# 5 An Introduction to Decentralized Exchanges

## 5.1 What is a Decentralized Exchange?

Decentralized exchanges (DEX) are permissionless transaction networks that act in a decentralized manner to enable the exchange of cryptocurrencies. They are perhaps one of the most significant developments of decentralized finance to date because they allow exchange that does not require third party intermediaries and/or custodial services to use (meaning users have control of their private keys). In order to exchange cryptocurrencies between people who do not know each other decentralized exchanges use smart contracts to secure transactions. In this introduction to decentralized exchanges, the concepts above will be laid out in detail to understand what they are, followed by a brief guide on how to use them. Readers are encouraged to do further research.

## 5.2 Differences between DEXs and Centralized Exchanges (CEX):

A centralized exchange is a custodial service that manages cryptocurrency for a user. This means that CEXs are managed by a third party. Having cryptocurrency in a CEX means that the CEX has the user's private keys instead of the user. There are advantages and disadvantages to using decentralized exchanges vs centralized ones. These differences closely resemble the advantages that decentralized finance (DeFi) have over traditional finance.

**The advantages to using decentralized exchanges are threefold:**

1) cryptocurrency availability;
2) greater anonymity;
3) reduced security risks.

In the first case, a CEX allows users to exchange based on what is available on the platform which means users are restricted in what they can trade. In the second case, a CEX tracks and stores all data while complying with KYC. Paying taxes is one thing, but this means that other actors could potentially track your portfolio and know how much is held. Thirdly, interacting with centralized exchanges is arguably more risky due

to more counterparty risks and greater possibility of getting hacked (having all of your tokens in one place, tokens not in a hardware wallet where they are held offline, centralized exchange goes down, company seizes or freezes funds by government orders, and so on).

**This is not to say that there are no disadvantages however. There are three major ones:**

1) at first there is a steeper learning curve because it requires the use of more applications and exchanging between different self-managed cryptocurrency wallets;
2) when interacting with riskier applications with vulnerabilities could lead to stolen funds;
3) interacting with unvetted tokens (always confirm the token smart contract address before exchanging assets).

Arguably the biggest disadvantage to using decentralized systems is the cost. It is noteworthy to mention however that the IMF April report of 2022 found DeFi to be overall less expensive than TradFi. Despite this fact most centralized exchanges have lower costs in comparison to decentralized exchanges. However, that competitive advantage is slowly decreasing as we will see later when discussing Layer 2 blockchains.

Many people purchase, hold, and trade cryptocurrency without ever using a DEX. This is because there are a wide variety of CEXs out there with easy to use on boarding methods from fiat to a broad range of cryptocurrency. Broadly speaking, CEXs use a model comparable to the current traditional financial model we have today. They are private companies who are beholden to shareholders which have a vested interest in generating profit. Even more alarming, because these institutions hold assets and exchange them they are (in some respects) comparable to a bank or broker.

CEXs are intermediaries who use contractual agreements between them and clients. There are a few worrisome outcomes that could occur, especially because (let's be honest) nobody reads user agreements. Even if the average person were to read these 100+ page documents the language is difficult to read and to properly interpret would require a lawyer. Even without these issues contracts signed by two parties carry a lot of counterparty risk.

**To summarize here is a short list of counterparty risk involved with signing a contract:**

1) How do we know they will keep their end of the bargain?;
2) How do we know they aren't using these contracts behind our backs to benefit themselves?;
3) How do we know we will not be censored or locked out if we do something that is disagreeable to the company/bank managing our holdings?;
4) How do we know that the agreement is just and valid?;
5) How do we know and verify that there aren't other contracts that are underlying the contract we are signing and what their relationships are?;

Even a short glance of the history of our system will reveal that this contractual mechanism is untrustworthy. One modern day example is the mortgage-backed security crisis of 2008 wherein insurance companies and banks rated packages AAA when they knew they were going to fail and bet against them to make obscene profits while governments bailed them out and millions of people were driven into poverty.

By comparison, DeFi's objective is to (hopefully) solve some of the issues with current financial agreements through the following:

1) Force transparency and clarity of the contract by being open and transparent;
2) Allow individuals to control their own assets and become responsible for them;
3) Create a global open source systems that anyone can use without risk of censorship;
4) Provide better yield (less than 1% in banks vs 8%~ on average in DeFi);
5) The protocol/code can be verified and looked at;
6) Permissionless and thus anyone can execute them;
7) As smart contracts can be run autonomously they guarantee an outcome that anyone can access without custodial authority;
8) Interact without middlemen;
9) Track collateral in real time and calculate exposure and leverage.

