UNIVERSITY of NICOSIA

Session 4.1

Decentralized Exchanges

BLOC 611: Introduction to Decentralized Finance

Objectives

- Define and demystify Decentralized Exchanges (DEXes)
- Explore the growth of DEXes and notable protocols
- Understand the concept of Automated Market Makers (AMMs)
- Understand the concept of Liquidity Pools
- Understand Liquidity Mining

Agenda

1. Centralized and Decentralized Exchanges
2. How DEXes work
3. Notable DEXes
4. Advanced topics on DEXes
5. Exotic Finance = Exotic Risks
6. Conclusions
7. Further Reading

Session 4.1: Decentralized Exchanges

1. Centralized and Decentralized Exchanges

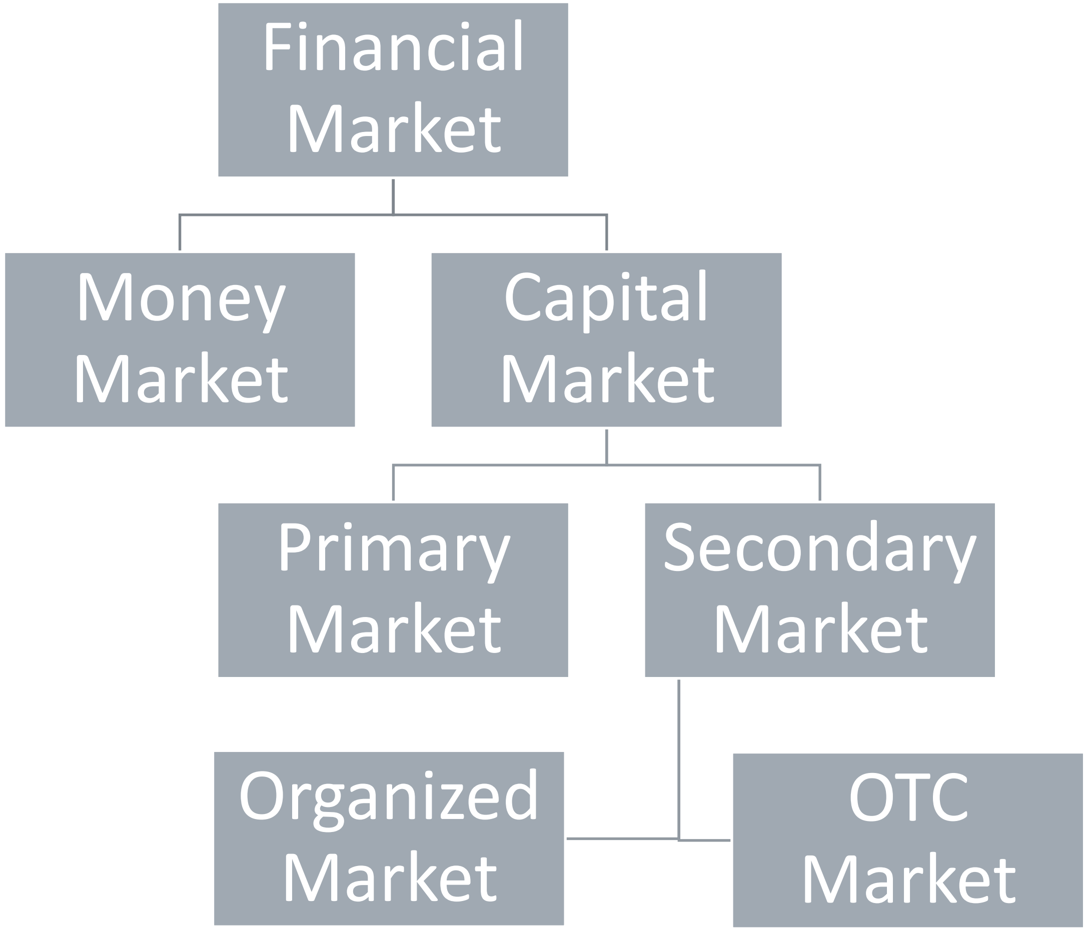
From real and financial assets to exchanges

Real assets are physical goods, such as commodities, real estate, land, and precious metals, that **derive value from their substance**.

In contrast, **financial assets** are non-physical and **derive value from contractual agreements**. Examples of financial assets include cash, stocks, bonds, and derivatives. Financial assets are traded in **financial markets.**

- Financial markets can be classified into:
  - **Money markets:** debt, short-term, highly liquid, credible issuers (low default risk)
  - **Capital markets:** debt, equity, long term, quality of issuers ranges
  - **Primary markets:** financial assets are first “created” and offered to the wider public for purchase
  - **Secondary markets:** financial assets are bought and sold, after their initial issuance
  - **Organized markets:** listing and trading follows formal rules, procedures and customs
  - **Over-the-counter markets** (OTC): listing and trading don’t abide by specific rules

Visualizing Financial Markets



Centralized Exchanges (CEXes)

- **Centralized exchanges** are financial markets where financial assets can be bought and sold.
  - Stock exchanges like the New York Stock Exchange (NYSE), Nasdaq, the London Stock Exchange (LSE), etc.
  - Cryptocurrency exchanges like Coinbase, Binance, Kraken, etc.
- The role of centralized exchanges
  - Centralized exchanges serve as an **intermediary**, providing a platform for matching buyer and sellers
  - Most individuals do not trade in the market directly, but instead do so through another **intermediary** called a **broker**
  - Brokers buy and sell financial assets on behalf of their clients for a fee. They may also serve as financial advisors.
  - Most brokers work for a brokerage firm, adding another layer of **intermediation**.
  - Online brokers have made investing in the stock market more accessible by offering reduced commissions.

Cryptocurrency Exchanges

Centralised cryptocurrency exchanges adopt many of the characteristics of their traditional counterparts. They serve **intermediaries** by being:

- A **platform** for matching buyer and sellers
- A **broker** by placing orders on behalf of their clients
- A **liquidity provider** by maintaining pools of assets
- A **custodian** for storing user assets
- A **portfolio manager** by providing information and even advice to their clients
- And even as an **underwriter** (usually the role of an investment bank) in Initial Exchange Offerings (IEOs)

○ Ironically, by serving so many roles, **cryptocurrency exchanges are more centralized than their traditional counterparts**.

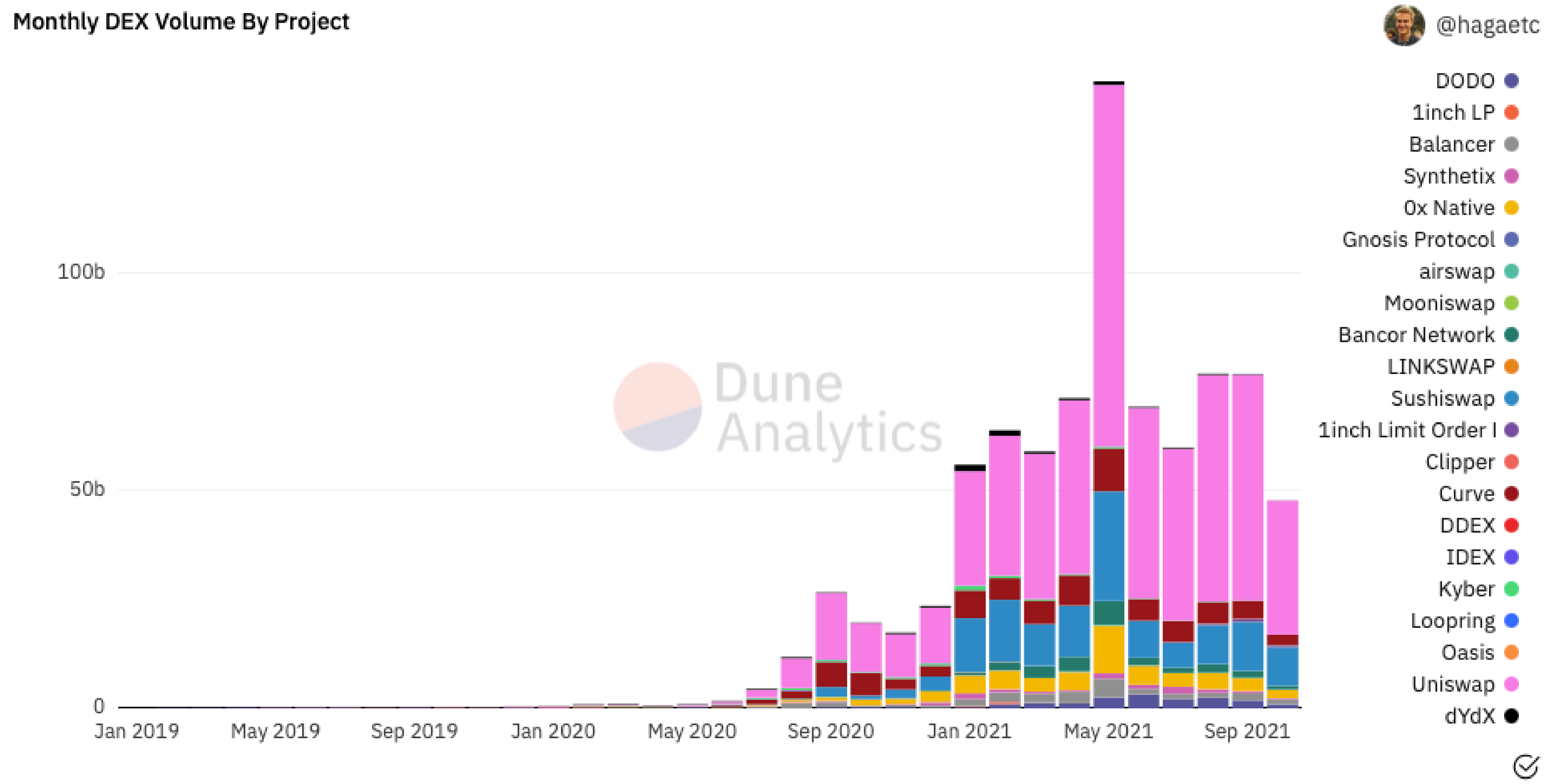
○ This comes with all the disadvantages of centralization that we discussed in previous chapters

