

# MASTERING DEFI



THE ULTIMATE BEGINNER'S GUIDE TO  
DECENTRALIZED FINANCE

# Index

[Index](#)

[Introduction](#)

[Quick Glossary](#)

[What is DeFi?](#)

[How does DeFi work?](#)

[Blockchain](#)

[Ethereum & Smart Contracts](#)

[The DeFi Ecosystem: Use Cases](#)

[Decentralized exchanges \(trading\)](#)

[Lending](#)

[Derivatives](#)

[Yield Farming](#)

[Insurance](#)

[Stablecoins](#)

[Governance](#)

[How governance works in practice](#)

[The Future of DeFi](#)

# Introduction

DeFi has grown at an unprecedented rate. In fact, the speed at which new concepts and innovations arrive is so dramatic that veterans and beginners alike fail with keeping up and understanding its ever-growing importance. As with any other subject, information overload is very likely unless we approach the right data in a structured, intuitive, and progressive way.

Mastering DeFi is a book written for beginners who are familiar with basic blockchain and crypto concepts but have not yet dared to tread into the world of decentralized finance. This book carefully explains every facet of DeFi, while placing a major emphasis on its use cases, features, and platforms.

While we initially provide you with an abstract understanding of DeFi's significance in not only the blockchain industry but in the real world as well, a major portion of the book revolves around comprehending specific and popular use cases as a way of gaining understanding decentralized finance through practical knowledge. By covering decentralized exchanges, yield farming, lending, derivatives, stablecoins, insurance, and other topics, the reader becomes capable of knowing how DeFi works at the level of an experienced user.

Before venturing further, we recommend our readers to glance through the quick glossary and explore fundamental DeFi words and concepts. Although crypto is known for its slang, there are indeed technical terms which must be understood before exploring a sector as complex as decentralized finance.

We would also like to note that the first edition of Mastering DeFi was written in April 2021 and that some of the information presented here might change with time. Most of the fundamental concepts will likely remain the same while various data points of financial nature will change.

## Quick Glossary

### **Audit**

Refers to a project's code being reviewed for soundness by a party outside of the organization. Typically, a DeFi protocol project will have a professional third party evaluate the code for feedback on weak points, allowing them to implement patches (if necessary) before going public.

### **APY**

Short for Annual Percentage Yield, APY is one of the most important concepts in DeFi. It refers to the return on investment you can expect from an asset in a one-year period. APY rates tend to fluctuate wildly in DeFi; therefore, they are best used as approximate measures.

### **AMM**

Automated Market Maker is a smart contract that holds liquidity reserves in the form of crypto assets. Users interact with the AMM when offering liquidity or trading cryptocurrencies. Essentially, an AMM is an alternative used in DeFi markets that removes the need for order books, which are traditionally employed by centralized exchanges.

### **CeFi**

Centralized finance, commonly used as a reference to projects like Celsius, Nexo, and BlockFi that operate like normal centralized organizations within the DeFi space.

### **TradFi**

Refers to traditional finance or centralized finance institutions like banks and other legacy institutions.

### **CEX**

Short for centralized exchange. CEXs include Coinbase, Binance, Huobi, Gemini, and Kraken.

### **DEX**

Short for decentralized exchange. DEXs include Uniswap, Curve, SushiSwap, 1inch Exchange, Synthetix, and Balancer.

### **Collateral**

Assets deposited and used to back a loan. Depositing collateral on crypto lending platforms like Compound and Aave is typically done to stake and receive APY while simultaneously borrowing more crypto.

### **Derivatives**

Financial products deriving their value from an underlying asset are known as derivatives.

**ERC-20**

Ethereum-standard cryptocurrency assets are built and issued using the ERC-20 protocol. Any cryptocurrency token issued on Ethereum is an ERC-20 by design.

**Flash loan**

A flash loan is an instant cryptocurrency loan that does not require collateral, KYC checks, or any other form of upfront investment from the borrower.

**Governance & governance tokens**

Governance refers to the maintenance, enforcement, and regulation of a decentralized protocol by token holders. Usually, when a DeFi protocol is released, it does so with a native asset which is used to participate in the decision-making process.

**Impermanent loss**

Impermanent loss refers to the loss of assets deposited while yield farming during extreme price swings.

**KYC**

Know Your Customer (KYC) is a basic identity check required by centralized financial institutions.

**Liquidity**

The amount of circulating supply for a given token paired with trading volume, exchange availability, and other trade factors determine how liquid or illiquid a token is.

**Liquidity pool**

Liquidity pools are smart contracts that hold onto a protocol's liquidity and distribute them to users.

**Liquidity provider**

DeFi participants who deposit their tokens into liquidity pools.

**LP token**

When a liquidity provider deposits tokens into a liquidity pool, their stake is represented by a minted LP token. The LP token represents the staked asset(s) and can yield farm other DeFi platforms or be exchanged back for the original assets.

**Decentralized Oracle**

Decentralized oracles provide both on and off-chain price data to blockchains / DeFi protocols.

**Slippage**

Slippage refers to the gap in price that exists between what you're willing to pay for an asset and the seller's best price.

**Smart Contract**

A blockchain-based, lightweight, programmable structure of code that executes functions as determined by the author. In practice, smart contracts run like autonomous programs that replace intermediaries and guarantee outcomes.

**Stablecoin**

Tokens with value backed by underlying assets or pegged to the value of another asset - usually a fiat currency like the U.S. dollar.

**Synthetics (synths)**

Synthetics are blockchain-based derivative trading products representative of other assets.

**Yield**

Yield is the amount earned by depositing or staking an asset in a DeFi platform.

**Yield farming**

Yield farming is the act of depositing, or staking, tokens, across DeFi platforms offering rewards for liquidity providers. Farming your tokens enables you to generate additional value from your assets by having them work for you.

# What is DeFi?

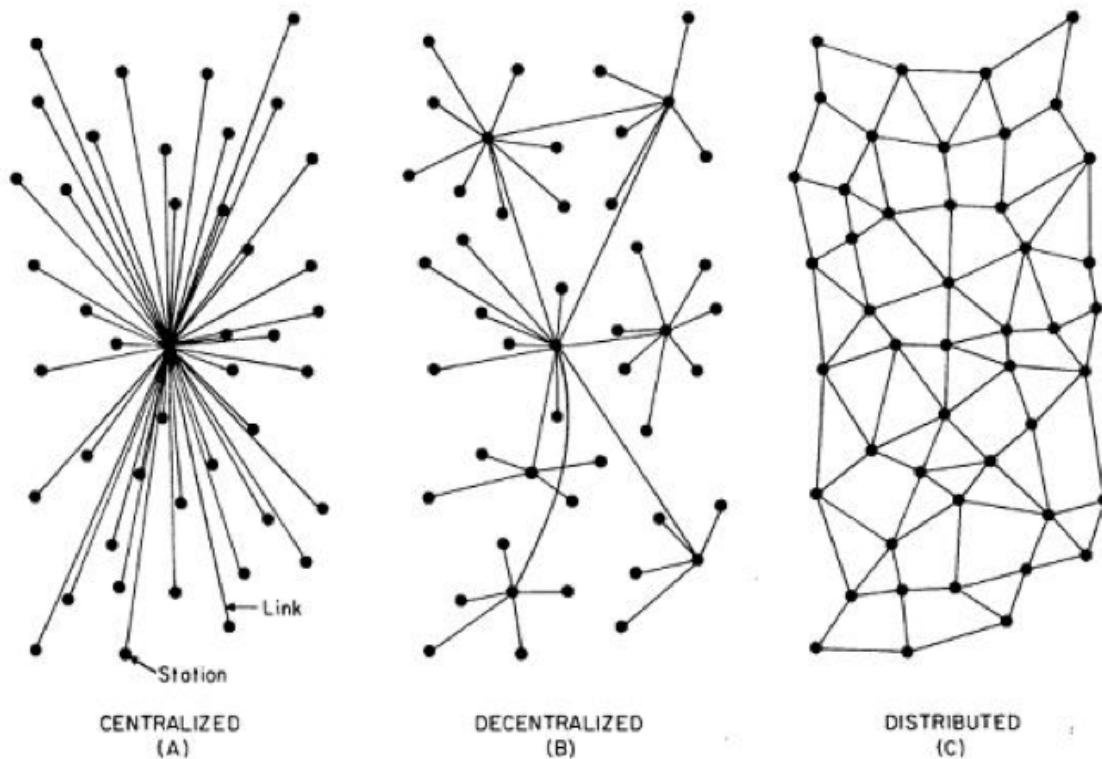
Decentralized Finance (DeFi) is a loose concept used to describe an ecosystem within the blockchain industry that offers traditional financial services and products in a decentralized way.

