees can also be gained in yield farming vaults** which accept deposits and then use strategies to optimize the amount of trading fees gained for the amount of funds deposited.

Leveraged Traders

In both traditional finance and crypto there is a **strong demand for leveraged trading**. Leverage allows a user to make larger bets on whether an asset will go up or down.

Let's explain this with an example where a \$MISC token is valued at \$100. A trader that has \$1000 in his account can buy 10 tokens and if they go up 50% he will make \$500. If he used 10x leverage he could borrow the funds to buy 100 tokens and if it goes up 50% he'll make \$5000 a 5x return on his investment. There are risks here where the trader gets liquidated on a small drop in price but there is still demand for this product in financial markets.

Leverage is often used on derivative products such as **options and futures contracts**. These contracts carry a funding rate premium which is a type of fee for the holder. If more people want to go long (betting the market will go up) than short then the longs will pay the shorts a premium.

This opens up the opportunity for a cash and carry strategy where a trader or protocol will buy 1 digital asset and then open a short position for the same amount. If the asset goes up or down they are hedged so it doesn't matter and they collect the funding rate premium.

FUTURES FUNDING RATE STRATEGY

BUY +1 **SELL -1**

FUNDING RATE PREMIUM +0.1%

SPOT MARKET **FUTURES MARKET**

BALANCED PRICE MOVEMENT IN UNDERLYING ASSET HAS NO EFFECT

https://jamesbachini.com James Bachini @james_bachini

We are only starting to see this come into DeFi as decentralized trading volumes increase but this will likely grow in the future and protocols such as [Perpetual Protocol](#) and [Ribbon Finance](#) are worth keeping an eye on to gauge the timing of this shift.

Governance Tokens

Governance tokens make up the majority of value creation in decentralized finance.

A borrowing and lending platform might offer 3% to lenders with another 20% made up from the distribution of governance tokens.

Pool	Base vAPY ?	Rewards tAPR ?	Volume ▼
tricroypto2 CRYPTO V2 [?] USDT +wBTC +WETH	1.15%	+4.05%→10.12% CRV	\$253.7m
mim USD MIM+3Crv	0.5%	+5.25%→13.12% CRV +0.00% SPELL	\$105.5m
3pool USD DAI +USDC +USDT	0.29%	+0.98%→2.45% CRV	\$54.5m
sUSD USD DAI +USDC +USDT +sUSD	3.3%	+3.11%→7.77% CRV +1.69% SNX	\$51.7m

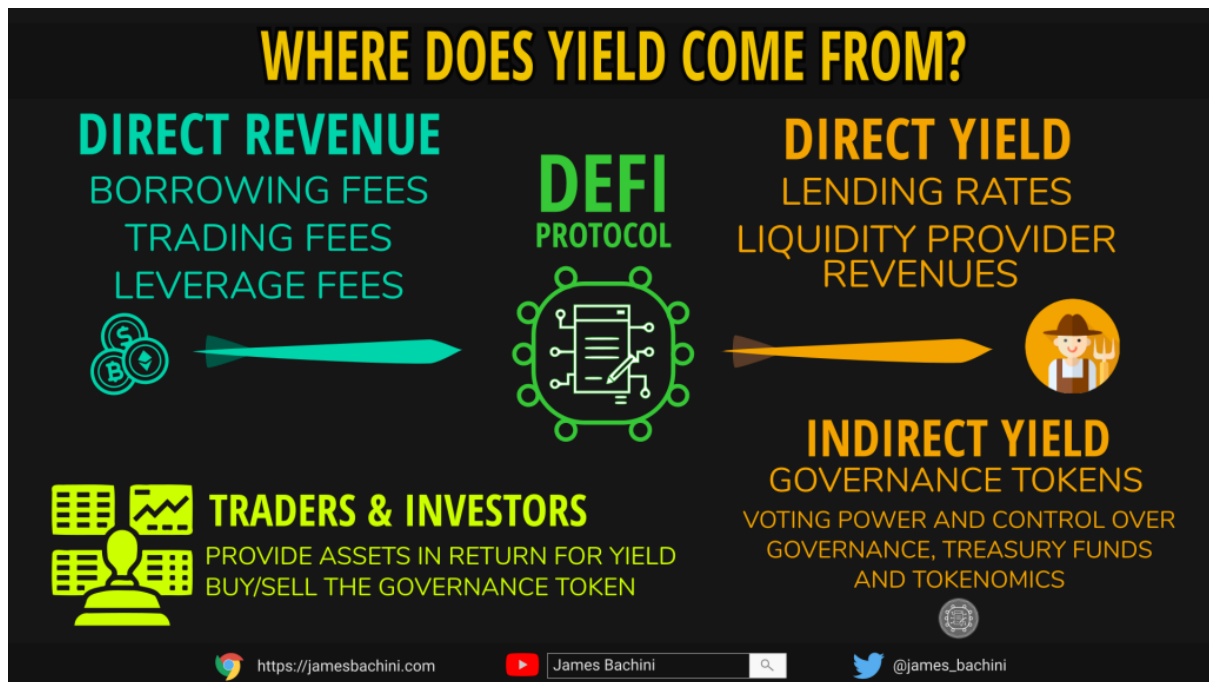
Curve gives depositors the trading fees from the platform but further incentivises liquidity with the distribution of governance tokens.

Governance tokens **hold a lot of value** because:-

- In the case of a DAO they control the future of the protocol through voting
- They often control vast treasury funds, Uniswap has \$7B in their treasury
- They control the flow and distribution of newly minted governance tokens

Often when the supply of a governance token is too high we see a price decline over time on exchange as they are sold off by yield farmers. When DeFi protocols get it right the

governance token price increases over time further incentivising adoption by yield farmers, investors and traders.



Ponzi or Value Creation

So much of the value in yield farming comes from the distribution of governance tokens that the whole system relies on us agreeing they hold value. Remember that **DeFi has only been around a couple of years and we've never had a bear market** since its inception. Inevitably we will see one and it will be a stress test for the economic models of many DeFi protocols.

Does that mean that DeFi and yield farming is a ponzi scheme? No. Clearly the protocols, decentralized exchanges and lending platforms are generating value. As long as they continue to be used they will continue to generate value for their token holders and liquidity providers.

Not all protocols are created equally however and eventually perhaps we see a **rush to quality as the platforms that generate direct revenues win** over the latest and greatest farm tokens.

Impermanent Loss

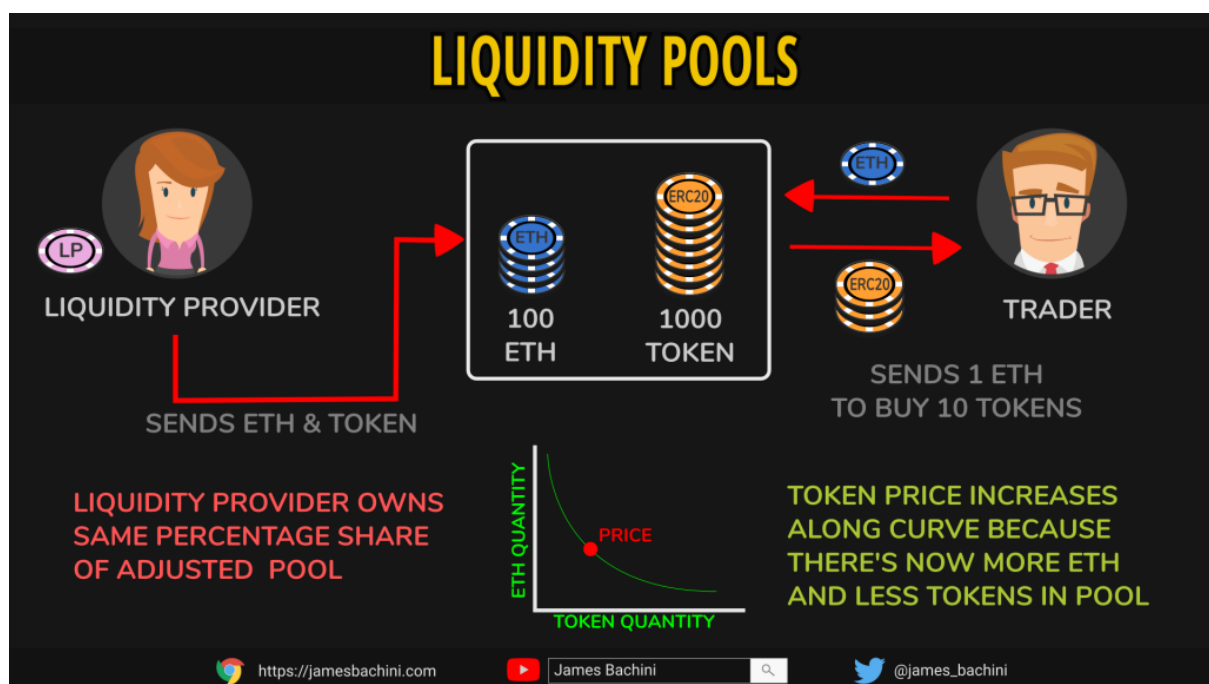
What is Impermanent Loss?

Impermanent loss is the effect where if one asset in a liquidity pool is purchased the price increases along the curve but there is less of that asset in the pool. The liquidity providers own the same percentage share of the total pool meaning they now own less of the more valuable asset.

If price returns the pool rebalances such is often the case with stablecoins however if the price keeps moving the loss or opportunity cost is very much permanent. For taking this risk liquidity providers are rewarded with trading fees.

Understanding Liquidity Pools

To fully understand impermanent loss we need to first know how liquidity pools function. Liquidity pools such as those used by popular automated market makers such as Uniswap and Sushiswap contain a pair of assets. A pool might contain a base asset such as ETH or USDT and a more volatile asset such as a new governance token for example.



A liquidity provider will send both assets to the pool. In return they will receive LP tokens which will entitle them to a share of the pool.*

A trader can use the pool to swap ETH for the token. This adjusts the ratio of quantities in the pool because they are adding ETH and taking away the tokens.

The liquidity provider still owns the same percentage of the total pool but it now contains more ETH and less tokens.

The price of the token is also adjusted because it is calculated based on the ratio of quantities in the pool. If traders keep buying the token the quantity is depleted and price goes up.

The liquidity pool contains less of a more valuable token. This is where impermanent loss comes in because the liquidity provider has lost some value in the pool.

To compensate the liquidity provider most automated market makers will charge a fee of around 0.3% per trade paid directly into the pool increasing its value over time.

