

*A Progress Report*

*on*

# **Decentralized Exchange built on EVM Blockchain**

*carried out as part of the course CSE CS3270 Submitted by*

***Shubh Gupta & Raghav Bhardwaj***

***Roll no – 199301305 & 199301224***

***VI-CSE Section - C***

*in partial fulfilment for the award of the degree*

*of*

**BACHELOR OF TECHNOLOGY**

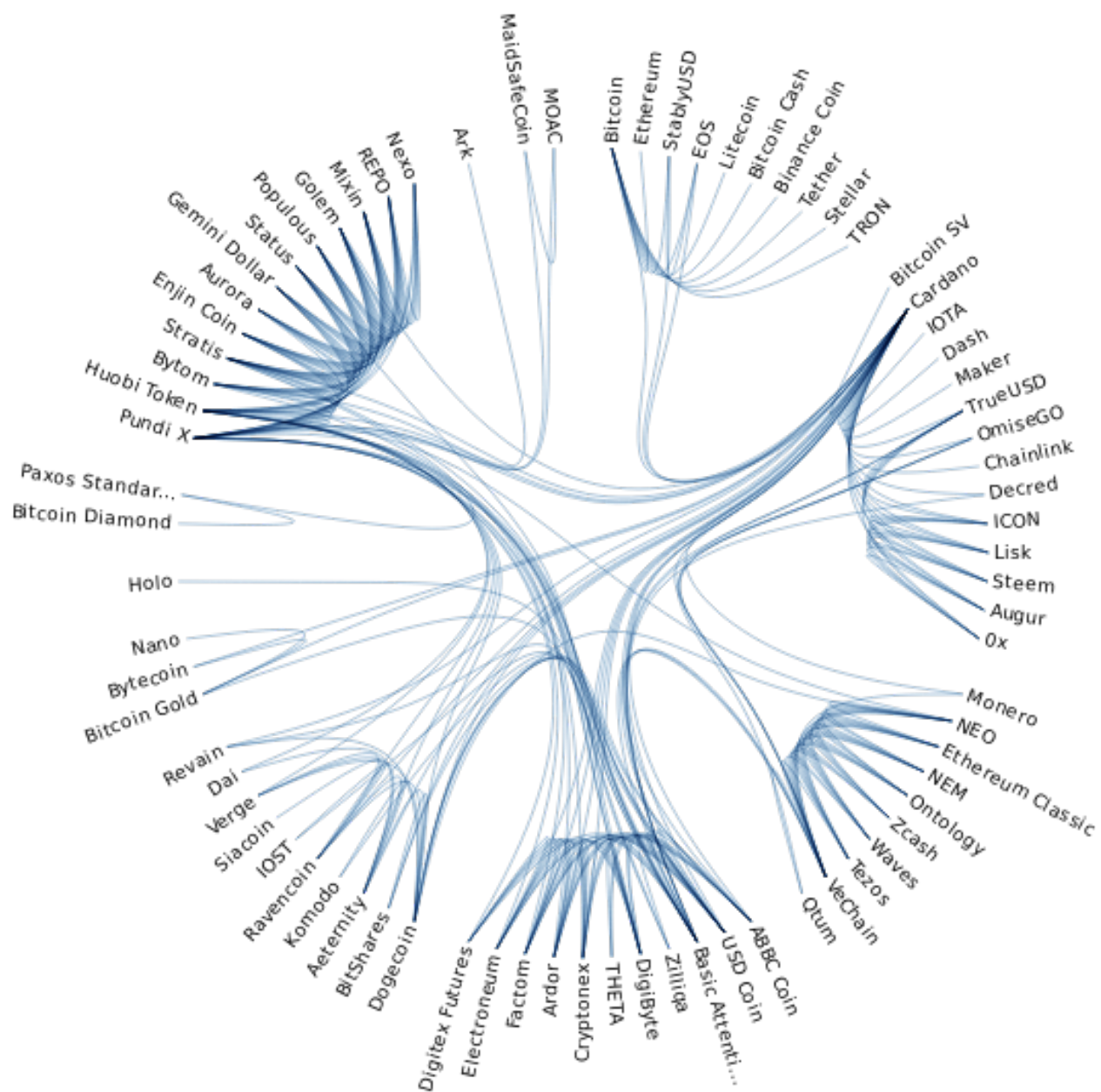
**In**

**Computer Science & Engineering**



**MANIPAL UNIVERSITY  
JAIPUR**

**Department of Computer Science & Engineering,  
School of Computing and IT,**



## Decentralized Exchange

# Abstract

With the revived interest in blockchain and cryptocurrency among both the general populace and institutional actors, the past year has witnessed a surge in crypto trading activity and accelerated development in the decentralized finance (DeFi) space. Among all the prominent DeFi applications, decentralized exchanges (DEX) with automated market maker (AMM) protocols are in the ascendency.

