UNISWAP - A CASE STUDY OF DECENTRALIZED EXCHANGES ON THE BLOCKCHAIN

Author: Nikolajs Koroļkovs, e-mail: hello@nick.tf, phone: +371 26189290
Scientific supervisor: Sergejs Kodors, PhD, e-mail: sergejs.kodors@rta.lv
Rezekne Academy of Technologies
Atbrīvošanas aleja 115, Rēzekne, LV-4601, Latvia

Abstract. The paper takes a close look at an emerging industry - decentralized finance on the blockchain. The goal of this paper is to compare centralized order book (CLOB)-based exchanges to automated market maker (AMM)-based decentralized exchanges (DEX) and analyze the challenges that AMM-based DEXes are facing today using Uniswap as an example.

Keywords: Uniswap, Decentralized exchange, DEX, AMM, Automated market maker, DeFi, Decentralized finance.

Introduction

Before the emergence of the Ethereum network blockchain technology has been a solution that was looking for a problem [1]. The original purpose of Bitcoin [2] has been to create a peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. But it has struggled to compete with existing payment systems due to the technical limitations [3] of its proof-of-work consensus algorithm and the questionable reputation of Bitcoin [4].

The important difference between Ethereum and Bitcoin is an introduction of Ethereum Virtual Machine (EVM) [5]. The key to the popularity of EVM and its Turing-complete language Solidity was that it allowed developers to write and execute code on the blockchain using smart contracts [6]. In a way, Ethereum blockchain network set out to be a global, decentralized computing platform [7]. According to “State of the DApps” [8], which is a not-for-profit curated directory of decentralized applications (DApps), over 4000 applications have been deployed on the Ethereum blockchain as of April 2022.

This paper will focus on the class of DApps that are used in decentralized finance. The Decentralised Finance (DeFi) market has experienced exponential growth since the summer of 2020 - the total value of crypto-assets locked in DeFi applications built on the Ethereum blockchain peaked in November 2021, exceeding 240 billion USD [9] – an increase from 14 billion USD a year earlier, according to the largest DeFi “total value locked” (TVL) aggregator DefiLlama.

The goal of this paper is to analyze the differences between DeFi and traditional centralized finance (CeFi). This is done by studying one of the most important sectors of financial markets – trading of digital assets. The paper will look at some advantages and disadvantages of AMM-based DEXes when compared against classical CLOB-based centralized exchanges (CEX). This includes studying the technical implementations and pinpointing the fundamental differences between the two. The paper will also highlight the regulatory challenges the DeFi sector is facing today.

Materials and methods

This paper is a case study of decentralized finance using Uniswap DEX as a subject. To gather information about DeFi and Uniswap the author will be using a collection of research papers that study AMMs and the blockchain technology, which is a form of Distributed Ledger Technology (DLT). Since DLT and DeFi are emerging fields, looking at the scientific publications won’t be enough - there is also a need to look at news articles, blog posts, social media, and source code repositories to gather and analyze information from various experts around the DeFi industry.

https://doi.org/10.17770/het2022.26.6950
Results and discussion

Earlier iterations of DEXes on the Ethereum blockchain, such as EtherDelta and IDEX, were implemented using limit-order based model [10]. They both managed their order books off-chain, since it’s impractical and too expensive to do that on-chain. Which meant that the degree to which they were decentralized was quite limited [11].

Uniswap was one of the first successful implementations of AMMs on the blockchain. It was created by Hayden Adams in 2018 [12] and the first version was based on a concept described by Vitalik Buterin in a blogpost [13]. Uniswap was built around a constant product formula [14], which in its simplified form can be viewed as $C = r_1 * r_2$, where $r_1$ and $r_2$ are reserves of the digital assets in a trading pool and $C$ is a constant. This formula is used to price assets in a pool.

As the project gained more traction and more support, it released new versions of the protocol - V2 [15] and V3 [16], that added new features to the exchange. Uniswap Labs, a company that was built around this project, has made V2 of Uniswap open source licensed under the GPL, which lead to the development of many Uniswap clones and competitors, some of which improved upon the platform’s weaknesses.

For example, Curve Finance [17] modified the constant product formula to facilitate stable coin swaps with lower fees and Balancer [18] tried solving the impermanent loss [19] problem of Uniswap by introducing multi-asset pools that lowered the potential impact of impermanent loss at the expense of complexity of market making in pools with more than 2 assets.