If the trader then sells their tokens they return them to the pool and take out their ETH. This rebalances the pool and both the price and quantities return to the original values however the fees have increased the total funds in the pool. The loss in value the liquidity provider originally suffered was indeed impermanent.

** On a side note Uniswap v3 introduced non fungible LP tokens which are specific to the concentrated liquidity position.*

Liquidity Provider Risk

Impermanent loss becomes an issue when price diverges between the assets and doesn't come back. In this situation a liquidity provider loses out because of the diminishing quantity of the asset that is increasing in price in the pool.

Price movement is relative to the base asset. If the liquidity pool is UNI/ETH and both ETH and the UNI token go up in value together relative to USD then there isn't actually any change in the pricing in the pool.

The liquidity provider risk is compensated by transaction fees. More active pools earn more fees because there are more trades in the pool.

Uniswap v3 introduced variable fee ranges to better align the risk of impermanent loss with the trading fee.

- Stablecoins 0.05%
 - Standard 0.3%
 - High volatility 1%
-

Calculating Impermanent Loss

Automated market makers use a simple formula $x * y = k$

X is the quantity of the base asset, Y is the quantity of the second asset, and K is the product constant of the pool.

Let's look at an example where the UNI/ETH pool contains 12605 ETH and 1,459,747 UNI tokens and one UNI costs 0.008635 ETH. The total value locked (TVL) in the pool is 25,210 ETH.

We can calculate the **product constant** as $12605 * 1,459,747 = 18,400,110,935$

Now let's assume that the Uniswap doubles in value relative to ETH. Even if this happens on centralized exchanges arbitrageurs will swap ETH for UNI tokens until the price is met in the liquidity pool. The price ratio will now be 0.01727 as the cost in ETH terms has doubled.

We can use the following formula to calculate the quantity of assets in the pool at any price point.

```
$uniQty = sqrt($priceConstant / $priceRatio);
```

```
$ethQty = sqrt($priceConstant * $priceRatio);
```

So in the UNI/ETH example we have the new quantities in the pool:

```
$uniQty = sqrt(18.4e9 / 0.01727) = 1,032,197
```

```
$ethQty = sqrt(18.4e9 * 0.01727) = 17,826
```

How would liquidity providers be affected by this price change?

The total pool including UNI tokens was originally valued at 25,210 ETH, it is now valued at 35,652 ETH because of the value increase in the UNI side of the pool. However if those same funds had just been held rather than committed to a liquidity pool they would be worth 37,815 ETH. **Our impermanent loss is 2,163 ETH or 5.7%**. Note this doesn't take into account fee accrual over our imagined time frame that the asset doubled in value.

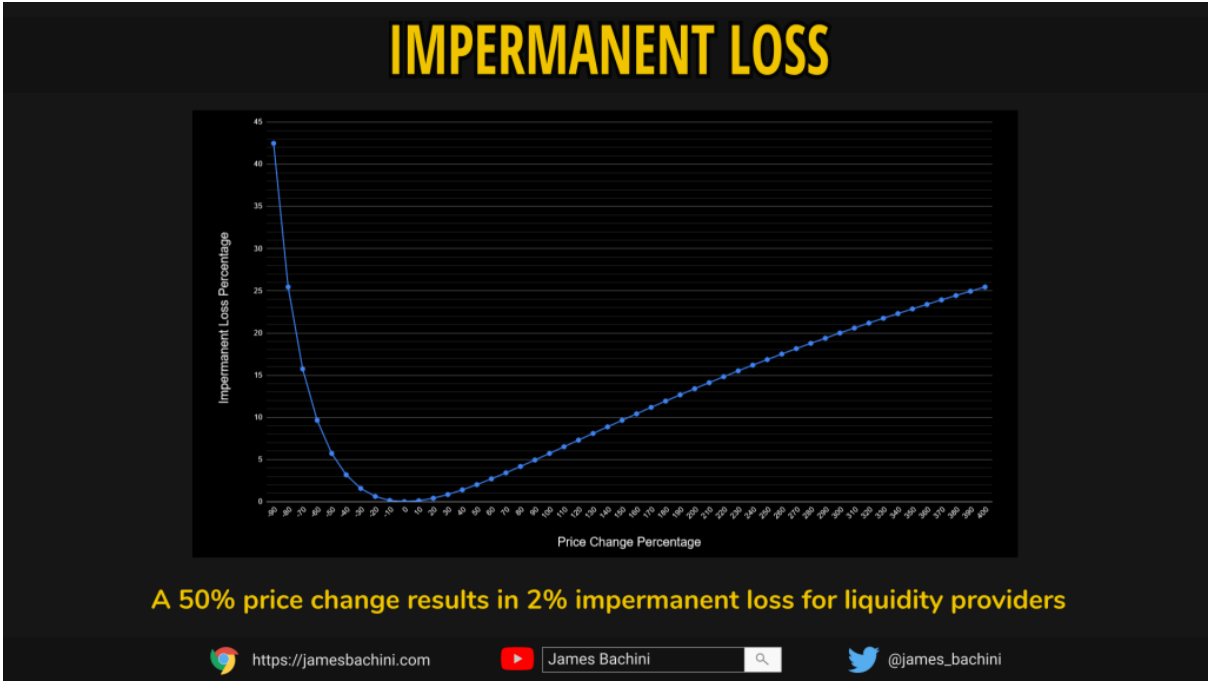
So we can put this formula into a Javascript function to calculate impermanent loss:

```
const baseQty = 12605;
const tokenQty = 1459747;
const futurePriceRatio = 0.01727;

const calcImpermanentLoss = (baseQty, tokenQty, futurePriceRatio) => {
  const productConstant = baseQty * tokenQty;
  const hodlStrategy = ((tokenQty * futurePriceRatio) + baseQty);
  const lpStrategy = ((Math.sqrt(productConstant / futurePriceRatio)) * futurePriceRatio) +
(Math.sqrt(productConstant * futurePriceRatio));
  const impermanentLoss = (hodlStrategy - lpStrategy) / hodlStrategy * 100;
  return impermanentLoss;
}

console.log(calcImpermanentLoss(baseQty, tokenQty, futurePriceRatio));
```

We can now use this function to plot a graph across many price points.



As a rough rule of thumb we can use this to calculate that a 50% price change relative to the base asset results in a 2% loss for liquidity providers.

The other side of this that we would need to consider is the fee revenue which isn't taken into account.

We can see how much fees have been accrued by checking trading volumes.

<https://info.uniswap.org/#/pools>



The Uniswap UNI/ETH pool for example has \$91m TVL (total value locked) and \$177m in 7 day trading volume.

The fee rate for that pool is 0.3% which means that over the seven days \$531,000 USD in fees has been added to the pool. This divided by the TVL means that for every dollar provided by liquidity providers they've increased their holdings by \$0.0058 which is roughly 30% APR. Note this doesn't take into account the effects of concentrated liquidity positions. From the impermanent loss chart we can calculate that the UNI token would need to lose in excess of 80% of its value relative to ETH over the course of a year for this to be unfavorable for liquidity providers.

Correlation Between Assets

An ideal situation for liquidity providers is a pool with lots of trading but very little price movement. Stablecoin pools for example like USDT/USDC get traded regularly but aren't expected to fluctuate in price.

Other assets tend to move in unison as well. ETH and DeFi tokens tend to go up and down together and the more established higher market cap coins have a higher correlation. In contrast, new tokens, meme coins and other highly volatile assets can have wide swings in price relative to any base asset leading to greater impermanent loss.

For established tokens we can use [Tradingview](#) to look at ranges and compare trading pairs.



In the example above we are plotting UNI/ETH and adding a comparison indicator for SUSHI/ETH. I've marked on the high time frame top and bottom of the range for UNI.

With all other things equal it seems UNI is less volatile compared to SUSHI which would benefit liquidity providers in that pool.

Hedging Price Movements

The issue with hedging impermanent loss is that it occurs in both directions and you need to have some idea of where the risk lies. If UNI reaches a level and looks like it's going to breakout and go up 50% against ETH it's trivial to take out a long position to cover the 2% risk to impermanent loss. However if that turns into resistance and the UNI token price crashes back down the hedge gets crushed and you still get an impermanent loss on the downside.

In the past it's been difficult to actively manage LP positions because ETH gas fees have been so expensive. With Eth2.0 and layer 2's I think there is going to be much more room for mitigating risk during periods of high volatility. There are a number of ways to measure market volatility but one of my favorites is the DVOL index from [Deribit](#). This is a forward looking indicator as it's based on the options positions and market participants expectations of the next 30 days volatility in Bitcoin price.



A rough rule of thumb is to divide DVOL by 20 to get a daily expected move in Bitcoin price.

So this can be used to get an idea of Bitcoin volatility which will affect the overall market. We can use simple technical analysis on TradingView as well to build a thesis of how volatile a specific trading pair is likely to be in the coming weeks. If Ethereum gas fees permit it during periods of peak volatility we can simply close the liquidity position until the market stabilizes.

Note that the worst times for liquidity providers will coincide with the periods where gas prices and network congestion are at their highest levels.

In the future it's not impossible to think that this could be automated within a smart contract strategy for managing liquidity positions.

DeFi Risk Framework

The high yields available in decentralized finance come with a downside. DeFi risk is real and if you are participating in the markets then you should know how to assess and manage that risk. By building a risk assessment framework for yield farms and DeFi opportunities we can better assess fair value and allocate capital accordingly.

Types of Risk In DeFi

When a user places funds into a new DeFi protocol the risk that they are exposed to can be broken down into four main areas.

Smart Contract Risk Flash loan attacks, hacks, bugs and lost funds

Counterparty Risk Rug pulls, personnel and organizational failures

Legal Risk Centralisation attracts legislation

Token Exposure Risk Price volatility and long term valuations

The next few sections look at how to assess these risks individually with a chapter at the end on how to [mitigate DeFi risk](#). If we can quantify and manage risk with greater accuracy then we can make better decisions when allocating capital.



Smart Contract Risk

Decentralized finance runs on code in the form of smart contracts across a peer to peer network of computers. These contracts often hold funds within the contract itself which makes them a target for hackers. Flash loan attacks have been used in the past to drain huge fortunes from vulnerable liquidity pools.

Lindy Effect

The [Lindy Effect](#) suggests that there is a correlation between something's current age and its life expectancy. The longer that thing has been around the more likely it is to survive. It is ironically named after the NYC restaurant that closed in 2017

In DeFi it's fair to perceive smart contracts that have held funds for some time as being safer than newly deployed smart contracts. Large protocols will have already been probed by hackers looking for any weakness. If it hasn't been hacked yet then it's less likely to be hacked... in theory.