Worth \$54 billion at the time of writing, the fastest growing crypto segment covers anything from loans and insurance to peer-to-peer payment networks, banking, and derivatives. Investors can access not only everything that financial institutions provide but also those products which can only be found in a revolutionary sector like DeFi.

The core idea behind decentralized finance is to provide both the banked and unbanked the opportunity to participate in a transparent, public, and permissionless financial network that requires no intermediaries. We can define DeFi with the help of its three fundamental principles.

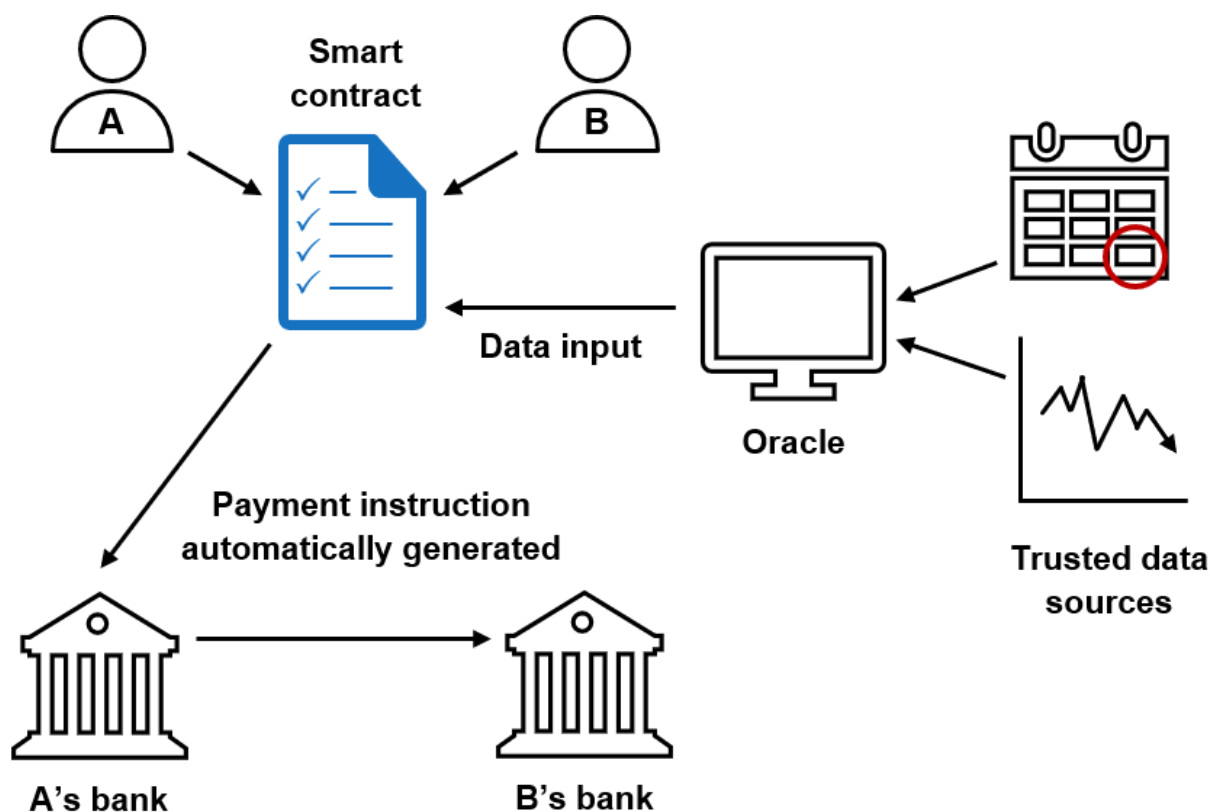
## 1. Decentralization

Decentralization plays an important role in DeFi. It distributes privileges and abilities often held by small central groups to the entire system. In this case, the decision-making process is handed over to a project's community rather than its developers, and there is no person who has more rights compared to someone else.



[Source](#)

To ensure real decentralization, blockchain developers rely on the use of smart contracts, which help by setting up rules and bringing automation. Since these smart contracts are open-source and contain lines of code that follow preimposed logic, it is impossible to 'cheat the system' and attain power over the network without anyone finding out. In the worst case, a developer will be ostracized after the community discovers the malicious flaws and refuse to join the network.



[Source](#)

DeFi is so ridiculously decentralized that developers are not forced to actively interact with a protocol for users to successfully utilize its services. Prices are now determined by decentralized price feeds called oracles, users retain personal custody over their assets, liquidations are initiated by smart contracts, etc.

Simply put, every component in DeFi is decentralized. This is a massive jump not only compared to traditional finance but to first-generation blockchain applications as well.

## 2. Transparency

Transparency became more important than ever after 2008. The economic crisis at the time brought on the realization that most major institutions are corrupted to the core and that they will use the system to suit their needs whenever the opportunity arises.

The fall and bailouts of major banks led to transparency becoming the only significant merit that financial systems should possess, and in DeFi, there is more of it than anyone can imagine.



Built on decentralized public blockchain networks like Ethereum and PolkaDot, DeFi projects are open-source and have their entire design on display. If requested, blockchain security companies will even audit a project in order to determine whether it has any exploits or security flaws.

With such a high level of transparency, it is almost impossible to be duped and make a decision or action to which you have not consciously agreed to.

### **3. Accessibility**

Accessibility is, for most of human history, more of a limitation than a quality. Before vast technological innovations, we only had access to what physically surrounds us at any point of any given time.

A person born before the internet was invented only had access to social circles in his near vicinity. Distance alone would determine the spectrum, condition, and the number of relationships. With the launch of social media platforms such as Facebook, Twitter, and MySpace, we have gained the chance to exponentially expand our circles via a global and interconnected digital network.

Finance has progressed in a similar way, and decentralized finance represents the latest evolutionary jump. Internet banking might have made it possible for anyone to access their bank account from the comfort of their home, but DeFi succeeded in offering financial services and products for those with absolutely no access to banks.

An internet connection and mobile phone is all that people need in order to make payments and take out loans. Considering that there are currently 1.7 billion unbanked individuals, having access to DeFi is more than a blessing.