Even more stunning, a study from the American Economic Review on market decentralization concluded the following in their abstract:

"Decentralized markets can allocate risk among traders with different risk preferences more efficiently, thus realizing gains from trade that cannot

be reproduced in centralized markets. Market decentralization always increases price impact. Yet, markets in which assets are traded in multiple exchanges, whether they are disjoint or intermediated, can give higher welfare than the centralized market with the same traders and assets."

In other words: exchange is more costly but there is less overall risk and there is more equitable distribution of overall resources. This may also help with wealth inequality, provided that blockchains are decentralized without large investors monopolizing them.

Despite these advantages, interacting with DeFi protocols carries risk on the blockchain. However, using DEXs for trading between cryptocurrencies has a significant history in comparison to liquidity pools and yield-bearing strategies to gain interest over time. If a user is exchanging known tokens on a DEXs that has a long standing history there is very little risk in doing so with proper security measures. DEXs are less vulnerable and are better time tested. Liquidity issues are also possible. Before finalizing a transaction make sure to double and triple check the cost due to these issues. When low liquidity occurs, higher slippage rates apply. Before interacting with or adding new tokens to a wallet (say MetaMask), users should be sure to verify the smart contract address, available on coingecko and other websites.

## 5.3 Introduction to Rollups

Arguably the biggest disadvantage to using decentralized systems is the cost. Currently most centralized exchanges have lower costs. However, that competitive advantage is slowly decreasing as we. In order to reduce fees it is necessary to use different networks. There are two options to choose from: using alternative security networks, also known as "Layer 1" blockchains, or transaction networks connected to security networks. Transaction networks are only available on Ethereum for now. They are also sometimes called "Layer 2" blockchains or rollups.

Due to fees, there is a learning curve to transact and trade in order to reduce them. It is important to do research and find what works for each individual user. At the beginning using simple trades and then working up to using multiple chains (especially rollups) could be a good way to get comfortable with the networks and programs before diving in deep.

Rollups execute transactions, bundle them up together, compress them into data, then port them over onto the blockchain they are attached to. By forwarding the transaction data on to Ethereum, roll-ups still use the security of the Ethereum blockchain. Their function is to convert computing power into data so that the main security layer (example: Ethereum) can focus on more important roles. The end result is reduced transaction fees because computational power is replaced with data.

The long and short of it is that rollups are a scalability solution that takes computation off-chain and feeds transaction data to a security layer. In addition, all data of a rollup is available in the security layer (in this case Ethereum). Rollup transaction execution and L1 data (Ethereum) update at the same time. Any Layer 1 that is compatible with the EVM can become an Ethereum rollup if their data is posted on Ethereum's chain at the same time as the state changes. The fund and exit mechanisms for these rollups are maintained by the Ethereum network (hence why Layer 1 is also sometimes called the "security layer").

## 5.4 Methods and Means

There are two broad ways to create a decentralized exchange: order books and automated market makers. Both these types use smart contracts. Order books have a more "classic" style look which is more familiar to users from a traditional finance background. Orders for different asset pairs at different rates are matched up and execute the trades between users. There are two broad categories of order books fall into: on-chain and off-chain. In order to understand what on-chain and off-chain means and how DEXs work we must understand smart contracts.

## 5.5 On-chain vs Off-chain order books

Smart contracts are codified financial agreements that run on a blockchain. A blockchain works as a ledger that records all prior transactions to know who owns what as the final sum. This means that a smart contract is deployed on a blockchain; it is immutable, permissionless, and censorship resistant. All smart contracts and information on a blockchain is called on-chain data. In order for this contract to be executed it must be fed information, also known as off-chain data because it refers to all information that isn't on the blockchain.

To summarize, on-chain DEXs use information that resides on the blockchain to determine the price, whereas off-chain DEXs use information that isn't on the blockchain. Off-chain data is preferred because on-chain data uses more computational power and is slower. The more information that can be transferred into data before it is ported on-chain, the less the cost and the faster the transaction will go through.