There are well known exceptions where bugs have been found in established code but for the most part this rule will hold true that new protocols hold more smart contract risk than existing ones.

Another consideration is the amount of funds locked in a contract. A protocol that isn't popular won't be as battle tested as something that's contained over \$1B in TVL for the past year.

Security Audits

Not all security audits are created equally and there's a huge divide between a Consensys or Certik program and an audit purchased from Fiverr.

The best security audits will provide a transparent report detailing:

- Amount of engineer hours committed
- Code coverage and ongoing monitoring
- Threat levels of any bugs found
- Code review and best practices
- Edge cases and fuzzing results

As a developer there is huge value in having a second and third pair of eyes look over your code with a sole focus on security. As an investor there is value in knowing the team has the confidence in their code to be audited and that the best minds in the industry are signing off on the protocol.

Bounty Program

Every well funded DeFi platform which handles funds should have a well managed bounty program. This offers white hat hackers (good guys) an incentive to investigate, report and fix bugs before they get exploited by the black hats (bad guys).

Bounty programs can be run in house or via a 3rd party intermediary such as [hackerone](#).

Code Quality & Originality

Code quality is a very difficult thing to quantify because what looks good to me might look spaghetti to another developer. By reading the code and getting a feel for how it was put together most devs will still be able to make a useful assessment.

Originality in blockchain development is what drives the industry forwards and gains traction for new protocols building on the cutting edge of financial technology. Unfortunately it can be bad thing when it comes to risk assessment.

Code reuse is recommended wherever possible because it leaves less room for bugs. There are the excellent [OpenZeppelin](#) libraries for example which can be imported and have been pre-audited. By using existing code and libraries that are already in the wild, developers can benefit from the Lindy effect. Obviously this isn't to say that innovative, original code is a negative overall, just that 1000 new lines of solidity is a negative from a smart contract risk perspective.

Counterparty Risk

Even the most decentralized protocols have some form of organization structure. That might be a development team, a corporation or a DAO (Decentralized autonomous organization).

When those organizational structures fail the investors are often hurt financially from the fallout. That might be from the extremes of a rug pull (developer draining the funds and

running off to Mexico) or simply token value decimation when an important team member leaves.

Doxed Team

There are a lot of benefits for developers to remain anonymous. There is a lot of pressure and negative sentiment thrown on blockchain developers. [Andre Cronje](#) of Yearn Finance fame talks a lot about this and is a victim of his own success. Unfortunately developers can not continuously create value at will and can't give everyone their Lambo.

A doxed team simply means a team that is not anonymous. A DeFi developer team that has no anonymous developers is becoming rarer but still provides a lot of value to investors.

There is far less chance of rug pulls by doxed teams as it's much harder to hide and recover professional integrity. It's also far easier for anonymous developers to walk away from a project once the post-hype bear cycle and social negativity sets in.

Transparency

It's not just a team's identities where transparency can provide value. How a team handles negatively perceived situations is a clue to how they will manage a project in the future.

Investors want to see fair distribution of information before price movements that would indicate insider trading.

The channels for communication are important too with Twitter, Discord and Medium being common avenues for news distribution. There's a risk benefit to being well connected with the development team and being agile enough to act on news flow before other market participants.

External Funding

Venture capital firms in the space tend to do better due diligence than individual investors. A DeFi protocol that has seed funding from well respected VC's in the space is more likely to have interests aligned with long term investors.

You don't hear of VC backed teams carrying out rug pulls or scamming investors. The seed funding can also add value by adding more personnel to a project and getting independent code audits. VC's will also be very wary of investing in projects that have exposure to significant legal risks.

Legal Risk

The promise of an untouchable self-regulating financial sector built on top of blockchains is somewhat far removed from the real situation in 2022. There's mounting pressure from regulators especially the SEC in the US who is determined to establish authority in the industry.

Centralisation

Regulators will first go over the low hanging fruit to make examples of the bad players and easiest to prosecute participants. **Centralisation invites litigation as it provides a target for regulators.**

If a project is governed by a DAO and the developers are anonymous it's going to take a significant effort to track down and prosecute anyone involved. Alternatively if there's a corporation set up to manage and pay costs for a project then it's far easier for a regulator to commence legal proceedings.

In the past year Uniswap removed obvious synthetic securities, Terra CEO Do Kwon got served 5 mins before going on stage to make a presentation and Coinbase was threatened with legal action if they released a 4% yield function on stablecoins.

From a risk perspective the easier it is to target a person or organization behind a DeFi protocol the more likely it is.

Securities and the SEC

At the head of these probes is Gary Gensler of the Securities and Exchange Commission in the United States. The US represents a huge market that most platforms can't afford to block. Yet there are more and more blocks and restrictions in DeFi UI's for American IP addresses.

Gary Gensler has lectured at MIT on blockchain technology. He was likely chosen to head the SEC because of this experience with the remit to gain "*control of the industry*".

The SEC has significant power as a financial regulator and adopts the sue first, ask questions later policy. Over the next few years I'd expect to see them exercise that power and make examples of some of the DeFi and CeFi platforms.

It's likely that they will initially target exchanges, synthetic stocks and any platforms that have the reach to disrupt traditional finance. These niches provide greater risk especially when combined with corporate management structures.

Legal Jurisdiction

The legal jurisdiction that a project operates in is a significant factor in assessing it's legal risk. China banned cryptocurrency for the 456th time and actually went as far as to kick out the miners from their state. Regulation and litigation is obviously a more significant risk for anyone operating in the US.

Tax Considerations

It's completely unclear where individuals stand on transactions made within smart contracts from a tax perspective. It's still early but the most significant DeFi tax risk is exchanging fiat (USD/EUR/GBP) for cryptocurrency which in most jurisdictions is a taxable event. In some

liquidity pools this happens every 13 seconds on each block which would create a bad situation if it was ever enforced as the whales would probably end up owing more in tax than there is money in the world.

Token Exposure Risk

Token exposure risk comes from holding a digital asset linked to a DeFi protocol. This is often a governance token distributed over time to users of the protocol. The user is then exposed to price volatility of that asset.

Liquidity & Exchanges

Liquidity is the ability to exchange one asset for another. Low liquidity tokens and micro cap projects provide significant opportunity for growth but also pose the risk of higher price volatility and issues with getting out of a position cost effectively.

The greater the amount of capital deployed the more this becomes an issue for a number of reasons.

- Larger orders into thinner order books create greater price movements against the trader
- DeFi transactions are public and large wallets are watched closely
- MEV become an issue over a certain size as sandwich trades come into play

The exchanges that a digital asset is traded on can play a big role in the liquidity and price volatility. A token that is already traded across all the big centralized exchanges will have market makers in place and large arbitrated liquidity pools on DEX's.

Impermanent Loss

Impermanent loss is perhaps the most significant risk in double sided liquidity pools. Consider two pools on Uniswap for example.

UNI-USDC and UNI-ETH

Uniswap's governance token has a greater correlation in price to Ether than it does to the USDC stablecoin. As the market goes up and down UNI and ETH tend to go up and down together relative to the dollar.

This means that there is more risk of impermanent loss on the UNI-USDC pool because whichever way price moves the liquidity provider will always be on the wrong side of the trade.

Impermanent loss is often compensated with higher fees and higher APY's for investors.

Narratives

If we could accurately predict future narratives in crypto markets it would make navigating them much easier. We can however speculate on what future narratives a protocol might have and how it will affect market sentiment.

For example next summer a lot of focus will be on Ethereum, the merge, staking etc. This will likely have some positive and negative narratives associated.

- The unlocking of 8m staked ETH which is likely going to result in some profit taking and short term price volatility
- The triple halvening event making ETH a deflationary asset
- Will staking and predictable, sustainable revenue generation appeal to institutional investors?
- Potential long-term disruption to high risk bond markets, money flow from trad-fi

Brainstorming future narratives can provide a SWOT like analysis of a project's market potential and risk level.

Liquidation Risks

Large price movements at times of high volatility can also cause issues with health factors. A common yield farming strategy is to deposit layer 1 assets such as ETH to a lending platform and borrow USD stablecoins using that collateral to be used in farms.

If the market moves down abruptly even if it's only a short term wick, a significant risk lies in meeting the collateral requirements for that position. Health factors and liquidation engines work differently across different platforms and it is always a case of balancing risk of liquidation with capital efficiency. Less leverage means leaving some chips on the table but during periods of high volatility when networks are congested it might be a price worth paying.

Technical Analysis

Some traders believe that technical analysis is the be all and end all while fundamentals don't matter. Others believe that it's the equivalent of astrology for 30 year old men.

Somewhere in the middle there is an opportunity to better understand the markets by drawing the obvious trend lines and support/resistance zones on a chart. It's obvious that price action greatly affects risk in terms of the market as a whole and individual assets.

Taking out a position at strong support after a liquidation cascade is considerably less risky than FOMOing into a parabolic asset at any price when markets are getting frothy. However our natural instincts act against us and the best opportunities to time the markets often feel uncomfortable and unnatural to risk-on.

Mitigating Risk In DeFi

There's a lot to take in from the sections above and at first glance it looks overwhelming. The DeFi sector is inefficiently priced and it'll likely stay that way as institutions will opt for the safest possible protocols. This presents an opportunity to outperform on a risk/reward basis by creating frameworks from which to assess and compare risk between protocols.

As investors we want exposure to the assets we believe will appreciate the most. As yield farmers we want the highest yields possible at the lowest risk possible on those assets.

Diversification

No DeFi contract is risk free. Perhaps Curve is considered the closest thing and the lower APY's reflect that investor sentiment. But investing all your funds in Curve puts all your eggs in one basket and that basket isn't going to get spectacular yields.

There's a benefit to distributing assets across different protocols as any disasters or areas of bad performance won't wipe out funds completely. This becomes more critical the further up the risk curve investors go to seek out higher yields from more risky farms with greater potential of loss.

While I wouldn't go as far to say that "diversification is the only free lunch in DeFi" it can play an important part in mitigating overall portfolio risk and **vastly reducing risk of ruin**.

System Trading & Web3 Bots

While most participants will interact with DeFi protocols via a website interface, the protocols functions are also accessible from web3 scripts.

This allows traders and investors to create risk management systems and put limits in place, then hard code them into a bot.

