Web3 Finace System Hack 101 - DEFI OR DEX 02

DeFi: Open markets, no central control. Accessible to all with Ethereum. Automated, secure, and transparent. No barriers, no downtime.

Decentralized Exchanges (DEXs) are peer-to-peer marketplaces that allow users to trade and exchange cryptocurrencies without interference from centralized authorities.

--> **Uniswap Smart Contracts - one of the most popular and oldest decentralized exchanges in the web3 ecosystem**.

To understand what Uniswap does, let's understand the functionality of a decentralized exchange.

Here's a few important terms to know:

- **Liquidity:** In simple terms, liquidity refers to how easily an asset can be converted into cash.
- **Decentralized Exchange (DEX):** A DEX is an exchange that doesn’t rely on a third party to hold users' funds. Instead, DEX users transact with each other directly.
- **Liquidity Pool:** A liquidity pool is a collection of digital assets accumulated to enable trading on a DEX. Since DEXs don’t follow an order book matching pattern, they need more liquidity than centralized exchanges to enable trades to go through. For this, they use a methodology called Automated Market Making (AMM). Due to this methodology, DEXs are also known as Automated Market Makers.
- **Automated Market Maker(AMM):** Automated market makers (AMMs) are part of the decentralized finance (DeFi) ecosystem. They are functions that dictate prices in accordance with supply and demand.

Extra-Note Decentralised financing (DeFi) has created a need for new forms of insurance. Large cryptocurrency deposits can be stolen or devalued within minutes. Smart contracts can contain unforeseen errors, making any funds they contain permanently unavailable. These risks require a new insurance system.

Order Book VS AMM

Order Book: In simple terms, an order book is like a marketplace where buyers and sellers come together to trade assets. It keeps a record of all the buy and sell orders placed by participants. It consists of two sides: the "bid" side where people offer to buy assets at a certain price, and the "ask" side where people offer to sell assets at a specific price. The order book matches these buy and sell orders to determine the price at which a trade can occur. It provides transparency by showing the current supply and demand for an asset, allowing participants to choose the price and quantity at which they want to buy or sell.

AMM (Automated Market Maker): AMM is a different approach to trading assets, particularly in decentralized finance (DeFi). Instead of relying on an order book, AMMs use a mathematical formula or algorithm to determine the asset's price and facilitate trades. AMMs typically work by creating liquidity pools where users can deposit their assets. These pools are used to automatically execute trades based on predetermined rules. AMMs ensure that there is always a constant liquidity supply for traders, even when there may not be enough participants to create a traditional order book. The prices in AMMs are determined based on the ratio of assets in the liquidity pool, using a formula such as the constant product formula (e.g., the popular Uniswap protocol). This allows for decentralized and continuous trading without relying on order matching.

Permissionless Systems

The second departure from traditional markets is the permissionless and immutable design of the Uniswap protocol. These design decisions were inspired by Ethereum's core tenets, and our commitment to the ideals of permissionless access and immutability as indispensable components of a future in which anyone in the world can access financial services without fear of discrimination or counter-party risk.

Permissionless design means that the protocol's services are entirely open for public use, with no ability to selectively restrict who can or cannot use them. Anyone can swap, provide liquidity, or create new markets at will. This is a departure from traditional financial services, which typically restrict access based on geography, wealth status, and age.

The protocol is also immutable, in other words not upgradeable. No party is able to pause the contracts, reverse trade execution, or otherwise change the behavior of the protocol in any way. It is worth noting that Uniswap Governance has the right (but no obligation) to divert a percentage of swap fees on any pool to a specified address. However, this capability is known to all participants in advance, and to prevent abuse, the percentage is constrained between 10% and 25%.

Uniswap as an AMM

Uniswap is a decentralized Automated Market Maker (AMM) protocol that allows anyone to swap token A for token B. As we just learned, an automated market maker works differently from a traditional order book model.