What are Decentralized Exchanges

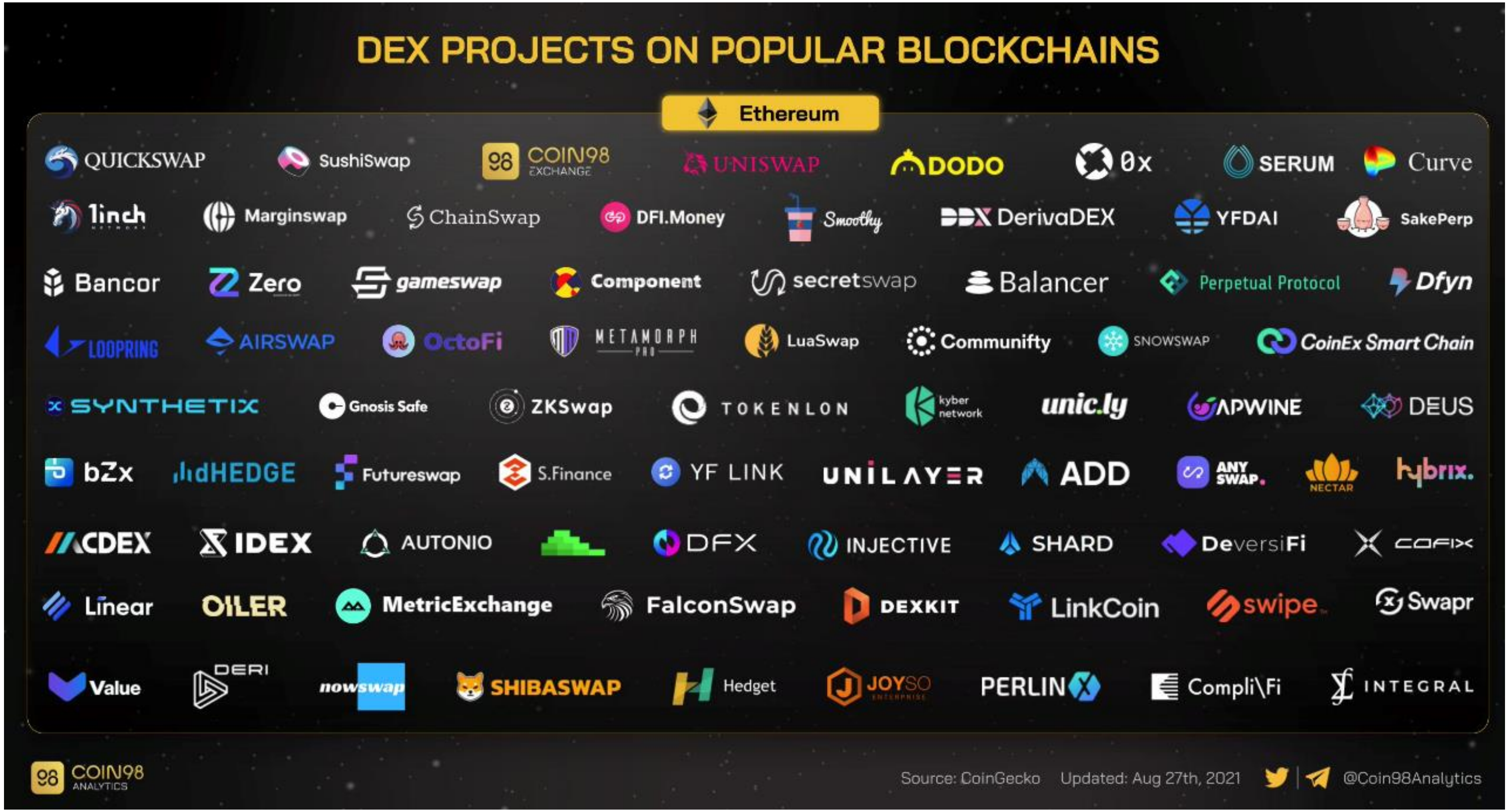
A **Decentralized Exchange (DEX)** is a decentralized application (dApp), that utilizes smart contracts to enable anyone to perform token swaps without the need of a third party.

- The main innovation and difference is that DEXes, unlike CEXes, **allow their users to trade in a peer-to-peer manner by reducing or even eliminating the the need for any intermediary.** This includes:
  - Brokers
  - Market Makers
  - Custodians
  - Investment Banks for Underwriting/Listing
  - Portfolio Managers
- Decentralized Exchanges instead use novel technologies and mechanisms to replicate the above, allowing for:
  - Self custody and privacy
  - Financial inclusion
  - Composability and interoperability with other DeFi Applications
  - Potential for lower transaction costs