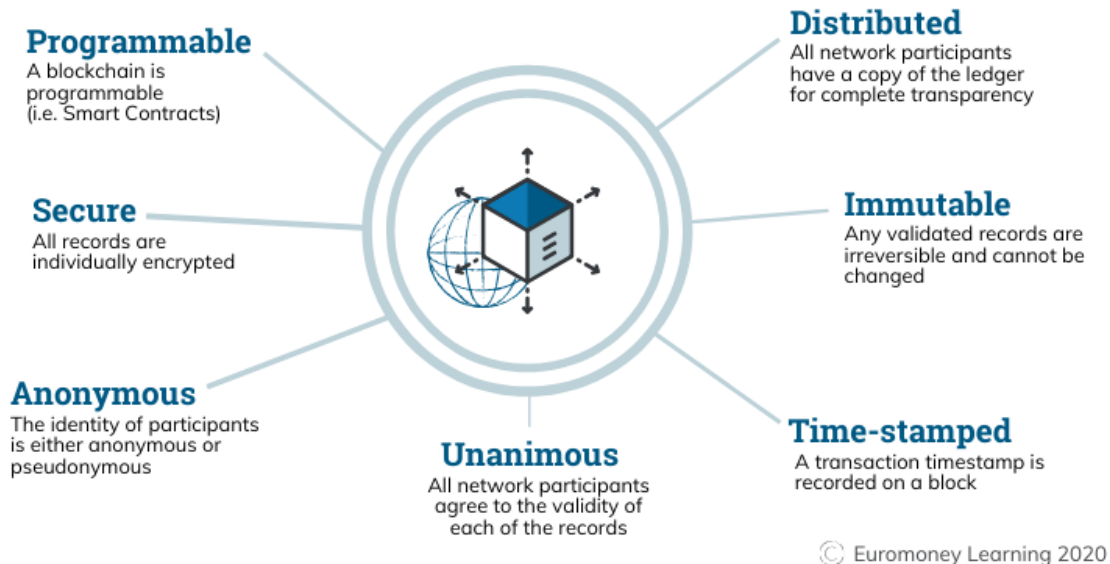
## **How does DeFi work?**

From a technical perspective, DeFi is a group of decentralized applications (dApps) primarily running on the Ethereum smart contract ecosystem that provides blockchain-based financial services without intermediaries. Therefore, understanding how DeFi works requires knowledge pertaining to three important topics: blockchain technology, Ethereum, and smart contracts.

### **Blockchain**

Blockchain technology is the foundation for not only DeFi but everything related to cryptocurrencies as well. In short, blockchains are digital ledgers that permanently record immutable data made out of blocks that are publicly shared with everyone.

# The Properties of Distributed Ledger Technology (DLT)



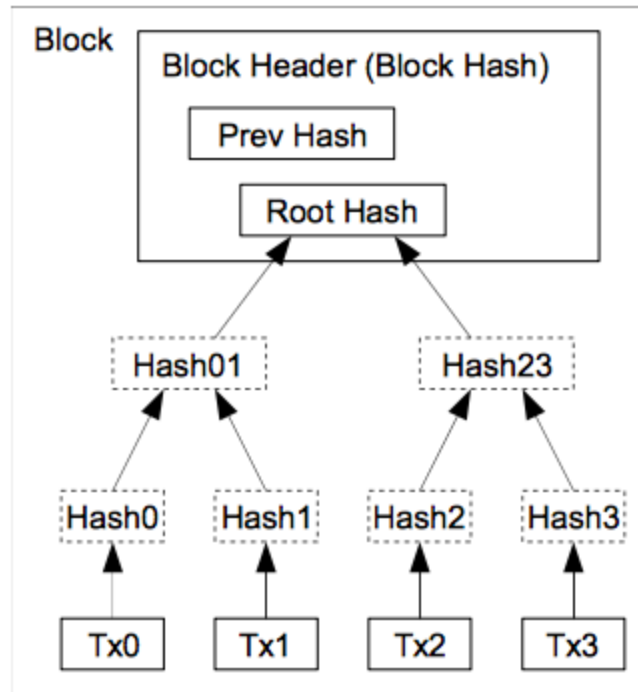
The main features of blockchain networks. [Source](#)

Bitcoin is the first blockchain network, launched in 2009, and it is a revolutionary concept for two major reasons: security and scarcity.

## Security

To process transactions, blockchain networks like Bitcoin use the Proof of Work (PoW) consensus model. PoW involves users called miners who use electricity and hardware power to solve complex mathematical problems in return for rewards, which are gained for confirming blocks.

A block is a group of signed transactions added by regular users who wish to move their coins. Each transaction contains a hash that proves its chronological order on the ledger. Consequently, all blocks have their hashes as well, which are connected to the hash of a previous block, thus forming a sequential chain of blocks.



**Transactions Hashed in a Merkle Tree**

*Chronologically ordering timestamped transactions by using the Merkle Tree concept*

[Source](#)

Since the entire ledger (a blockchain's transaction history) is distributed among thousands of nodes in the form of copies, it is next to impossible to attack Bitcoin. For example, a malicious individual would need to control more than half of the network's nodes (machines run by miners) in order to establish a different consensus and agree to another version of the blockchain.

## **Scarcity**

Bitcoin is scarce because it has a limited supply of coins. Unlike fiat currencies, it is impossible to infinitely print and issue new coins to the blockchain since the limitation is literally programmed into the cryptocurrency. There will only ever be 21 million Bitcoin in existence, and the circulating supply will slowly expand as more miners release coins on the market.

Scarcity enables Bitcoin to behave like a store-of-value asset, meaning that it can serve as a safe haven or hedge in times of need, which is why investors refer to Bitcoin as 'digital gold.' Combined with great cryptographic security, the feature of scarcity makes Bitcoin one of the best-performing investment assets of all time.

## Ethereum & Smart Contracts

Ethereum is another cryptocurrency that brings additional utility to blockchain technology with the help of smart contracts, which are coded in the Solidity programming language to create a rich dApp environment that adds on-chain features other than payments.

As mentioned earlier, smart contracts are pieces of self-executable computer programs that act autonomously and activate on the basis of predetermined conditions. While their execution speed may be slow in contrast to centralized data systems, smart contracts bring important benefits to the table, such as decentralization, security, and transparency.

Anyone can read and evaluate a smart contract's code to determine whether it is malicious or not - which is a dark contrast in comparison to the banking world. Moreover, smart contracts do not pick sides and only follow what they are told to do, which ensures that a transaction on Ethereum will never take a surprising turn.

Smart contracts are essentially neutral 3rd-party intermediaries that process deals and agreements made between at least two individuals. They remove the need for trust in an otherwise trustless system since users can utilize smart contracts instead of relying on the good faith of the other side. Additionally, they make it possible to bypass centralized intermediaries like exchanges and banks, which would traditionally aid users with on-chain deals.

To summarize, Ethereum can be seen as a version of Bitcoin that possesses smart contract functionality - which makes it capable of executing computational logic and facilitating features that are otherwise uncommon in first-generation blockchains.

### **Gas Fees**

In DeFi, users interact directly with smart contracts. All products and services are non-custodial, meaning that assets can remain in the user's wallet and do not have to be deposited onto the platform.