A risk management engine might have price limits to close positions, it might be used to manage health factors on borrowing platforms or it could be used to optimize concentrated liquidity positions.

The opportunity is there for developers to build out programs that give them a clear advantage in the markets.

Analysis & Allocation

The vast majority of market participants won't be accurately pricing risk which provides an opportunity for pro-active investors.

Effective analysis and allocation of funds in line with the best opportunities at any given time will ensure the best chance of outsized returns. DeFi markets change fast and the highest APY's don't last for long. It's capital efficient to move funds regularly and always be researching new projects, pools and reevaluating your investment thesis.

Setting Up A Wallet

The most popular digital wallet for Ethereum and EVM compatible chains is Metamask. Metamask can be used to set up and manage accounts, transfer funds between accounts and interact with web3 applications.

It's worth noting that there is no perfect way to store digital funds and various risks apply to different methods. For large amounts it is worth considering purchasing a hardware wallet or cold storage solution.

A cold wallet is a way of storing funds by keeping the private key offline. An example would be when the Winklevoss twins who were early adopters for Bitcoin purchased a laptop, set up a private key/public key pair, divided the private key in to 3 parts, each part was duplicated and then put each of the six parts in a different bank security box across the country. This is an extreme example of keeping keys secure. The main idea is to make it (almost) impossible for hackers to gain access to your keys if they aren't connected in any way to the internet.

For most users a hardware wallet such as those made by Ledger and Trezor can provide sufficient security and keep their funds offline until they are needed.

Another option for managing digital funds is a multisignature (multisig) wallet. It requires multiple signatures from different parties to transfer funds. For example a Gnosis multisig wallet might be set up by a team who want to secure their treasury funds. There might be 5 team members who are signatories on the account and it may be set to require at least 3 signatures for a transaction. Each user will be given a private key/public key pair via a digital wallet like metamask. They can then propose and sign any transactions to transfer funds which won't go through until 3 team members have signed off on the transaction. Multisig wallets are used to mitigate the risk of theft, lost keys and hacked funds.

Testnets

Testnets provide a way to experiment with DeFi without taking any financial risk. You can choose a testnet such as the *Ropsten Testnet* from the metamask connections tab. Then google "Ropsten faucet" to receive some free testnet ETH.

Almost all DeFi protocols will be deployed on one or more of the testnets. If you visit Uniswap and connect via metamask with the testnet selected, you will see a notification message that you are connected to the testnet rather than mainnet.

When trying out new things in DeFi both beginners and advanced users alike will often use a testnet to experiment and get familiar with the process of moving funds around. Developers will usually deploy contracts to a testnet and carry out checks before deploying to a mainnet which costs real Ether.

Block Explorers

A block explorer provides a user interface for anyone to search for transactions, accounts, contracts and blocks on a blockchain network.

Etherscan is Ethereum's block explorer and is a pillar of the industry. When a user sends a transaction they'll often be quoted a confirmation tx address which can be copy and pasted into etherscan to see the details of that transaction.

The screenshot shows the Etherscan website interface. At the top, there's a navigation bar with 'Home', 'Blockchain', 'Tokens', 'Resources', 'More', and 'Sign In'. Below the navigation bar, the main heading is 'The Ethereum Blockchain Explorer'. There's a search bar and a featured section with a link to 'Yield Farms!'. The main content area is divided into several sections: 'ETHER PRICE' showing \$3,056.01, 'MARKET CAP' at \$359,351,574,235.00, 'TRANSACTIONS' at 1,298.29 M, 'DIFFICULTY' at 9,191.51 TH, 'MED GAS PRICE' at 88 Gwei, and 'HASH RATE' at 687,589.65 GH/s. There's also a 'ETHereum TRANSACTION HISTORY IN 14 DAYS' chart. Below these are two columns: 'Latest Blocks' and 'Latest Transactions'. The 'Latest Blocks' column shows a list of blocks with their IDs, miners (like Miner Ethermine and Miner BeePool), and the amount of ETH. The 'Latest Transactions' column shows a list of transactions with their IDs, from/to addresses, and the amount of ETH. At the bottom of each column, there are links to 'View all blocks' and 'View all transactions'.

<https://etherscan.io>

Yield Farming

Yield farming is the process of deploying capital to DeFi protocols, lending platforms and liquidity pools to capture the highest possible return on investment.

When an investor commits funds to a financial instrument they expect a return on that investment in the form of capital appreciation. ROI is a measure of that return, it can be

calculated via the formula: $(\text{final value of investment} - \text{initial investment}) / \text{total cost of investment including fees} \times 100\%$.

Yield farming can be a low risk passive strategy but more often yield farmers operate a cat and mouse game of looking for new protocols to get in early on and start earning the best rewards. Often yield farmers will only participate in a single farm for a period of a few days or weeks before switching to the next project that wants to bootstrap liquidity and is offering incentives to do so.

An example would be a user that holds Ether and wants to gain a yield on that holding for passive income. They could deposit the Eth to a lending platform and take a loan in a USD pegged stablecoin. They would then use the stablecoin to provide liquidity to a new protocol that is launching and distributing their governance token. If all goes well they make a high ROI on their strategy, pay off the loan and pocket the profit.

However if the value of ETH drops or something goes wrong with the protocols they are using they risk losing their initial Ether which is being used as collateral.

What Comes Next

In this section we will take a peek into the future to see the changes that may be coming as the industry evolves and matures.

Regulation

Within crypto circles regulation is usually regarded as a potentially damaging problem that should be avoided where possible. Not all regulation is bad and having a more regulated crypto market would open it up wider to institutional investors.

One positive big change will be the approval of Bitcoin ETFs (exchange traded funds) on US markets like the New York Stock Exchange. There are currently around a dozen applications awaiting approval by the SEC (American securities regulator). ETFs will provide a familiar, safe investment vehicle for hedge funds and family offices to gain digital asset exposure.

A problem evolves from the need for anti-money laundering regulations (AML) which requires financial institutions to collect personal data on their customers (KYC - Know your customer). This is to prevent financial crimes and stems from the government's need to control financial markets and transactions. A government can currently freeze assets from a criminal enterprise for example preventing the use of that capital for further crimes.

In truly decentralized finance there is no central party to regulate and enforce KYC requirements. The blockchain community was born from a libertarian background and users tend to prefer not to share their personal details. This is a somewhat unsolvable problem and governments may eventually need to embrace the loss of control.

Over time the increasing money supply through borrowing and quantitative easing leads to inflation and the devaluation of such currencies. Will regulators step in if the migration to digital assets starts to have a negative impact on fiscal control?

“Our Financial Policy Committee has assessed cryptoassets and concluded that they do not currently pose a risk to monetary or financial stability in the UK”

Bank of England

Central Bank Digital Currencies

It's been rumored that China is in the later stages of testing and may be the first major nation to launch a CBDC.

It's unlikely that CBDC's will run on existing blockchains like Ethereum but may use custom enterprise grade forks which would make them somewhat compatible with existing DeFi infrastructure.

Having a compatible CBDC that worked in the DeFi space would appeal to many users due to the backing of a national government. It's possible if China is first to launch a CBDC then it could compete with US dollar stablecoins as the base asset for decentralized finance.

Bridging Traditional Finance

Commercial banks are only starting to dip their toes into blockchain technology and decentralized finance opportunities. The incumbent enterprises in traditional finance will naturally be slower to adapt to the changing market conditions. This provides a window of opportunity at this moment in time.

Banking isn't currently a developer driven industry and often tech requirements will be outsourced to external dev teams. It's going to take years if not decades for them to update their legacy systems to fully integrate digital currencies and decentralized finance.

In the nearer term there is a growing demand for mobile banking services with prepaid debit cards. Some of these mobile banking apps are already offering customers the ability to hodl funds in cryptocurrency and then transfer them across to the local fiat currency on a prepaid card to pay for goods and services.

The term hodl came from a December 2013 BitcoinTalk forum post by an intoxicated user declaring *"I AM HODLING"*. Having misspelled holding the post led to the term sticking and is now widely used within the community. It simply means to hold on to an asset through the ups and downs. Often quoted as hold on for dear life.

These companies are generally more fintech focused and could potentially move faster to offer DeFi services on the backend. For the next generation of consumers it may seem alien to stand in line at a high street bank to open an account when they can just download an app and manage their finances from their mobile phone.

Multichain

Ethereum's virtual machine has become the industry standard for smart contracts and has been forked and modified into numerous alternative chains. Here are some of the most widely used and notable EVM compatible chains.

All of these blockchains can be accessed using the networks tab in metamask.

Polygon - A side chain formerly known as Matic that has gained a strong and thriving DeFi ecosystem. Polygon benefited from low transaction fees to gain traction in 2021 when the Ethereum network was suffering from increasing congestion. Polygon uses a proof of stake consensus mechanism.

Binance Smart Chain - Considered CeDeFi which really is centralized decentralized finance. Consensus is achieved from the 21 *approved* block producers. With the support of the biggest digital asset exchange this network has grown and is widely used for borrowing, lending, trading and yield farming.

Optimism - A layer 2 scaling solution which has some big players on board in the DeFi space. Uniswap and Synthetix are launching with roll out of Optimism.

Arbitrum - A competing layer 2 scaling solution with similar optimistic roll up technology.

Avalanche - Avalanche is a multichain project in itself but their contract chain known as the C chain is EVM compatible.

HECO - Huobi Eco Chain is an EVM compatible side-chain from the Chinese exchange.

ZKsync - A zk rollup layer 2 scaling solution. Uses zero knowledge proofs to validate data.

Harmony - A sharded proof-of-stake EVM compatible blockchain.

Further Reading

<https://ethereum.org/en/defi/> The official Ethereum website contains a primer on DeFi

<https://defipulse.com/> A curated list of DeFi protocols ranked by TVL

<https://jamesbachini.com> My personal blog contains posts about defi, blockchain development and portfolio management.

<https://github.com/OpenZeppelin> Source code for various token standards

About The Author

I'm James Bachini and I'm based in Cambridgeshire, England and whenever possible Capbreton, France.

I started out doing web design for local clients in my late teens. Around 2005 I discovered Google pay per click ads and by 2010 I was running high volume performance marketing campaigns to affiliate networks. I was in the right place at the right time just as affiliate marketing was taking off and affiliates had a competitive edge over brand advertisers.

In 2011 I started my blog at <https://jamesbachini.com> to educate and document my journey.

Between 2017 and 2020 I worked on a blockchain project focused on monetisation of web content. The project ultimately failed but it gave me conviction in the blockchain sector and the merits of cryptocurrencies.