Order books are primarily a match-making system. This provides more flexibility than AMMs (seen below). Despite this enhanced flexibility, order books are perceived as less user friendly and if there aren't enough orders on the books then this could lead to liquidity problems as there aren't enough trades going on at once for that particular asset pair. This is particularly problematic when it comes to coins with low volume (small cap) cryptocurrencies. If a user is used to ordering books and wants to use them then CEXs are a better place to go for now while rollups gain transactions.

## 5.6 Automatic Market Maker

Automated market makers (AMM) use liquidity pools (also known as liquidity farms) instead of waiting for matching orders. In other words outside users provide liquidity to the DEX. Liquidity pools are used to transfer funds using smart contracts. A user exchanging cryptocurrency will send their tokens to a decentralized exchange and a token provided by a pool will be given back in exchange for the same price (minus fees).

Users receive rewards (at a fluctuating rate) in exchange for supplying the pool with more liquid. The liquidity pools help users exchange funds because the pools act as a hub in between tokens. Therefore, instead of matching users, an AMM will send corresponding amounts to the user who is swapping one cryptocurrency for another. In the most basic AMM system, liquidity in the contract determines the price by looking at the available amount of money vs other assets. In other words, as supply increases or diminishes in a pool the price will either increase or decrease. As they do, other exchanges receive this same information and update so that prices theoretically remain the same throughout the market.

This system makes it easier to execute transactions on the blockchain because though this leads to less flexibility and less tools, AMMs

are more universalised, easier to use, and more specialized for the average user. Usually, a charting website such as tradingview is used in conjunction with an AMM to know the historical price, volume, indicators, and other information.

In truth there is little difference between using AMMs and order-book DEXs. Both provide the same basic function, but under the hood is slightly different. Currently most DEXs and DeFi protocols in general are AMM-based. It has simply been the prefered route to go because it simplifies some of the problems of order books and liquidity while keeping things simple for users. Since there is locked value in the decentralized exchange through liquidity pools and farms it simply eliminates half of the exchange problem. Sellers and buyers are pre-matched so there are less worries.

## 5.7 DEX Aggregators

In more recent times, DEX aggregators have started coming to the forefront. These tools use a similar AMM DEX that is cross-compatible between multiple chains. This means that cross-chain swapping is much easier because the DEX looks at all other DEXs in its database to find the most cost-effective route possible. This eliminates the need to use multiple swapping mechanisms to send different tokens between different networks.

## 5.8 A Short Introduction to Using Decentralized Exchanges

The type of decentralized exchange used is dependent on the chain. The goal of this section will be to introduce the major DEXs and give general guides on how to use them. MetaMask (a popular ERC-20 token wallet) takes somewhat of a learning curve, however there are many guides that can be found online including on MetaMask's own website. It is beyond the scope of this article to teach users how to use it.

Cryptocurrency is evolving very fast so what is true in this chapter can change quickly. In a few months or even years from now things could be radically different so it is important to keep that into consideration. By and for the most part having tokens on different chains requires different

DEXs so it is important to stay organized, decide on what networks to use, and strategize before transfering funds.

As previously mentioned, there are many decentralized exchanges, each of which use different networks. Currently, the main security networks are Ethereum, Avalanche, Solana, Near, Polkadot, and many others. The main transaction networks that are hosted on the Ethereum blockchain are Arbitrum, Optimism, Starksnet, and ZKSync. Sometimes in order to avoid fees to trade cryptocurrencies networks need to be switched. In order to do that it is recommended to use the metamask wallet and add the different networks you are using (example: Ethereum, Arbitrum, and Avalanche) to your account. This means managing multiple wallets and finding cost effective ways of sending cryptocurrency to those networks. For the sake of convenience there is a list of several tools and the latest updates to find DEXs below, and includes useful information like the total locked value in a liquidity pool, marketcap, what networks they are compatible with, and so on.

## 5.9 A few DEXs to consider to reduce trading fees

### Uniswap

By far the most popular decentralized exchange is uniswap, which mainly functions with the on Ethereum network and is also compatible with Arbitrum and Optimism. Uniswap is the go to DEX for the Ethereum network because it has the most history, and thus is safe to use. Because arbitrum and Optimism are transaction layers they have less tokens hosted on their networks. Uniswap is easy to use. Once your wallet is connected, select the tokens you want to exchange, select the token you want to receive, and then go through the procedure. To switch networks, select from the options at the top right of the screen.