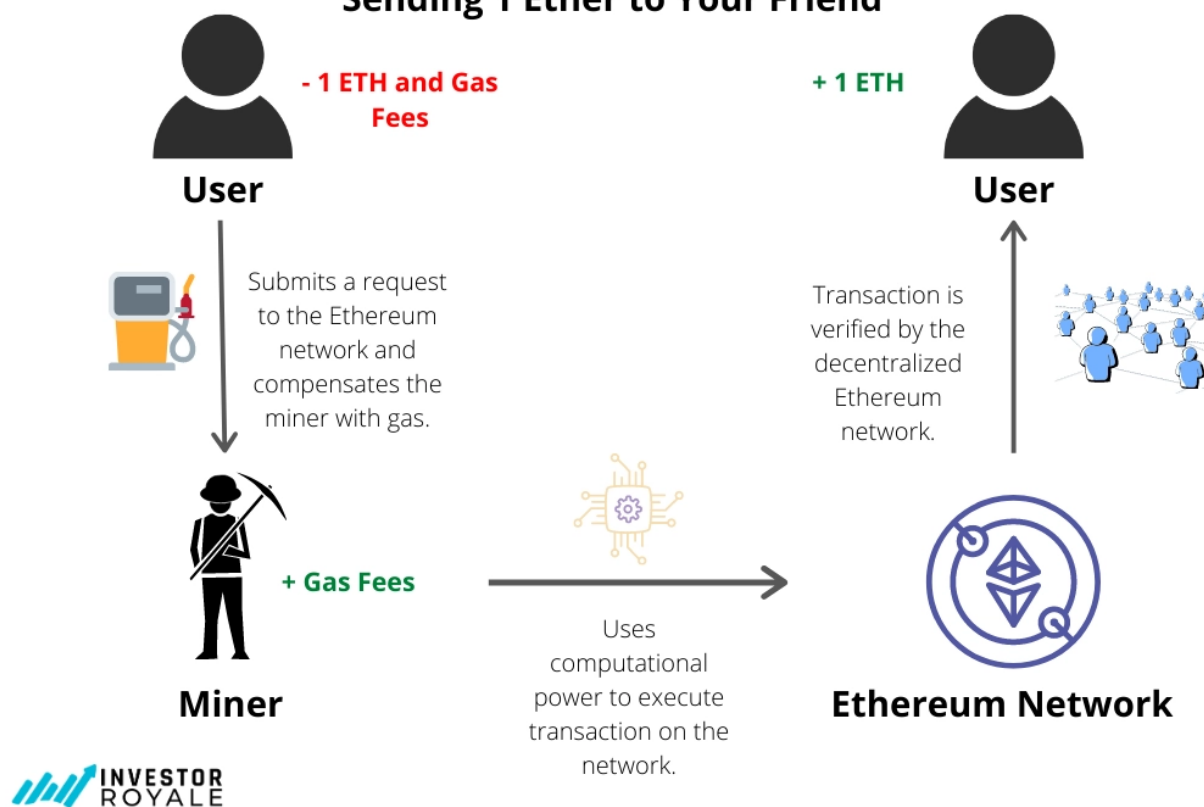
For example, an individual can swap tokens on Uniswap directly via his MetaMask.wallet. The tokens in question never enter Uniswap's native crypto wallets. Instead, the tokens are swapped with other tokens contained in the exchange's smart contracts.

While the non-custodial feature does significantly heighten the level of decentralization in DeFi, it has a costly disadvantage that can deter investors.

A centralized exchange usually processes internal trades to transfer assets, an act that does not charge any additional fees apart from the trading fees. Since a DEX does not directly hold the assets and the user must interact with smart contracts, all transactions charge Ethereum's gas fees.

# How Ethereum Gas Powers Transactions

## Sending 1 Ether to Your Friend



[Source](#)

All blockchain networks are supported by miners, a group of users who host nodes and confirm transactions. To attract these miners and operate in the first place, blockchains must reward them with transaction fees.

Transaction fees on Ethereum are called gas fees. Gas is spent on every possible smart contract transaction or activity, including transferring tokens, checking balances, calling a smart contract function, and more.

Gas has one more function: it sets priorities for different tasks. The more complex a task is, the more expensive it is. Therefore, gas functions as a limitation that prevents the network from being overloaded by cheap and simple tasks.

In the case that there are not enough miners and that Ethereum faces a surge in activity, the blockchain experiences an effect called network congestion. Within that moment, gas fees skyrocket, and the gas price for all transactions increases.

Network congestion can last for weeks, if not months, and the blockchain's state can return to normal only if demand falls down. Fees can, in some cases, range from \$40 to \$100 per

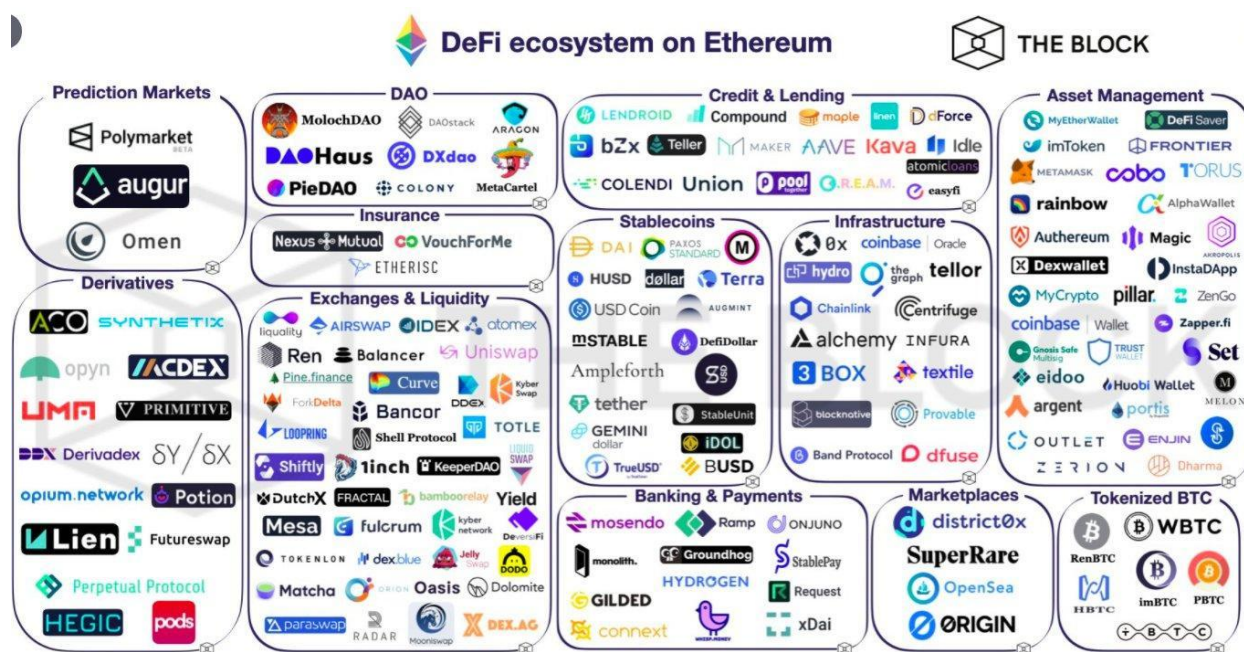
transaction, if not more. Investors who trade small sizes are naturally inclined to pause their DeFi activity during this period of time since fees account for a significant portion of their transactions.

## The DeFi Ecosystem: Use Cases

If DeFi is an abstract thought that cannot be instantly understood, the best way to wrap one's mind around decentralized finance is by exploring its ecosystem and use cases.

DeFi is a vibrant segment of the blockchain industry that meets the demands of everyone and everything. If there exists a financial service or product in the real world, there is surely a blockchain version of it on Ethereum.