Cryptocurrency exchanges provide a crucial source of liquidity to the global cryptocurrency market, facilitating billions of dollars in trading volume on a daily basis. As this market expands, leading exchange platforms continue to scale in response to the demand for digital assets, offering asset custody, new trading features and functionality, and access to an ever-growing number of digital assets.

Every app that is built on a blockchain platform today, boasts the fact that it is decentralized. So, it's not surprising that crypto exchanges should want to jump on the bandwagon and create their own decentralized exchange (DEX), where there's no middleman, just traders swapping tokens with each other. Decentralized exchanges are interesting because they offer a number of advantages over traditional exchanges. For example, they're immune to hacks and manipulations.

# Table Of Content

1. Introduction
  - 1.1 Scope
  - 1.2 Product Scenarios
2. Requirement Analysis
  - 2.2 Functional Requirements
  - 2.3 Non-Functional Requirements
  - 2.3 Use Case Scenarios
3. System Design
  - 3.1 Design Goals
  - 3.2 System Architecture
4. Work Done
  - 4.1 Development Environment
  - 4.2 Proof of Concept
  - 4.3 Results & Discussion
  - 4.4 Individual Contribution of Projects Members
5. Conclusion & Future Plan

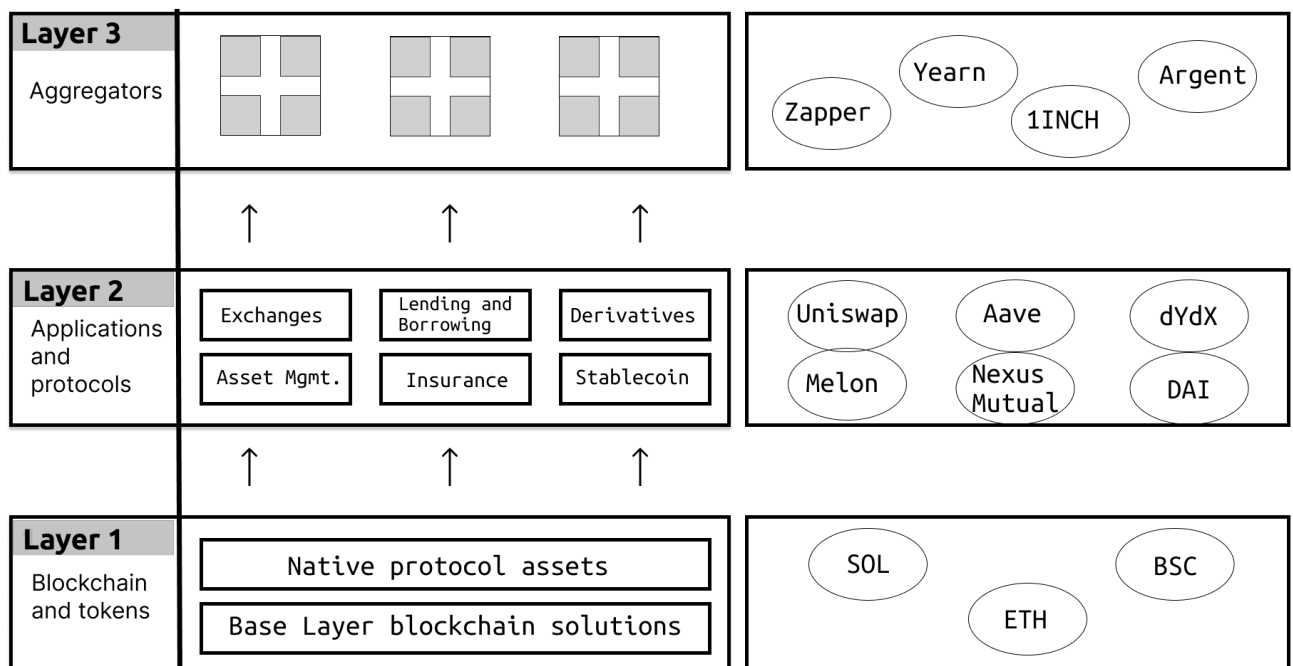