By late 2020 I was working on algorithmic cryptocurrency trading systems using data driven analytics similar to what I had been using in performance marketing optimisation. Fortunately I was in the right place at the right time once again.

In 2021 a new cryptocurrency bull market took off and I found myself managing a substantial portfolio of crypto assets. This led me to focus my attention on managing that portfolio and learning as much as possible about risk management, trading and emerging blockchain technologies as quickly as possible.

I create content on my blog and on my YouTube channel where I talk about blockchain development, decentralized finance, trading and portfolio management.

I hope that you've enjoyed this book and that it opens a path for you to go on and experiment with DeFi.

DeFi Definitions & Terminology

[AML \(Anti-Money Laundering\)](#)

[AMM \(Automated Market Maker\)](#)

[API \(Application Programming Interface\)](#)

[APR / APY \(Annual Percentage Rate / Yield\)](#)

[ASIC \(Application Specific Integrated Circuit\)](#)

[ATH \(All Time High\)](#)

[Address \(Wallet Address\)](#)

[Airdrop](#)

[Altcoin](#)

[Arbitrage](#)

[Audit](#)

[Bag Holder](#)

[Block Confirmation](#)
[Block Height](#)
[Block Reward](#)
[Blockchain](#)
[Bonding Curve](#)
[Bug Bounty](#)
[Bull/Bear Market](#)
[CEX \(Centralized Exchange\)](#)
[Cold Wallet / Cold Storage](#)
[Collateral](#)
[Composability](#)
[Compound Interest](#)
[Consensus](#)
[Contract Address](#)
[DAI](#)
[dApp \(Decentralized Application\)](#)
[DAO \(Decentralized Autonomous Organization\)](#)
[DEX \(Decentralized Exchange\)](#)
[Decentralization](#)
[Deflationary Token](#)
[Degen](#)
[Delegated Proof of Stake](#)
[Deposit](#)
[Derivative](#)
[Digital Signature](#)
[Distributed Ledger](#)
[Double Spend](#)
[EIP \(Ethereum Improvement Proposals\)](#)
[ERC20 Token](#)
[ERC721 Token](#)
[EVM \(Ethereum Virtual Machine\)](#)
[Etherscan](#)
[FOMO](#)
[Fair Launch](#)
[Fiat Currency](#)
[Financial Primitive](#)
[Flash Loan](#)
[Fork \(Hard Fork / Soft Fork\)](#)
[Gas \(Ethereum Gas Fees\)](#)
[Genesis Block](#)
[Gwei](#)
[HODL](#)
[Halving](#)
[Hardware Wallet](#)

[Hash / Hashing](#)
[ICO \(Initial Coin Offering\)](#)
[Immutability](#)
[Impermanent Loss](#)
[KYC \(Know Your Customer\)](#)
[Layer 2](#)
[Leverage](#)
[Liquidation](#)
[Liquidity Mining](#)
[Liquidity Pool](#)
[Liquidity Provider](#)
[LP Tokens \(Liquidity Provider Tokens\)](#)
[Mainnet](#)
[Margin](#)
[Market Cap](#)
[Market Maker](#)
[Maximalist](#)
[Merkle Tree](#)
[Metamask](#)
[Mining](#)
[Multi Signature Wallet \(MultiSig\)](#)
[Node](#)
[NFT \(Non-Fungible Token\)](#)
[Oracle](#)
[P2P \(Peer-To-Peer\)](#)
[Private Key](#)
[Proof of Stake \(PoS\)](#)
[Proof of Work \(PoW\)](#)
[Protocol](#)
[Public Key](#)
[Pump and Dump](#)
[ROI \(Return On Investment\)](#)
[Rebalance](#)
[Rollups](#)
[Shard. Sharding](#)
[Slippage](#)
[Smart Contract](#)
[Solidity](#)
[Stablecoin](#)
[Staking](#)
[Sub-Chain / Side-Chain](#)
[Synthetic Assets \(Synths\)](#)
[Testnet](#)
[Token](#)

[Token Burns](#)
[Tokenomics](#)
[TradFi](#)
[TVL \(Total Value Locked\)](#)
[Validator](#)
[Volatility](#)
[Web 3.0](#)
[Whale](#)
[Yield](#)
[Yield Aggregator](#)
[Yield Farming](#)
[Zero Knowledge Proofs \(ZKP's\)](#)

AML (Anti-Money Laundering)

Regulations applicable in most international markets aimed at preventing criminal activity. Anti-Money Laundering regulations require organizations providing financial services to monitor and report on suspicious activity relating to money laundering. Regulated crypto operators such as exchanges often enforce users to carry out [KYC procedures](#) and provide personal data to meet these requirements.

AMM (Automated Market Maker)

An automated market maker uses a pair of assets in a pool which are deposited by a liquidity provider. A trader can then trade one asset within the pool for the other paying a fee. The price will fluctuate with demand along a liquidity curve. Popular examples of automated market makers are [Uniswap](#), [Sushiswap](#) and [Pancakeswap](#).

API (Application Programming Interface)

An API provides an end point for developers to connect to so they can gain access to data and execute functions programmatically. Exchanges will provide API access and API keys for their users so they can trade programmatically using trading bots and scripts.

APR / APY (Annual Percentage Rate / Yield)

APR represents the annual percentage rate charged or earned for borrowing or lending money. However this doesn't take into account the effect of compounding. If interest is paid

out monthly the lender will earn interest on their interest. This compounding effect is taken into account using the APY calculation but not with APR.

ASIC (Application Specific Integrated Circuit)

An ASIC device is a noisy little box about a foot long that carries out a high powered hashing calculation around 10 trillion times every second. The devices are manufactured specifically for mining cryptocurrency. ASIC mining devices are estimated to consume around 0.5% of the world's energy usage, primarily for mining Bitcoin.



ASIC Bitcoin Mining Hardware

ATH (All Time High)

When a cryptocurrencies price makes a new ATH it means it is more expensive and valuable now than it ever has been in the past.

Address (Wallet Address)

A Bitcoin or Ethereum address is a synonym for a public key. It's the address that you share with someone so they can send funds to your wallet.

Airdrop

When a new project launches a token it is quite common that they create an initial distribution via an airdrop. This provides a set amount of free tokens to anyone that meets

certain requirements. These may be promotional in nature or simply to users who have previously interacted with their services. In September 2020 Uniswap distributed 400 UNI tokens via an airdrop to anyone that had previously used the platform.

A curated list of airdrops: <https://etherscan.io/airdrops>

Altcoin

An altcoin is any cryptocurrency other than Bitcoin. It stands for alternative coin and stems from when Bitcoin completely dominated the markets.

Arbitrage

In crypto markets arbitrage is big business. Networks of bots will scour centralized and decentralized exchanges looking for mispricing between assets. Arbitrage can be as simple as buying an asset on one exchange and hedging the position by selling on another or it can be more complex such as when triangular arbitrage exposes three way price discrepancies.

Audit

A security audit is performed by an external organization on a project's smart contract code. It provides some reassurance but by no means guarantees of the safety of funds within a smart contract. Not all auditors are created equally and an audit by a leading firm such as [Certik](#) carries more weight.

Bag Holder

A bag holder is someone that is holding an asset which they purchased either at an inflated price or at a time when it was more desirable. In pump and dump type schemes the traders who are left with tokens after the price crashes are called bag holders.

Block Confirmation

Exchanges and payment protocols often implement a minimum number of block confirmations to deposit funds. Each time a miner finds a hash and the block is finalized it counts as a block confirmation. So if a transaction requires 3 block confirmations this will be the block that contains your transaction plus two more on top to be completed.

Block Height

Block height is the number of blocks within a blockchain. This is often used as a de facto timing mechanism within smart contracts as developers can estimate the block height at a particular time in the future based on the average block times.

Block Reward

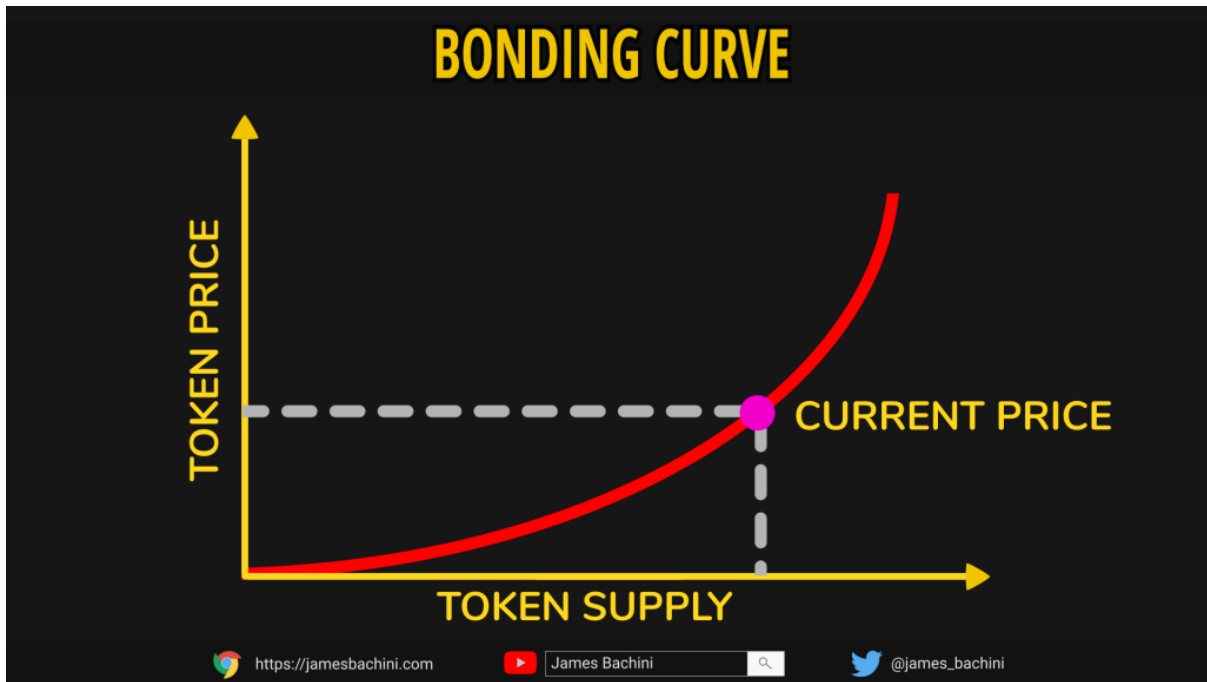
Block reward includes the mining fees and any transaction fees paid to miners when they find a hash which meets the difficulty rating. Each block will carry a reward for helping secure the blockchain which is how many cryptocurrencies distribute the supply of the token.