There are three versions of Uniswap, but in this section, we are mainly walking through V2 for the following reasons:

1. V1 is too simple and does not have all the modern features.
2. V3 is more efficient than V2 and it also optimizes funds utilization by adding “tick,” making it much more complicated.

Architecture overview of Uniswap V2.

Core

Core is for storing funds and managing them. It contains two smart contracts, **Pair** and **Factory**.

- **Pair:** Smart contract that has functionality for swapping, minting and burning tokens.
- **Factory:** Creating and tracking pairs, SImple word Deploying contracts

Periphery

Periphery, obviously, contains smart contract to interact with **Core**. It also contains two smart contracts, **Router** and **Library**

- **Router:** Interacting with the core. Provides function such as `swapETHForExactTokens`, `swapExactETHForToken`, etc.
- **Library:** Some function like `getReserves`, `getAmountIn`, `getAmountOut`, etc.

Uniswap V3

Uniswap V3 is the forthcoming new and improved DEX that will run on the Ethereum blockchain and be powered by the same automated market maker (AMM) model as V2.

V3 is loaded with new developments aimed at maximizing returns for traders and liquidity providers, minimizing price slippage, and managing downside risks.

Uniswap V3 boosts the efficiency of its AMM model, which is one of the most significant features to observe when comparing DEXs.

Through the introduction of a **concentrated liquidity** concept, liquidity providers have the ability to supply their assets within a definite price range for which they deposit liquidity.

Moreover, they have given tier-based rewards based on the degree of risk they are taking on in any particular pool. This can incentivize more liquidity providers to participate as the rewards would potentially help offset some of their potential losses in supplying liquidity to a wider price range.

The combination of these features enhances the efficiency of the AMM model that supports Uniswap V3's DEX, which would benefit traders thanks to more liquidity. Furthermore, liquidity providers can also possibly gain higher returns on their capital with as much as **4000x** efficiency.

Uniswap has been a victim of its own success, receiving heavy criticism that its popularity is slowing down the Ethereum network and causing transaction gas fees to skyrocket. Also, Uniswap has seen the repeated exploitation and copying of its code by competitors like Sushiswap and Binance Smart Chain

Uniswap v3 boosts the efficiency of its **AMM** model, which is one of the most significant features to observe when comparing **DEXs**.

Through the introduction of a **concentrated liquidity** concept, liquidity providers have the ability to supply their assets in a definite price range for which they deposit liquidity.

Top 3 of V3

Before we start looking at the Advanced Terms, let's take a quick look at the top three features of V3.

1. **Concentrated Liquidity**

Concentrated liquidity is the main concept behind V3. In V3, liquidity pools (LPs) can choose a custom price range when providing liquidity. This allows for concentrating capital within ranges where most of the trading activity occurs.

To achieve this, V3 creates individualized price curves for each of the liquidity providers. LPs earn trading fees that are directly proportional to their liquidity contribution in a given range.

2. **Capital Efficiency**

Concentrating liquidity offers much better capital efficiency for liquidity providers. When V3 launches, the maximum capital efficiency is **4000x** better than V2.

This will be achievable when providing liquidity within a single 0.1% price range. On top of that, the V3 pool factory will be able to support ranges as granular as **0.02%** — which translates to a maximum of **20,000x** capital efficiency relative to V2. 🥳

3. **Active Liquidity**

V3 also introduces the concept of **active liquidity.** This concept means users can provide liquidity for a particular price range, say when Bitcoin is between 10k-20k. This is an enormous opportunity for liquidity providers to start collecting all trading fees because of the pricing range.

This could be seen as contrasting to the open-source philosophy of Blockchain. The team announced the time-delayed license for Uniswap v3. This means that Uniswap v3 Core has launched under the Business Source Licence 1.1. This has limited the use of the Uniswap v3 source code in commercial or production use for up to two years.

They decided to do this to prevent potential future copycats, such as SushiSwap. However, all code needed for external integrations isn't affected by this license.

Uniswap v3 is not only enabling a higher return on capital for its users, but it also brings new possibilities to the developer community to build an ecosystem around it.