DEX trading volume over time



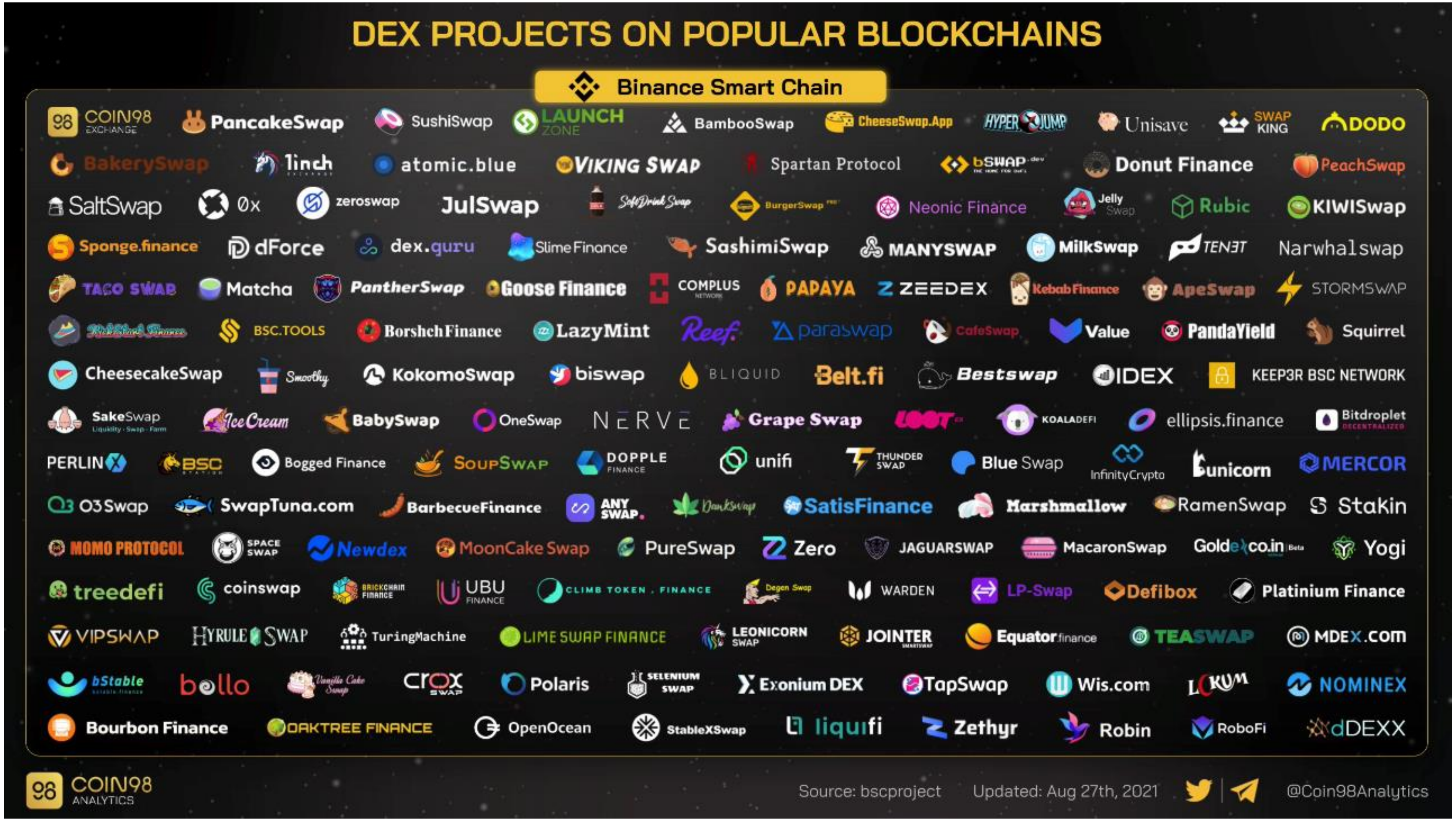
DEXes on Ethereum



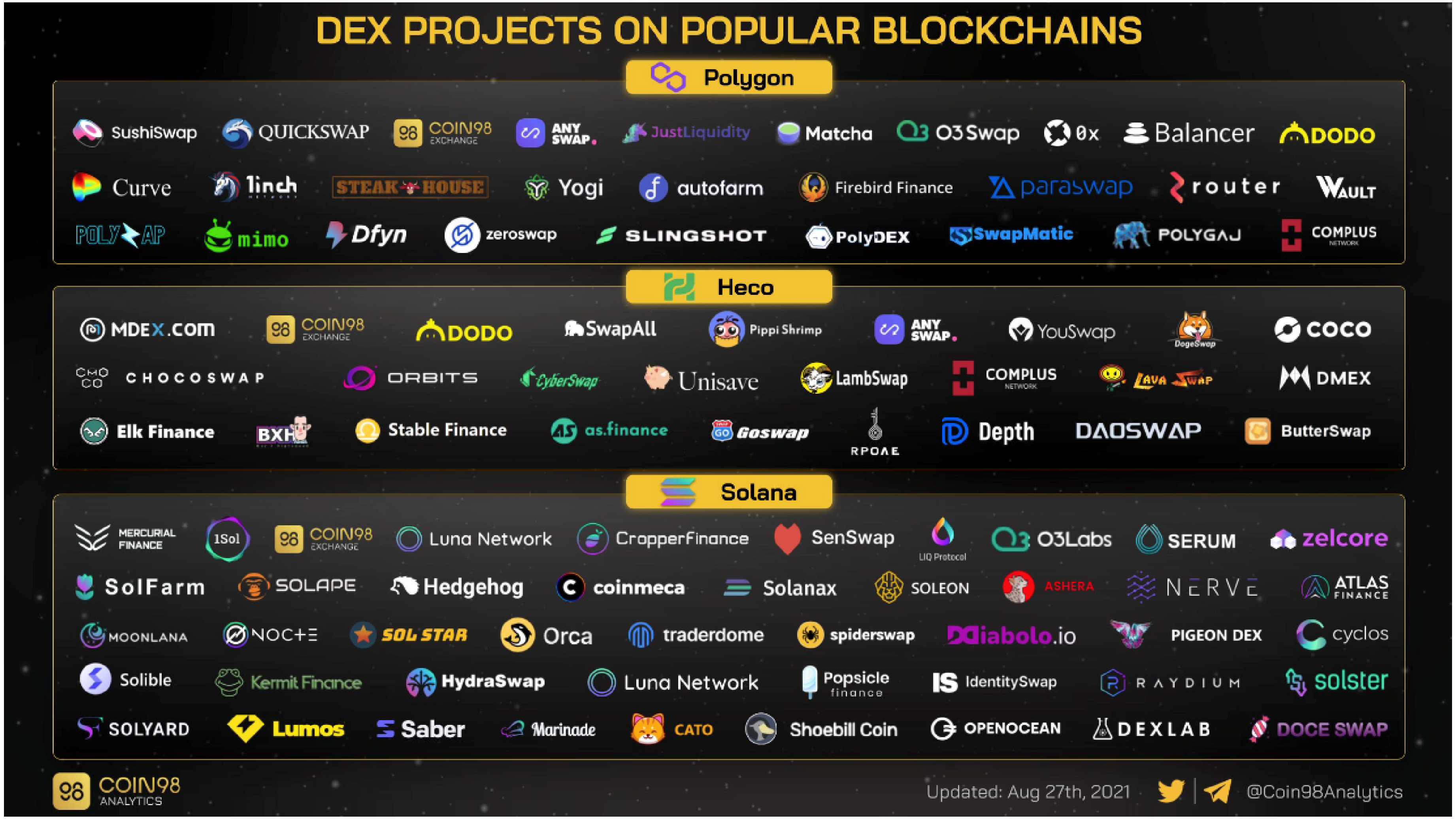
DEX PROJECTS ON POPULAR BLOCKCHAINS

Source: CoinGecko Updated: Aug 27th, 2021 @Coin98Analytics

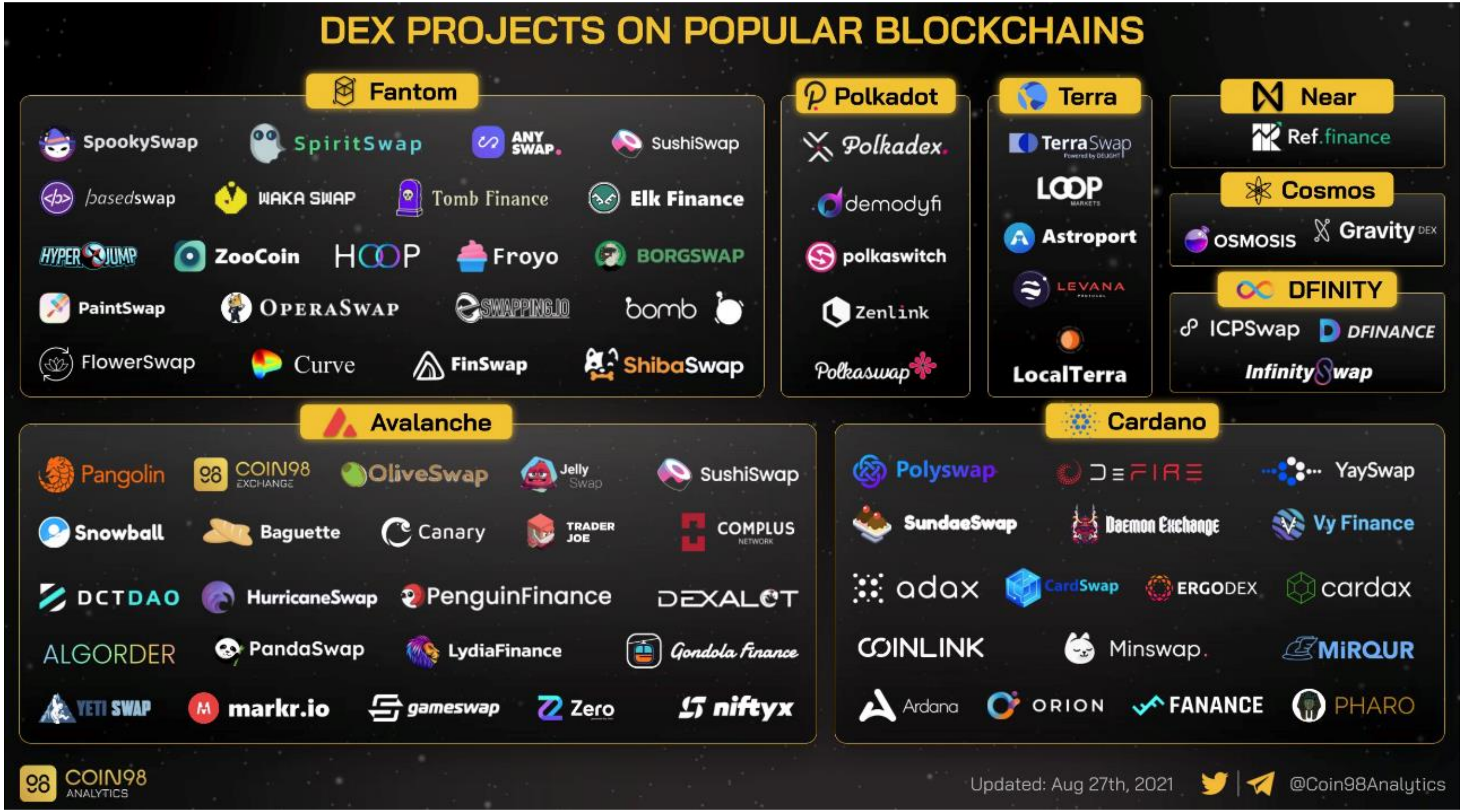
DEXes on BSC


DEX PROJECTS ON POPULAR BLOCKCHAINS
Binance Smart Chain
COIN98 EXCHANGE
PancakeSwap
SushiSwap
LAUNCH ZONE
BambooSwap
CheeseSwap.App
HYPER JUMP
Unisave
SWAP KING
DODO
BakerySwap
1inch
atomic.blue
VIKING SWAP
Spartan Protocol
bSWAP
Donut Finance
PeachSwap
SaltSwap
0x
zeroswap
JulSwap
SoftDrink Swap
BurgerSwap
Neonic Finance
Jelly Swap
Rubic
KIWISwap
Sponge.finance
dForce
dex.guru
Slime Finance
SashimiSwap
MANYSWAP
MilkSwap
TEN3T
Narwhalswap
TACO SWAP
Matcha
PantherSwap
Goose Finance
COMPLUS NETWORK
PAPAYA
ZEEDEX
KebabFinance
ApeSwap
STORMSWAP
BSC.TOOLS
BorshchFinance
LazyMint
Reef
paraswap
CafeSwap
Value
PandaYield
Squirrel
CheesecakeSwap
Smoothy
KokomoSwap
biswap
BLIQUID
Belt.fi
Bestswap
IDEX
KEEP3R BSC NETWORK
SakeSwap Liquidity · Swap · Farm
IceCream
BabySwap
OneSwap
NERVE
Grape Swap
LOOT
KOALADEFI
ellipsis.finance
Bitdroplet DECENTRALIZED
PERLIN
BSC STATION
Bogged Finance
SoupSwap
DOPPLE FINANCE
unifi
THUNDER SWAP
Blue Swap
InfinityCrypto
Unicorn
MERCOR
O3Swap
SwapTuna.com
BarbecueFinance
ANY SWAP
Dankswap
SatisFinance
Marshmallow
RamenSwap
Stakin
MOMO PROTOCOL
SPACE SWAP
Newdex
MoonCake Swap
PureSwap
Zero
JAGUARSWAP
MacaronSwap
Goldex co.in Beta
Yogi
treedefi
coinswap
BRICKCHAIN FINANCE
UBU FINANCE
CLIMB TOKEN FINANCE
Degen Swap
WARDEN
LP-Swap
Defibox
Platinium Finance
VIPSWAP
HYRULE SWAP
TuringMachine
LIME SWAP FINANCE
LEONICORN SWAP
JOINTER
Equator.finance
TEASWAP
MDEX.com