Blockchain

A blockchain is a chronologically stacked collection of blocks of data interlinked with cryptography. Each block contains a reference to the underlying block so that no middle block can be edited without changing every block on top of it.

Bonding Curve

A mathematical formula or curve used to define a relationship between price and supply of an asset. Bonding curve contracts are used by some projects to increase the price of a token being sold as the supply increases.



Bug Bounty

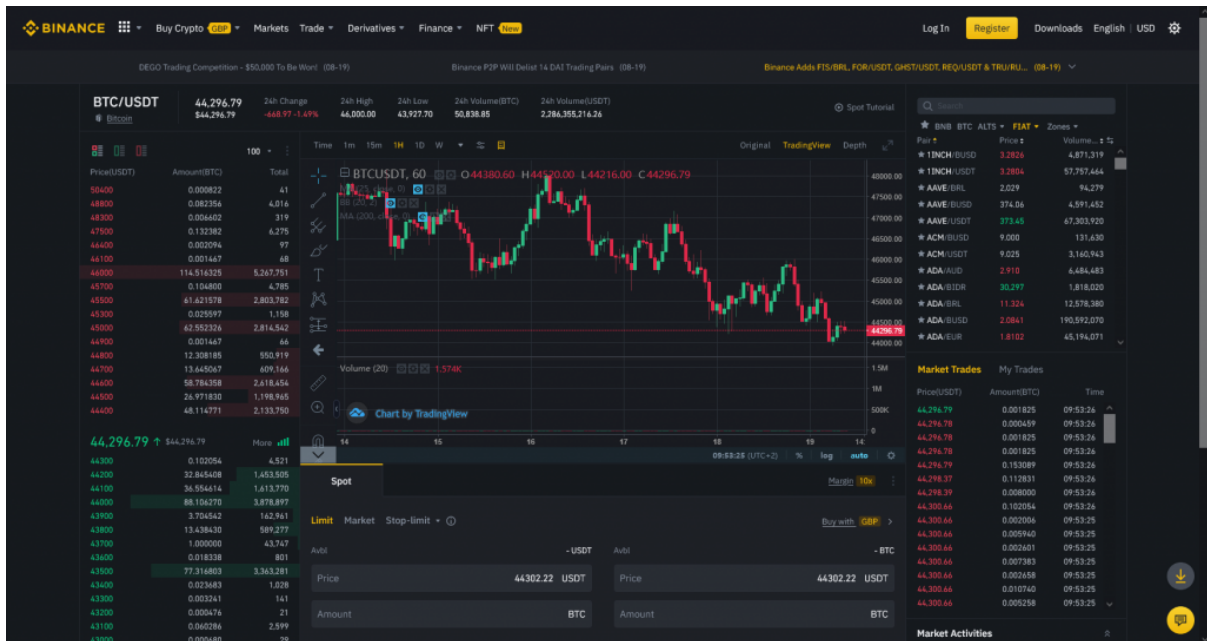
A bug bounty is an offer of payment or reward for finding a security vulnerability in a code base. Bug bounties are often used to incentivise white hat hackers to ethically notify the core development team so they can patch the fault before anyone else becomes aware of the issue. Companies like Hacker One are used as intermediaries between hackers and development teams with top hackers earning in excess of one million USD a year.

Bull/Bear Market

A bull market is used to describe a market that is trending upwards with the price of an asset inflating. A bear market is the opposite when a market is in decline. A trader can be bullish or bearish depending on their current market bias or sentiment.

CEX (Centralized Exchange)

A CEX or centralized exchange is a trading platform like [Binance](#) or [FTX](#) where a central company runs it. These exchanges are usually order book based with a matching engine to connect buyers and sellers.



Cold Wallet / Cold Storage

A cold wallet is a way of storing funds by keeping the private key offline. An example would be when the Winklevoss twins who were early adopters for Bitcoin purchased a laptop, set up a private key/public key pair, divided the private key in to 3 parts, each part was duplicated and then put each of the six parts in a different bank security box across the country. This is an extreme example of keeping keys secure. The main idea is to make it (almost) impossible for hackers to gain access to your keys if they aren't connected in any way to the internet.

Collateral

When taking out a futures position or borrowing funds on a lending platform collateral is used to secure the loan. So a futures platform may give you 20x leverage. This means you need to post \$100 in collateral, which may be USD stablecoins, Bitcoin or some altcoins, and then you can trade with \$2000 positions. Note leveraged trading leads to liquidations which loses the collateral on account.

Composability

In DeFi terms composability is the potential for smart contracts that form the DeFi protocols to interact with each other. A contract might connect to a lending platform to take out a flash

loan and then use those funds to interact with an automated market maker to swap tokens for example.

Compound Interest

When a user invests a sum of money an annual rate of interest will often be quoted. However interest is usually paid out more regularly, sometimes as often as every block. This means that the interest we get paid today will start earning interest itself tomorrow. This interest on our interest is known as compound interest and it is very powerful. Albert Einstein described compound interest as “the eighth wonder of the world”. Note that APR rates don’t include compound interest and APY rates do. If we invest \$100 in a yield farming protocol with an APR of 100% that pays interest daily we end up with \$271.46.

Consensus

A decentralized network of machines acting together as one need to decide on the current state of the network. In blockchain this might be the ability to finalize a block and move forwards with the chain. To do this the network will have code which forms it’s consensus algorithm. Normally more than 50% of the nodes will need to agree for consensus to be reached.

Contract Address

A smart contract address is like the post code of a smart contract on a decentralized network. It maps to the memory address of the executable code on the virtual machine. When we want to interact with a contract we often need the contract address. A common example of this is a token address which describes where to find that token contract.

DAI

DAI is a stablecoin token pegged to the USD. It was launched in late 2017 by [MakerDAO](#) and immediately underwent a stress test as the crypto markets crashed. The token is stabilized through the use of overcollateralized loans, often in the form of Ethereum. It was perhaps the first decentralized finance protocol to gain attention and adoption.

dApp (Decentralized Application)

When we interact with apps we will generally download a binary to our phones or visit a central website. A dApp in contrast to this can be compiled and built from source code on our local machines. They will often use a blockchain to share and manipulate data in a decentralized way. While it's possible to compile a dApp from source more often a user will visit a website which hosts the dApp and interacts with it from there.

DAO (Decentralized Autonomous Organization)

DAO's provide the governance mechanism for many DeFi protocols. It is based on a voting mechanism where proposals are submitted and then voted on by holders of governance tokens. Votes that get passed change the course or parameters of the protocol.

DEX (Decentralized Exchange)

Decentralized exchanges include order book based exchanges like IDEX and automated market makers like Uniswap. An orderbook exchange will list bids and ask prices and users will be able to place orders into the book which are filled by a matching engine. An automated market maker uses a liquidity pool of two assets which can then be traded against the pool along a price curve.

Decentralization

The entire blockchain sector is built around the concept of decentralization. This means that a network has no central point of failure and is instead built around equal peers. Decentralization is not a binary concept and networks can become more or less decentralized over time.

Deflationary Token

A deflationary token is an asset where the circulating supply reduces over time. It becomes more rare often through a burning process where tokens are sent to an address which no one has access to.

Degen

Short for degenerate which in DeFi terms can be used both as an insult and a compliment at the same time. It is usually assigned to a trader, yield farmer or NFT collector who takes on high risk strategies. Someone who trades meme coins with their life savings on leverage would be considered a degen.

Delegated Proof of Stake

DPoS is a consensus algorithm where stakers can allocate their voting capacity to 3rd party nodes on the network. It removes the need for stakers to run nodes themselves as they can simply vote through a node operator providing trust in that party acting in their interest to secure the blockchain.

Deposit

When we send funds to a new platform we are depositing funds. Centralized exchanges will often provide deposit addresses where you can “load up” your account.

Derivative

A derivative is a financial instrument that is used to gain exposure to an underlying asset. In crypto the most popular example is that of perpetual futures contracts. Quarterly futures and options contracts are other forms of derivatives. In crypto markets derivatives are traded at greater volumes than the underlying spot markets. This means there is more buying and selling of Bitcoin futures than there is of actual Bitcoin.

Digital Signature

Transactions need to be signed before they are sent to the nodes that form the blockchain network. This is achieved via a private key, public key pair and is usually done in the background via a digital wallet such as metamask. The transaction data will be hashed and then signed using the private key and elliptic curve cryptography. This will then be sent to nodes along with the public key to prove the sender approves the transaction. The nodes have a cryptographic function to check if the signature matches the public key for the account.

Distributed Ledger

A decentralized network can hold a list of funds pertaining to who owns what. This distributed ledger provides a way to store and transfer assets without 3rd party approval.

Double Spend

Bitcoin's initial breakthrough was to solve the double spend problem which ensures a user on a decentralized network can't send their coins to different addresses on different peers. The consensus mechanism ensures that only one block will move forwards and that can only include a single spend of the tokens.

EIP (Ethereum Improvement Proposals)

When Ethereum goes through an upgrade it's initially put forward as an EIP. These are then quoted when the changes are put into place. EIP-1559 for example gained attention in 2021 because it redirected transaction fees from miners to a burn address reducing the distribution of new tokens.

ERC20 Token

The majority of crypto tokens use an ERC20 token contract. Anything that is traded on Uniswap or Sushiswap is ERC20 or a variation built on top of it. The ERC20 token contains functions to create, transfer, approve spend and check balances.

Open Zeppelin ERC20 Token Template:

<https://github.com/OpenZeppelin/openzeppelin-contracts/tree/master/contracts/token/ERC20>

ERC721 Token

The ERC721 token is the industry standard token used for NFT's. It contains many of the standard ERC20 token functions alongside additional functions to declare and modify ownership and store metadata. Metadata contains the data which the NFT represents; it is often a hash of the data rather than the data itself.

Open Zeppelin ERC721 Token Template:

<https://github.com/OpenZeppelin/openzeppelin-contracts/tree/master/contracts/token/ERC721>

EVM (Ethereum Virtual Machine)

A virtual machine is like a version of windows running in a window on your laptop. Think of it as an operating system running as an application on top of the main operating system.

Ethereum's virtual machine is designed to run across a network of nodes that agree on the persistent state of data on the network. It's not just Ethereum that uses EVM, it's also used by alternate chains like Binance smart chain, Polygon and HECO.

