universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master 's Thesis

„Decentralized Exchanges "

verfasst von / submitted by

Rumen Lazov, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2023 / Vienna, 2023

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066 974
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Banking and Finance
Betreut von / Supervisor:	Univ-Prof. Mag. Günter Strobl, PhD

Acknowledgements

First, I want to thank my family for the chance that they have given me to be where I am today and for the continuous support over the past 5 years during Bachelor and now Master. They have inspired me to give my best and their faith in me is the thing that kept me going when times get hard.

Second, I want to thank my supervisor, Mr. Strobl, for agreeing to supervise my thesis. He was one of the very few teachers in both bachelor and master that was able to light a spark in me to read, learn and study the topics that he presented in class. Honestly, his course in Bachelor "Finance 2" was a turning point for me, as I wasn't sure what I would like to study afterwards in Master and after his course I knew where and how I want to continue my studies.

I would also like to thank all of my professors, colleagues and friends throughout these 5 years. My group of 4-6 close friends in the faculty were my constant motivation to try to be better, to even compete in a sense with them and also, they were the ones who had my back during the bad days.

Last, but not least, I would like to thank one specific professor who was able to make me understand what real hard studying means. This professor would be hard to forget, but I highly appreciate what he was able to teach me without even knowing it. Because of personal reasons I won't mention his name, only write his initials - O.A.

Abstract

Cryptocurrencies are a very new and at the same time very interesting topic for the past 4 to 6 years. Unfortunately, not a lot of people understand these new currencies, especially the technology behind them - the so called Blockchain.

This new technology is part of the rapidly growing and expanding Decentralized Finance, which enables exchanges and transactions of cryptocurrencies without the need of a third-party (for example a bank). This means that this peer-to-peer finance doesn't need a centralized authority to control or dictate how or what operations need to be executed. The main features of DeFi include easy and quick access, transparency and efficiency.

The aim of this Master thesis is to analyze and provide further information about Decentralized Exchanges, compare their concepts and properties with Centralized exchanges, as well as introduce a model about the liquidity provision in a decentralized exchange. In order everything to be as understandable as possible we will dive deep into the underlying mechanism and protocols of Decentralized Finance.

The main decentralized exchange that will be discussed in this thesis is Uniswap and it will be compared later on with the largest centralized exchange (Binance). DeFi will be further analyzed with the help of a self-made mathematical model, which will confirm the main assumptions arising from these exchanges. The mathematical model is a mixture of other models from different working papers and it mainly shows that liquidity provision on automated market makers is stable in equilibrium as well as that asymmetric information is the main cause of arbitrage opportunities. How and why my model differentiates itself from the others will be discussed in chapter 7.

My research showed that the problem with asymmetric information in decentralized markets is very severe, leading to negative profits of liquidity providers, as well as even liquidity freezes and withdrawals. DeFi, (or Automated Market Makers), in a lot of ways dominates or is similar to CeFi (Limit Order Market), but still has certain flaws. Some of the flaws can be avoided with the help of adjustments in the system or to be more specific with more convex pricing curves. The possible adjustments as well as future research topics will conclude the thesis.

Abstrakt

Kryptowährungen sind seit 4 bis 6 Jahren ein sehr neues und gleichzeitig sehr interessantes Thema. Leider verstehen nicht viele Menschen diese neuen Währungen, insbesondere die Technologie dahinter – die sogenannte Blockchain.

Diese neue Technologie ist Teil des schnell wachsenden und expandierenden Decentralized Finance, das den Austausch und die Transaktionen von Kryptowährungen ermöglicht, ohne dass ein Dritter (z. B. eine Bank) erforderlich ist. Dies bedeutet, dass diese Peer-to-Peer-Finanzierung keine zentrale Behörde benötigt, die kontrolliert oder vorschreibt, wie oder welche Vorgänge ausgeführt werden müssen. Zu den Hauptmerkmalen von DeFi gehören einfacher und schneller Zugriff, Transparenz und Effizienz.

Ziel dieser Masterarbeit ist es, dezentralisierte Märkte zu analysieren und weitere Informationen darüber bereitzustellen, ihre Konzepte und Eigenschaften mit zentralisierten Märkten zu vergleichen und ein Modell zur Liquiditätsbereitstellung in einem dezentralisierten Markt vorzustellen. Um alles so verständlich wie möglich zu machen, werden wir uns eingehend mit den zugrunde liegenden Mechanismen und Protokollen des DeFi befassen.

Der wichtigste dezentralisierte Markt, der in dieser Arbeit besprochen wird, ist Uniswap und wird später mit dem größten zentralisierten Markt (Binance) verglichen. DeFi wird mit Hilfe eines selbst erstellten mathematischen Modells weiter analysiert, das die wesentlichen Annahmen, die sich aus diesen Märkten ergeben, bestätigen wird. Das mathematische Modell ist eine Mischung aus anderen Modellen aus verschiedenen Arbeitspapieren und zeigt hauptsächlich, dass die Liquiditätsbereitstellung auf Automatisierten Market Makern im Gleichgewicht stabil ist und dass asymmetrische Informationen die Hauptursache für Arbitragemöglichkeiten sind. Wie und warum sich mein Modell von den anderen unterscheidet, wird in Kapitel 7 besprochen.

Meine Untersuchungen haben gezeigt, dass das Problem mit asymmetrischen Informationen in dezentralisierten Märkten sehr schwerwiegend ist und zu negativen Gewinnen der Liquiditätsanbieter sowie sogar zum Einfrieren und Abheben der Liquidität führt. DeFi (oder Automatisierte Market Maker) dominiert in vielerlei Hinsicht CeFi (Limit Order Market) oder ähnelt diesem, weist aber dennoch gewisse Mängel auf. Einige der Mängel können durch Anpassungen im System, genauer gesagt durch konvexere Preiskurven, vermieden werden. Die möglichen Anpassungen sowie zukünftige Forschungsthemen werden den Abschluss der Arbeit bilden.

Abbreviations

AMM… Automated Market Maker

BTC… Bitcoin

CeFi… Centralized Finance

CEX… Centralized Exchanges

CPMM… Constant Product Market Maker

Dapps… Decentralized Applications

DeFi… Decentralized Finance

DEX… Decentralized Exchanges

ERC20

ETH… Ethereum

LOM… Limit Order Market

LP… Liquidity Provider

LS… Liquidity Supply

PoW… Proof-of-Work

PoS… Proof-of-Stake

STBC… Stablecoin

USDT

WETH

Table of contents

1. Introduction

The rapid growth of cryptocurrencies during the last few years is the main factor for the emergence of new and different kinds of international financial exchanges, leading to the development of the so-called decentralized exchanges. The total market capitalization of cryptocurrencies in 2021 peaked at $2.9 trillion[1]. This led unfortunately to many speculations, scams, as well as attacks on some exchanges, because of which the total market capitalization on the cryptocurrency market fell down to only $798 billion by the end of 2022.

The new financial system called decentralized finance (DeFi) is built on safe distributed ledgers[2] that are comparable to those used by cryptocurrencies. DeFi does not rely on intermediaries and integrated institutions. Instead, so called DApps[3] which have open protocols are used to run the blockchain and handle the transactions. Example for DApps are automated market makers (which will be discussed and analyzed later on in detail) as well as price oracles[4]. The most crucial and important application in DeFi are the smart contracts. They are used to enforce agreements and the execution of the transactions is deterministic and secure. (Lehar, A., and C. Parlour, 2021) Afterwards all changes and transactions are saved on the blockchain and are publicly observable. Money is saved on digital wallets and individuals can transfer funds in a couple of minutes. The only thing that is required in order to use DeFi and transfer funds is internet connection. In contrast to centralized finance, DeFi doesn't impose fees because of the use of its services like banks, rather than that fees are paid out to miners[5] as part of the transaction so that orders (transactions) are executed correctly. Further details about the miners will be provided later on in the chapters to follow.

1.1 Motivation

As a former student of the University of Vienna studying Business Administration in Bachelor and now Banking and Finance in Master, the topics related to new concepts or technologies in the banking and finance world were always of great interest to me. Almost everyone nowadays knows or has heard of cryptocurrencies, or more specifically Bitcoin and Ethereum.

[1] See more: https://www.statista.com/statistics/730876/cryptocurrency-maket-value/
[2] See more: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
[3] See more: https://www.bitpanda.com/academy/en/lessons/what-is-a-dapp
[4] See more: https://docs.uniswap.org/contracts/v2/concepts/core-concepts/oracles#:~:text=A%20price%20oracle%20is%20any,phone%20as%20a%20price%20oracle.
[5] See more: https://www.coinbase.com/de/learn/crypto-basics/what-is-mining

Since the rapid growth in 2020 as well as 2021 these new digital currencies and the technology behind them were introduced in lectures and Blockchain was one of the things that took my attention at the very first moment. This has led to an ongoing research about the topic for the last 2 years, collecting information and data, as well as even investing small amounts in these exchanges for a better understanding how the whole system works.

As there is a lot of literature on the cryptocurrencies, there hasn't been a lot of research on the blockchain and whether or not these new exchanges are safe and if not – how and when do problems arise and how they can be solved. This thesis aims not only to further analyze and compare centralized and decentralized finance, but to also represent a model that shows how the system operates, where are its strengths and weaknesses.

1.2 Research Results

As already mentioned earlier the thesis compares centralized and decentralized exchanges, then focuses explicitly on automated market markets (more specifically on the liquidity provision), implementing a mathematical model showing the following results:

- Trading volume of an informed trader is proportional to the aggregate size of the liquidity pool
- If there are no fees informed traders can always extract profits from the liquidity suppliers (frontrunning arbitrage)
- When no fees are taken into consideration, liquidity providers extract profits only if a noise trader takes part in the exchange (noise traders trade because of non-fundamental reasons
- Liquidity provision in equilibrium is stable

1.3 Structure

The structure of the thesis is made in a very simple, systematic and understandable way so that even readers without theoretical background in the topic should be able do understand the underlying concepts and mechanisms.

The thesis will begin with a brief introduction of the topic, followed by a technical background of Blockchain and the infrastructure behind decentralized finance. Afterwards, a literature review will be provided which will give readers information about previous researches related to the topic. Next, Uniswap[6] will be analyzed in detail and it will be the starting point of a deep research and comparison of AMM and LOM. Furthermore, examples about liquidity

[6] Uniswap is the biggest decentralized exchange up to date. See https://v2.info.uniswap.org/home

provision, liquidity freezes, price impact and arbitrage opportunities will be introduced and discussed, followed by the main model of the thesis which will showcase step by step the research results written earlier. The future implications of DeFi as well as future research topics will conclude the thesis.

2. Background

The main purpose of this chapter is to familiarize the reader more closely with the theoretical and technical part of the topic so that the upcoming chapters can be better understood. The chapter will begin with a brief introduction of traditional finance before cryptocurrencies, as well as pointing out some key limitations and disadvantages of traditional finance institutions. Afterwards, cryptocurrencies will be briefly explained, followed by a differentiation between the two main Blockchain systems. The Infrastructure of DeFi will play a crucial part in this chapter as almost everything that readers need to know about the Ethereum Blockchain will be explained and will be useful for the better understanding of future chapters. Decentralized Exchanges (DEXs) will conclude this chapter and will serve as a starting point for chapter 4 when talking about Uniswap.

2.1 Traditional Finance

For thousands of years, people have traded or bought goods through some form of currency. The most basic, known and standard way to buy goods is via cash transaction.

2.1.1 Cash Transactions

Usually a coin or a note represents cash. During the cash transaction an object and its unit of value are exchanged and transferred.

Figure 1: Cash Transaction

https://www.dreamstime.com/hand-holding-money-hand-banknotes-cash-payment-receiving-money-icon-hand-holding-money-hand-banknotes-cash-payment-image115680589

Important to note in this case is that during this kind of transaction there is no third-party involved to control whether or not the transaction was properly executed. But in order for a cash transaction to take place both parties need to be at the same location at the same time. In the modern world that we live in this imposes a significant problem and has led to the implemenation of digital currency and electronic payments.

2.1.2 Electronic Payments

The ideal payment system would involve electronic money transfers using currency data files. These data files will still be seen as physical cash; they retain its benefits, but they could move freely across electronic networks. The following picture represents in a very simple way how most of the transactions today are executed. A buyer goes on the internet and buys himself a good. He/She transfers money and waits for the order to be delivered.

Figure 2: Electronic Transaction

https://www.passion-entrepreneur.com/604-e-commerce.html

It may seem easy and trouble-free, but digital cash can lead to the so called "double spending problem"[7]. Basically the cash files that we talked about can be copied as much as you want for a very low cost and this feauture is highly undesired for money. This is where financial instituions take over.

2.1.3 Central Authority

In order to mitigate the risk of the double spending problem banks operate as a financial inter-mediary during the transaction, assuring that the deal goes as planned and that the money is not double spent. This is what we call a Centralized Financial System[8]. In such systems banks and other third parties hold the funds and enable the transfer of funds between parties and banks charge fees for the execution of transfers. Very important thing to add to this segment

[7] https://www.bitpanda.com/academy/en/lessons/what-is-double-spending-and-why-is-it-such-a-problem/
[8] https://www.investopedia.com/decentralized-finance-defi-5113835

and for the future of the thesis is that Cryptocurrencies can also be traded through centralized institutions, not only through decentralized exchanges.

2.2 Limitations and disadvantages of traditional finance

We live in a centralized world where banks and governments are the main and core factors for money supply. Since banks exist they have monitored and structured transactions that would otherwise have too much transaction costs. But, every system has its limitations and risks. My research shows that CeFi has five key limitations:

1. Centralized control

2. Limited access

3. Inefficiency

4. Lack of interoperability

5. Non-transparency

Arguably, the biggest limitation of CeFi is the non-transparency. Customers of banks don't actually know how healthy their bank is and don't have enough information to make optimal financial choices. For example, people don't know whether or not a given interest rate on a loan is reasonable.