bStable
bello
Vanilla Cake Swap
CROX SWAP
Polaris
SELENIUM SWAP
Exonium DEX
TapSwap
Wis.com
LOKUM
NOMINEX
Bourbon Finance
OAKTREE FINANCE
OpenOcean
StableXSwap
liquifi
Zethyr
Robin
RoboFi
dDEXX
COIN98 ANALYTICS
Source: bscproject
Updated: Aug 27th, 2021
@Coin98Analytics

DEXes on other Blockchains



DEXes on other Blockchains (continued)



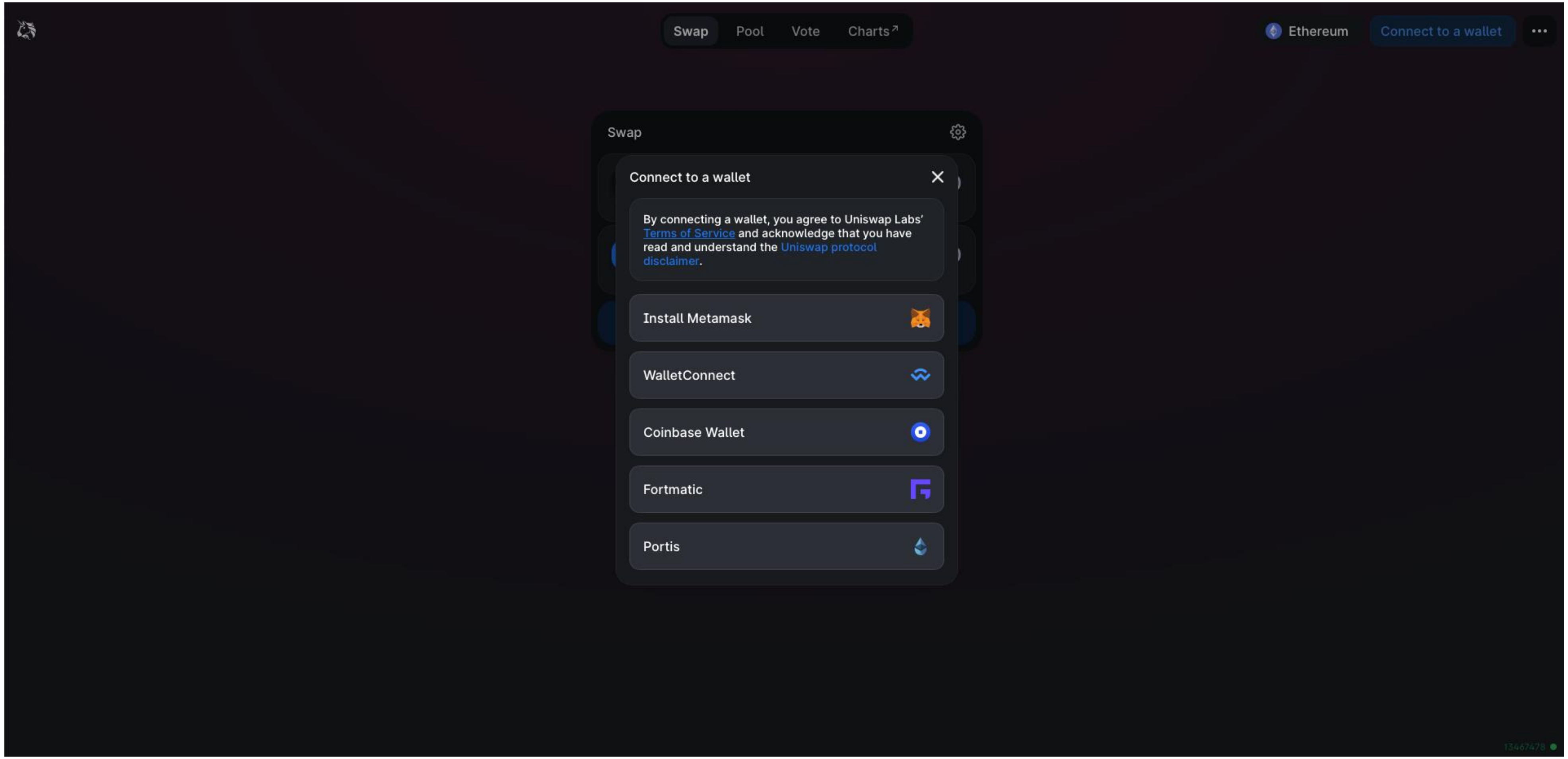
To say that DEXes are popular **would be an understatement**

They are perhaps **the most fundamental** component of DeFi

Using a DEX

- To use a DEX, a user must connect a compatible wallet (like **Metamask**) to it.
  - Connecting a wallet to a DEX basically means allowing the DEX smart contract to view the wallet contents (balances) and, depending on the approvals provided by the user, transacting on specific tokens up to specific amounts (or without limits).
- DEX interfaces are typically relatively simple and user-friendly:
  - Users simply choose their trading pair (e.g. ETH/DAI) and set an amount for the token to sell.
  - The DEX will offer an estimated amount for the token to buy, as well as inform the user about the price impact of the trade (see next slide).
  - Should the user accept the terms offered (both on the DEX user interface and the wallet), the transaction is submitted to the blockchain. The trade is executed when the transaction is confirmed on-chain.
  - Users can also set their own desirable values regarding price slippage and transaction fees (or simply let the values of the DEX's default settings).
- High transactions fees constitute, at the moment, the biggest disadvantage of DEXes, especially those using Ethereum as their underlying L1 protocol.