# Introduction

## Scope

With the revived interest in blockchain and cryptocurrency among both the general populace and institutional actors, the past year has witnessed a surge in crypto trading activity and accelerated development in the decentralized finance (DeFi) space. Among all the prominent DeFi applications, decentralized exchanges (DEX) with automated market maker (AMM) protocols are in the ascendancy, with an aggregate value locked exceeding \$100 billion at the time of writing.

AMM-based DEX bear attractive features such as decentralization, automation, and continuous liquidity. With traditional order-book-based exchanges, the market price of an asset is determined by the last matched buy and sell orders, ultimately driven by the supply and demand of the asset. In contrast, on an AMM-based DEX, a liquidity pool acts as a single counterparty for each transaction, with a so-called conservation function that prices asset algorithmically by only allowing the price to move along predefined trajectories.

### The DeFi tech stack



## Product Scenarios

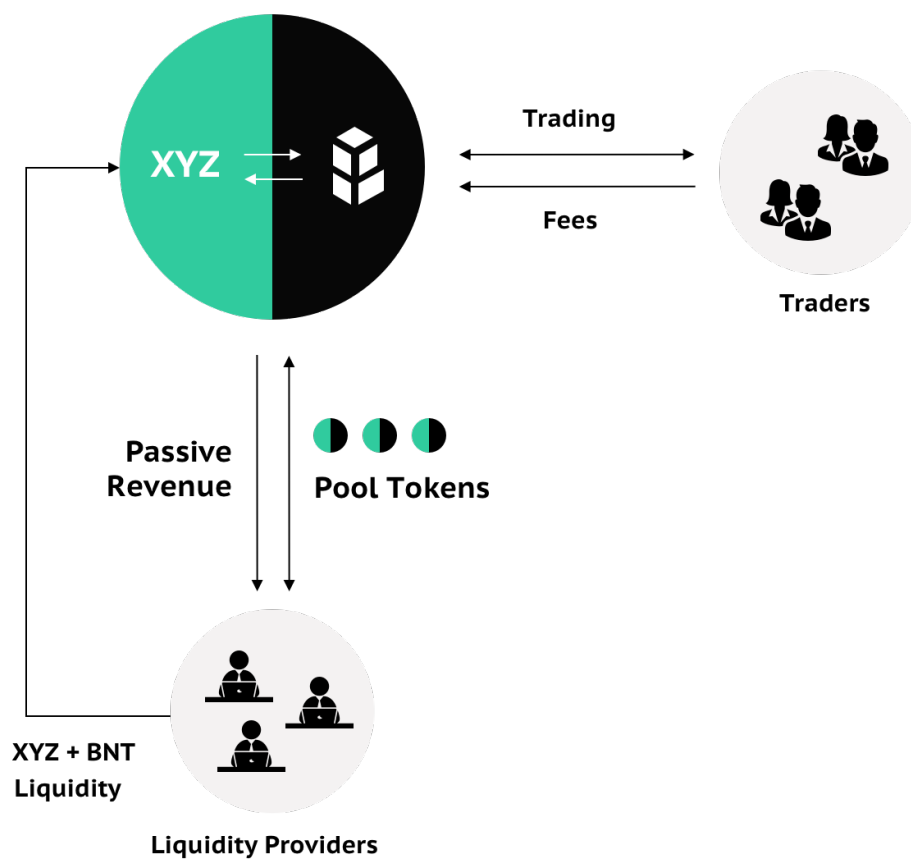
This presents AMMs-based DEX's main components, including different actors and assets, as well as their generalized mechanism and economics:

### Actors

1. Liquidity Provider
2. Exchange User (Trader)
3. Protocol Foundation

### Assets

1. Risk Assets
2. Base Assets
3. Pool Shares
4. Protocol Tokens



# Requirement Analysis

## Function Requirements:

1. Should have a robust trading engine & Orderbook.
2. A good UI/UX Platform
3. Should Have AMM integration.
4. Crypto Wallet integration
5. A good working Admin Panel.
6. Users' login data should be saved and should not be required to login after each session.