The ecosystem grows day by day, and each month we see at least a few projects which are on the road to establishing their dominance on the market. According to data from DeFi Pulse, the entire DeFi sector contains \$55 billion worth of crypto assets, and the top 10 projects host at least a billion dollars in collateralized value.



[Source](#)

Although most of the largest projects are decentralized exchanges and lending protocols, there are also other notable use cases that we will individually explore in the next section.

### Decentralized exchanges

Decentralized exchanges (DEXs) are the heart of DeFi. They are the very first DeFi service to become popularized among crypto investors, partially due to the fact that they offer non-custodial decentralized trading.

Centralized exchanges (CEXs) are operated by financial services companies in the format of order books maintained by market makers (MMs). Despite the fact that CEXs offer decentralized crypto assets, their platforms are inherently centralized.

Centralization is an issue that negatively affects security, trust, and privacy. Such exchanges are prone to hacks, government bans, misuse of exchange data, identity leaks, and various other problems.

On the other hand, DEXs are managed by developers, and their format is based on the use of smart contracts. Their smart contracts execute trades, hold liquidity, process withdrawals/deposits, and anything else that you can think of. As such, there is effectively no intermediary that interacts with user funds or controls them.

Some of the most popular DEXs include Uniswap, Bancor, dYdX, PancakeSwap, and SushiSwap. While most work on the basis of Automated Market Makers (AMM), some DEXs offer a CEX-like experience by using order books.

Custodianship is the main difference between these two methods. In the first case, investors execute trades directly from their wallets. In the second case, investors must deposit funds on the DEX before being able to trade.

Since the mechanism of order books is well known, we will focus on the innovative concept of AMMs.

## Automated Market Makers

An Automated Market Maker is a smart contract that holds on-chain liquidity reserves, acting as a replacement for order books. An AMM attracts liquidity from so-called liquidity providers, who are financially incentivized to temporarily lend their cryptocurrency in return for rewards in the form of fees.



Schematic overview of Uniswap's AMM [Source](#)

Rather than trading with an exchange's order book, users trade with other users by interacting with a smart contract. Such a system has its set of advantages and disadvantages.

### **Advantages:**

- **Decentralization.** Smart contracts are predefined agreements that operate by autonomously executing commands. Combined with governance models, DEXs effectively transfer ownership of both the platform and assets to its users. Obviously enough, there is no centralized entity.
- **Non-custodial.** Traders and liquidity providers interact with DEXs directly from their crypto wallet, retaining full custodianship of their assets. All transactions are subsequently defined and processed via smart contracts.
- **No manipulation.** CEXs are infamous for manipulating markets and conducting insider trading. With no one there to benefit from such actions, DEXs clearly have no ways of directing prices into their favor.
- **Security.** Hosting DEXs is often done in a distributed manner to prevent attacks. Moreover, hackers can only interact with liquidity pools on a trading platform and not with the users that interact with the exchange.
- **Token accessibility.** Thanks to their decentralized nature, everyone can list an asset on DEXs without having to rely on a vouching or verification system operated by the platform's owners.

### **Disadvantages:**

- **Liquidity limitations.** Centralized exchanges also depend on liquidity provided by their users, but not to the degree of reliance that decentralized exchanges have. DEXs traditionally have no liquidity pools on their own, so they must be filled by yield farmers who contribute their assets for other traders to use. Without them, the exchange cannot offer trading services.
- **Speed.** Less efficient order execution compared to their counterpart, which is mainly brought on by the traditional lack of advanced trading tools.
- **Volume and slippage.** DEXs have picked up on volume, but without an order book and market maker, users suffer extreme slippage rates - especially with large orders.
- **Fees.** No order book also means no low fees. All users pay a fixed trading fee, along with gas fees charged by the Ethereum network. When congested, the network charges hundreds of dollars for a single transaction.

### **Constant Product formula**

From a technical perspective, the main goal of an AMM is to maintain a 'Constant Product.' The constant product is an algorithm used to maintain equal reserves of two assets that form a trading pair, which have a 1:1 supply ratio.



Uniswap uses the following formula to maintain a constant product:

$$x * y = k$$

In this formula, x and y represent the reserve balances of two tokens in a liquidity pool. Any trade on an AMM must not affect the unchangeable k (constant product) as it can result in a liquidity imbalance.

Liquidity providers who fuel these pools are, therefore, 'forced' to provide equal amounts of both tokens. For example, if we want to provide liquidity to an ETH/USDT pool and only have 2 ETH (worth \$4,440), we must also provide \$4,440 worth of USDT. Using the aforementioned formula, we receive the following constant product:

$$2 \text{ ETH} * 4400 \text{ DAI} = 8,800$$

Without any trades, the figures remain the same. But if a trader wishes to buy 1 ETH, he will take a single Ether out of the pool and give the proportional amount of USDT tokens in return.

However, the buyer also has to pay an additional amount of USDT compared to the original price (1 ETH = \$2,200 USDT) as a premium. The larger amount of ETH the trader wishes to buy, the larger the premium will be - which ensures that the pool never runs out of liquidity.

Since the premium ensures a constant ratio, K always remains the same.

## Lending

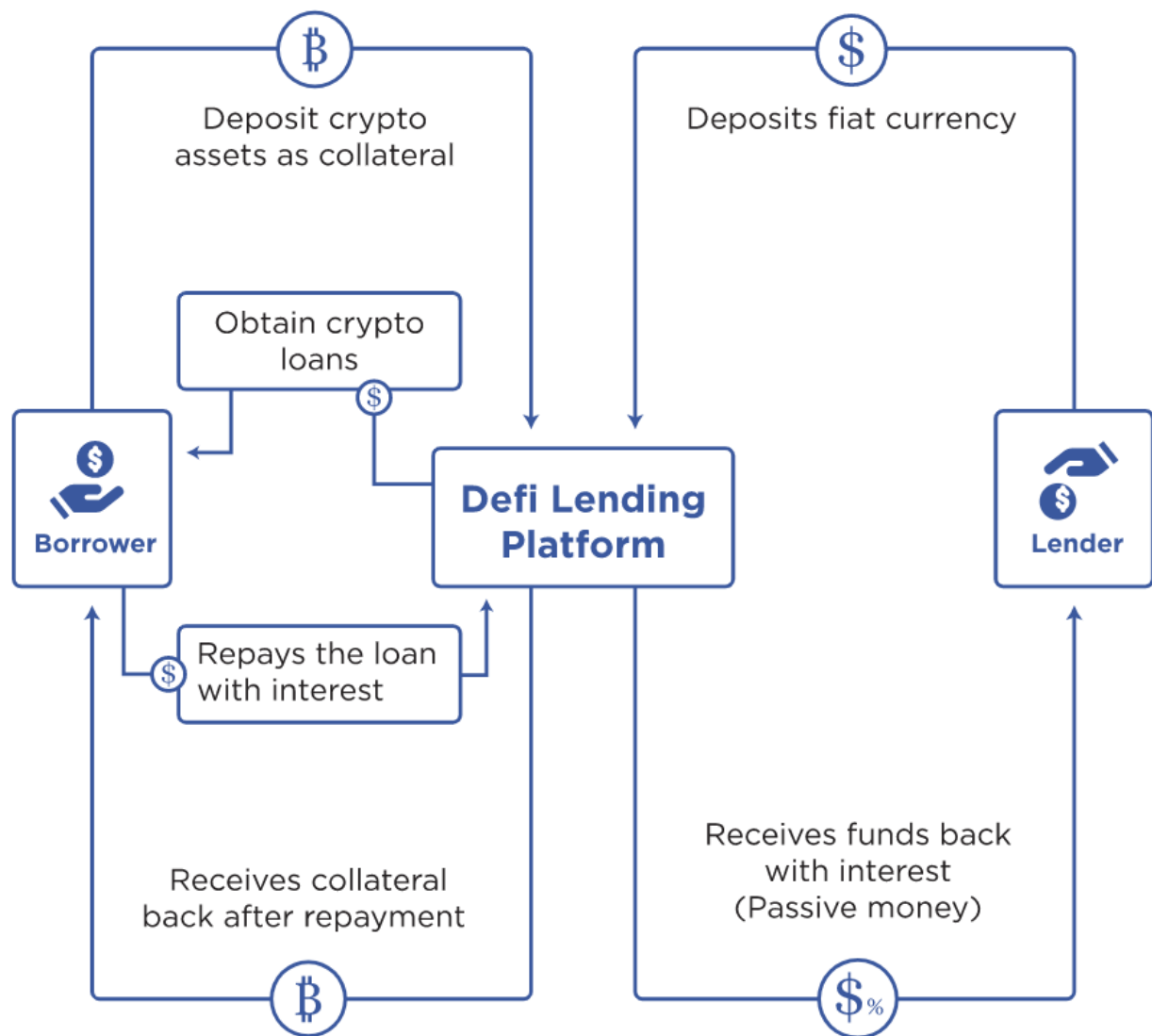
Lending & borrowing is the second-largest use case in DeFi.