Advantages of AMM-based DEXes in comparison to CLOB-based CEXes

1) Censorship-resistance. Trustless blockchain networks, along with permissionless and immutable nature of smart contracts that were used to build Uniswap, have the potential to deny one authority the power to prevent users from using the trading platform. Centralized exchanges like Binance can arbitrarily prevent users from accessing the platform according to their terms of service [20].

2) Uniswap V2 has introduced the ability to use flash loans to trade digital assets. Flash loans provide users with the ability to borrow digital assets with no collateral if the assets get returned to the pool within the same blockchain transaction [21]. Flash loans take advantage of a unique property of Ethereum blockchain - atomicity of transactions [22].

3) According to the latest study [23], Uniswap V3 offers deeper liquidity on popular trading pairs than the leading centralized exchanges, such as Binance, Coinbase and Kraken. Deeper liquidity means lower slippage on trades, which could make prices of digital assets more stable.

4) Becoming a liquidity provider on AMM-based DEXes is an easy and trustless process, that can allow retail investors with no technical expertise and prior knowledge to become market makers in a trading pair and benefit from the ability to get a proportional cut of fees from all the trades performed on the platform [24]. This process is subject to significant counterparty risks, such as adverse selection and principal-agent problem [25].

5) AMMs rely on traders that participate in arbitrage to adjust the exchange rates of tokens across the market. In volatile markets such as cryptocurrency trading market this generates extra trading volume that benefits liquidity providers in AMM liquidity pools [26].

6) Uniswap V2 has introduced the potential to use the smart contracts of the trading pairs to calculate the time-weighted average price (TWAP) of the token [27]. Uniswap V3 has made further improvements to TWAP functionality [28]. As a result of that a lot of projects in DeFi have started using Uniswap as a price oracle [29]. It’s worth noting that some researchers have argued [30] that manipulating such an oracle could be less expensive than originally anticipated.

Disadvantages of AMM-based DEXes in comparison to CLOB-based CEXes

1) CEXes have been targeted by some high-profile hacks in the past [31], but the chances of third parties exploiting DeFi protocols are higher because of smart contract risk. The compiled bytecode and the state of all the deployed smart contracts are public [32] and anyone can
analyze them to try and find an attack vector. Bugs in proprietary software can exist for years without bringing any harm to the system. Due to the public nature of smart contracts, their inefficiencies, bugs, and logic errors get exploited on a regular basis [33] [34] [35]. Because of how devastating the impact from smart contract vulnerability can be, a new industry has emerged to try and solve the problem - smart contract security auditing [36].

2) The non-custodial nature of DApps can also be a disadvantage. For example, losing the private key to a non-custodial cryptocurrency wallet would mean there is no way to recover the funds, unlike an account on a CEX such as Binance, where recovery mechanisms exist.

3) To sell or buy a digital asset on a blockchain a user must submit a transaction. These transactions can sometimes get stuck due to a low gas fee in a period of high network activity [37]. This can lead to bad user experience. In fact, modern CEXes settle transactions faster than DEXes due to the need for a blockchain to reach consensus. So, trade settlement speed with the technology that exists today will be faster in a centralized solution [38].

4) Most DEXes that are competing with Uniswap, such as Sushiswap [39] and Pancakeswap [40] are running AMM implementations of open-sourced Uniswap V2 smart contracts. These pools have low capital efficiency [41]. CEXes typically offer APIs [42] that allow trading bots to cancel and repost new orders into an order book for free so market making in CEXes will require more effort but lead to better capital efficiency.

5) Impermanent loss (IL) is one of the main risk factors for market makers in both CEXes and DEXes. Impermanent loss is the loss incurred by a market making position versus keeping the initially allocated amounts fixed, it happens when the ratio of tokens A and B in a pool changes. This is even more relevant for Uniswap V3, since it can potentially increase [43] the IL of a liquidity provider while offering better capital efficiency.

6) High-frequency trading in traditional stock markets has been brilliantly covered by Richard Lewis in a book called “Flash boys”. Due to Ethereum having a public pool of pending transactions called mempool [44], digital asset trading on DeFi is plagued by frontrunning [45], which leads to similar abuses of retail traders at the hands of trading bots.

7) The regulatory challenges that the DEXes are facing is the hurdle that is hurting institutional adoption without which widespread adoption of DeFi is highly unlikely. This problem gets looked at in the next section of the paper.