As already said, costs incurred through traditional finance can be very high. For example, if you wish to transfer money from a bank account in Bulgaria to a bank account in Austria you will get a fee for this transaction that amounts to around 10 Euros. Of course, it depends from which and to which country you want to transfer funds, but most of the banks will charge between $15 and $30 for the execution of an international transfer.

Banks need to be certified from the central bank and identified by the government. Banking services are limited in some countries which lead to geographical limitations. This results not only because of the high fees when sending funds internationally, but also because some transactions need days or even weeks until they are executed.

Another limitation of the centralized financial system is the long processing time of transactions. For many transactions people still go or are obliged to go to intermediaries, which makes the process slower compared to DeFi. This is specifically the case when moving/sending big amounts of capital internationally.

Other limitations of centralized finance include the low interest rate[9] in recent years that the banks are imposing as well as inefficiencies because of difficulty to conduct small operations and security.

As can be seen, traditional finance institutions are imposed to a lot of risks and limitations. Because of the imperfections of the system, new forms of currencies as well as systems have been developed in recent years to decrease the risks mentioned above and to improve the way transactions are executed. Very important to notice in these new systems is that they don't rely on financial intermediaries (third-parties) to execute or control transactions. The new form of currency that is going to be discussed in the following chapters and subchapters are the cryptocurrencies.

2.3 Cryptocurrencies

Cryptocurrencies are a new type of digital currency which uses cryptography[10] to secure transactions (Harvey, Campbell R., Cryptofinance (January 14, 2016). The name "cryptocurrency" was given because this new form of payment system uses a so-called encryption with which transactions are verified. They use a decentralized system where a record of all transactions is being stored and where new transactions are being issued. A public ledger keeps track of all transactions that involve money transfers. The public ledger is called Blockchain. Decentralized means that no one has control over the ledger and that everyone can inspect, share and trust it.

A digital payment system known as cryptocurrency doesn't rely on banks to validate transactions. Peer-to-peer technology[11] makes it possible for anybody, anywhere, to transfer and receive payments. Payments made using cryptocurrencies do not exist as actual physical coins that can be transported and exchanged; rather, they only exist as virtual inputs to an electronic database that detail individual transactions. Cryptocurrencies are stored in digital wallets and in order to transfer data from wallets to public ledgers or the other way around really complex and advanced coding is needed.

Owning cryptocurrency doesn't mean that you own something tangible. You only have a so-called private key with the help of which you can move or transfer a unit of a certain currency from one wallet to another It may seem easy and trouble-free, but digital cash can lead to the

[9] Interest rates have been either negative or around 0 for the last 2 years. As the thesis is conducted the rates have risen to 3,75%.
[10] https://www.techtarget.com/searchsecurity/definition/cryptography
[11] https://www.blockchain-council.org/blockchain/blockchain-role-of-p2p-network/

so called “double spending problem”[12]. Basically the cash files that we talked about can be copied as much as you want for a very low cost and this feauture is highly undesired for money. This is where financial instituions take over.

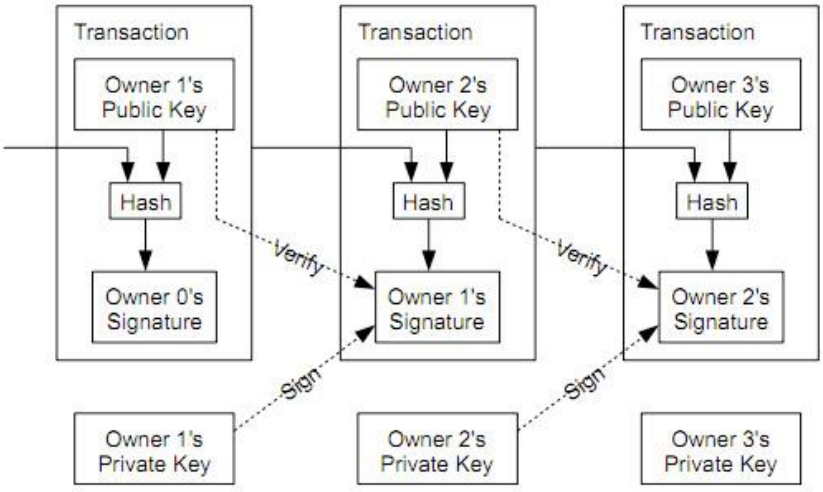
The main underlying mechanism of DeFi is Blockchain. With the help of smart contracts and other decentralized applications transactions are executed and stored on the publicly available ledger (Capponi, Agostino, and Ruizhe Jia, 2021). In the following subchapters we will break down the most important components in this new system and provide a comparison between the Bitcoin and Ethereum Blockchain.

2.4 Blockchain

Blockchain was founded and introduced by Satoshi Nakamoto (see Nakamoto, Satoshi, “Bitcoin: A peer-to-peer electronic cash system,” 2008) back in 2008 and its aim was to serve as a public distributed ledger specifically for Bitcoin transactions. The first cryptocurrency that implemented Blockchain was Bitcoin and this was also the first ever crypto to overcome the double-spending problem mentioned earlier. The Bitcoin Blockchain will therefore as an example in the following subchapters for a better understanding of the underlying mechanisms.

2.4.1 Structure

When someone wants to send cryptocurrency to another person, they create a transaction which contains important information such as the amount of cryptocurrency being sent, the recipient's public address, and a digital signature from the sender that proves the transaction is valid.



[12] https://www.bitpanda.com/academy/en/lessons/what-is-double-spending-and-why-is-it-such-a-problem/

Figure 3: Transaction on the Blockchain

https://bitcoin.stackexchange.com/questions/10279/explainations-about-chaining-of-transactions

As a transaction is generated, it is broadcast to the whole blockchain network of computers, called nodes (Catalini, Christian and Gans, Joshua S., Some Simple Economics of the Blockchain (April 20, 2019)). Nodes work together and validate transactions. When the validation over is the transactions are added to the public ledger with all previous transactions. The whole process of validating nodes and blocks is called mining[13]. A transaction that has been uploaded to the blockchain cannot be changed, erased, or reversed. This assures that all blockchain transactions are visible, safe, and tamper-proof (Lehar, Alfred and Parlour, Christine A., March 22, 2020).

The essential building components of a blockchain are called blocks. They include transaction information such as the sender, receiver, and amount, as well as a unique digital signature. Each block in the chain contains a cryptographic hash of the preceding block in the chain, resulting in a secure and tamper-proof record of all transactions in chronological sequence. After a block has been validated and added to the blockchain, it cannot be changed or removed, making it a permanent and immutable record of all transactions.

Once the transaction is created, it is broadcast to the entire network of computers or nodes on the blockchain. These nodes, using a process called mining, then work to validate the transaction and add it to the ledger of all previous transactions. A transaction cannot be changed, removed, or reversed after it has been added to the blockchain. This makes sure that the transactions on the blockchain are safe and visible to everyone.

A peer-to-peer network and a distributed data disclosed server are used to operate a blockchain database independently, followed by the validation which is conducted from a collaboration of users who are motivated by their self-interest (De Filippi, Primavera, The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies (September 14, 2016). With the help of Blockchain the double spending problem cannot arise because it controls and verifies each transaction. This means that the system cannot approve a unit of value that has been already transmitted, resulting in the solution of the problem before.

[13] Mining is the process which validates new transactions on the Blockchain and during the process it is said that miners mine new Bitcoins because of the fees that they receive from assuring that the transaction is conducted successfully.

2.4.2 Blocks

Blocks are the basic units that make up a blockchain. They contain information about transactions, such as the sender, receiver, and amount, as well as a unique digital signature. Each block contains a cryptographic hash of the previous block in the chain, which creates a secure and tamper-proof record of all the transactions in chronological order (Schär, Fabian, April, 2021). Miners compete to add new blocks to the blockchain by solving complex mathematical puzzles, which also helps to protect the network against fraud and double-spending. Once a block is verified and added to the blockchain, it cannot be altered or deleted, making it a permanent and immutable ledger of all transactional history.
Sometimes blocks can be in competition which results in a so-called fork. In addition to a secure hash-based history, every blockchain features a predefined method for scoring distinct versions of the history so that the one with the highest score can be chosen above others (Taskinsoy, John, October, 2019). Not all blocks are included in the chain. The blocks that were left behind and not chosen are called orphan blocks.

Peers who support the database have access to different copies of the history on the blockchain at different times. In the end only one version with previous history can be included into the chain and this will be the highest scoring version. The process is the following: A peer receives the previous version, but with an additional block. If this is the highest scoring version, he then rewrites his own database and transmits the new information and chain to the other peers.

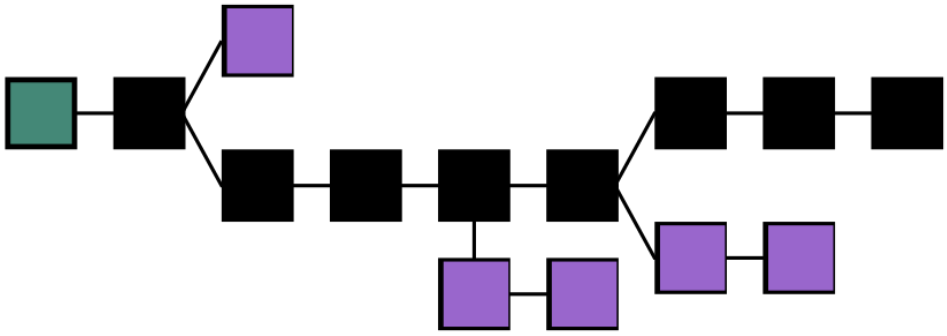


Figure 4: Blocks on the Blockchain

https://commons.wikimedia.org/w/index.php?curid=16043262

On the figure above, we can see a representation of a Blockchain. The green block on the left side is called the genesis block and it is the very first block in the chain. The purple blocks illustrate orphan blocks which were not selected for inclusion and exist out of the main chain.

Black blocks represent the main chain. Only one chain during the whole process can be the right one and this is the longest chain of blocks since the genesis block.

After everything said about the blockchain arises the question who actually verifies these transactions. As we already know in the centralized world this is done by intermediaries for example, but in the decentralized world this is done by Miners.

2.4.3 Mining

Miners are participants on the blockchain and compete against each other to update the ledger (Lehar, Alfred and Parlour, Christine A., March 22, 2020). The reason behind this competition is that they get compensation from verifying transactions. When you send money from your wallet to another wallet you will incur a small transaction fees[14] which is actually the miner's reward from verifying the order.

Mining doesn't only mean to verify the legitimacy of transactions. Because of the work that miners do it is said that they actually mine for example new Bitcoins during the whole process. This is their reward for updating the blockchain. Basically everyone can become a miner, you just need to download the software and install the latest version of the Bitcoin blockchain. Unfortunately, this is not as easy as it seems.

In order to become a miner and to actually get rewarded for your work you will need a lot of computer power, because there exist so called mining farms[15], where they have thousands of powerful machines as well as access to very cheap electricity. Competition is very high and the resources that you need to spend are enormous.

In the following subchapter the blockchain of Ethereum will be explained and compared with the Bitcoin blockchain. As already said in the very beginning the Ethereum Blockchain will be the main focus of the thesis.

2.5 Ethereum Blockchain

In 2015 Ethereum[16] launched its first platform and created its Genesis Block. Since then, the Ethereum platform is a place for creating decentralized applications, businesses, trading and

[14] The transaction fees for the validation depend on the transaction itself. In some cases traders can also reward the miners with a higher fee so that their transaction gets executed first. This is because miners operate on the first come first serve principle.
[15] It was said that around 60% of all mining farms were located in China before a couple of years, but after some regulatory changes in the country most of the mining farms are now located in the US.
[16] See https://ethereum.org/de/

communication. You retain control over your own data and what is shared, so using Ethereum doesn't need you to give up all of your personal information. Ether, the coin utilized by Ethereum, is used to pay for certain operations on the Ethereum network.

With some significant distinctions, Ethereum was introduced in 2015 and builds on Bitcoin's innovation. Both allow you to use digital currency without banks or payment processors. On the other hand, since Ethereum is programmable, you may create and run DApps on its platform. The result of this is a blockchain that can be programmed and used for anything.

The platform itself as well as Ethereum don’t really have restriction on what they can achieve. The main idea of the platform was and still is to support innovation. Opposed to Bitcoin which can be seen as a payment network, Ethereum can serve as a market place for services, smart contracts, apps as well as even games. The most important part of it is that nobody can censor you.

2.5.1 DApps

Decentralized applications or shorter DApps are used and developed on the Ethereum platform. They use smart contracts to execute orders, then save the data on the Ethereum Blockchain.

Digital apps and programs known as "decentralized applications" (DApps) exist and operate on a peer-to-peer (P2P) computing network or on a Blockchain rather than a single computer (Brummer, Christopher J., March 24, 2022). Thus, they are independent of all other authorities' jurisdiction and supervision.

Applications like Uber, Instagram or Twitter operate on computer systems which are owned by a company and this computer systems allows them to control how the app functions. On one side, there may be a number of users, but only one company has authority over the backend. In comparison decentralized applications are open-sourced application which function in a decentralized environment and cannot be controlled from a single entity.[17]. For instance, a developer may build a blockchain-based Twitter-like decentralized application (DApp) that allows any user to broadcast messages. As for all transactions, messages also cannot be deleted, as they are stored on the Blockchain and cannot be erased.

[17] See more: https://www.bitpanda.com/academy/en/lessons/what-is-a-dapp

DApps are the tools used to remove third-parties or middlemen from a range of activities. They even include different kinds of games, interactions as well as maybe the most important thing – self-executing contracts. One can basically use Dapps for almost everything, including using them as plugins for showing adverts, they can collect crypto donations and many more functions depending on your needs. The purpose of Dapps is to serve as a protective mechanism that can protect users and ensure a safe system.