The modern economy thrives on loans, and without them, most advanced financial activity is barred off for the average person. Whoever cannot take out a loan cannot start a business or purchase real estate either.

The only way to borrow funds is by requesting a loan from an intermediary, which is usually a bank. To protect their interests, banks only lend funds to trusted individuals who meet criteria like a good credit score, stable job, a minimum amount of collateral, and other factors.

There are various constraints and challenges provided by these requirements which can prevent a person from taking out loans, making them exclusively to a specific group of people.

DeFi lending protocols fend off this exclusivity by eliminating all barriers, which is especially beneficial to the bankless. Being decentralized and accessible, these protocols are available to people of all backgrounds, races, and locations. As long as one can provide necessary collateral, it is possible to take out a loan and use the newly gained funds.



LeewayHertz

[Source](#)

Apart from collateral, there are no other requirements. Moreover, lending protocols do not use pervasive identity checks like Know-Your-Customer (KYC) policies. It may sound bizarre to someone only familiar with traditional finance, but a DeFi user can anonymously request a loan and receive it in the span of mere minutes.

Famous lending protocols include Compound, Aave, Maker, and bZx. In total, they host \$26 billion worth of collateralized assets which accounts for almost 50% of the entire DeFi market.

### Lending in practice

Every lending platform consists of two sides: lenders and borrowers.

Just like traders, both sides interact via liquidity pools contained within smart contracts. While lenders supply assets and earn interest, borrowers take out loans and pay interest on their debt.

Every cryptocurrency has its own liquidity pool and interest rate, denominated in APY (Annual Percentage Yield). The APY rate differs from asset to asset and increases or decreases based on the laws of supply and demand.

It is worth mentioning that APY rates range from 3% to 20% (and even higher in extreme cases), which makes lending in DeFi far more profitable compared to banks. APY rates can also be fixed or variable, depending on the platform. In the first case, a user who lends his assets will receive a constant interest that never changes. In the second case, the interest rate can go up or down depending on market conditions.

## **Flash Loans**

Lending protocols also offer a unique type of loan called a flash loan. A flash loan requires no upfront collateral, and users can request millions of dollars if they wish. However, the catch is that flash loans need to be repaid almost instantly.

As a matter of fact, flash loans have a life cycle lasting only one transaction block. Before the next block arrives, the user must repay the loan. If he fails to do so, the original transaction is reverted, and the funds are lost. Flash loans are primarily used for swift tasks such as arbitrage trading and debt refinancing. Their major disadvantage is that flash loans are so complex that they are vulnerable to security exploits.

To summarize, lending protocols effectively act as intermediaries between lenders and borrowers who interact by taking or providing crypto funds. Lenders have the benefit of receiving higher than average interest while borrowers gain the ability to instantly take out loans without filing tons of paperwork in a completely anonymous and safe way.

## **Derivatives**

Aside from simple token swapping, DeFi also targets complex trading products. More advanced decentralized exchanges offer decentralized derivatives which derive their value from an underlying asset such as a currency, stock, index, or commodity.

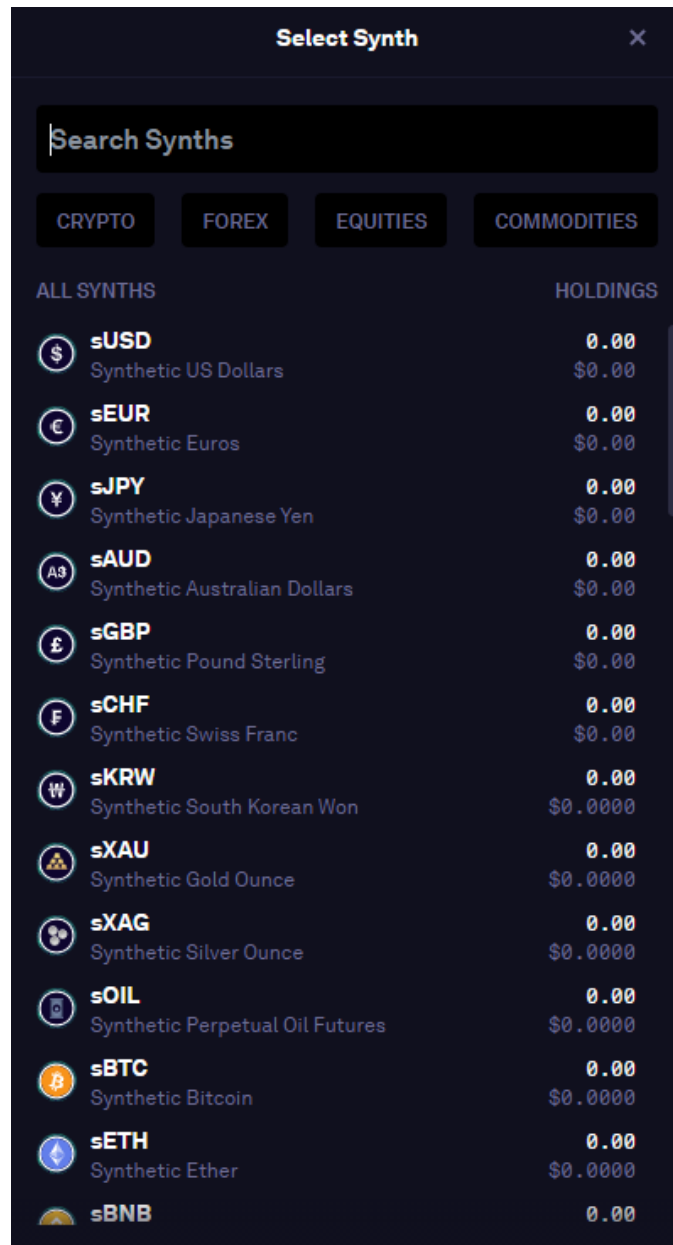
Notable derivatives products include futures, options, and synthetic crypto assets. Certain investors trade derivatives in order to hedge against volatility or to speculate against assets and use additional leverage. Due to their risky nature, a majority of crypto investors refrain from trading derivatives. Nevertheless, the DeFi derivatives market still plays a key role.