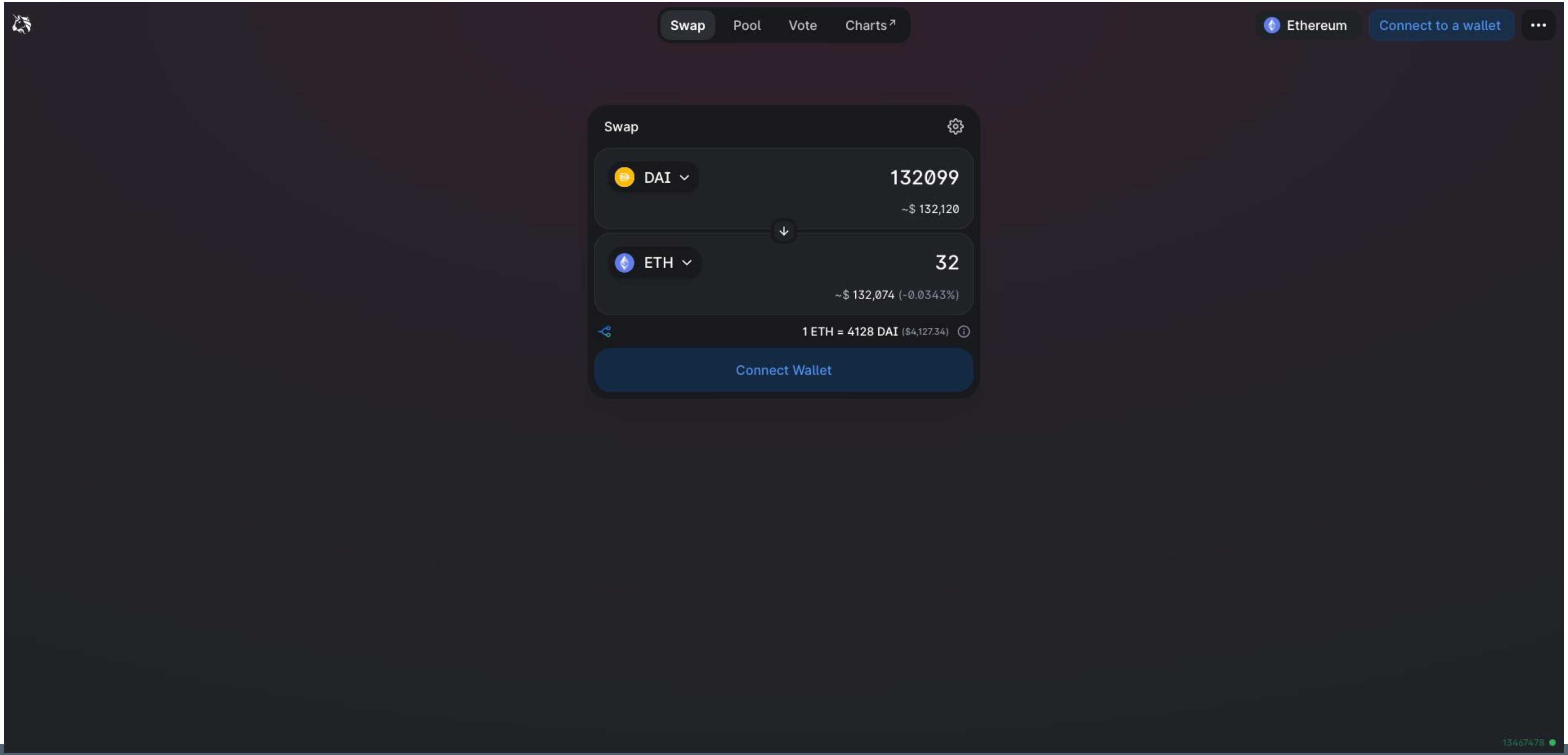
Example: Connecting a wallet to Uniswap



Connect to a wallet ✕

By connecting a wallet, you agree to Uniswap Labs' Terms of Service and acknowledge that you have read and understand the Uniswap protocol disclaimer.

Example: token swap (DAI to ETH) in Uniswap



Swap

DAI 132099
~$ 132,120

ETH 32
~$ 132,074 (-0.0343%)

1 ETH = 4128 DAI ($4,127.34)

13467478 ●

Session 4.1: Decentralized Exchanges

2. How DEXes work

Order books vs Automated Market Makers (AMMs)

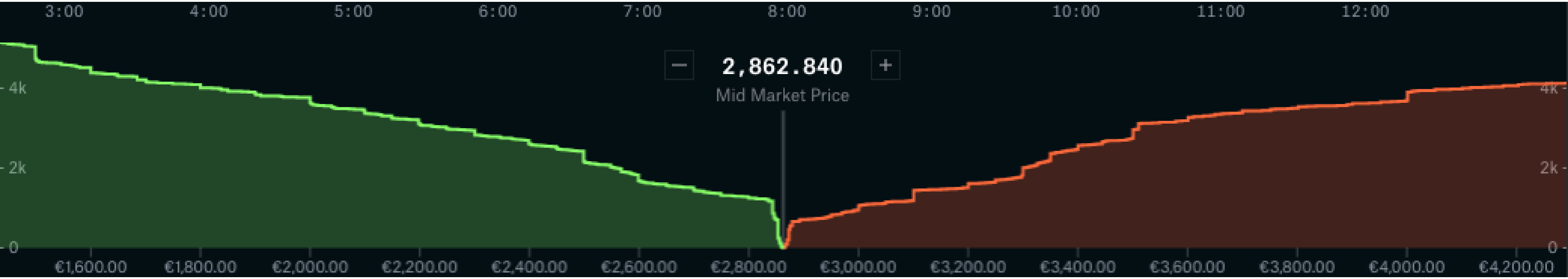
There are two primary categories of DEXes: those that rely **on order books** versus **AMMs and liquidity pools**.

○ To understand the difference, we must understand the role of an **order book.**

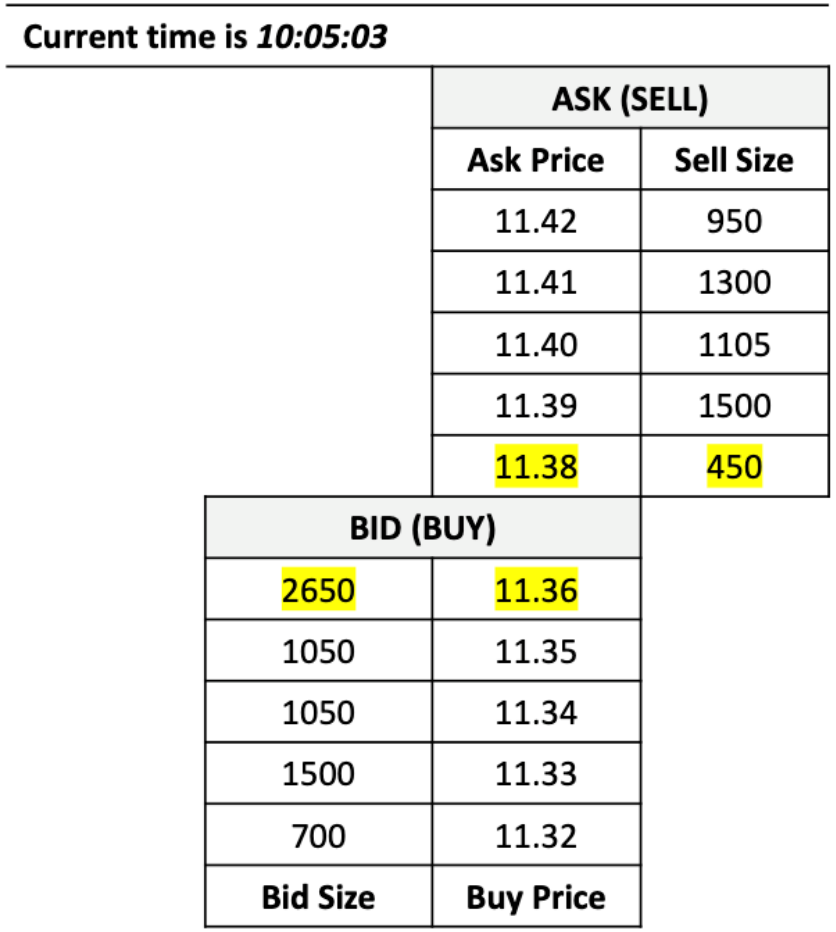
- An order book shows the volume of buy (bid) and sell (ask) orders for an asset, at every price level.
- The current price of the asset is determined by where the bid and ask **meet**.
- Order books essentially match buyers and sellers, facilitating price discovery.
- They are suitable for **liquid markets**, as they minimize **slippage**, or the difference between the expected and actual price of a trade.
- Centralized Exchanges are liquid, as they rely on Market Makers, whose job is to maintain, at all times, bids and asks in the order book. Liquidity is provided by the market maker's limit orders, as well as, from the orders entered by other traders or investors.
- However, in **illiquid markets**, order books often result in high slippage, wait times, and spreads*

*The bid-ask spread, or the distance between the maximum price someone is willing to pay (bid) and the minimum price someone is willing to sell (ask) is an indicator of market liquidity