Etherscan

A block explorer provides a user interface for anyone to search for transactions, user accounts and blocks on a blockchain network. Etherscan is Ethereum's block explorer and is a pillar of the industry. When a user sends a transaction they'll often be quoted a confirmation tx address which can be copy and pasted into etherscan to see the details of that transaction.

<https://etherscan.io/>

FOMO

FOMO stands for fear of missing out. It's the feeling you get when you work in the industry only to find out your Uber driver has outperformed your portfolio because he invested in a meme token that went viral on TikTok. Fomo can lead us to invest at the worst possible time when markets are toppy and due for a correction.

Fair Launch

The concept of a fair launch token was popularized by Yearn Finance when they released their governance token without any team allocation or VC interest. They simply gave it away to the people that were using the protocol. This created a strong community which benefits the project to this day.

Fiat Currency

Government backed currencies such as the US dollar and Euro are known as fiat currencies. The issuance of new supply is often obfuscated through borrowing mechanisms, fractional reserve banking and quantitative easing. Inflation inevitably eats away at the real value of fiat currencies over time.

Financial Primitive

Simple financial products such as loans and insurance can be classed as financial primitives. They are the fundamental financial services that a protocol may provide. In a DeFi sense, financial primitives are often used to describe the complete ecosystem around which a token's economics is built.

Flash Loan

The concept of a flash loan is quite abstract in that it lets a user borrow millions of dollars with no collateral but only for a few seconds. A flash loan must be paid back in the same block that it is borrowed or the transaction will fail. It's best explained through an example. A user will take out a flash loan for a stablecoin and then use these funds to swap for token A, in the same block they will swap token A for token B and then token B back to stablecoins. If the triangular arbitrage trade resulted in more stablecoins being received they will pay back the loan in the same block and profit the remaining funds. Flash loans have also been used to carry out flash loan attacks which give hackers access to huge amounts of capital to manipulate prices on liquidity pools.

Fork (Hard Fork / Soft Fork)

The blockchain sector prides itself in being transparent which includes the vast majority of code being open source. This means that it can be forked, copying existing code to our own project and then modifying it from there. When major changes are pushed out a subset of the nodes may not accept them continuing with alternate or pre-existing code. This division of nodes is known as a hard fork. An example of this took place on Bitcoin where Bitcoin Cash split off due to a debate over block sizes.

Gas (Ethereum Gas Fees)

When we place a transaction on the Ethereum network we have to pay a transaction fee known as a gas fee. The fee varies widely depending on network congestion and usage. At times of peak demand it can cost in excess of \$100 to make a simple token swap.

You can check the latest gas fees at: <https://ethgasstation.info>

Genesis Block

The first block on a blockchain is known as the genesis block. Bitcoin's genesis block famously included an encoded message saying "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Gwei

Ethereum's native token Ether (ETH) can be broken down into one billionth denominations known as Gwei. These are used more in development than on user interfaces. Think of it like cents to dollars. 1 ether = 1,000,000,000 gwei.

HODL

In December 2013 BitcoinTalk forum user GameKyuubi posted a somewhat intoxicated message declaring "I AM HODLING". Having misspelled holding the post led to the term sticking and is now widely used within the community. It simply means to hold on to an asset through the ups and downs. Often quoted as hold on for dear life.

Original post: <https://bitcointalk.org/index.php?topic=375643.0>

Halving

Halving or halvening events occur when a tokens distribution of new supply to miners is cut in half. This occurs approximately once every four years on the Bitcoin network with the next halving due in 2024.

List of cryptocurrency halving events: <https://halvingdates.com>

Hardware Wallet

A hardware wallet is a small USB type device that stores private keys and the funds associated with them in a secure manner. It can often be disconnected completely from the internet making it more difficult for hackers to gain access.

Hash / Hashing

A hash is a code which represents some data. If we imagine all data can be broken down into binary ones and zeros. A hashing algorithm can be used to calculate a value of that data. The algorithm is one way meaning you can calculate the hash from the data multiple times but can not calculate the data from the hash. If just one byte of the data changes the hash will change completely. The most common hashing algorithm is known as SHA256, a 256-bit (32 bytes) hash usually printed out as a hexadecimal number of 64 digits.

ICO (Initial Coin Offering)

New projects launching a token will often offer that token in exchange for funds to bootstrap their project. There was an ICO boom towards the end of 2017 which slowly evolved to IDO's (Initial dex offerings) and IEO's (initial exchange offerings).

Immutability

Blockchains are immutable because no one is able to change the existing data. Blocks are interlinked and stacked on top of each other with each new block containing a hash of the underlying block. Changing a block from 3 days ago would mean every block since would need to be recalculated and rewritten.

Impermanent Loss

When a liquidity provider deposits funds to an automated market maker they receive fees in exchange for accepting the risk of impermanent loss. If one asset goes up in price and the other goes down the pool will fill up with the lower value asset. The liquidity provider is always on the bad end of price action. If the price returns back to the base level such as often is the case with stablecoins, no impermanent loss will be suffered however if the price move is permanent so is the loss.

KYC (Know Your Customer)

KYC regulations require financial organizations to collect personal and organizational data on their customers and report any suspicious activity. It is used to prevent money laundering and is a requirement of any regulated financial institution. Users will often have to complete KYC steps when signing up to a new exchange to lift withdrawal limits and features.

Layer 2

L2's are sub-chains that form consensus based on smart contracts which live on the layer 1 main chain. Optimistic rollups are an example of layer 2 scaling solutions which promise faster, cheaper transactions with the benefit of layer 1 security.

Leverage

When a trader makes a trade with leverage they are effectively borrowing money to place that trade. If the trade goes against them they risk being liquidated if the loss comes close to exceeding their collateral position. For example a user can deposit \$10 to an exchange, purchase a Bitcoin futures position worth \$200 with 20x leverage but if the price of Bitcoin drops close to 5% they risk getting liquidated and losing their deposit.

Liquidation

When using leverage it's important for the protocol or exchange to prevent losses exceeding the collateral posted. For this reason a liquidation engine will sell positions to recap funds automatically if a margin requirement is not met. Liquidation engines work differently across the industry but many market sell assets which can cause liquidation cascades and highly volatile price action.

Liquidity Mining

Protocols often require funds to operate. For example a lending and borrowing platform needs a float and lenders before they can start lending. DeFi protocols will often bootstrap initial funding through liquidity mining. This is the incentivisation to get users to deposit funds

to the platform. This may take the form of distributing governance tokens to early adopters or providing high APY returns for staking LP tokens for the ETH/Native pair providing a liquid market for the governance token.

Liquidity Pool

A liquidity pool usually contains a pair of assets which can be swapped. For example a Uniswap liquidity pool might have ETH as the base asset and an ERC20 Token as the traded asset. Price is calculated along a curve dependent on the quantity of assets in the pool. If someone starts buying the ERC20 token with ETH it pushes the price up as more ETH is added and the ERC20 tokens are removed from the pool.

Liquidity Provider

A liquidity provider will usually provide a pair of assets such as ETH and ERC20 tokens in equal weighting to a liquidity pool. They will earn fees whenever someone trades in that liquidity pool. When providing liquidity they will receive LP tokens in return (see below).

LP Tokens (Liquidity Provider Tokens)

LP tokens act like a receipt for the funds deposited and they will automatically be sent to the same address that deposited the funds. LP tokens can be transferred and can often be staked on DeFi platforms in return for staking rewards.

Mainnet

A trade made on margin is executed using borrowed money. A percentage of the total trade value is kept on account as collateral to cover potential losses. If losses exceed collateral a liquidation event will occur and the trader will lose the collateral posted.

Margin

A trade made on margin is executed using borrowed money. A percentage of the total trade value is kept on account as collateral to cover potential losses. If losses exceed collateral a liquidation event will occur and the trader will lose the collateral posted.

Market Cap

The market cap or capitalization of a cryptocurrency is calculated by multiplying the circulating supply by the token price. This is usually a debatable issue with leading websites not including vested tokens and treasury wallets in the circulating supply.

Market Maker

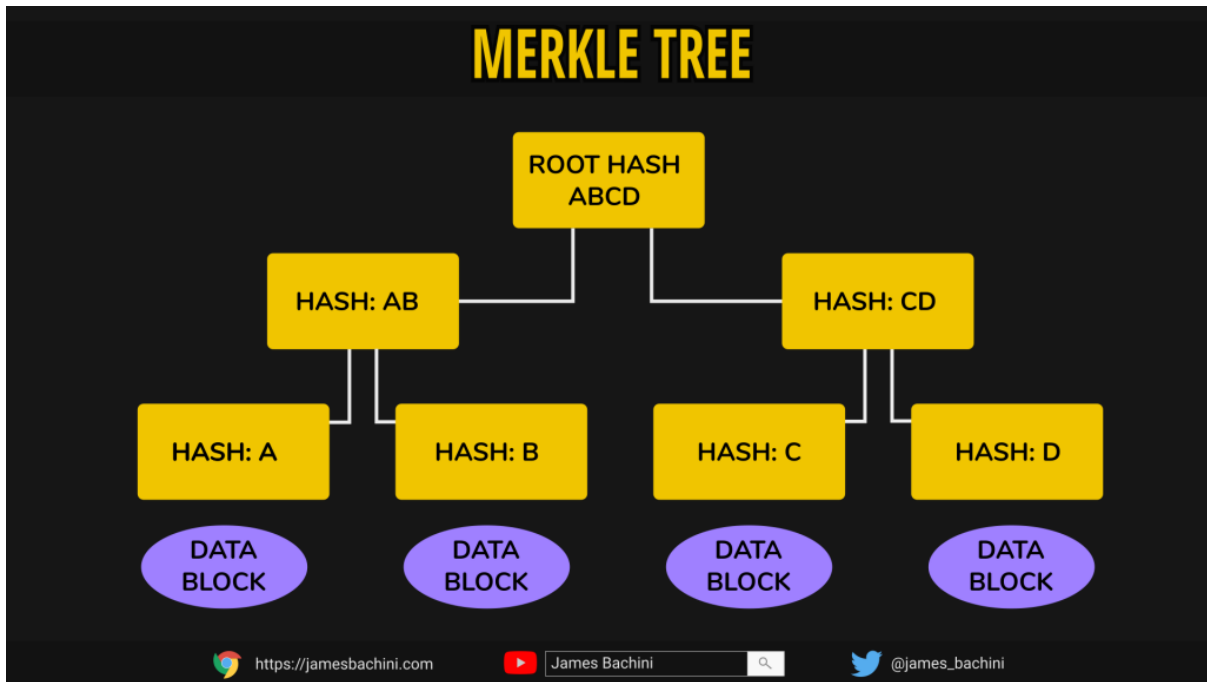
A market maker will provide liquidity to an order book on a traditional exchange. They will often place both bid and ask to buy and sell the same asset at a varying spread away from the current market price.