Decentralized applications can have different kinds of purposes:

- Act as a supporting tool in peer-to-peer transactions for example like currency exchanges

- Tracking tool for goods which can increase safety and transparency in the supply chain management

- To verify or store identity information or to even serve as application for passports or voting systems

- Track property ownership, store documentation and facilitate deals between buyers and sellers without the need of a third-party.

- Store information about healthcare records; increase communication between healthcare professionals and assure cooperation between

- Serve as a digital learning platform, which would've been an optimal idea during the pandemic in the last 2-3 years. It would stimulate students and make the interaction between them and their teachers more interesting.

2.5.2 Smart contracts

Smart contracts are essentially programs that run when certain criteria are satisfied and are recorded on a blockchain (Schilling, Linda and Harald Uhlig, 2019).
They provide Ethereum a lot of flexibility and set it apart from other cryptocurrencies. They are often used to automate the implementation of a contract to ensure that all participants would achieve the desired outcome without tan intermediary monitoring the whole process.

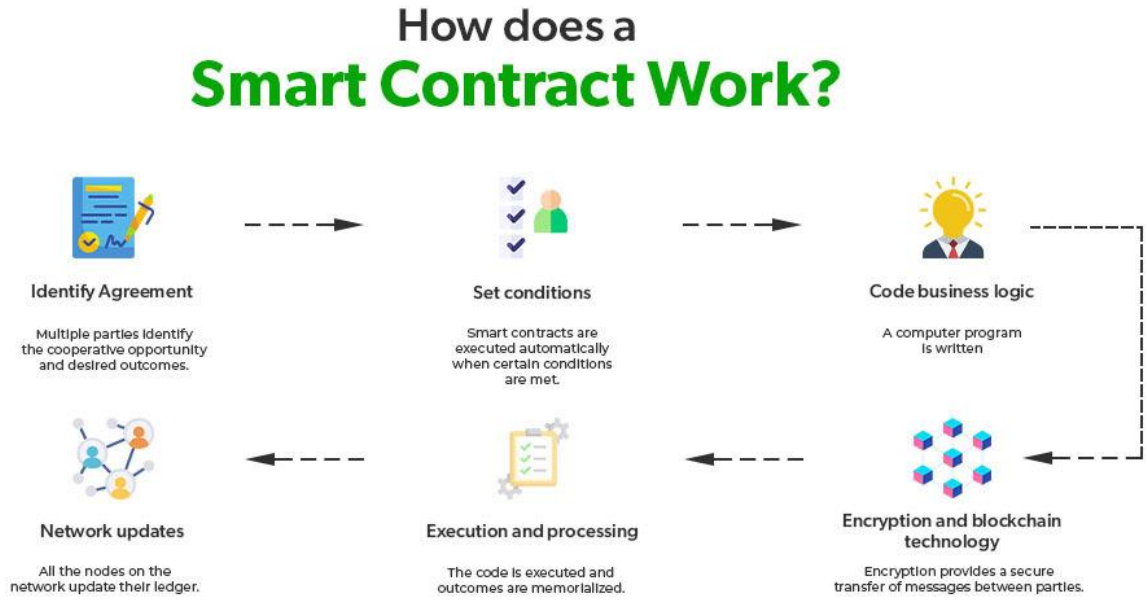


Figure 5: Smart contract mechanism

https://www.geeksforgeeks.org/smart-contracts-in-blockchain/

Smart contracts work by the principle of if/when…then… statements, which are written in a code on the Blockchain (Lehar, A., and C. Parlour., Decentralized exchanges (2021). Preset specifications need to be met and validated before the system conducts the trade or activity. These specifications or activities might include transferring payments to the certain parties, providing notifications or even the registration of a new vehicle. After every single transaction the blockchain is updated. This implies that the transaction cannot be modified, and that the results are only visible to authorized people.

Smart contracts can be conducted in various ways as well as have all thinkable specifications. This makes the platform a very attractive way for users to feel safe and to make sure that the tasks, agreements or anything else is executed in the right time and in the right way. Participants have to determine and establish how their data are going to be represented on the ledger when completing the transaction. This is very important because programmed terms cannot be amended after the smart contract starts to execute the order.

Smart contracts are the real reason behind the benefits of Decentralized Finance. These benefits include:

1. Speed and efficiency – once the smart contract and its conditions are set, the execution of it happens immediately. This includes as well the removal of fees and time delays that occur in financial intermediaries.

2. Transparency – there is no doubt about the information shared around the participants because the encrypted records are stored and visible to everyone.

3. Security – Transactions on the blockchain are very hard to hack. Earlier we said that every single block has the information of the previous one which would mean that a potential hacker needs to alter the whole chain in order to hack a single record. This is not only time consuming, but also very hard and not optimal, because miners are competing with each other to validate the transaction.

Smart contracts can also be used in traditional finance, not only in the blockchain system. The parties in the transaction agree on an "oracle" which is basically external information that will update the main information on the Blockchain and verify whether or not the agreement is fulfilled. If the agreement is not fulfilled the oracle will take on its own appropriate actions.

Smart contracts can be without a doubt very useful and helpful in traditional finance. For example, a deal between two parties that haven't conducted business with each other before and aren't living in the same country can eliminate the risk of adverse selection and high fees by using a smart contract that will serve as a guaranty that everyone becomes their part of the deal in the end.

As there are plenty of benefits involved in smart contracts, there are also a couple of limitations and challenges associated with them. Firstly, there is a lack of regulations concerning blockchain and all of its components. Secondly, they are very hard to implement. These are fairly new concepts and mechanisms which are still researched and it will take time until they are fully understood, but are definitely something to watch for. Lastly, smart contracts cannot be changed. Once the smart contract is up and running no changes can be made, which means that a new contract will always be added to the Blockchain no matter what.

2.5.3 Oracles

Oracles are apps that collect, validate, and communicate external data (off-chain data) to smart contracts operating on the blockchain (Angeris, Guillermo, and Tarun Chitra, 2021).

Oracles can not only get off-chain data and publish it on Ethereum, but they can also "push" information from the blockchain to other systems.

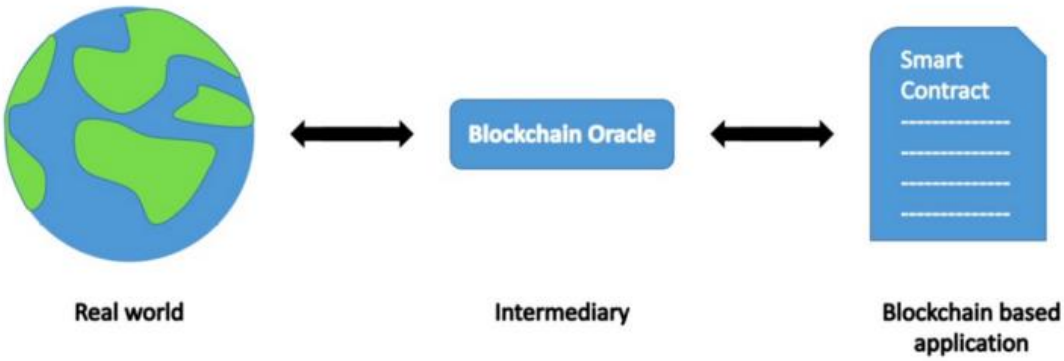


Figure 6: Oracles

https://academy.moralis.io/blog/explaining-oracles-what-are-blockchain-oracles

Oracles can be defined as bridges between smart contracts on the blockchain and the off-chain data sources. They are mechanisms with which a smart contract with off-chain data can be executed. Smart contracts can only access data that is on the chain, without oracles they can never access off-chain information.

Oracles can differ depending on the data that we obtain, models and system architecture. To be more precise oracles can be from one or multiple data sources, they can be centralized or decentralized as well as immediate-read, publish-subscribe or request-response (Egberts, Alexander, The Oracle Problem - An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems (December 12, 2017). One can divide oracles into three main groups - input oracles, output oracles and computational oracles. Input oracles extract external information used by smart contracts on the blockchain. Output oracles transfer information from the blockchain to external applications ad computational oracles are basically oracles that execute off-chain computations (Abdeljalil Beniiche, A study of Blockchain Oracles, 2020).

Oracles are important for the system because Ethereum is a deterministic system, but external information or agreements between people aren't always straightforward[18]. In order for blockchains to have deterministic executions, they constrain nodes to obtain consensus based

[18] See more: https://ethereum.org/en/developers/docs/oracles/

on basic binary questions like true or false using the data that is already stored on the block-chain.

Determinism is the most important and critical thing in Ethereum. Thousands of nodes process transactions all around the world and in they should end up with the same results after the same transactions. As Ethereum doesn't have a centralized authority to rely on whether or not given information is true or not, in the case where two different nodes execute the same contract but have different result would break the consensus mechanism and Ethereum will have no more value as a decentralized system.

2.5.4 Stablecoins

Stablecoins are nothing else but digital money with fixed value. These coins are asset-backed cryptocurrencies pegged to a currency like the US Dollar which means that their value is constant and not volatile in regards to standard cryptocurrencies (Harvey, Campbell R. and Abou Zeid, Tarek and Draaisma, Teun and Luk, Martin and Neville, Henry and Rzym, Andre and van Hemert, Otto, September 1, 2022). Even if Ethereum's price changes it wouldn't affect the price of stablecoins.

The aim of stablecoins is to serve as an alternative to the highly volatile cryptocurrencies, for example like Bitcoin. Bitcoin's price in early 2020 was around $5,000 and in April 2021 the price had gone up to the record breaking $63,000. Afterwards the price kept falling drastically down and then going up again and at the moment that this thesis is written the price of Bitcoin is around $23,000. Although this volatility is somewhat beneficial for traders it prevents the normal execution of transactions as the volatility makes them into risky speculations for both buyers and sellers. Clearly, nobody wants to make a loss after a transaction that results in a sudden price drop after some time.

One of the most famous and iconic stories dates back to 2010 when one night a dad wanted to buy himself and his daughter two pizzas[19]. The price that he needed to pay for both pizzas was around $40 and the asked on the phone if it's possible to pay with bitcoin. He offered 10.000 Bitcoin for both pizzas because that much bitcoin amounted to $40 at that time. In today's market this amounts to hundreds of millions of dollars. Of course, at that time Bitcoin hadn't the same value as today and not a lot of people even knew that this cryptocurrency

[19] See more: https://www.investopedia.com/news/bitcoin-pizza-day-celebrating-20-million-pizza-order/

existed. There are a lot of other similar cases and people have regretted their decision and that's why stablecoins were invented so that a person can enjoy his pizza and save his Ethereum.

A way to perfectly describe what stablecoins are and what their meaning in the cryptocurrency world is are the following sub points:

- Stable value – you can redeem one USD Coin for one US dollar.
- Backed by fully reserved assets
- Powered by Ethereum
- Global Exchanges

Stable coins can be forged and used in a very simple way – you have to open up an account at coin base, convert one US dollar into one USD Coin and then you can start trading globally. There are no fees included in the conversion and you can convert your USD Coin back into US dollars whenever you want.

In recent years the demand for stablecoins has increased by a lot. They are global and the only thing that you need in order to send and receive stablecoins all around the world is an Ethereum account and a wallet. In the following picture we can see the market capitalization of the top stablecoins at the time this thesis is written:

CURRENCY	MARKET CAPITALIZATION	COLLATERAL TYPE
Tether	$68,300,366,088	Fiat
USD Coin	$41,856,486,392	Fiat
Binance USD	$16,261,967,304	Fiat
Dai	$5,100,006,140	Crypto
Frax	$1,021,237,198	Algorithmic
TrueUSD	$949,252,423	Fiat
Pax Dollar	$930,622,139	Fiat
Gemini Dollar	$572,408,927	Fiat

Figure 7: Top Stablecoins at the moment the thesis is conducted

https://ethereum.org/en/stablecoins/#main-content

As we can see from the picture the highest market capitalization coins are Tether, USD Coin, Binance USD and Dai. In the empirical analysis the USD Coin will play an important role in understanding the difference between centralized and decentralized exchange platforms.

In general, there are 4 types[20] of stablecoins depending on their collateral:

- Fiat backed – this is the most known and basic type, you simply purchase a stablecoin with your fiat currency usually a US dollar and later you can cash it in and redeem money in your currency. The shortcoming of this type is that it is entirely centralized because tokens are issued by people and that it needs auditing in order to ensure companies that they have enough reserves.
- Crypto backed – these stablecoins are backed by other cryptocurrencies like Ethereum and their price highly depends on the value of the underlying asset. This can be very volatile as the value of Ethereum and other cryptocurrencies fluctuate and as we said earlier these coins have and must have a stable price. In order to mitigate this risk from the arising fluctuations and ensure stable prices these coins are overcollateralized. Example: A crypto backed stablecoin worth 1 US dollar has an underlying crypto asset worth at least $2. This means that if the price of Ethereum goes down, you have to use more Eth to back the stablecoin, otherwise it will lose its value. The shortcoming of this type of stablecoins is that it's less stable than fiat-backed coins and that you need to monitor the value of the crypto collateral.
- Algorithmic – probably one of the most interesting stablecoins because there is no collateral needed. In other words, these coins are not asset-backed. The way that it functions is the following: an algorithm sells coins when the price get down to a certain level and the same algorithm buys tokens when the price is higher than a certain level. This means that the number of coins in the system changes all of the time, which also means that the number of coins that you own will also change. This isn't particularly a bad thing because the share that you have will still be the same.
- Precious metals – these coins are the same as the fiat backed stablecoins, but in this case they use precious metals like gold for example in order to maintain their value. These stablecoins are considered to be very safe and to not have almost any volatility.

There are many ways to get stablecoins. One way would be using a swap. As most decentralized exchanges function this way, you can swap your token for a stablecoin. A second way

[20] Stablecoins: https://ethereum.org/de/stablecoins/

would be to directly buy stablecoins, either from centralized exchanges like Binance or from decentralized exchanges like Uniswap, which will be our main discussion topic in the chapters that will follow. A third way would be by earning stablecoins. As many decentralized applications use stablecoins you can actually work on projects that are part of the Ethereum network and you will be rewarded with stablecoins. Another way to get stablecoins is by borrowing. In this case you will have to offer crypto as collateral, but you have to pay it back afterwards.