Example: Order Book for ETH-EUR

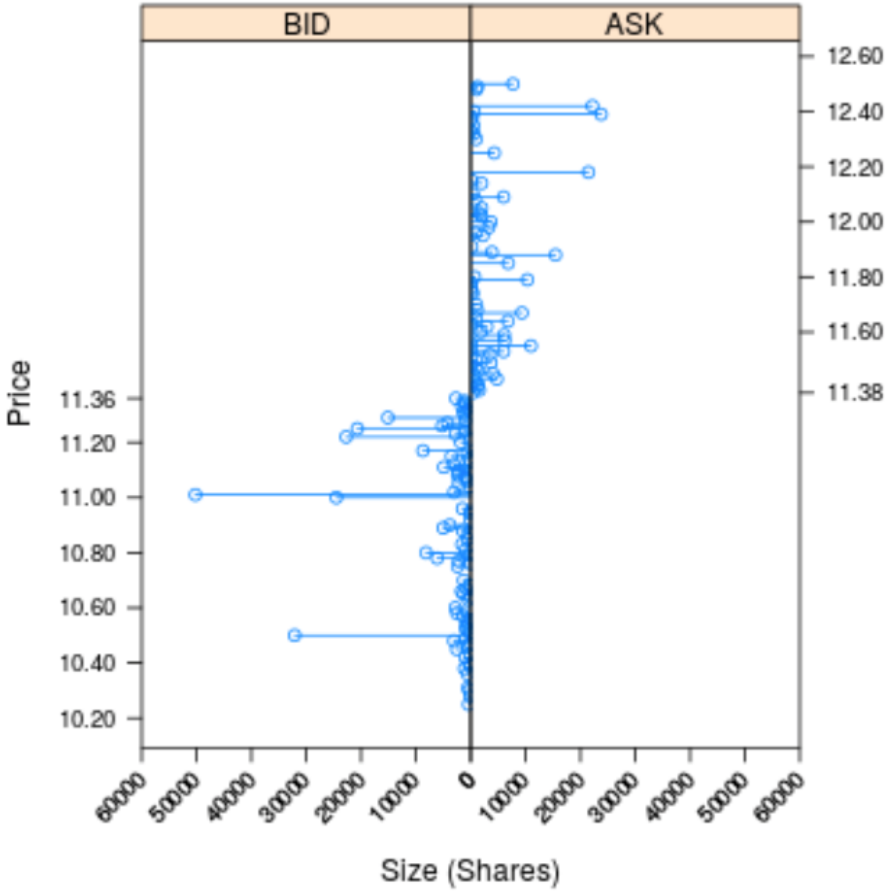


Example: Order Book



Current time is *10:05:03*

	ASK (SELL)	
	Ask Price	**Sell Size**
	11.42	950
	11.41	1300
	11.40	1105
	11.39	1500
	11.38	450
BID (BUY)		
2650	11.36	
1050	11.35	
1050	11.34	
1500	11.33	
700	11.32	
Bid Size	**Buy Price**	



Definitions: Liquidity pools

DEXes were initially illiquid

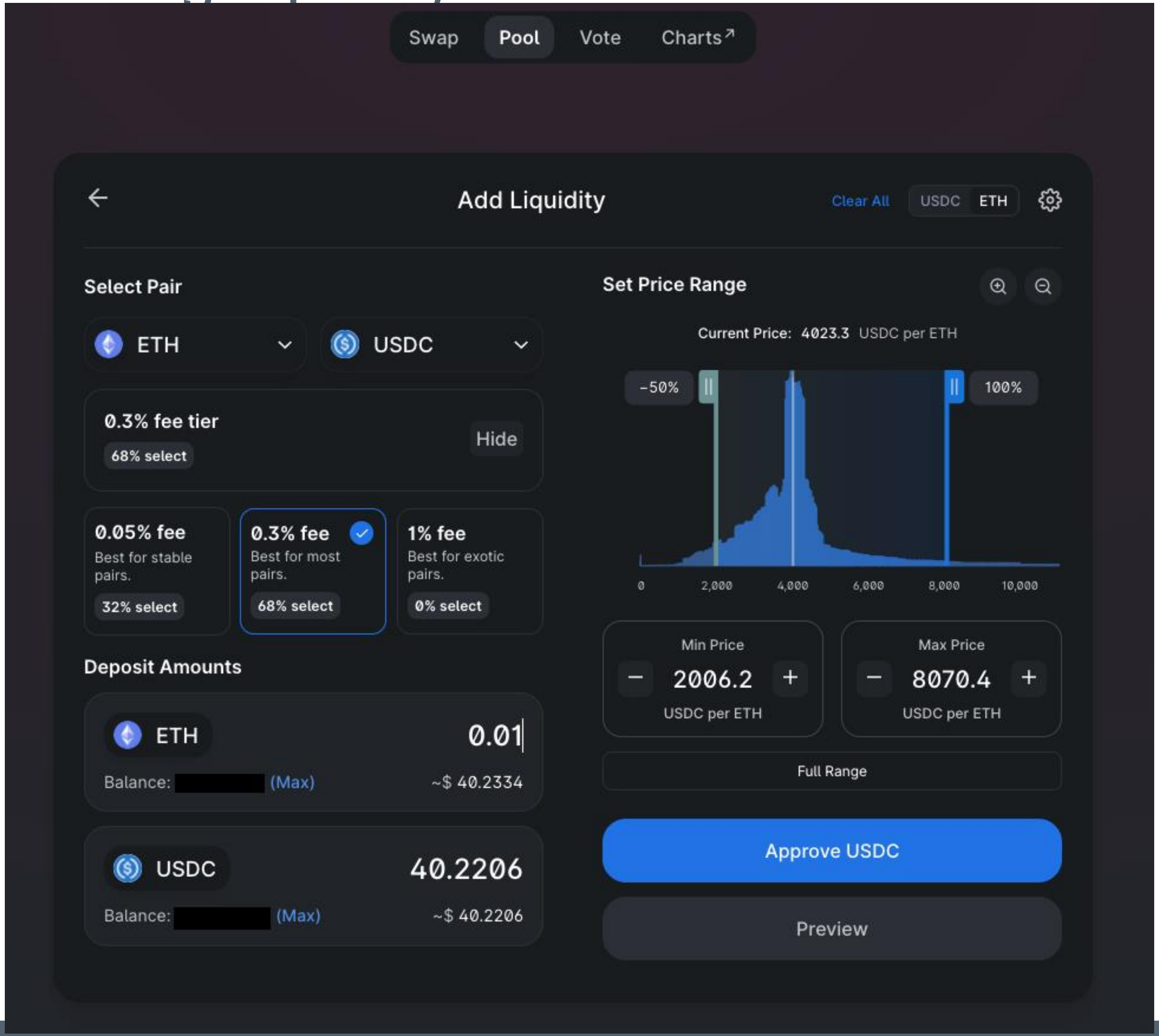
- This meant that trade execution would be slow and transaction slippage high (inverse relationship with order book depth).
- The slowness would be further aggravated by block confirmation times.
- Another problem is that maintaining an order book on the blockchain would be prohibitively slow and expensive due to fees.

A solution came in the forms of Liquidity Pools (LPs) - one of the most foundational mechanisms in the DeFi ecosystem.LPs are They are an essential part of AMMs, lending/borrowing platforms, yield farming, synthetic assets, insurance, etc.

A liquidity pool is a reserve of funds which are held in a smart contract.

- They are used to facilitate decentralized trading by **ensuring sufficient liquidity at any given time**.
- **Bancor** was the first protocol that utilized the mechanism of LPs, but they were popularized by **Uniswap**.
- Today, the vast majority of DEXes function under the LP model, with very few using the order book model.
- Other popular DEXes that use LPs are **Sushiswap**, **Pancakeswap**, **Curve** and **Balancer**
- **Anyone can become a market maker by providing liquidity for a token pair.**
- This also means that there are no traditional listing requirements for cryptocurrencies, such as those found in cryptocurrency and stock exchanges.

Definitions: Adding liquidity to a LP



Add Liquidity

Select Pair

ETH

USDC

0.3% fee tier

68% select

0.05% fee
Best for stable pairs.
32% select

0.3% fee ✓
Best for most pairs.
68% select

1% fee
Best for exotic pairs.
0% select

Deposit Amounts

ETH 0.01
Balance: [redacted] (Max) ~$ 40.2334

USDC 40.2206
Balance: [redacted] (Max) ~$ 40.2206

Set Price Range

Current Price: 4023.3 USDC per ETH

Min Price
− 2006.2 +
USDC per ETH

Max Price
− 8070.4 +
USDC per ETH

Definitions: Automated Market Makers (AMMs)

- AMMs are another foundational mechanism of decentralized exchanges.
  - They are **algorithms that determine how the liquidity of LPs becomes available to traders.**
  - With AMMs, traders transact directly with the liquidity pools instead of with one another.
- **Liquidity pools solve the problem of liquidity availability; AMMs solve the problem of price discovery**.
- AMMs eliminate the need for order books; Liquidity pools eliminate the need for centralized liquidity providers and formal listing requirements
- There are different types of AMMs which we will cover in the following slides

Relevant Quote

> “In two minutes, some can spin up a market and provide liquidity, and they don’t need to be extremely sophisticated or have a vast amount of capital, or work with other professional market makers, so it essentially removes this gatekeeper in the creation of liquidity.”