The most popular DeFi derivatives protocols are Synthetix and bZx (Fulcrum). Both of them host roughly \$2.3 billion in value. While the figure is extremely low compared to other niches like

decentralized trading and lending, derivatives platforms are growing swiftly, and their adoption rate rises along with the introduction of new projects and features.

## Derivatives on Synthetix

Synthetix is the largest DeFi derivatives protocol, and its products are called synths. These synths are different as opposed to traditional derivatives due to the fact that they tokenize their underlying assets.



Select Synth		
Search Synths		
CRYPTO FOREX EQUITIES COMMODITIES		
ALL SYNTHS		HOLDINGS
 <b>sUSD</b> Synthetic US Dollars		0.00 \$0.00
 <b>sEUR</b> Synthetic Euros		0.00 \$0.00
 <b>sJPY</b> Synthetic Japanese Yen		0.00 \$0.00
 <b>sAUD</b> Synthetic Australian Dollars		0.00 \$0.00
 <b>sGBP</b> Synthetic Pound Sterling		0.00 \$0.00
 <b>sCHF</b> Synthetic Swiss Franc		0.00 \$0.00
 <b>sKRW</b> Synthetic South Korean Won		0.00 \$0.0000
 <b>sXAU</b> Synthetic Gold Ounce		0.00 \$0.0000
 <b>sXAG</b> Synthetic Silver Ounce		0.00 \$0.0000
 <b>sOIL</b> Synthetic Perpetual Oil Futures		0.00 \$0.0000
 <b>sBTC</b> Synthetic Bitcoin		0.00 \$0.0000
 <b>sETH</b> Synthetic Ether		0.00 \$0.0000
 <b>sBNB</b>		0.00

A list of synths on [Kwenta](#)

A synthetic asset (synth) is simply a tokenized derivative that mimics the value of another asset. For example, a stock like Gamestop would have a tokenized version called sGME (synthetic GME), which represents the real stock. Its price would be tracked via a decentralized oracle such as Chainlink, and it could be traded by anyone.

Synths are especially helpful because they improve financial accessibility. Someone who does not have access to the U.S. stock market would otherwise have no way to trade an asset like GME. Moreover, investors do not have to hold the underlying asset and have an easier time trading, buying, or selling assets.

In the case of Synthetix, DeFi's decentralization is particularly advantageous due to the fact that anyone can create a synth. Since blockchain-based synths can track all kinds of underlying assets, the sky's the limit when creating derivatives.

## Yield Farming

Yield farming is closely related to how decentralized exchanges work, and it is currently the number one use case in DeFi.

Yield farming is definable as a passive income strategy that enables investors to earn more crypto by using existing crypto assets. Essentially, yield farmers provide their cryptocurrency to a decentralized exchange in the form of liquidity to earn rewards.

A decentralized exchange incentivizes yield farmers by rewarding them with trading fees, which are gained from users who execute trades using the yield farmer's liquidity. Such a system forms a symbiotic relationship between the DEX, traders, and liquidity providers, where each side receives something.

Instruments	TVL ▾	APR
 WBTC-WETH	\$1b 0.01909 SLP	11.26%
 SUSHI-WETH	\$431,514,665 1,142,720 SLP	37.46%
 USDC-WETH	\$371,546,344 3.01531 SLP	26.02%
 DAI-WETH	\$280,885,817 2,427,514 SLP	36.14%
 WETH-USDT	\$242,286,791 1.97346 SLP	35.10%
 YFI-WETH	\$176,420,337 5,118 SLP	38.56%

An example of yield farming opportunities on [SushiSwap](https://sushiswap.com)

Each farmer earns fees proportionally to his contribution in a liquidity pool. The yield farming process can last for an unlimited amount of time. However, users are incentivized to jump from one pool to another in order to chase highly competitive yield rates. In yield farming, yield rates are considerably higher compared to other similar activities.

Popular yield farming platforms include Uniswap, Curve Finance, SushiSwap, Yearn Finance, Cream Finance, and many others. Most of them are decentralized exchanges that use AMMs, which means that yield farming is an inherent feature for DEXs.

When yield farming, the investor retains custody over his assets by receiving liquidity provider (LP) tokens in return. LP tokens represent the investor's share of the pool, and they must be redeemed in order to receive the original funds back. However, yield farmers can also use LP tokens by depositing them to other pools and farming more assets. Therefore, it is possible to earn double the rewards by simultaneously accessing two passive income strategies.

### Impermanent loss

The issue with providing liquidity to exchanges is that yield farmers face the dangers of impermanent loss (IL). Impermanent loss is the opportunity cost of holding onto an asset for speculative purposes versus farming it to gain rewards.

IL is almost unavoidable due to the fact that cryptocurrencies are volatile assets. If an asset loses or gains too much value from the moment of being deposited to a pool, the yield farmer would be better off by simply storing the assets in a wallet. In the best case, the user will make a little less money than he would have by doing nothing. In the worst case, the user will have less money after withdrawing compared to what he has originally deposited.

For the duration of the farming process, impermanent loss is unrealized. The moment a yield farmer leaves the pool and redeems his tokens, the loss is realized. Therefore, farmers can avoid losses by waiting for prices to retrace to their initial value.

### **Minimizing impermanent loss**

The best methods to avoid IL are by either joining pools with relatively low volatility or by joining pools with high yield rates.

In the first case, the chance of facing impermanent loss is low since the assets themselves do not gain or lose too much value in a short time frame. By the end of the process, the realized losses will either be small or non-existent.

In the second case, the yield rate can be high enough to offset the losses incurred by impermanent loss. Since liquidity pools use exchange fees to distribute rewards to yield farmers, it is possible to profit greatly from a sudden jump in trading volume. Even if one suffers impermanent loss, the money gained from farming will be enough to remain profitable.

Certain yield farming platforms are designed to minimize IL. For example, Curve Finance only offers liquidity pools with stablecoins and wrapped tokens - both of which hold onto a stable price point. Since there is little to no volatility, it is possible to yield farming without experiencing impermanent loss. However, yield rates are naturally lower compared to other liquidity pools.

## **Insurance**

Smart contracts may be decentralized and transparent, but they are prone to security exploits which can result in millions of dollars in losses. Even audited DeFi projects can still possess exploits, and if that is the case, a hacker can completely drain its liquidity pools.

In contrast to centralized exchanges, DEXs are not obliged to protect or reimburse their clients in the event of an exploit. There are no insurance funds, which often exist on crypto exchanges like Binance, Gemini, and Coinbase.

↕	Nexus Mutual ↕	Etherisc ↕	CDx ↕
Primary Product	Smart Contract Insurance	Flight Delay Insurance	Exchange Insurance
System	Risk Pool	Risk Pool	Credit Default Swaps
Native Token	NXM	DIP	CDX
Live	Ethereum Main-net (Bootstrap Phase)	Ethereum Testnet	No
Decentralized	Yes	Yes	Yes

Insurance protocols compared. [Source](#)

On that account, DeFi investors must use insurance protocols in order to protect their existing funds. These protocols not only protect against technical risks (exploits) but against liquidity risks and administration risks as well.

### How coverage works

Nexus Mutual and Oryn are the two largest DeFi insurance protocols. Both host roughly \$400 million worth of crypto assets.

When users apply for insurance, they pay for so-called 'coverage,' which covers the user in specific events. As previously noted, it is possible to be covered in the event of a smart contract exploit. A yield farmer who provides a high amount of liquidity might decide to cover his assets, and in this case, he must state the coverage amount and coverage period.