Because of the high demand for borrowing of stablecoins, they also have a quite good interest rate. Stablecoins can be deposited into lending pools where agents will earn interest. It is the same like in the real world - you offer/deposit stablecoins and you can withdraw your interest or coins at any time. In the following subchapter we will look more closely at the main underlying consensus mechanisms of blockchain and make a comparison between them.

2.6 Proof of work vs. proof of stake

The most known characteristic of cryptocurrencies is that they are decentralized. Because of the fact that there is no central authority transactions need to be verified with the use of nodes and underlying mechanisms that we already talked about. There are two main ways that crypto transactions can get verified. The first one is via proof of work (PoW) and the second way is via proof of stake (PoS).

2.6.1 Proof of work

Proof of work exists since the very beginning of blockchain. This is why it is not a surprise that Bitcoin was the first and main cryptocurrency that uses this network for verification. In a network like that all nodes/computers in the network compete with each other so that they add a transaction on the blockchain which would yield them Bitcoin in return.

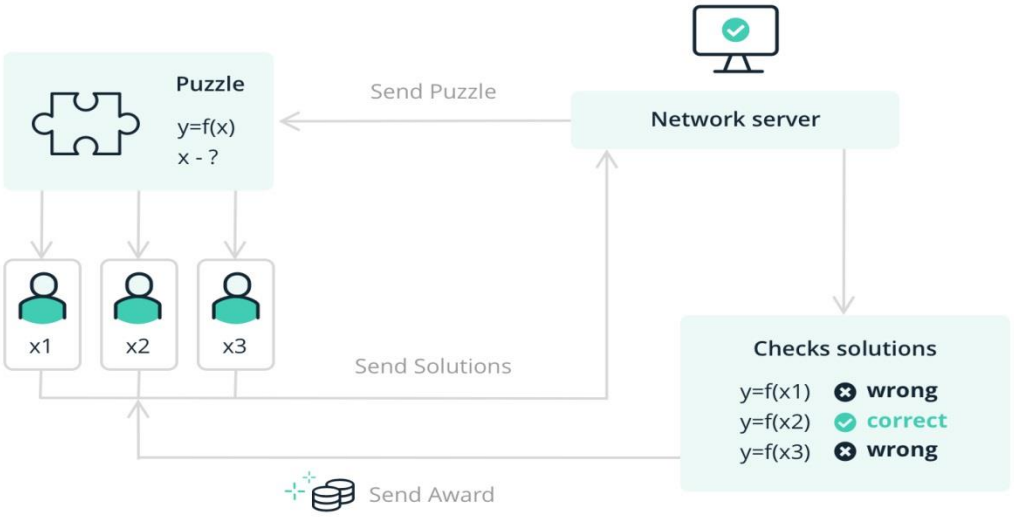


Figure 8: Proof of Work mechanism

https://www.ledger.com/de/academy/blockchain/was-ist-proof-of-work

PoW requires an increasingly large amount of energy which makes it also really difficult for someone to double-spend crypto. The high usage of energy is also one of the biggest problems concerning Bitcoin in recent years because people are concerned about the environment. The system gets bigger and bigger and in order for the network to function correctly even more power is needed.

Although this network consumes a lot of energy it can be said that PoW is a more decentralized and open system than proof of stake because it is based on competition between miners. On the other hand, because of the high-power usage transactions are also slower. For example, one Bitcoin transaction is completed in around one hour.

2.6.2 Proof of stake

Proof of stake is another consensus mechanism to validate entries into a blockchain and to ensure that the database is safe. PoS is an alternative to PoW and is less risky when talking about network attacks. In a lot of ways this new mechanism dominates the old one, in the sense that miners need to solve cryptographic puzzles in the proof of work system and in proof of stake validators are required to stake their tokens hoping to earn transaction fees.

The improvements of PoS include:

- Energy efficiency
- Lower hardware requirements leading to low entry barriers
- Lower chances of attacks on the system
- Better security because more nodes secure the network

PoS is a mechanism that doesn't need a lot of computational power because blocks on the blockchain are validated using the machines of coin holders. Owners of coins stake their coins as collateral so that they can have a chance to validate blocks and later on to become validators.

Figure 9: Proof of Stake mechanism

https://www.ledger.com/de/academy/was-ist-proof-of-stake

The confirmation and validation of data and transactions is done by validators who are chosen at random. Unlike PoW this new system randomizes who will receive fees from the validation process. As already said, coin holders have to stake a certain amount of coins which in Ethereum for example is 32 ETH. After the amount is staked a person can participate in the process as a validator. In order for a block to be finalized it needs to be validated by more than one validator, otherwise it cannot be closed. For example, Ethereum has a so called "sharding" which means that a validator will add the verified transaction to a shard block. This shard block needs to be then verified by at least 128 validators in order to be finalized.

We can say that both PoS and PoW are very similar consensus mechanisms because both of them validate information and transactions and because each of them is able to maintain the blockchain, but their approaches are very different.

2.7 Power consumption

A technology like blockchain is naturally attached to very big power consumption. This was and still is a major problem associated to the mining of cryptocurrencies and execution of transactions because of its negative impacts on nature. Some of the cryptocurrencies and to be more specific Bitcoin and Ethereum are said to consume more energy than whole countries. For example, Bitcoin is said to consume so much energy that it exceeds the annual energy consumption of a country like Norway[21].

As already explained, in order to keep a proof of work system up and running requires increasingly high energy consumption. Because of that, cryptocurrencies were and still are subjects to massive accusations and critics. Of course, reducing or changing the way such a system works is not an easy task, but Ethereum was able to it.

On the 15th of September last year Ethereum was able to transition from a PoW to a PoS consensus mechanism. This marked the biggest upgrade in the crypto world since the existence of blockchain. The upgrade of Ethereum was called “The Merge”.

2.8 The Merge

Without a doubt the biggest upgrade related to cryptocurrencies happened in September, 2022. Not only was the transition planned for many years before that, but the possible outcomes were also shared with the public. The upgrade transitioned Eth to a proof of stake mechanism (Kapengut, Elie and Mizrach, Bruce, February 25, 2023).

The Merge[22] was an event that everyone more familiar with Ethereum was waiting for the past couple of years. The biggest and most important part of the upgrade is that it was able to reduce Ethereum’s required energy consumption to the mind-blowing 99.95%, which created a safer network imposing significantly lower carbon costs.

[21] See more: https://www.cepsa.com/en/planet-energy/sustainable-innovation/the-high-energy-cost-of-cryptocurrencies#:~:text=The%20most%20famous%20of%20the,pressure%20on%20the%20power%20grid.
[22] See more: https://ethereum.org/en/roadmap/merge/

The update represented the merge between Ethereum's original execution mechanism Mainnet which was part of Eth since the very beginning with a PoS execution mechanism called Beacon Chain. The network became more stable and safer, and eliminated the need for intensive mining and energy consumption. This upgrade was an innovation to the crypto world which imposed more sustainability, safety and scalability. The vision of Ethereum founders was from the very beginning to transition its blockchain to a proof of stake consensus mechanism.

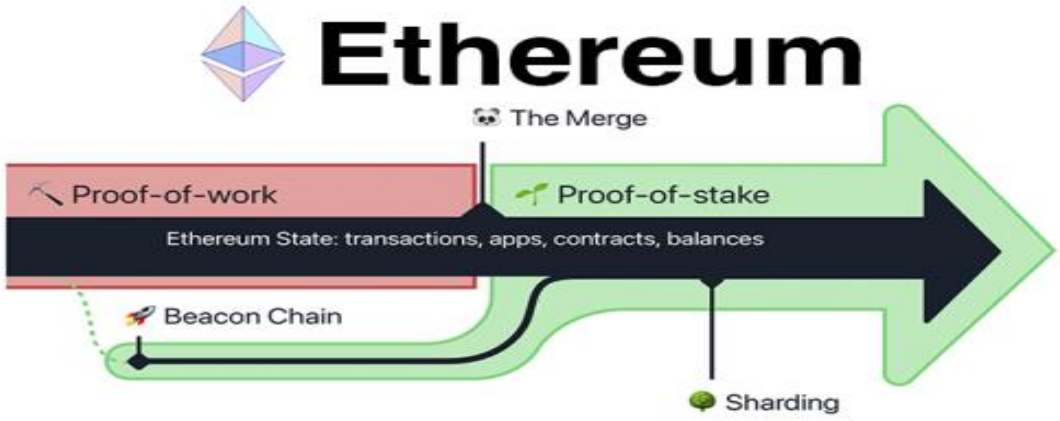


Figure 10: The Ethereum Merge explained

https://block-builders.de/ethereum-vor-the-merge-welche-quellen-zeigen-an-ob-alles-glatt-laeuft/

Developers were working on the transition and preparing for it from the very beginning of Ethereum. The Beacon Chain was created and launched in December 2020 as separate blockchain and it was running parallel to Mainnet.

Initially, the Beacon Chain wasn't able to process Mainnet transactions. The way that it operated was by reaching consensus by agreeing on active validators and their account balances. The new blockchain was intensively tested and at some point, it was fully capable to reach consensus based on real world data. Beacon chain became the main consensus mechanism for all data after the merge.

The Merge marked the official adoption of the Beacon Chain as the driver of block creation. Mining was no longer used to generate valid blocks. Instead, proof-of-stake validators have taken over this duty and are in charge of validating all transactions and suggesting blocks.

Very important to add to this is that nothing was lost during The Merge. All history and transactions were untouched. The reason behind this is that the upgrade was in such a way

conducted that not only did Mainnet merge with Beacon chain, but all of its transaction history on Ethereum's blockchain merged as well.

This historic moment marked the beginning of a more safe and sustainable Ethereum, also called by some people a green blockchain. The Merge made it possible for Ethereum for further and future upgrades which wouldn't be possible under the proof of work consensus mechanism. This gives Eth the opportunity to achieve its full potential in regards to sustainability and security.

2.9 Security and Safety

Blockchain avoids some of the hazards associated with centrally kept data by storing it throughout its peer-to-peer network (Levy, Adam, Blockchain, NFT, Metaverse and Cryptocurrency, 2022). A "51% attack on the system"23 basically leads to the double spending problem mentioned earlier. Such an attack would aim to have control of the network, or at least a little bit more than half of it so that it can change records on the blockchain. This then leads to the problem which Blockchain initially overcomes.

In order everything to be as safe as possible and users to feel secured, a so-called public key was invented. This key is a separate and very important part of the Blockchain and uses a different kind of cryptography, which is named as "Public Key Cryptography". Public keys are nothing else than addresses. It functions in a very similar way as a password. In this case this address or password is used to grant users access to their assets. This way when tokens are exchanged in the system they are associated with an address. It is said that every that every single transaction is not only stored on the Blockchain, but also that the data stored on it is incorruptible.

The blockchain is replicated on every node in a decentralized system (Levy, Adam, Blockchain, NFT, Metaverse and Cryptocurrency, 2022). The data quality is insured through database replication and computational trust. There are no official copies and there are no preferences between users on the Blockchain. At the very beginning Blockchains needed a lot of computational power arising from mining farms, which I mentioned earlier, so that transactions could be validated and so that blocks could be constructed and forwarded to the other nodes. Transactions are then broadcasted through the system.

[23] See more: https://ieeexplore.ieee.org/iel7/6287639/9312710/09567686.pdf

Blockchains use a variety of time-stamping mechanisms (John, Kose and O'Hara, Maureen and Saleh, Fahad, Bitcoin and Beyond (November 1, 2021), such proof-of-work, to serialize changes. Proof of stake is one of the later consensus mechanisms. Sadly, such systems need a lot of maintenance and they demand a lot of computing power to validate data. This, of course, can get expensive at some point, leading to risk of centralization.

2.10 DEX(s)

Decentralized exchanges (DEXs) are peer to peer trading platforms where transactions between crypto buyers and sellers are executed without the need of a central authority. They are based on smart contracts in the Ethereum blockchain. Transactions are verified and carried out in a decentralized matter where numerous nodes act as validators of information in the network.

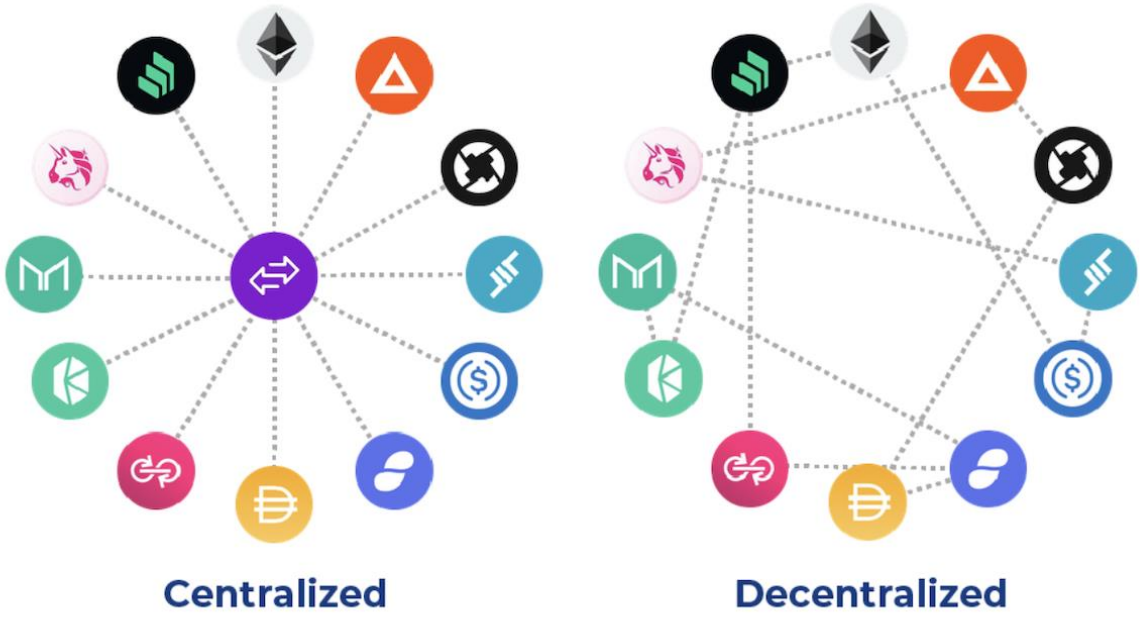


Figure 11: Centralized vs. Decentralized Systems

https://medium.com/coinmonks/cryptotypes-decentralized-exchanges-and-marketplaces-xcc-dxm-1020ea090188

DEXs introduced to the world new pricing algorithms which have the ability to change the market structure that we know. These new algorithms are called automated market makers (AMM). Before the creation of automated market makers almost every single transaction was executed through centralized exchanges which use centralized limit order books (LOBs). However, everything changed during the summer of 2020 with the creation of the new market

making algorithm. Since then there are only two such algorithms – AMMs and LOBs. These two algorithms will be analyzed in detail and compared in the following chapters.