### Zigzag Exchange

ZigZag Exchange is a relatively new exchange in the ZKSync network that uses an order book layout. As far as application on the ZKSync network ZigZag is relatively well known and is a noteworthy mention to this list for low fees while interacting with exchanges with a layout similar to some centralized exchanges or TradFi brokers. To use it, connect a Metamask wallet, find the desired trading pair, and go through the steps to buy and sell.

### DyDx

This derivatives exchange uses an order book as its method of trading assets. As it is a derivative DEX, it takes side bets on the overall price of the market rather then exchanging cryptocurrency via public/private key transaction. DyDx requires a deposit in their system in order to trade. It is also possible to do so on margin. The more a user deposits in DyDx the less fees they have to pay.

### Argent

While not a DEX, Argent is a great way to buy crypto currency and directly on board onto the rollup of your choice. This reduces fees in the long term if a user wishes to mostly use rollups. This is because most CEXs as of now do not have direct onboarding methods to L2s. It is a mobile app however so there are more potential security risks than having a wallet on a computer.

### Loopring

Loopring is another orderbook DEX which uses ZKSync's rollup consensus mechanism (zkRollups) while also using zkSNARKs, a mechanism that encrypts transactions on the blockchain by "blackboxing" them, making them untraceable. In order to take full advantage of low transaction fees on Loopring, it is required to make an L2 loopring wallet using metamask or a similar wallet compatible with ERC-20 tokens.

### Rubic

Rubic is a cross-chain liquidity DEX aggregator. It boasts 12 L1 chains to switch from, over 15,000 assets, and 60+ interconnected DEXs, fiat-on-ramps, and bridges as of early May 2022. It operates by taking a bunch of DEXs and joining them together in the most cost efficient way while providing an interface that is simple and easy to understand. This means that switching between Layer 1 networks (Ethereum tokens on the Ethereum network to Avalanche tokens on the Avalanche network for example) is very simple to do using their application. For now Rubic only has Arbitrum as a roll-up option. Rubic's interface is very similar to uniswap's and other AMM DEXs.

### Matcha

Matcha is a DEX aggregator with 7 different chains. It does not do cross-chain swaps like Rubic, however it is more roll-up heavy. As far as using DEXs to exchange cryptocurrencies using roll-ups is concerned, Matcha is well trusted and often used on those networks. Despite being relatively new, it is a good alternative to using uniswap to consider. Once again, a straightforward AMM DEX that functions much the same as the others mentioned above.

## 5.10 Ways to earn money without trading

With so many decentralized exchanges floating around there are many arbitrage opportunities and the possibility to provide liquidity to earn interest on crypto by joining “pools” or “farms”. These activities are slightly more risky and require more knowledge to find the right pools to join. It is a way to generate more interest then the current TradFi banking system and on the whole provides returns.

Arbitrage, on the other hand, is something that is generally programmed. In other words, bots find these opportunities and trade on them. Occasionally “flash loans” (loans that must be paid back in a short amount of time or within the next purchase) are generated during arbitrage for an increased profit.

## 5.11 In Summary

As we can see, there are a wide variety of DEX’s to choose from, each with their own advantages and disadvantages. Most need an individual to already own cryptocurrency. Decentralized methods of onboarding fiat to cryptocurrency do exist such as peer to peer exchanges like bisq, localmonero, or CEXs. However it remains that the DEX used is dependent on what chain that the cryptocurrency is on. Therefore it is important to consider the network first and then look into all the options before deciding. As we previously saw, transaction layers are the better way to go. Therefore, Arbitrum, Optimism, Starksnet, ZKSync, and to some extent Polygon (which is currently working on becoming a roll-up) are all viable options to reduce fees. They use the Ethereum layer as the security base, therefore it is reasonable to assume that the funds are safe unless a user gets scammed, the DeFi protocol used is hacked, or other such risks.

## 5.12 Conclusion

Decentralized exchanges are a way to exchange assets on the blockchain without the need to use third party intermediaries. There are several advantages and disadvantages to using them. The main types of exchanges are order book-based or AMM-based. Despite the hood being different underneath and some interface differences there is little difference from the end-user's perspective. Using cryptocurrency does carry risk and unlike a fiat transfer, there is no request that can be made if there was a mistake. Everything on the blockchain is permanent. However, immutability and transparency comes with its own advantages.