Hayden Adams,

Uniswap Inventor

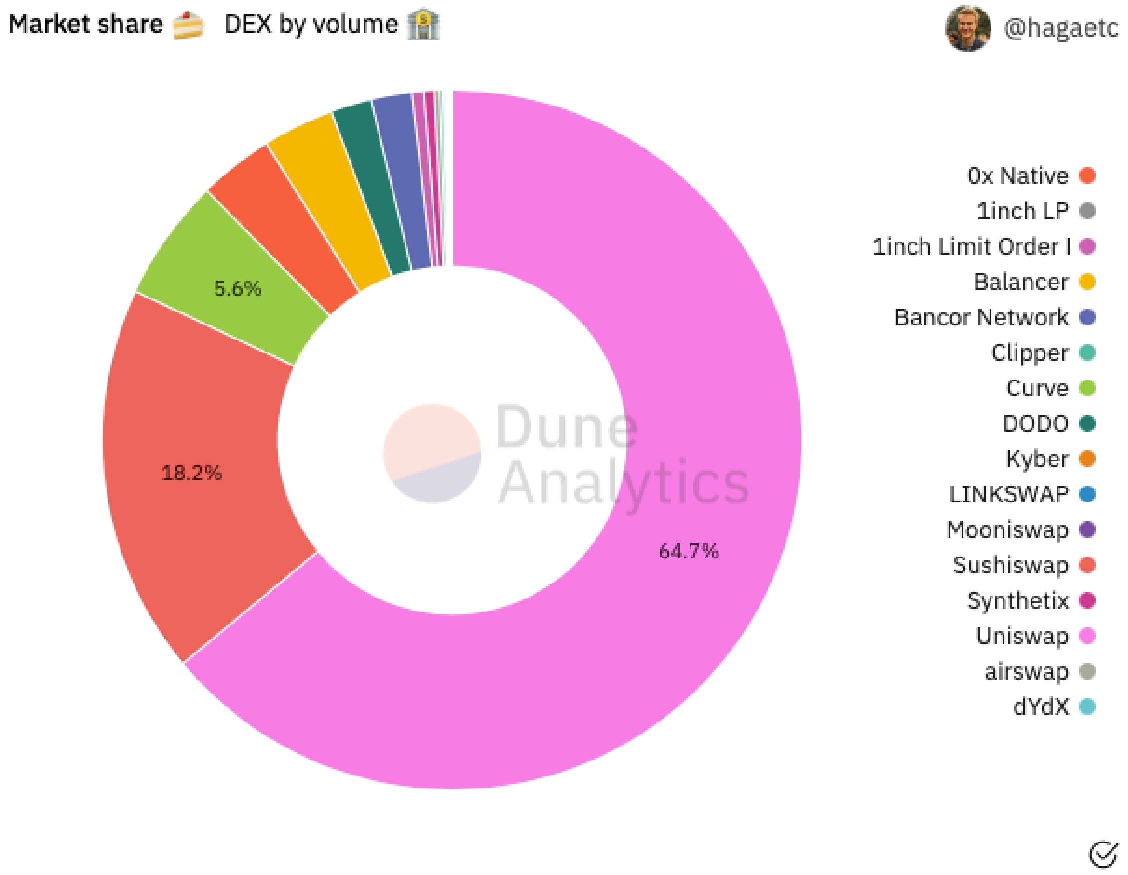
Centralized vs Decentralized Exchanges

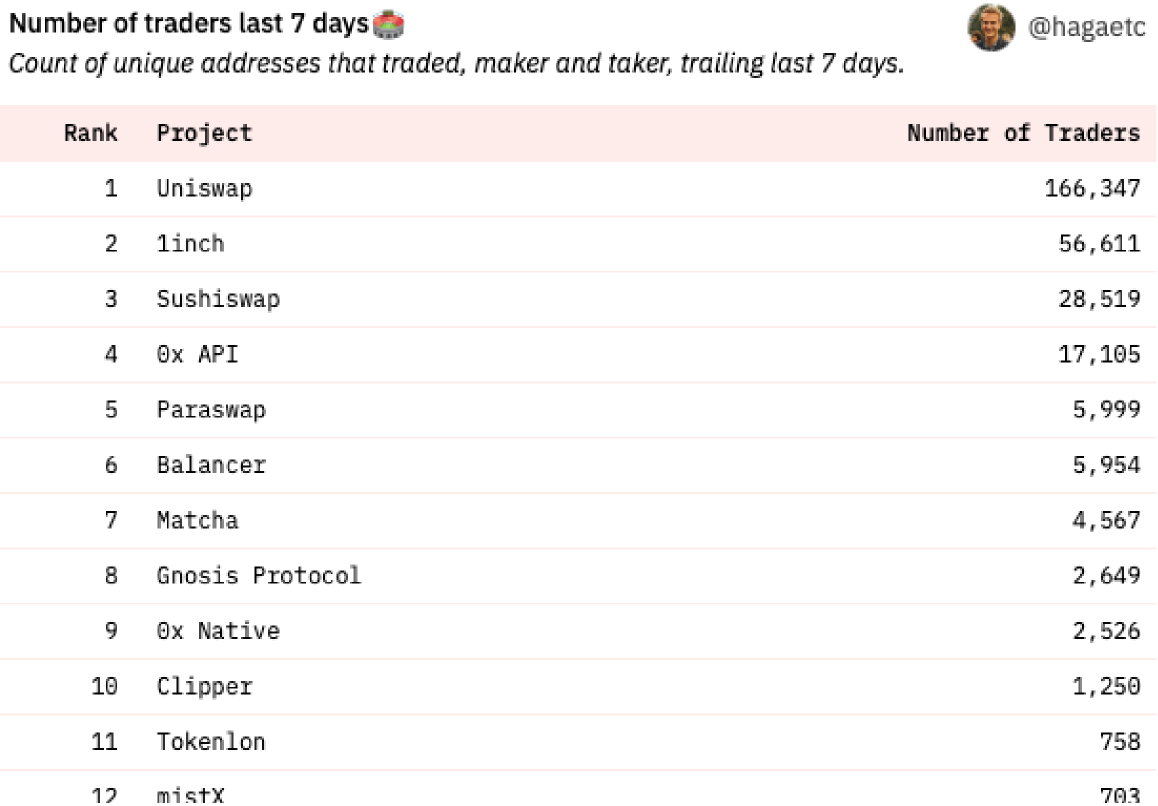
Feature	CEX	DEX
Access to trading	Vetted individuals or institutions	Anyone including smart contracts
Privacy	KYC & AML laws mean no privacy	Pseudonymity for all participants
Transparency	Exchange operator is audited	Trades verifiable on-chain
Brokers	Popular and necessary for most investors	Practically non-existent
Price determined by	Order books	Automated Market Makers
Liquidity provided by	Centralized entities that own a significant volume of a financial asset	Any human or machine agent, usually in small quantities
Fees	A variety of fees apply, ranging from trading to custody, consulting, etc.	Usually trading fees & transaction fees
Asset Listing	Through formal regulated procedures	Immediate, unregulated
Regulations	Strictly regulated	Still grey area

Session 4.1: Decentralized Exchanges

3. Notable DEXes

Popular DEXes by market share





Number of traders last 7 days @hagaetc

Count of unique addresses that traded, maker and taker, trailing last 7 days.