As already said, the new algorithms were introduced to the world in 2020. The biggest decentralized exchanges back then introduced were Uniswap and Sushiswap which are still the biggest exchanges. Both exchanges (especially UniSwap) have nowadays a bigger trading volume than some centralized exchanges. On the following graph we can see the trading volume of different decentralized exchanges with Uniswap being the one with the biggest trading volume:

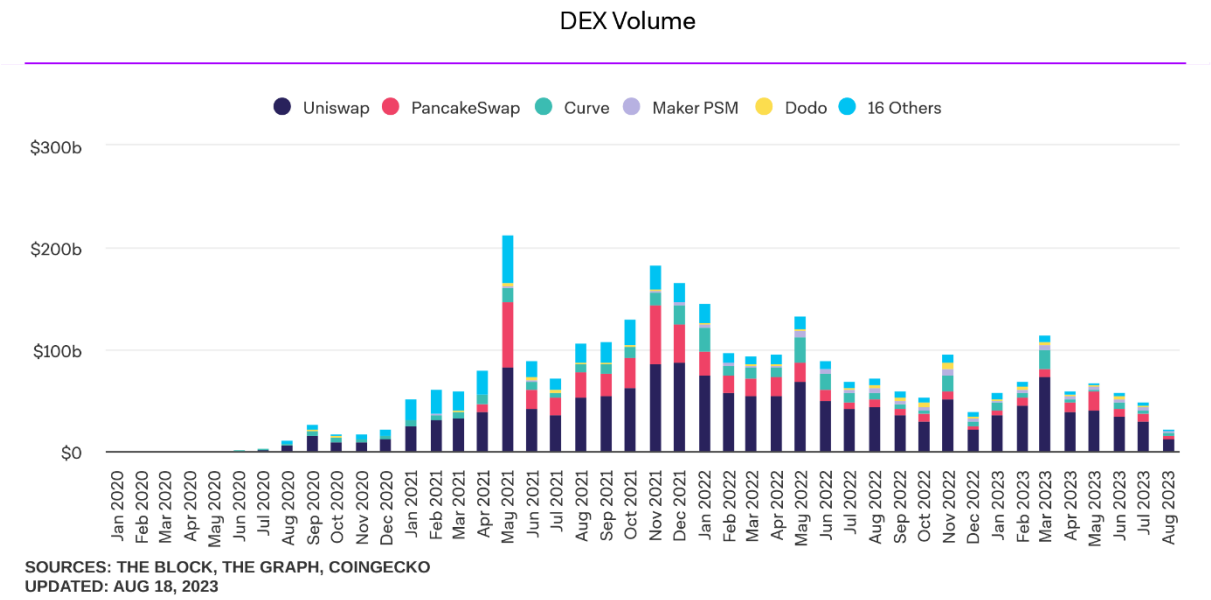


Figure 12: Transaction Volume on Decentralized Exchanges per August 2023

https://www.theblock.co/data/decentralized-finance/dex-non-custodial

The underlying setup of these new exchanges is what sets them apart from the traditional financial markets. Financial markets operate with the help of centralized limit order books and in order for investors to gain access they need to go through many intermediaries which is time consuming. With decentralized exchanges it is the opposite way. The exchange is executed as a swap where both parties only need to connect their digital wallets with the app. They can choose the amount, afterwards sign the order, which get executed as already said by the smart contract and then just wait until the transaction is executed. After the order is signed the smart contract starts immediately with the execution and implementation of the order. Afterwards all transactions and data are stored on the Ethereum Blockchain.

The idea behind these algorithms is very simple and at the same time very innovative. Transactions are always the exchange between two tokens on the blockchain. Users have to implement the deal as a smart contract which locks in the token that is going to be sold subject to the other coin that is going to be received from the transaction. Afterwards, an atomic swap is being initiated from the smart contract which basically means that the buyer receives the bought tokens and the seller receives the payment tokens. The swap is verified by the miners on the blockchain ensuring that the smart contract is executed accordingly (Park, A., The Conceptual Flaws of Constant Product Automated Market Making, 2021).

Functional simplicity aside, the economically relevant promise and possible genius of decentralized swap exchanges is that they use the smart contracts functionality of the blockchain to aggregate and automate the provision of liquidity (Park, A., The Conceptual Flaws of Constant Product Automated Market Making, 2021. As we will see in the following chapters, liquidity suppliers can deposit and trade their assets against other assets or cash in so-called liquidity pools, which function as swap exchange market. All transactions in the liquidity pool earn fees which benefit the liquidity providers as they have certain risks from depositing liquidity in the pool. More details on that will follow in chapters 5 and 6.

3. Literature Review

As there are a lot of papers and articles regarding Blockchain and cryptocurrencies for the past 7-8 years, there are still not a lot of papers based on decentralized exchanges and how the function because of the mathematical complexity of the topic. However, there are enough working papers that help understand how these new exchanges work and to even give suggestions for improvements. This chapter will aim to familiarize the readers with articles similar to the thesis as well as to showcase most recent researches regarding decentralized exchanges. The main studies used for the thesis are going to be broken down.

The main articles that were used to conduct the thesis concern the topics related to Uniswap, Automated Market Makers, Limit Order Books, Liquidity Provision, Equilibrium Liquidity pools, liquidity freezes, price volatility, arbitrage opportunities, competition among arbitrageurs and pricing curves.

There are a couple of papers that analyze AMMs from different angles. Most closely related to this thesis is the work from Lehar and Parlour (2021). They analyze automated market makers and limit order books as well as compare liquidity providers' returns on both exchanges. The authors try to show the conditions under which automated market makers dominate limit order books. They also show empirical results that token prices on Uniswap track those at Binance where a centralized order system is used and that liquidity provision in equilibrium is stable.

The paper from Agostino Caponi and Ruizhe Jia (2021) is also a very important article for the conduction of the thesis. They state that the pricing curves that are implemented on AMMs allow arbitrageurs to extract profits from liquidity providers. Because of this the price of liquidity provision rises as liquidity providers want to insure themselves or it can lead to a liquidity freeze if the volatility of the tokens gets too high. They find out that the gas price volatility is more than 50% less for stablecoin pairs in comparison with other exchanged coins and suggest that a more convex pricing curve has a stronger price effect, which limits arbitrage but also decreases the profit of investors.

Aoyagi and Ito (2021) investigate how the presence of centralized and decentralized exchanges affects market pricing and trading behavior. They demonstrate that liquidity in DEXes supplements liquidity in CEXes, owing to the fact that informed and liquidity traders have distinct preferences for submission venues. In this thesis we will argue that asymmetric information is the main reason for the rise of arbitrage opportunities at AMM because

Arbitrageurs can take advantage of liquidity providers thanks to the publicly available information. In the papers of Aoyagi and Ito as well as of Lehar and Parlour asymmetric information is the main reason behind arbitrage problems.

Another very interesting and similar paper is the one from Barbon and Ranaldo (2021) where they are comparing the price and liquidity efficiency between centralized and decentralized exchanges as well as the transactions costs between different decentralized exchanges. They find out that the trading cost on decentralized exchanges are higher than in centralized exchanges because of the fixed costs of gas fees. They also suggest that DEXs can turn to an alternative to CEXs.

Park (2021) demonstrates that, regardless of the AMM pricing mechanism, front-running arbitrage always exists. He then demonstrates that uniform pricing reduces arbitrageurs' benefit from frontrunning while perhaps incentivizing order splitting. The victims of frontrunning arbitrage in Park (2021) are liquidity demanders whose transactions are delayed due to the public observability of transactions in the blockchain mempool. In my model instead, arbitrage arises due to deviations between the spot exchange rate and the fundamental rate, and imposes a loss on liquidity providers.

4. Uniswap

Uniswap launched in November 2018 and it was the biggest decentralized exchange ever built on the on the Ethereum Blockchain. It was felt like something revolutionary because of the fact that it excluded third parties/intermediaries from the transactions. Uniswap uses an automated market maker (AMM) system, which allows users to trade tokens based on a mathematical formula rather than relying on traditional supply and demand mechanics. This means that Uniswap provides liquidity to token holders, allows them to make trades quickly and securely, and also enables users to become liquidity providers by providing tokens to the protocol in order to earn fees.

Uniswap is the biggest decentralized exchange to date with committed liquidity supplies over 9 billion USD across cryptocurrencies. At the time this master thesis is conducted it is estimated that the daily traded liquidity in Uniswap amounts to 1.14 billion USD. Uniswap is an exchange platform that lets you swap a certain cryptocurrency for another. At the very beginning in 2018 there were only swaps between Eth and Maker token possible. Until now there were 3 versions of Uniswap starting with version 1 (V1).

Uniswap's first version allowed users to exchange any ERC20 token for the native currency token Ether. If there was no existing liquidity pool for a specific trading pair one can simply create a new pool by specifying the token which he wants to trade in the Uniswap factory contract. The first version of Uniswap served as a proof-of-concept for a novel decentralized market. The Uniswap protocol (Uniswap) serves as a venue for automated liquidity provision on Ethereum and operates without maintenance, offering an unstoppable platform for ERC20 token conversion. As long as Ethereum remains, Uniswap V1 will continue to function, and thus far, it has performed well for a range of use cases.

2 years after that V2[24] was released which enabled the direct trade of any token pairs and included Thether (USDT) which is the largest stable coin to date. Our second version of Uniswap, Uniswap V2, has a lot of new features and enhancements. Any ERC20 token may be directly pooled with any other ERC20 token on Uniswap V2. Although end users can still utilize native ETH through helper contracts, wrapped Ether (WETH) is implemented in place of it in the core contracts.

[24] See https://blog.uniswap.org/uniswap-v2

All liquidity pools in Uniswap V1 were between ETH and an individual ERC20 token. A benefit of having a constant numeraire is that users may swap any ERC20 for any other ERC20 by routing through ETH. The ideal option for Uniswap V1 was ETH since it is the most liquid Ethereum-based asset and doesn't pose any additional platform risks. For liquidity providers, who may keep a wider range of ERC20 token denominated positions without having to be exposed to ETH, the addition of ERC20 token/ERC20 token pools in Uniswap V2 can be helpful. Direct ERC20/ERC20 pairings can also raise prices since using ETH to route a swap between two other assets, like DAI/USDC, requires fees and slippage to be paid on two other pairs rather than just one. Two ERC20 tokens may still be swapped even if they are not directly paired and do not share a pair as long as there is a path between them.

Flash swaps on Uniswap V2 let you take as much of any ERC20 token as you like without paying anything up front and use them anyway you choose (run arbitrary code), provided that at the conclusion of the transaction execution, you either:

- Pay for all withdrawn ERC20 tokens.
- Pay for a portion of ERC20 tokens and give the remainder back.
- Return all withdrawn ERC20 tokens.

Even though the supplied ERC20 tokens are to be returned as part of a flash swap, liquidity provider fees are enforced by deducting 0.3% from all input amounts. On Ethereum, it frequently happens that a string of transactions has a high initial cost but a low overall cost or even a net profit at the conclusion of the string. Flash swaps are tremendously helpful for multi-step transactions using Uniswap since they eliminate upfront capital needs and pointless restrictions on order-of-operations.

In many aspects, decentralization aims to broaden involvement and eliminate the primary points of malfunction. The first version of Uniswap is already very decentralized, trustworthy, and censorship-resistant. But it must keep developing and getting better if it is to serve as the foundation of a just and open financial system.

The code for Uniswap V2 contains a minor protocol charge mechanism to pave the way for self-sustainability. At launch, the liquidity provider cost will be 0.30% and the protocol fee will fall back to 0. The protocol charge will increase to 0.05% and the liquidity provider cost to 0.25% if it is enabled.

Uniswap V3 was launched in May 2021 and the update introduced concentrated liquidity and multiple fee tiers. The integrated features make Uniswap V3 the most efficient and flexible automated market maker ever. Oracles in version 3 are now cheaper and easier to integrate, as well as fees are slightly lower than in version 2. We can summarize that Uniswap 3 introduces the following improvements:

- Concentrated liquidity - providing each LP with fine-grained discretion over the price bands to which their capital is allocated. Individual holdings are pooled together to create a single curve that customers may trade against.
- Multiple fee tiers that enable LPs to get fair compensation for assuming various levels of risk

Uniswap v3 characteristics include:

- Compared to Uniswap v2, LPs may supply liquidity with up to 4000x more capital efficiency, giving them larger returns on their money.
- Low-slippage transaction execution that can outperform both centralized exchanges and stablecoin-focused AMMs is made possible by capital efficiency.
- LPs can considerably raise the amount of preferred assets they own while lowering their downside risk.

Oracle integration for Uniswap is now simpler and less expensive. Time-weighted average prices (TWAPs) for any time period over the last 9 days can be requested from V3 oracles. As a result, integrators are no longer required to checkpoint past data. Even with these revolutionary design advancements, v3 swaps on the Ethereum Mainnet have a somewhat lower gas cost than v2.