Maximalist

Maximalism is a mindset in which someone feels that a single coin or token holds value above everything else. Bitcoin maximalism arose towards the end of 2017 with maxi's declaring everything else in the sector worthless. More recently we've seen more Ethereum maximalism where proponents believe that alternate chains are meaningless.

Merkle Tree

Merkle trees are a data structure where hashes are used for verification. A root hash can be used to verify underlying blocks of data provided across an untrusted peer to peer network. It's possible to verify each block of data contains the commitment from the root hash.



Metamask

The most popular digital wallet for Ethereum and EVM compatible chains is Metamask. It can be installed as a browser plugin or via a mobile app. Metamask can be used to set up and manage accounts, transfer funds between accounts and interact with web3 applications.

Mining

In the sense of proof of work consensus mining involves hashing a block of data over and over again each time changing a random variable to get a different hash. If a hash meets a set difficulty level the miner will finalize the block and the chain moves forward. Mining is generally carried out on high powered ASIC devices. The industry has been criticized for excessive electrical usage.

Multi Signature Wallet (MultiSig)

A multisignature wallet or multisig is a digital wallet that requires multiple signatures to transfer funds. For example a Gnosis multisig wallet might be set up by a team who want to secure their treasury funds. There might be 5 team members who are signatories on the account and it may be set to require at least 3 signatures for a transaction. Each user will be given a private key/public key pair via a digital wallet like metamask. They can then propose

and sign any transactions to transfer funds which won't go through until 3 team members have signed off on the transaction. Multisig wallets are used to mitigate the risk of theft, lost keys and hacked funds.

Node

A node is a computer operating on a distributed [peer to peer network](#). Each node will connect to multiple other peers to share information and data across the network. Not to be confused with Node.js which is a Javascript runtime and development tool.

NFT (Non-Fungible Token)

Non fungible tokens are one offs. Whereas one bitcoin is worth the same amount as any other one bitcoin, a NFT is unique and is only worth what someone is willing to pay for it. NFT's are used to digitally represent art, digital assets and liquidity receipts.

Oracle

Smart contracts can not connect to external data sources such as API's. For this reason to get information into a contract it must be provided by a service such as an oracle. Oracles can provide any type of data but in DeFi it is usually price data from centralized exchanges. This is useful for developers to prevent the risk of price manipulation on-chain.

P2P (Peer-To-Peer)

A peer-to-peer network is a collection of computers all talking to each other in a group. There is no central server or data provider and data is communicated by whispers between the peers.



Private Key

A private key is a set of one's and zero's often represented in hexadecimal alphanumeric format. It acts as the primary data input for account creation in cryptocurrency because the public key is derived from the private key. Private keys, as the name suggests, should be kept private as anyone who has access can sign transactions and take any funds in the account.

Proof of Stake (PoS)

In a proof of stake network token holders vote on the finalization of blocks. It is assumed that token holders will be most financially incentivised to secure the blockchain. The network will find consensus by the block which has the most votes in terms of staked tokens. In practice slashing mechanisms and limits are put in place to further prevent malpractice between stakers.

Proof of Work (PoW)

In a proof of work consensus mechanism a block is hashed repeatedly until a hash is found to match a set difficulty. Hashing is carried out on specialized hardware known as ASIC devices. Proof of work is often criticized for its excessive electrical consumption but complemented for its extreme decentralization.

Protocol

A protocol is used to describe a smart contract or collection of smart contracts which provide a service in decentralized finance. The frontend of the service is referred to as the platform while the backend is described as the protocol although these terms are often used interchangeably.

Public Key

A public key is the same as your address. On Ethereum it will start with 0x... to show it's a hexadecimal address. The public key is derived from an accounts private key however it is not possible to find the private key from a public key. When we want a user to send us funds we will share our public key and they will send funds to that address.

Pump and Dump

A pump and dump scheme is an ethically questionable trading method where a token is bought up and then announced to a trading group. As traders pile in it pushes the price up to a point where it's unsustainable. The token price then dumps as there's a rush to the exits and as everyone tries to cash out. Anyone left with tokens at the end is considered a bag holder.

ROI (Return On Investment)

When an investor commits funds to a financial instrument they expect a return on that investment in the form of capital appreciation. ROI is a measure of that return, it can be calculated via the formula: $(\text{final value of investment} - \text{initial investment}) / \text{total cost of investment including fees} \times 100\%$

Rebalance

When allocating assets to a diversified portfolio the individual assets will move away from their target allocations as prices fluctuate. Rebalancing is the process of selling a partial amount of any assets that have gone up in price and buying any that have gone down in price. This rebalances the portfolio back to the target allocations. It can be used to somewhat automate the process of buying low and selling high.

Rollups

Roll ups are a form of layer two scaling solution. Transactions are rolled up in an amalgamation process and stored in an inbox within a layer 1 smart contract. The transactions are processed via external nodes on layer 2 taking a lot of the execution and computational work away, then state is updated and sent back to layer 1. A dispute mechanism is used to prevent misuse between validator nodes on layer 2.

Shard, Sharding

A shard is a subset of data and sharding is used by data management software to break down large data sets into more manageable packages. By the end of 2021 the ethereum blockchain will be over 1TB in size and transferring this data across a decentralized network potentially could become more difficult. Sharding will enable nodes to work with a subset of the entire blockchain which will ease the computational burden of past transactions.

Slippage

The price movement caused by an order is called slippage. When an asset is traded on exchange the quoted price is often the midpoint between the leading bid and leading ask price. However when a market order is placed it can take out more than just the leading price eating into the order book and removing liquidity.

Smart Contract

Code compiled to run on a blockchain network such as Ethereum are known as smart contracts. They are essentially just programs written in a text editor, much like any other coding language. Smart contract code is deployed to the network via a process known as migration.

Solidity

The main coding language used to create smart contracts on the Ethereum network is called Solidity. It's a statically typed language designed around the Javascript syntax making it familiar for web developers.

Stablecoin

A token that is pegged to an underlying asset such as the US Dollar is known as a stablecoin. Stablecoins are very important in DeFi because they can be used to provide collateral in a less volatile asset. Different stablecoins have various mechanisms in place to follow their base asset however there is no guarantee and it's possible for stablecoin tokens to decouple from their peg.

Staking

DeFi protocols will often incentivise funding and liquidity providers by distributing a governance token to staked funds. A user can either use the protocol or purchase the governance token on exchange and use this to stake and earn further funds.

Sub-Chain / Side-Chain

Ethereum is open source code which means it can be forked and changed by anyone who understands how it works. Sub-chains like Polygon are modified copies of the Ethereum code that run a separate chain in parallel. Some protocols will deploy smart contracts across multiple side-chains.

Synthetic Assets (Synths)

Synthetic assets are a derivative product which aims to track an underlying asset. A user can trade stocks, index funds, commodities and cryptocurrencies using synthetic assets. They are backed by a liquidity pool which acts as a balancing and funding mechanism for the protocol. If all the synthetic assets go up at the same time then the liquidity pool diminishes in value. In practice the diversified nature of the assets works well to keep things in balance.

Testnet

A testnet is a playground for developers and end users to try out things with valueless funds. A developer can get free testnet ETH from a faucet and use this to deploy their smart contracts. A user can use their free ETH to try out new DeFi platforms and experiment with the latest innovations without risking any funds.

Token

A token is built on a smart contract that stores ledger of who owns what. The majority of cryptocurrencies are built on the ERC20 token standard. Tokens often include functions for minting, transfer between accounts, approving spend by 3rd parties or contracts and checking balances of accounts.

Token Burns

Sometimes token contracts include a burn function otherwise it is sufficient to send funds to the 0x00 address which no one has a private key for... unfortunately as it contains over \$1.5B in tokens.

Tokenomics

For a token to go up in value the demand must outweigh the supply on exchange. The economics of the token ecosystem are known as tokenomics. There are various methods to try and increase demand and reduce supply such as staking, fee burning and holder benefits.

TradFi

TradFi refers to traditional finance. The institutions of Wall Street and the square mile in London would be considered TradFi.

TVL (Total Value Locked)

Smart contracts can contain funds locked within the contract itself. A good example of this is the liquidity pools on automated market makers like Uniswap. The smart contract address

owns the funds until a user redeems them. The total value locked within a smart contract or protocol is often expressed in USD terms.

A list of DeFi projects ranked by TVL: <https://defipulse.com>

Validator

A user can stake their tokens on a proof of stake network and run a node to actively participate in the validation of the blockchain. Validator nodes connect to the peer-to-peer network to process transactions and blocks.

Volatility

Many cryptocurrency assets are described as being highly volatile. This means that the price can swing wildly in both directions. Bitcoin often has 50%+ drawdowns and altcoins are even more volatile. In 2018 many tokens lost 95%+ of their USD value causing disruption throughout the industry.

Web 3.0

The first version of the web was a publishing platform built on the idea of print media. Website publishers would produce content for consumers to read. Web 2.0 was the revolutionary rise of social networks where users themselves create the content. Web 3.0 is the decentralization of content and social networks. The concept promises social networks with no single point of control where no entity can sell your personal data.

Whale

A crypto whale is an affectionate term used to describe someone that has a very large holding in cryptocurrency. These are generally early adopters, crypto funds and high net worth individuals.

Yield

The return on investment we can get from staking or lending can be described as yield. This is usually provided by a platform as an APR figure or APY figure (includes compound interest).

Yield Aggregator

A yield aggregator will automate some of the yield farming process by claiming staking rewards and then restaking to compound the returns.

Yield Farming

Yield farmers operate a cat and mouse game of looking for new protocols to get in early on and start earning the best rewards. Often yield farmers will only participate in a single farm for a period of a few days or weeks before switching to the next project that wants to bootstrap liquidity and is offering incentives to do so.

Zero Knowledge Proofs (ZKP's)

Zero knowledge proofs use cryptographic methods to verify data without sharing the actual data. In cryptocurrency ZKP's can be used to validate a transaction without revealing whose wallet was used to send the funds. This adds the potential for a privacy aspect to an otherwise transparent blockchain system.