## Non-Functional Requirements:

1. It Should support both cross chain & on chain protocol.
2. Flexible & multiple payment systems.
3. Provide different DEX aggregation for different DEX.
4. Should have low gas fees & faster transaction time.
5. Should not be susceptible to arbitrage.
6. Should be open source & open to community building.
7. Should have a large Liquidity pool.

## Use Case Scenario:

### A: The Exchange

- Minimise execution costs while maximising availability for liquidity providers
- Variable, depending on setup of governance and holders of governance tokens
- Develop and deploy AMM mechanism & function
- AMM: Calculate price offered based on token balance and AMM function
- Collect transaction fees, mint tokens to distribute to liquidity providers as reward

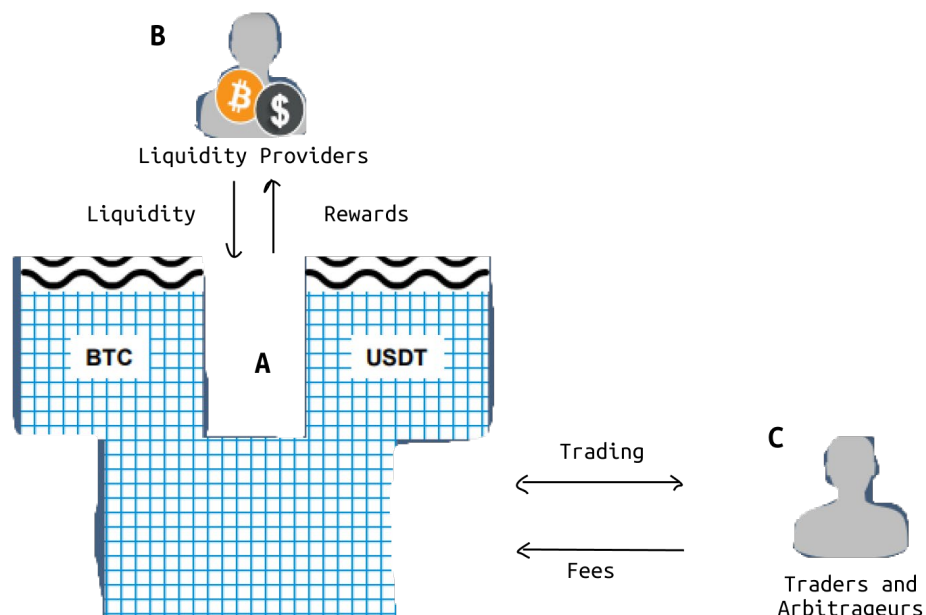
### B: Liquidity Providers:

- Maximise rewards generated from liquidity provided
- Provide tokens into liquidity pools
- Earn a share of trading fees and reward tokens
- Move funds between different liquidity pools in search of highest yields ('yield farming')

### C: Traders and arbitrageurs:

- Minimise trading cost
- Execute arbitrage opportunities
- Pay a transaction fee on every trade
- 'Regular' traders: Trade against price offered by AMM
- Arbitrage traders: Discover arbitrage opportunities between external markets and AMM prices, execute to bring prices in line with market