In June 2023 a new fourth version of Uniswap (V4)[25] was introduced to the audience which for the moment only has draft code released. Uniswap v3 balanced an exceedingly complicated tradeoff space with a strong, passionate approach to liquidity supply. Increased costs and increased complexity of the code accompany new functionality. The aim is that this new version is built in public and that the community contributes to the final steps of the new version. The process is considered to last a couple of months.

[25] See https://blog.uniswap.org/uniswap-v4

With Uniswap v4, they hope to introduce "hooks," which will enable anybody to choose between these tradeoffs. Hooks are contracts that execute at different times during the lifespan of a pool operation. Pools may either provide whole new capabilities or make the same choices as v3.

Along with this flexibility, the design of Uniswap v4 provides efficiency and cuts expenses. A novel "singleton" contract is introduced, in which all pools are included under a single smart contract. We think the hooks and singleton design together provide for an immensely potent platform, allowing for quick, secure pool modification and effective routing across several pools. Fast, expressive AMM innovation is brought by Uniswap v4 inside a potent ecosystem.

5. AMM vs. LOM

AMMs use collaborative liquidity providers to replace competitive market makers in a typical exchange trading environment. By depositing their tokens, every token holder may become a liquidity provider and get a portion of the pool, establishing a new market structure based on liquidity pools.

Each asset combination in an automated market maker (AMM) like Uniswap makes up a separate pool or market. By adding the pair proportionately to the current pool, agents provide liquidity. By eliminating one asset and introducing another, agents seek liquidity. The average price paid is derived based on the relative fraction of the two exchanged assets and is established by a predetermined downward-sloping, convex relationship. This is referred to as a bonding curve (Lehar, A., and C. Parlour. 2021). The convexity implies that larger orders have a larger price impact. Additionally, the liquidity suppliers receive a proportionate charge from each liquidity demander.

In order to structure my research, I focus on two key differences between an AMM and a limit order market. The AMM first mutualizes the benefits and drawbacks of providing liquidity: Liquidity providers do not compete. Because strategic liquidity providers are in direct competition with one another, the costs and benefits of supplying liquidity vary depending on the liquidity source in the limit order book.

Second, pricing impact in the AMM is deterministic. The bonding curve, in particular, sets the transaction price and is completely predictable given the size of the liquidity pool and incoming order. Liquidity providers, on the other hand, pick to post in the limit order market at a price that maximizes their profits and could even purposefully eliminate liquidity.

Competing liquidity suppliers publish prices in the stylized limit order book market to trade off unfavorable selection risk versus lucrative liquidity supply. Of course, each liquidity provider expects to get nothing if there are two of them competing in the same market. Each source of liquidity has an incentive to invest in order to locate trade opportunities where he need not compete. This expresses the notion that liquidity is inexpensive if two providers are in price competition. However, if they engage in competition on other aspects, like speed, it can raise the cost of liquidity.

6. Constant Product Market Maker CPMM

The AMM supports the trading of two tokens, whose exchange rate is decided by a curve pinned down by the pricing function. The "tip" amount—also known as the "gas fee"—offered to the validators of the underlying blockchain determines the priority of a transaction's execution rather than its arrival order. Whether or not to deposit their tokens depends on the liquidity providers. Investors exchange tokens and reap the rewards of possessing particular token kinds. The spot token exchange rate may fluctuate from its basic value as a result of external shocks to the fundamentals or price effect brought on by investor trades. While liquidity providers issue exit orders for withdrawing their tokens, arbitrageurs strive to take advantage of this price deviation. The arbitrageur whose request was carried out first ex-tracts the whole benefit from the arbitrage while liquidity providers split the loss imposed by the arbitrage.

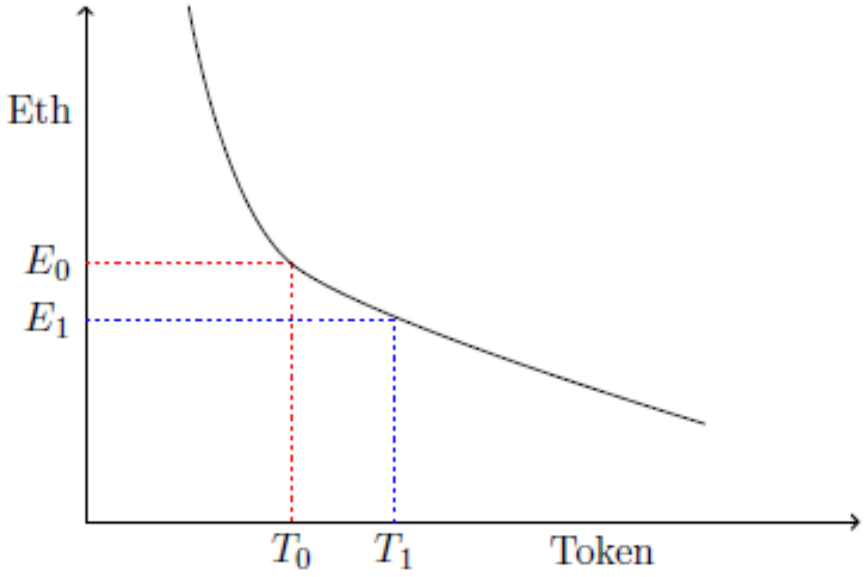
6.1 Liquidity provision

A pair of coins make up each swap pool. Eth, the native cryptocurrency on the Ethereum Blockchain, is one of the currencies most often used, as we see below. The other general coin will be referred to as the "token," and we will typically utilize Eth as the numeraire. The token and Eth are both deposited into the pool by an agent that wants to give liquidity to their favorite pool. The pool's current ratio determines the Eth to token deposit ratio. A share of a liquidity token is awarded to an agent that makes such a deposit. This third token is unique to the pool and denotes the portion of the overall liquidity pool that each liquidity provider contributes. The liquidity pool's value may increase or decrease depending on how the pool transacts with users. In order to get payment for their portion of the liquidity pool in an equal amount of ETH and tokens, liquidity providers may exchange their liquidity tokens at any moment. Because each trade is subject to a 30bps fees, which is then redeposited into the pool, providing liquidity has the potential to be profitable.

6.2 Trades

Let's say a trader wants to purchase the token. In this scenario, he will add Ethereum to the pool and take out the token. The amount he must deposit or withdraw is determined by the bonding curve shown in Figure 1. The ratio of the two currencies' respective quantities determines the inferred price that the pool is quoting at any given time. In this scenario, someone interested in purchasing a modest number of Tokens would pay or get E0. Consider someone who wants to sell part of the Token in order to exchange a bigger quantity. This would imply

that the trader contributes to the pool an amount of T1–T0 tokens. In exchange, the quantity of Eth in the pool would decrease and he would get E1 - E0.



(Lehar, A., and C. Parlour., Decentralized exchanges (2021). Working paper.)

The bonding curve method therefore automatically establishes the terms of trade.

As a result, if T is the total number of tokens and E is the total amount of ETH in the contract's liquidity pool, the conditions of trade are set up so that any post-transaction quantities come before any fee income.

Terms of trade: $\mathbf{k = E_0 * T_0 = E_1 * T_1}$

To put it another way, the sum of the token and ETH amounts is always on the bonding curve. The quantity of liquidity put in each pool determines the value of k.

6.3 Liquidity Fees

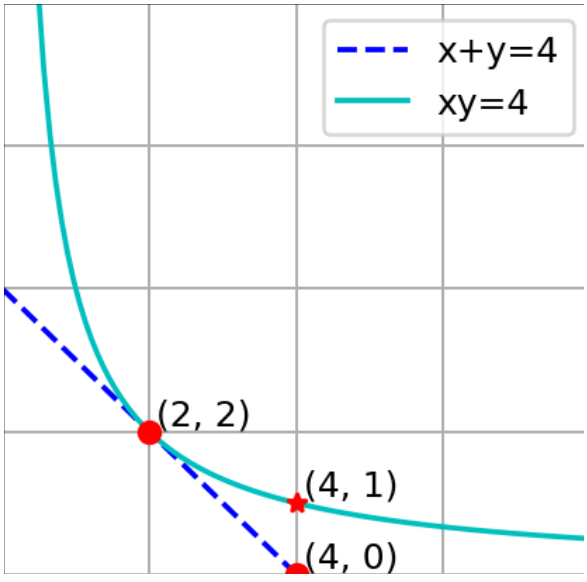
The above-mentioned terms of trade didn't include the liquidity fees that users need to pay when buying or selling tokens/liquidity. Of course, the remuneration is important for the liquidity providers. Assume that an agent wishes to trade ETH for tokens to understand how the charge impacts trades and pricing. The exchange charges a fee that is advantageous to those who have liquid assets. The effective quantity of exchanged Ether is (1 - τ)e. This leaves us with E′ = E + (1 - τ)e which is the post transaction liquidity pool balance prior to fee income.

6.4 Price Impact

As the pricing curve becomes more convex, price effect grows. As a result, for both investors and arbitrageurs, a larger convexity results in less transacted volumes. As a result, the gains that arbitrageurs take from the pool and the excess that investors seize are reduced. If the convexity of the curve is not excessively high, liquidity providers have greater incentives to deposit as the convexity of the curve increases. The advantage of lower arbitrage losses is outweighed by the cost of lower fee income on investor trades if convexity rises over a certain point. The graphic below shows how price impact would change depending on the convexity of the bonding curve.

Assume there are two of each type of token: A and B. exchange rates are set at 1, transactions have no effect on the price, and 2 tokens A can be traded for 2 tokens B if the pricing curve is linear. Only 1 token B can be exchanged for 2 tokens A if the price curve is the constant product curve. The marginal exchange rate, which changes from 1 to 0.25 as a result of the deal, is affected in terms of price.

The constant product pricing curve has a bigger convexity than the linear pricing curve, which results in a higher price effect and explains why 2 tokens A are traded for fewer than 2 tokens B.



(Capponi, Agostino, and Ruizhe Jia, 2021, The Adoption of Blockchain-based Decentralized Exchanges, working paper.)

6.5 Arbitrage opportunities

The spot exchange rate deviates from its fundamental value in response to the entry of an investor or a shock to the value of a token. For arbitrageurs, this variance offers a potential opportunity. Liquidity providers send withdrawal orders, whereas arbitrageurs submit orders.

6.5.1 Stale Price Arbitrage Opportunity

Arbitrageurs have an opportunity due to a token value shock. Assume that either token A or token B experiences a shock, and the fundamental exchange rate changes. The spot exchange rate at the AMM becomes "stale" and no longer accurately reflects the fundamentals. Consider the case when token B is affected by the shock and its fundamental value changes from p_1(B) to p_2(B) = (1+ ϵ) p_1(B.) Then, trading tokens A for B could be advantageous for arbitrageurs. This trading opportunity is referred to as stale price arbitrage.

6.5.2 Reverse Trade Arbitrage Opportunity

The price impact of an investor's trade might also cause AMM prices to deviate from fundamentals, which presents a chance for reverse trade arbitrage. Assume a "type A" investor shows up to observe this. As a result of the investor exchanging tokens B for tokens A, there are less tokens A and more tokens B in the AMM. The spot rate at which tokens A and B are exchanged rises as a result, exceeding the fundamental exchange rate. Arbitrageurs may find it lucrative to engage in trading in the reverse direction of the investor if the variance is sufficient. Therefore, the price impact generated by the investor's original transaction is only temporary since the arbitrageur's opposite trade will reverse the price shift she made. By doing so investors support both liquidity providers and arbitrageurs who gain from the price effect of their transactions.

7. Framework

The following model focuses primarily on liquidity supply and tries to prove that liquidity provision in equilibrium is stable. The main focus and starting point of the model is the constant product market maker, because of whom we are able to derive most of our formulas and afterwards results.

The introduction of asymmetric information plays a crucial role in the determination of liquidity provision as you will see that liquidity providers do not know the future liquidation value of their asset after supplying liquidity in the pool. Instead, traders are informed and can observe information about the true value of the asset. This gives them the choice whether or not to participate in the market and take up liquidity if the price of the assets deviates from its true value.

For instance, the informed trader would take token Y out of the liquidity pool and add token X in its place if the price of token Y (relative to token X) on a centralized exchange was higher than the price suggested on the automated market. In other words, the informed trader removes the most valuable assets from the pool and replaces them with the least value ones. As a result, anytime a deal is executed by an informed trader, the liquidity pool's value decreases, resulting in a negative selection cost for LPs. In the DeFi sector, the cost is occasionally referred to as an impermanent loss[26] but is not connected to informational frictions (e.g., Angeris, Kao, Chiang, Noyes and Chitra, 2019).

The model follows the standard assumptions from other papers and has similar results for some parameters. The difference in the following model in regards to the models of Lehar or Capponi is that they look at longer periods and that there is an innovation in some period and if there was an innovation the arbitrageur comes to the exchange and trades. If there was no innovation liquidity trader comes to the exchange and afterwards an arbitrageur would try to exploit arbitrage opportunities. In their models they also consider gas fees, which I assume in my model that there are no fees in order to simplify the equations. In the following model either an informed trader comes to the exchange or a noise trader. It doesn't depend whether or not there is an innovation. The arrival of the noise trader is the way to show how liquidity

[26] The impermanent loss is the loss liquidity suppliers suffer when the value of the assets that they deposited in the beginning changes. The bigger the change in value the bigger the loss they suffer. The impermanent loss can be counteracted with trading fees, otherwise LPs wouldn't supply liquidity.

providers can actually make profits when there are no arbitrageurs and no fees on the exchange.

7.1 Model Description

The model is based on a two-period economy which we denote as t = (0,1).

We assume that there are unlimited numbers of liquidity providers, as well as one information trader and one noise trader.

There are two assets that are being traded in the market – a digital token (Ethereum) and cash. The digital token in the model will be denoted as e (Ethereum).