Coverage amount represents the value of assets that is paid out in the event of a smart contract incident. Coverage period accounts for the time period during which the user can utilize his insurance.

For example, a yield farmer who plans to contribute crypto assets on Uniswap can visit Nexus Mutual and apply for a coverage option that lasts two weeks and covers 50% of his contributed liquidity. If an exploit occurs during this timeframe, Nexus Mutual initiates a Claims Assessment procedure and reimburses the yield farmer.

## Stablecoins

Stablecoins are cryptocurrencies pegged to the value of fiat currencies. Since cryptocurrencies are volatile, stablecoins are used as a hedge to protect oneself against extreme market conditions. Moreover, they are also used to quickly secure profits by converting cryptocurrencies into what is essentially a tokenized form of fiat.



# StableCoins Types



The U.S. Dollar is the dominant stablecoin in the crypto market. The method of pegging a token's value against the dollar is different from stablecoin to stablecoin, and each project uses its own system to ensure zero volatility.

## Types of stablecoins

We can divide stablecoins into two categories: fiat-collateralized and crypto-collateralized.

Fiat-collateralized stablecoins are backed by real fiat held within a project's reserves. Tether is the most popular example of a fiat-collateralized stablecoin, and its USDT token is pegged to \$1 by maintaining reserves of \$1 per minted USDT token. Investors must trust Tether to hold enough fiat reserves for their crypto supplies. Their reserves are held in financial institutions and banks. All of these facts combined mean that fiat-backed stablecoins are centralized.

Crypto-collateralized stablecoins are backed by cryptocurrencies rather than fiat. For example, DAI is built on top of the Ethereum network and uses smart contracts to maintain a \$1 peg. Since smart contracts are public, users have the ability to confirm whether there is enough collateral to back DAI's token supply. On that account, DAI is a decentralized stablecoin.

Decentralization is a critical component of how the DeFi market works, and stablecoins like DAI are extremely important for DeFi to stay 100% decentralized.

# Governance

In the blockchain industry, governance models establish a system in which investors have a direct say in how a project is designed and in which direction it is heading. Much like a company's shareholders, community members can voice their opinions and actively contribute to the decision-making process.

Governance establishes absolute decentralization and delegates all planning to a project's investors rather than its developers.

When writing a paper about Decentralized Autonomous Organizations (DAO), Ethereum co-founder Vitalik Buterin referred to governance models as companies that work without managers. Instead of relying on a small group of executives, the entire system utilizes smart contracts that process, execute, and accept various tasks and decisions.

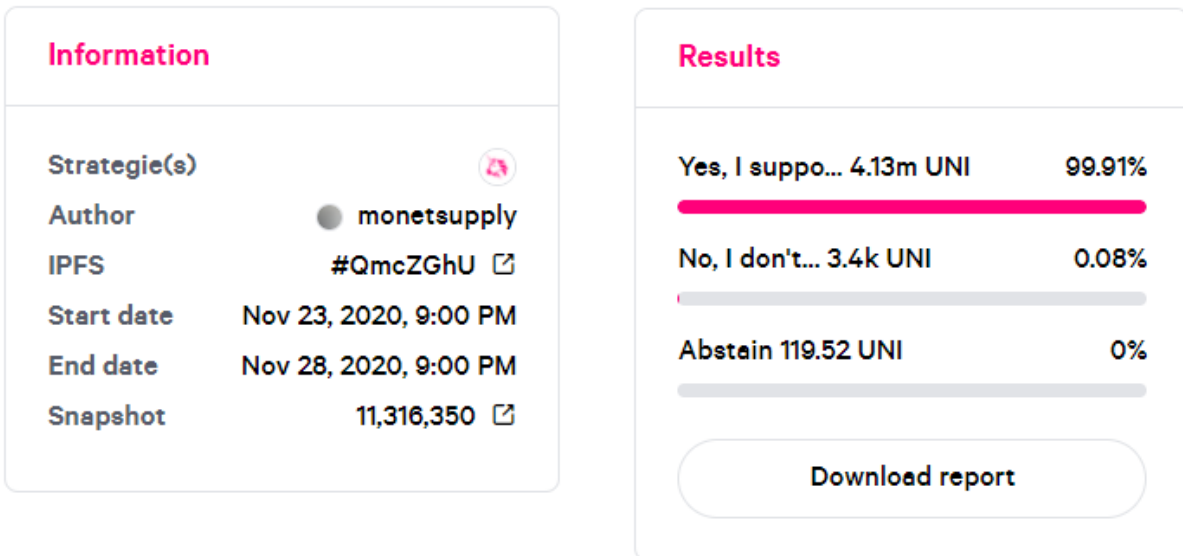
Governance is important for DeFi because it transfers ownership of a protocol to its community. Most projects have a governance token that grants users voting rights and the ability to create governance proposals.

Ideally, governance tokens are fairly distributed. This can be done by airdropping a portion of the cryptocurrency's supply to active users, which is what Uniswap did with the launch of UNI in September 2020. At the time, Uniswap distributed 60% of UNI's genesis to the community via a 400 UNI airdrop.

Otherwise, decentralized protocols can launch a governance token by simply listing it on an exchange without any fair distribution. Investors who are bullish on the project's future will then invest in the token and gain voting rights by doing so. Since token holders are also voters, investors will be incentivized to make the best possible decisions.

## **How governance works in practice**

The act of voting and participating in governance revolves around the use of governance tokens. Once dispensed, holders can propose changes and vote on existing proposals. Additionally, community members are free to discuss governance issues and upcoming features on online forums hosted by the project.



Snapshot of a Uniswap [governance proposal](#)

All acts of governance require that the instigator locks governance tokens into smart contracts for the duration of the process. Locking tokens is not only necessary to fight against proposal spam, but to ensure that users spend more time on creating higher-quality proposals before sending them out.

For a proposal to be even considered, it must establish a quorum. Essentially, each governance proposal must have a minimum number of voters who have cast their vote. If the results favor the proposal, smart contracts will approve it, given that the quorum has been reached.

## The Future of DeFi

According to data from blockchain analytics platform Dune Analytics, the number of DeFi users increased from 93,000 in January 2020 to 1.8 million in April 2021. Simultaneously, the market's valuation increased from \$700 million to \$58 billion during the same time period.

Despite rising to the surface during both a stock market crash and pandemic, decentralized finance succeeded in becoming the industry's next big thing. DeFi moved on from being just a niche and utterly destroyed the fear of turning into another ICO-like fad. Moreover, its vicious performance was good enough to spark fear into crypto's centralized exchanges, which have lost a significant portion of liquidity to DEXs.

The disruptive potential of DeFi is obvious. A new decentralized future is upon us, and it should not be strange in an industry like blockchain. However, there are still a great deal of obstacles that we must overcome before reaching mass adoption.

Smart contracts are still prone to exploits, anonymous developers still behave like vultures by launching rugpull projects, and the fear of regulations still tower over our heads. For now, DeFi is crypto's wild west, and both creators and users need to reach a certain level of maturity in order for the niche ecosystem to establish itself as a prominent and serious sector in this new decade.

Reaching a perfected and balanced state will take several years, and the timeline will depend entirely on the community and its behavior. Living in uncertain and chaotic times, it is clear that disruptive technologies are more likely than ever to shift into the real world and that this is our chance to make fundamental changes. The road may be long and full of hardships, but one thing is sure: the future of finance is decentralized.