## **Visualisation of an exchange utilising an AMM and liquidity pool**





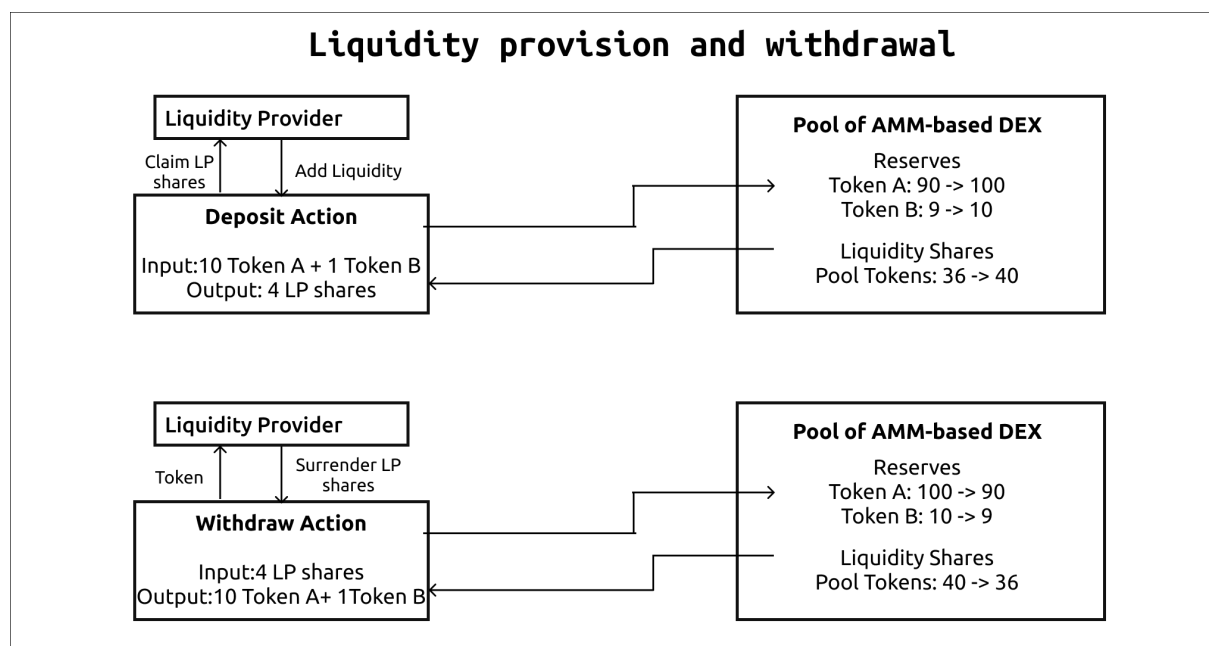
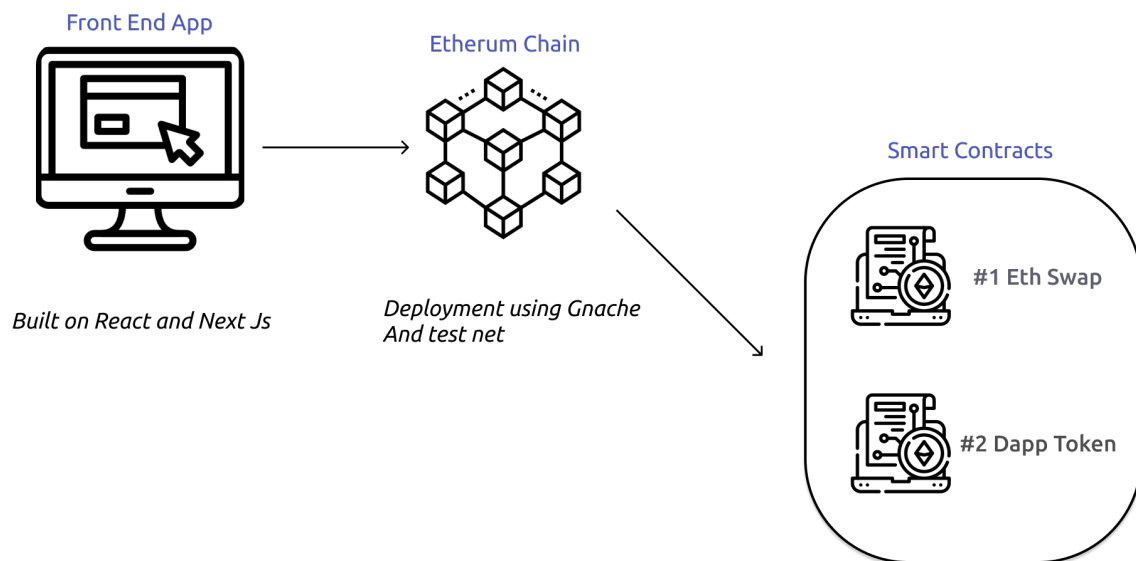
# System Design

## Design Goal:

1. High-level Security: As mentioned above, decentralized exchange systems are more secure than centralized ones since the users' funds are not stored in online wallets within the crypto platform. The users get more independence when conducting transactions. Also, it significantly reduces the risks of hacks and breaches.
2. Transactions' Transparency: Blockchain systems allow the users to track all transactions and their statuses. It makes every transaction transparent and available to the public.
3. Complete Anonymity: Unlike centralized exchanges, DEX platforms don't require the customers to provide their personal information to perform any transaction. Thus, a decentralized crypto exchange system is much more convenient for those who want to remain anonymous. When using DEX, users can avoid passing a common identification process that includes sharing their full name, personal ID details, etc.
4. Unlimited Number of Tokens: Centralized cryptocurrency exchange apps have strict limits on the available tokens and coins. A CEX platform should follow numerous regulations and include only legalized tokens. Meanwhile, DEX platforms have no limits and may include any tokens as soon as they appear on the blockchain.
5. No Intermediaries: Instead of using third-party services, decentralized platforms are based on smart contracts. It means that no intermediaries are involved in the transaction process. Thus, the counterparty risks are minimized, and the direct exchange participants have complete control over each transaction.