It is assumed that the price of the token is equal to $\boldsymbol{p_0}$ before the game starts.

Because of some liquidity shocks or shifts in the prices on other exchanges the price of the asset changes in the first period (t=0) to $\boldsymbol{\tilde{p} = p_0(1+ \sigma)}$, where σ can be interpreted as the volatility of the asset.

In period t = 2 the asset is liquidated at $\boldsymbol{\tilde{p}}$.

7.2 Traders

During period t=0 and t=1 an informed trader or a noise trader arrives in the market in order to trade.

In the first case of the model the informed trader observes the price $\boldsymbol{\tilde{p}}$ with a probability of $\boldsymbol{\theta \epsilon (0, 1)}$ at **t = 0.**

The informed trader participates in period t=0 and tries to exploit arbitrage opportunities by buying the asset when σ = + σ and selling the asset when σ = - σ.

We denote the cash in the market as **a** and assume for simplicity that the trader trades all of his units of cash at once (**a** > 0). Angeris et al. (2019) shows that if the trader splits trade it's going to be costlier than if he spends all of his cash at once.

In the second case of the model **(1 - $\boldsymbol{\theta}$),** the informed trader cannot observe $\boldsymbol{\tilde{p}}$ and doesn't participate in the market. If the informed trader doesn't participate the expected price in the final period would be the same as the price before the game started, $\boldsymbol{p_0}$. Not only that, but a noise trader is hit by some exogenous liquidity shock in t = 0, which can be interpreted as a trading

or lending need, and participates in the exchange. The noise trader buys or sells d > 0 units of the token or cash with equal probability and we assume that he trades everything at once.

7.3 Liquidity Providers:

We assume that there is a continuum of risk neutral LPs, (i ϵ Θ). The risk neutral liquidity providers are assumed to be in perfect competition.

In **t=0,** LPs choose the optimal amount they want to supply in order to maximize their profits. Because of the way automated market makers are structured, liquidity providers don't have control over the price of the trades that are being executed. That's why they cannot adjust their prices of liquidity because they cannot monitor the market. Because of that they choose to withdraw their liquidity from the market at t = 1 so that they can obtain hopefully a positive return. In the following model gas fees are not considered because of simplification reasons and LPs withdraw their liquidity after they observe the first trade because arbitrage imposes adverse selection costs and the LPs try to avoid that.

7.4 Exchange

As already mentioned decentralized exchanges form liquidity pools where assets can be traded for cash or for other tokens. In this case our liquidity pool is comprised of tokens and cash. As earlier mentioned the price of the liquidity pool is determined by the constant product market maker algorithm.

We know that in order for the price of the asset to stay constant the amount of tokens and cash in the pool also have to be constant or to be in the same proportion as in the beginning. Any disbalance in this ratio would lead to a change in the price of the asset and arbitrageurs will try to obtain this benefit. An easy example is that if she wants to supply an amount of **a** cash and **e** units of Ethereum at t = 0, it has to satisfy the condition mentioned earlier in order to keep the price in the liquidity pool constant, or $\boldsymbol{p_0}$.

$$\mathbf{a} = \boldsymbol{p_0}\mathbf{e}$$

In order the equations and results of the model to hold I have written down the following 2 assumptions**:**

1. In order for the non-arbitrage condition to hold the liquidity pool has to have $\bar{a} \geq 0$ and $\bar{e} \geq 0$ units of cash and Ethereum tokens before the exchange starts. This leaves us with the following expression about the price of the trading pair:

$$\boldsymbol{p_0 = \frac{a}{e}}$$

2. It must be satisfied that d < $\bar{a}$. This condition makes sure that the trading volume of the noise trader doesn't exceed the initial amount of cash in the pool.

Let's say that an infinite small trade occurs. I denote $\boldsymbol{a_{i,0}}$ and $\boldsymbol{e_{i,0}}$ as the cash and asset supplied by the liquidity provider. Then the CPMM will require that $\boldsymbol{a_{i,0} = e_{i,0}\, p_0}$ to hold so that the execution price $\boldsymbol{p_0 = \frac{a+a_{i,0}}{e+e_{i,0}}}$ stays constant. This way I can derive an expression about the aggregate cash and tokens that are in the liquidity pool at t = 0:

$$\boldsymbol{A_0} = \bar{a} + \int_{i\in\Theta} a_{i,0}\mathrm{di}$$

$$\boldsymbol{E_0} = \bar{e} + \int_{i\in\Theta} e_{i,0}\mathrm{di}$$

(1)

8. Calculations and Results

I start with the case when the informed trader observes $\tilde{\boldsymbol{p}}$ and there is a positive jump in the price of the asset, i.e. when the price becomes:

$$\tilde{\boldsymbol{p}} = \boldsymbol{p_0}(1+\boldsymbol{\sigma})$$

8.1 Informed trader comes to the exchange

8.1.1 Positive Jump in Asset Value

When the informed trader observes the new price, he will sell his units of cash which are denoted as $\boldsymbol{\delta}$ in order to obtain $\boldsymbol{\delta_E}$ units of Ethereum. We can specify the state of the liquidity pool after every step of the model by a tuple. In our case we can denote the liquidity pool before the model starts as $\boldsymbol{T_0} = (\boldsymbol{A_0}, \boldsymbol{E_0})$. After the trader observes the price and trades his cash for the asset the liquidity poll changes to $\boldsymbol{T_1} = (\boldsymbol{A_1}, \boldsymbol{E_1})$, with $\boldsymbol{E_1} = \boldsymbol{E_0} - \boldsymbol{\delta_E}$ and $\boldsymbol{A_1} = \boldsymbol{A_0} + \boldsymbol{\delta}$.

(2)

As already mentioned the CPMM algorithm states that the two time periods as well as the trading quantities must be equal. This leads to the following expression:

$$\boldsymbol{k_0} = \boldsymbol{E_0 A_0} = (\boldsymbol{E_0} - \boldsymbol{\delta_E})(\boldsymbol{A_0} + \boldsymbol{\delta})$$

From there we can easily derive how many units of Ethereum he bought when paying $\boldsymbol{\delta}$ units of cash:

$$\boldsymbol{\delta_E} = \frac{\boldsymbol{E_0}.\boldsymbol{\delta}}{\boldsymbol{A_0}+\boldsymbol{\delta}},$$

(3)

Then, the unit price of Ethereum is:

$$\frac{\boldsymbol{\delta}}{\boldsymbol{\delta_E}} = \frac{\boldsymbol{A_0}+\boldsymbol{\delta}}{\boldsymbol{E_0}}$$

Now that the liquidity pool has changed after the transaction, the new or updated state of it is equal to $T_1 = (A_1, E_1)$. If there is a following trade after the first exchange then it will be executed with the updated state of T_1. This means that the price would change to:

$$\boldsymbol{p_1}(\boldsymbol{\delta}) = \frac{\boldsymbol{A_1}}{\boldsymbol{E_1}} = \frac{(\boldsymbol{A_0} + \boldsymbol{\delta})\text{\^{}}\boldsymbol{2}}{\boldsymbol{E_0 A_0}}$$

The non-arbitrage requirement establishes the endogenous quantity of informed trading ($\boldsymbol{\delta}$), preventing the additional round of trading from turning a profit. This suggests that must satisfy the following condition:

$$\boldsymbol{p_1(\delta) = \tilde{p} = (1+\sigma)p_0}$$

As a result, the price of buying one unit of the asset on the market (the LHS) is equal to the price at which the asset will be liquidated (the RHS). The informed trader can achieve this condition because she knows σ.

8.1.2 Negative Price Shock

Having in mind the non-arbitrage condition that we just applied for the case above, the same will have to hold for the case when there is a negative price shock. i.e. – **σ**. We get:

$$\boldsymbol{p_1(-\delta) = \frac{(A_0-\delta)\text{^}2}{E_0 A_0}} = (1\text{-}\ \boldsymbol{\sigma})\boldsymbol{p_0}$$

This means that the informed trader is selling $\boldsymbol{-\delta}$ **(< 0)** units of cash in order to take on arbitrage opportunities when there is a negative price shock. Solving both equations, we can obtain the informed trader's optimal trading strategy and explain the following 2 propositions:

Proposition 1:

- The informed trader's optimal trading quantity equals:

$$\delta^*_\sigma = \begin{cases} A_0\left(\sqrt{1+\sigma}-1\right) & if\ \tilde{\sigma} = +\sigma \\ A_0\left(1-\sqrt{1-\sigma}\right) & if\ \tilde{\sigma} = -\sigma \end{cases}$$

- From the equations above we can say that the optimal trading size of the informed trader is proportional to the cash liquidity pool $\boldsymbol{A_0}$ and that it increases in $\boldsymbol{\sigma}$. Summarizing Proposition 1 from above it makes it easy to see that informed trader's trading quantity is proportional to size of the cash liquidity pool $\boldsymbol{A_0}$**.** This means that if $\boldsymbol{A_0}$ is large, then the informed trader will trade a bigger amount when trying to obtain arbitrage opportunities, which means that the price impact is very small. In other words, the bigger the liquidity pool, the more the arbitrageur can extract from the pool in regards to the volatility of the asset value. Importantly, the trading quantity of the informed trader is proportional to the aggregate size of the cash pool, $\boldsymbol{A_0}$. When $\boldsymbol{A_0}$ is large, the price impact of a trade is small,

meaning that the informed trader can trade a large quantity when she consumes arbitrage opportunities. Put differently, the larger the size of the liquidity pool, the more arbitrage opportunity the informed trader can exploit given the size of the jump in the asset value (σ).

If we substitute $\boldsymbol{\delta}$ in $\boldsymbol{E_1 = E_0 - \delta_E}$ and $\boldsymbol{A_1 = A_0 + \delta}$ for δ_σ^* we can obtain the value of the liquidity pools after the exchange:

$$\mathbf{E_1^{IT,\sigma}} = \frac{\mathbf{E_0}}{\sqrt{\mathbf{1+\tilde{\sigma}}}} \tag{4}$$

$$\mathbf{A_1^{IT,\sigma}} = \mathbf{A_0}\sqrt{\mathbf{1+\tilde{\sigma}}} \tag{5}$$

Where IT and σ represents the informed trading when the Ethereum volatility isσ.

8.2 The Cost of Adverse Selection

Now that all possible information as well as formulas about the liquidity pools have been obtained and discussed is time to focus on the expected profits of the LPs in the case when an informed trader exchanges Ethereum for the liquidity.

We denote the LPs share in the liquidity pool to be $\frac{a_{i,0}}{A_0}$. When the liquidity provider decides to withdraw her liquidity and convert her Ethereum tokens into cash at the end of the game she obtains:

$$\boldsymbol{V_{IT,S}(a_{i,0},\tilde{\sigma}) = \frac{a_{i,0}}{A_0}(A_1^{IT,\sigma} + \tilde{p}\, E_1^{IT,\sigma})}$$

Subscripts "IT" and "S" denote the return of supplying liquidity when it was bought from the informed trader.

Another option for liquidity providers is to not supply liquidity at all and stay inactive in the market. If she holds the portfolio and stays inactive she will have an expected return of:

$$\boldsymbol{V_H(a_{i,0}) = a_{i,0} + E\,[\tilde{p}]e_{i,0} = 2a_{i,0}} \tag{6}$$

Proposition 2

- The liquidity trader's ex ante expected gross return from supplying $\boldsymbol{a_{i,0}}$, given A_0, when trading with the informed trader is given by:

$$V_{IT,S}(a_{i,0}) = E_{\sigma}[V_{I,S}(a_{i,0},\tilde{\sigma})] = a_{i,0}(\sqrt{1+\sigma} + \sqrt{1-\sigma})$$

(7)

- When the informed trader exchanges Ethereum for cash, the liquidity provider's expected return is always negative, no matter how much liquidity he has supplied. I write it as:

$$V_{IT}(a_{i,0}) = V_{IT,Supply}(a_{i,0}) - V(a_{i,0}) = -a_{i,0}C_{AS}(\sigma)$$

where

$$C_{AS}(\sigma) = 2 - (\sqrt{1+\sigma} + \sqrt{1-\sigma}) > 0 \qquad \textbf{Adverse Selection cost}$$

This Adverse Selection cost showcases the impermanent loss that liquidity providers suffer when supplying liquidity. This points out the so-called impermanent loss that the LPs suffer when they suffer a loss from supplying liquidity. It is intuitive that informed traders buy the asset only if there is a positive jump in the price of the asset ($+\sigma$). Although cash is injected to the liquidity pool the transaction is executed at the stale price which deviates from $\boldsymbol{p_0}$. LPs suffer a loss because when liquidating their order, they receive a less valuable asset and release a more valuable asset.

Looking at the adverse selection cost, $\boldsymbol{C_{AS}(\sigma)}$, we can see that it is increasing in $\boldsymbol{\sigma}$. Thus, we can confirm Proposition 1 from the earlier that an informed trader trades a larger quantity when the price deviation is large and positive, which induces a more severe AS problem.

Additionally, Proposition 2 may be confirmed since the AS cost, $\boldsymbol{C_{AS}}$, for each LP is directly related to the amount of individual liquidity supply ($\boldsymbol{a_{i,0}}$) rather than total aggregate liquidity ($\boldsymbol{A_0}$). The cost of informed trading is proportional to the aggregate liquidity size ($\boldsymbol{A_0}$), as shown by Proposition 1, and each LP owns the share of the aggregate liquidity pool ($\frac{a_{i,0}}{A_0}$). As a result, from the perspective of each LP, the adverse selection cost continuously increases as she supplies more liquidity $\boldsymbol{a_{i,0}}$) and is proportional to $\frac{a_{i,0}}{A_0} * \boldsymbol{A_0}$.

8.3 Noise Trader

LPs don't have incentives to supply liquidity if traders are informed. Some transactions have to generate positive returns otherwise there will be no liquidity. This is the case if the noise trader takes part.