**DeFi and regulatory challenges**

The chairman of the SEC Gary Gensler has signaled that the regulators will focus more on exchanges that facilitate the trading and creation of digital assets that need to be registered with the SEC [46]. Some of the tokens that are traded on Uniswap can be considered securities [47].

Uniswap governance token UNI, which Uniswap announced on September 16th of 2020, is the only digital asset Uniswap Labs has released [48], and it was done not in exchange for money, but to reward loyalty. Classifying UNI token as a security will require it to pass a Howey test [49]. Since UNI is a governance token, it possesses unique characteristics that frustrate a simple Howey test application. A governance token implemented as a loyalty program decentralizes governance to loyal members of the community and cuts against the first element of the Howey test in requiring an exchange of money.

That’s not to say that Uniswap Labs and its advisors and investors have not benefitted from the UNI token. UNI token emission, supply schedule and distribution [50] is showing that Uniswap’s team and venture capital investors will have a disproportionate amount of power [51] in the early stages of governance, even though they are unlikely to use it considering the potential damage to their reputation and the impediment to the success of the protocol. Still, it begs the question – how decentralized Uniswap really is?

Nonetheless, when it comes to potential legal problems Uniswap as a company can’t be looked at in the same way as BlockFi [52] and EtherDelta [53] that were involved in investigations conducted by the SEC that led to fines and settlements, since Uniswap isn’t making any promises regarding the potential profit from the investments [54] and it makes sure that the potential investors are aware that only they are liable for their actions. Still, it remains an open question whether the Uniswap terms of service and disclaimer [55] will protect the developers of the project from the SEC when it decides to
regulate decentralized exchanges that are using smart contracts on the blockchain to facilitate trading.

The problem lies in the fact that the laws are constantly evolving, and the SEC is trying to keep up with the new technology by proposing new amendments [56] to the Securities Exchange Act. These amendments redefine what constitutes an exchange and could potentially force companies like Uniswap Labs to adopt and maintain a suite of compliance programs covering disclosure obligations, trade reporting, anti-financial crimes, and suspicious activity reporting, as well as passing qualification exams. Complying with this would be impossible given the immutable nature [57] of Uniswap contracts.

Since liquidity pools and trades on these exchanges run in permissionless manner [58] Uniswap developers have no way of stopping people who want to use the smart contracts of the exchange even if they shut down the website. In fact, according to a tweet from Hayden Adams [59], most of the trading volume on Uniswap in 2021 didn’t come through the official website but instead came from trading bots, website forks and wallets. The only way to stop people from using these smart contracts would be through extreme reputational damage to Uniswap, which a high-profile lawsuit or an unfavorable ruling of the SEC theoretically might be able to accomplish.

As far as dealing with other exchanges that do not have a legitimate company behind them, it’s going to be up to the government to track the movement of digital assets on the blockchain and look for unlawful activities like tax evasion and money laundering. And the recent signing of a new deal with a blockchain analytics firm AnChain.AI to help monitor and regulate the DeFi industry [60] goes to show that the SEC takes these matters seriously. In addition to cataloguing and monitoring known wallets tied to illicit actors, AnChain.AI has built a predictive engine that can be used to identify unknown addresses and transactions that could be suspicious.

Conclusions

Even though the new generation of AMM-based DEXes are offering some interesting technical solutions and novel approaches to solving old problems, until the regulatory woes and the issues with usability are resolved the widespread adoption of DeFi is unlikely, it will remain a tiny niche on the global market. Even as adoption grows, it is likely that instead of using non-custodial wallets most investors will get exposed to DeFi via third parties, such as Binance, Revolut or Paypal. Non-custodial nature, censorship resistance and the appeal of high risk/high reward are compelling enough to attract risk-tolerant investors, so DeFi is here to stay, and, despite all the problems, it has a real use case and a target audience.

There are some interesting developments in other areas of decentralized finance that might help with institutional adoption, for example Aave Arc and Maple Finance, that are permissioned lending platforms on the blockchain that are compliant with KYC and AML regulations. It will be interesting to see if they will bring more institutional capital into the DeFi sector.

Regarding technical evolution of DEXes, it’s fair to say that the open-source nature of smart contracts on the blockchain and a huge influx of venture capital [61] into DeFi startups has allowed for a rapid increase in quality and security of decentralized applications. Current blockchain solutions can run into problems with scalability [62], but that’s to be expected since the industry is in its infancy and the networks are in active development [63] and are constantly evolving. DLT is still in the era of growing pains, high-profile hacks, and non-stop innovation.

Bibliography