## System Architecture:

1. Front End App using Reach & Next Js.
2. Working environment for the Ethereum chain using Gnache & test net.
3. Smart Contracts built using solidity – Ethereum Swap & Dapp Token



# Work Done

## Development Environment:

1. Remix IDE: An open source Ethereum IDE we can use to write, compile and debug Solidity Code.
2. Ganache: Ganache is a personal Ethereum Blockchain used to test smart contracts where you can deploy contracts, develop applications, run tests and perform other tasks without any costs.
3. Truffle: Truffle is a development environment, testing framework and asset pipeline for Ethereum, aiming to make life as an ETH developer easier.
4. Proof Of Concept – Using Moralis, 1INCH DEX API & Metamask.

A proof of Concept based on the concept of Decentralized Exchange using –

HTML/CSS, JS

Moralis backend


1INCH DEX API

Metamask integration.


Dex

Metamask Login Logout

Swap

 ETH

1

 cETH

49.34709463

Estimated Gas: 419039

Swap

## Results & Discussion:

AMM-based DEX bear attractive features such as decentralization, automation, and continuous liquidity. With traditional order-book-based exchanges, the market price of an asset is determined by the last matched buy and sell orders, ultimately driven by the supply and demand of the asset. In contrast, on an AMM-based DEX, a liquidity pool acts as a single counterparty for each transaction, with a so-called conservation function that prices asset algorithmically by only allowing the price to move along predefined trajectories.

The emerging DEX market encompasses distinct segments. Each platform uses various implementations of order books, liquidity pools, or other decentralized finance (DeFi) mechanisms like aggregation tools to offer novel and experimental financial instruments

## Individual Contribution of Project Members:

- **Shubh Gupta** , learnt the intricacies of solidity, blockchain and the backend required to run a Decentralized Exchange Platform. Also read up on the current DEFI Space and its limitations and looked into different DEX currently being used.
- **Raghav Bhardwaj**, started working on the initial prototype of the UI/UX learning React Js and Next js , looking into the Truffle framework on which the project is going to be built on, and methods which can be implemented. As well as working on FIGMA diagrams and all the System design hierarchy.
- **Both Shubh Gupta & Raghav Bhardwaj**, learn solidity and how a blockchain as well as Decentralized platform works.

# Conclusion

With important qualities like decentralisation, persistence, anonymity, and auditability, Blockchain has proved its potential to revolutionise established industries.

We conclude that there are time varying returns to liquidity provision. These returns are higher when there is more liquidity provided consistency with a liquidity externality. Our data is consistent with an equilibrium pool size – for large pools an increase in liquidity flows leads to future liquidity withdrawals, while for smaller pools growth in pool size lead to more liquidity 1 additions. Similar to mutual fund flows we document that there appears to be “yield chasing” in liquidity pools. High past returns lead to future inflows while low past returns lead to future outflows. Liquidity use is also persistent.

Future Plans is to provide more Decentralized Exchange platforms on a single platform and providing DEX aggregations for all these third party DEX out there.

This provides more inter and outer chains swaps as well as faster transaction which can be done in backend and user are not bothered.

# References

- Observable HQ Edge Bundling : <https://observablehq.com/@d3/bilevel-edge-bundling> .
- Altoros: Blog on Digital Transformation  
<https://www.altoros.com/blog/blockchain-for-insurance-reduced-fraud-and-streamlined-claims/>
- Decentralized Markets:  
<https://www.investopedia.com/terms/d/decentralizedmarket.asp> .
- Atomic Swaps : <https://medium.com/coinmonks/how-to-build-your-own-decentralized-exchange-based-on-atomic-swaps-using-oracle-3ee4858f128d> .
- SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols : <https://arxiv.org/abs/2103.12732> .