In this subchapter we suppose that a noise trader arrives to exchange and needs to trade $\bar{d}= \pm$ d unit of cash with equal probability. If this happens, she causes the following change to the liquidity pools:

$$E_1^{N,d} = \frac{E_0 A_0}{A_0 + \tilde{d}}$$

$$A_1^{N,d} = A_0 + \tilde{d}$$

I denote with N the noise trading and with d the cash that the noise trader exchanges. The noise trader's behavior is completely independent of $\tilde{\sigma}$ since she is not aiming to obtain arbitrage opportunities, rather motivated by some non-fundamental trading reasons. The noise trader buys and sells with equal probabilities; thus, we can derive the ex-ante expected return of the LP from the exchange with the noise trader:

$$\boldsymbol{V_{N,Supply} = \frac{a_{i,0}}{A_0} E_{d,\sigma}[C^{N,d} + (1+\tilde{\sigma})p_0 E^{N,d}] = a_{i,0}(1+\frac{A_0^2}{A_0^2 - d^2})}$$

(8)

If we use V_H from equation (6), we get the following result:

$$\boldsymbol{V_N(a_{i,0}) = V_{N,Supply}(a_{i,0}) - V_{Hold}(a_{i,0}) = a_{i,0} \frac{d^2}{A_0^2 - d^2} > 0}$$

(9)

Proposition 3:

- The predicted net profit from providing liquidity and engaging in trading with the noise trader is strictly positive.
- V_N decreases in the aggregate size of the liquidity pool.

The final equation shows that trading in this case isn't affected by adverse selection and that liquidity providers always extract positive profits from the trade. The main reason and difference to the informed trading is that $E_1^{N,d}$ is fully independent from the true price of the asset. We saw already on page 43 that the ex-post quantity of the token declines/increases when its value is expected to increase/decrease. This generates the loss for the liquidity providers.

Taking it back to the rule that every trade on the decentralized market must satisfy k = AE. Convexity implies that when a trade with random quantity of d is traded, then the ex-post quantity of Ethereum liquidity increases in expectation.

8.4 Equilibrium Liquidity Supply

Until now we saw that a trade with the informed trader would lead to adverse selection costs and a loss to the liquidity providers, as well as that a trade with the noise trader will result in a positive return for the LPs in expectation. The most important part of the thesis will follow as I will analyze the behavior of liquidity providers in equilibrium when they try to balance the profits and costs by determining an optimal $\boldsymbol{a_{i,0}}$

Optimal Liquidity Supply

Combining the two equations from the previous pages about the expected profit of the LP when trading with the informed trader and the noise trader we can deliver an expression about the ex-ante expected profit of the LP when supplying $a_{i,0}$:

$$\boldsymbol{V(a_{i,0}) = (1 - \alpha)V_N + \alpha V_I = a_{i,0}[(1-\alpha)\frac{d^2}{A_0^2 - d^2} - \alpha C_{AS}(\sigma)]}$$

(10)

The first part of the final equation shows us the positive return that the LP obtains when trading with the noise trader and the second part shows us the loss that the LP suffers from trading with the informed trader. In order to find the liquidity provider's optimal liquidity supply it needs to solve the following problem:

$$\mathbf{a_{i,0}^* = \arg\max V(a_{i,0})}$$

(11)

Lemma 1. LPs optimal liquidity provision is given by:

$$\boldsymbol{a_{i,0}}^* = \begin{cases} \infty & \text{if } d > d_0 \text{ ,} \\ \in [0, \infty) & \text{if } d = d_0, \\ 0 & \text{if } d < d_0 \end{cases}$$

Where

$$\boldsymbol{d_0 = A_0\sqrt{\frac{\alpha J(\sigma)}{1-\alpha+\alpha J(\sigma)}}}$$

(12)

The result follows from equation number 10, which states that if the trade with the noise trader dominates the one with the informed trader and in this case dominating the adverse selection, then every single liquidity provider would want to supply as much liquidity as possible since he will get a positive return. If this is not the case, then the LP would choose the outside option by not trading and setting $a_{i,0} = 0$. Basically, the profit of trading with the noise trader becomes larger when the following holds: the noise trader supplies trades a larger quantity of d so that the aggregate size of the liquidity in the pool gets sufficiently small, $\boldsymbol{A_0}$**;** the probability of the noise trader coming to the market is higher than the probability of the informed trader coming and that the cost of adverse selection is sufficiently small, (J).

Because of the fact that $\boldsymbol{A_0}$ and $\boldsymbol{d_0}$ are increasing in $\boldsymbol{a_{i,0}}$**,** the aggregate size of liquidity in equilibrium can be expressed as:

$$\boldsymbol{A_0^*= d\sqrt{1+\frac{1-\alpha}{\alpha J(\sigma)}}}$$

(13)

We can say that A_0^* is stable because the equilibrium doesn't converge or diverge to 0 even if there are some small temporary disturbances in the parameters.

The size of market liquidity at equilibrium is defined by the last equation. Informed trading and more severe asymmetric information hurt liquidity, whereas noisy trading enhances liquidity provision.

Furthermore, in competitive environment, the equilibrium liquidity tends to be stable. If A_0 fluctuates because of some small disturbances in the parameters and is pushed away from its equilibrium size A_0^*, the competitive force brings $\boldsymbol{A_0}$ back to the equilibrium stand.

Providing more liquidity is ideal for each LP if the total liquidity is less than $\boldsymbol{A_0^*}$ since V ($\boldsymbol{a_{i,0}}$) increases in $\boldsymbol{a_{i,0}}$. As a result, LPs increase the pool's liquidity and raise $\boldsymbol{A_0}$ as long as $\boldsymbol{A_0^*}$ > $\boldsymbol{A_0}$. It will continue to rise until $\boldsymbol{A_0 \geq A_0^*}$ holds. The benefit of each LP, however, decreases

in $\boldsymbol{a_{i,0}}$ if $\boldsymbol{A_0 > A_0^*}$. Then, when LPs remove liquidity from the pool, $\boldsymbol{A_0}$ falls until it maintains that $\boldsymbol{A_0^* \geq A_0}$. As a result, the stable and unique equilibrium is given by $\boldsymbol{A_0 = A_0^*}$.

9. Future Research

Reading through the papers of Alfred Lehar as well as Augustino Capponi I was really fascinated how they were able to compare centralized and decentralized exchanges in a very detailed way. In both papers the authors use data that they either got from Binance for the centralized exchanges or from running their own archive node on the Ethereum Blockchain. I was able to get in contact with the authors of both papers but unfortunately I cannot do such a research because of time, costs and data storage.

In the future I hope that I will have the chance either individually or with the help of other motivated people to try to recreate or in a way update their data sets and results that they got. In the paper of Capponi and Jia the authors state that the current pricing curves expose the LPs to arbitrage losses and leads to higher costs for liquidity provision as well as even to liquidity freezes in some cases. They were able to implement a model with a new socially optimal pricing curve that can actually balance the arbitrage losses and the price impact from trades. This would be a perfect way to continue my thesis having in mind the results that I got from the model. In order to conduct such a research I would also need to involve the fees of the exchange into the model because without the fees LPs would always suffer arbitrage losses because of the front running arbitrage.

10. Conclusion

After couple of months of writing the thesis while also working in finance, I was able to find and analyze a lot of information, data as well as mathematical models. As it may seem straightforward sometimes, the topic is for sure not easy to understand. As there are many speculations about Blockchain and Bitcoin that Satoshi Nakamoto is a fake name or that this person doesn't exist or that these exchanges were only made to serve as a financial pyramids and fall once they reach their maximum I cannot predict their outcome in the future years. I can only say, that as in every other exchange, doesn't matter if centralized or decentralized, there are still a lot of risks and speculations.

I think that the model that I was able to introduce and analyze had great outcomes and is a really good starting point for almost everyone. The fact that we can prove that arbitrage exists and that it is legal and people do millions of dollars because of this is in my opinion a great start for something bigger in the future as research. As we found out, if there are not fees liquidity providers are always going to suffer losses because of informed traders, or in other words they suffer from the front running arbitrage. This is why I implemented into the model a noise trader in order to see how the liquidity pools as well as the profit function of the LPs change. This way I was able to find a unique threshold for the model and for the liquidity supply in equilibrium.

It will be definitely interesting to see how this new system will evolve in the upcoming years. I personally think that the Ethereum Blockchain will continue to grow and prove itself even more as a stable system and cryptocurrency. From what I have heard and read online, there will be a new version of Uniswap in the upcoming months or years, which should be able to almost eliminate the front running arbitrage and give liquidity suppliers better chances to make profits from supplying liquidity because of new forms of fees as well as new instruments embedded into the system. In any case, the future is bright and I think this is only the beginning of this new decentralized world.

References

Abadi, Joseph and Markus Brunnermeier, “Blockchain economics,” Technical Report, mimeo

Princeton University 2018.

Abdeljalil Beniiche, A study of Blockchain Oracles, 2020

Adams, H. 2020. Uniswap. https://uniswap.org/blog/uniswap-v2/.

Adams, Hayden, Noah Zinsmeister, and Dan Robinson, “Uniswap v2 core,” 2020.

Angeris, Guillermo, Hsien-Tang Kao, Rei Chiang, and Charlie Noyes, 2019, An Analysis of Uniswap markets, Working Paper

Angeris, Guillermo, and Tarun Chitra, 2021, Improved price oracles: Constant function market makers, Working paper Stanford University

Antonopoulos, Andreas M, Mastering Bitcoin: unlocking digital cryptocurrencies, O’Reilly Media, Inc., 2014.

Aoyagi, J., and Y. Ito. 2021. Coexisting exchange platforms: Limit order books and automated market makers. Working Paper.

Barbon, A., and A. Ranaldo. 2021. On the quality of cryptocurrency markets: Centralized versus decentralized exchanges. Working paper

Brummer, Christopher J., Disclosure, Dapps and DeFi (March 24, 2022)

Capponi, Agostino, and Ruizhe Jia, 2021, The Adoption of Blockchain-based Decentralized Exchanges, working paper.

Catalini, Christian and Gans, Joshua S., Some Simple Economics of the Blockchain (April 20, 2019)

Chen, Long, Lin William Cong, and Yizhou Xiao, “A Brief Introduction to Blockchain Economics,” 2019

De Filippi, Primavera, The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies (September 14, 2016)

Egberts, Alexander, The Oracle Problem - An Analysis of how Blockchain Oracles Undermine the Advantages of Decentralized Ledger Systems (December 12, 2017).

Harvey, Campbell R., Cryptofinance (January 14, 2016)

John, Kose and O'Hara, Maureen and Saleh, Fahad, Bitcoin and Beyond (November 1, 2021)

Kapengut, Elie and Mizrach, Bruce, An Event Study of the Ethereum Transition to Proof-of-Stake (February 25, 2023)

Lehar, Alfred and Parlour, Christine A., Miner Collusion and the BitCoin Protocol (March 22, 2020)

Levy, Adam, Blockchain, NFT, Metaverse and Cryptocurrency, 2022

Nakamoto, Satoshi, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

Park, A., The Conceptual Flaws of Constant Product Automated Market Making, 2021

Schilling, Linda and Harald Uhlig, “Some simple bitcoin economics,” Journal of Monetary Economics,2019

Schär, Fabian, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets (April, 2021)

Xu, J., N. Vavryk, K. Paruch, and S. Cousaert. 2021. Sok: Decentralized exchanges (DEX) with automated market maker (AMM) protocols

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

https://www.dreamstime.com/hand-holding-money-hand-banknotes-cash-payment-receiving-money-icon-hand-holding-money-hand-banknotes-cash-payment-image115680589

https://www.passion-entrepreneur.com/604-e-commerce.html

https://www.statista.com/statistics/730876/cryptocurrency-maket-value/

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

https://www.bitpanda.com/academy/en/lessons/what-is-a-dapp

https://docs.uniswap.org/contracts/v2/concepts/core-concepts/oracles#:~:text=A%20price%20oracle%20is%20any,phone%20as%20a%20price%20oracle.

https://www.coinbase.com/de/learn/crypto-basics/what-is-mining

https://v2.info.uniswap.org/home

https://www.dreamstime.com/hand-holding-money-hand-banknotes-cash-payment-receiving-money-icon-hand-holding-money-hand-banknotes-cash-payment-image115680589

https://www.passion-entrepreneur.com/604-e-commerce.html

https://www.bitpanda.com/academy/en/lessons/what-is-double-spending-and-why-is-it-such-a-problem/

https://www.investopedia.com/decentralized-finance-defi-5113835

https://www.techtarget.com/searchsecurity/definition/cryptography

https://www.blockchain-council.org/blockchain/blockchain-role-of-p2p-network/

https://commons.wikimedia.org/w/index.php?curid=16043262

https://ethereum.org/de/

https://www.bitpanda.com/academy/en/lessons/what-is-a-dapp

https://ethereum.org/en/developers/docs/oracles/

https://www.investopedia.com/news/bitcoin-pizza-day-celebrating-20-million-pizza-order/

https://ethereum.org/en/stablecoins/#main-content

https://ethereum.org/de/stablecoins/

https://www.ledger.com/de/academy/blockchain/was-ist-proof-of-work

https://www.ledger.com/de/academy/was-ist-proof-of-stake

https://www.cepsa.com/en/planet-energy/sustainable-innovation/the-high-energy-cost-of-cryptocurrencies#:~:text=The%20most%20famous%20of%20the,pressure%20on%20the%20power%20grid.

https://ethereum.org/en/roadmap/merge/

https://block-builders.de/ethereum-vor-the-merge-welche-quellen-zeigen-an-ob-alles-glatt-laeuft/

https://ieeexplore.ieee.org/iel7/6287639/9312710/09567686.pdf

https://medium.com/coinmonks/cryptotypes-decentralized-exchanges-and-marketplaces-xcc-dxm-1020ea090188

https://www.theblock.co/data/decentralized-finance/dex-non-custodial

https://blog.uniswap.org/uniswap-v2

https://blog.uniswap.org/uniswap-v4