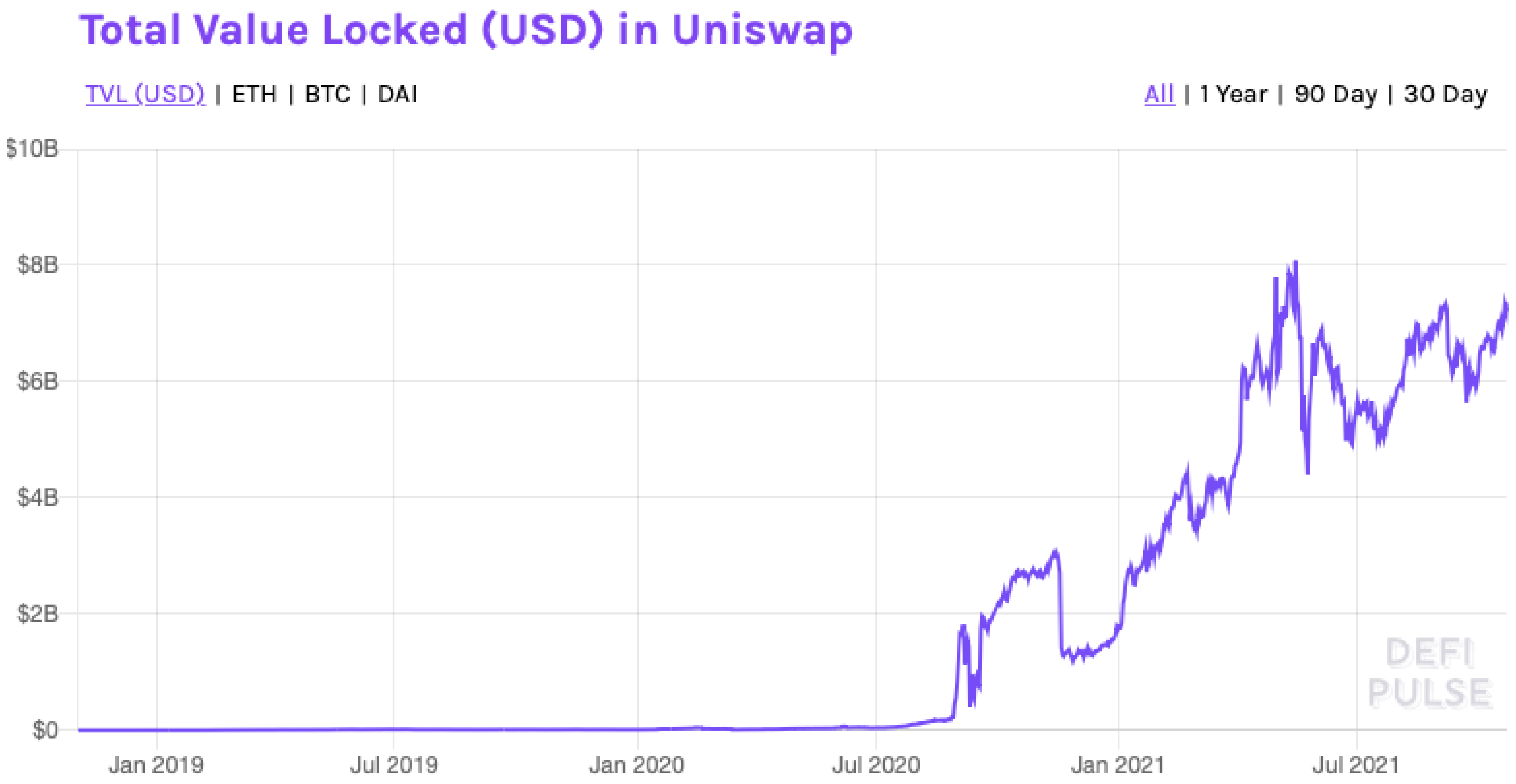
Rank	Project	Number of Traders
1	Uniswap	166,347
2	1inch	56,611
3	Sushiswap	28,519
4	0x API	17,105
5	Paraswap	5,999
6	Balancer	5,954
7	Matcha	4,567
8	Gnosis Protocol	2,649
9	0x Native	2,526
10	Clipper	1,250
11	Tokenlon	758
12	mistX	703

Uniswap

Uniswap is, by most metrics, the most popular decentralized exchange.

- It was deployed on Ethereum in 2018 and was one of the first to utilize and AMM system, and the one that popularized the constant product formula (see later).
- Uniswap has gone through various iterations; version 3 was deployed in May 2021.
- In its latest version, it offers a new mechanism for managing liquidity, through which LPs can determine their price range for providing liquidity.

Uniswap TVL

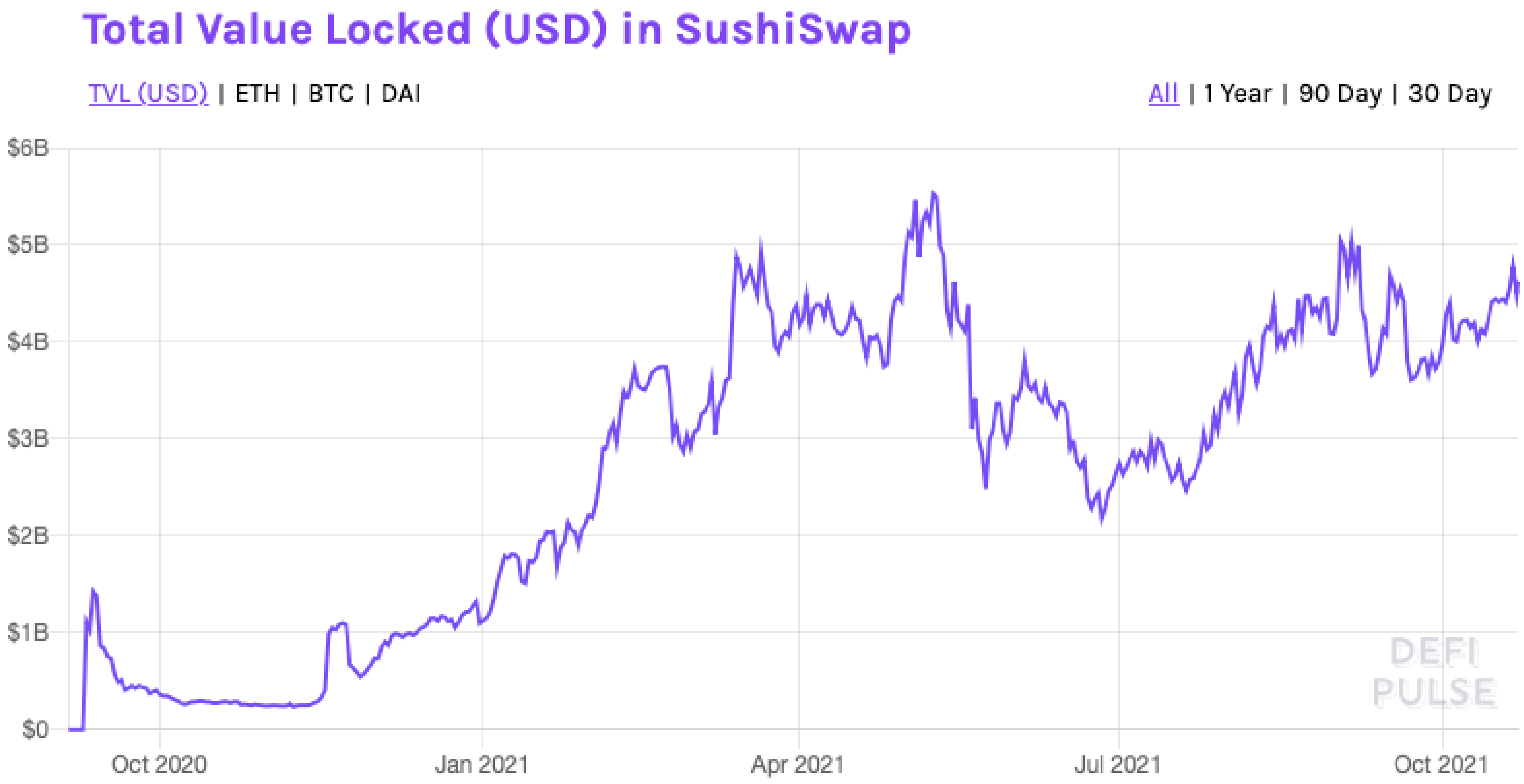

Total Value Locked (USD) in Uniswap
TVL (USD) | ETH | BTC | DAI
All | 1 Year | 90 Day | 30 Day
$10B
$8B
$6B
$4B
$2B
$0
Jan 2019
Jul 2019
Jan 2020
Jul 2020
Jan 2021
Jul 2021
DEFI PULSE

SushiSwap

SushsiSwap is a decentralized exchange launched in August 2020 on Ethereum by a pseudonymous developer, Chef Nomi. It was a fork (copy) of Uniswap and utilised the same constant product formula. SushiSwap is famous for launching a “vampire attack” on Uniswap in an attempt to bootstrap liquidity (more on that on the next slides). Following more such events, like a “rug-pull” from the core developer, the Sushsiswap project moved to a team of developers and has started to evolve beyond its Uniswap roots.

- Today, in addition to a decentralized exchange, SushiSwap offers two more products, Kashi and Misho
    - Kashi allows users to lend and borrow cryptocurrencies, as well as create new markets
    - Misho is a mechanism for launching new tokens.

Sushiswap TVL



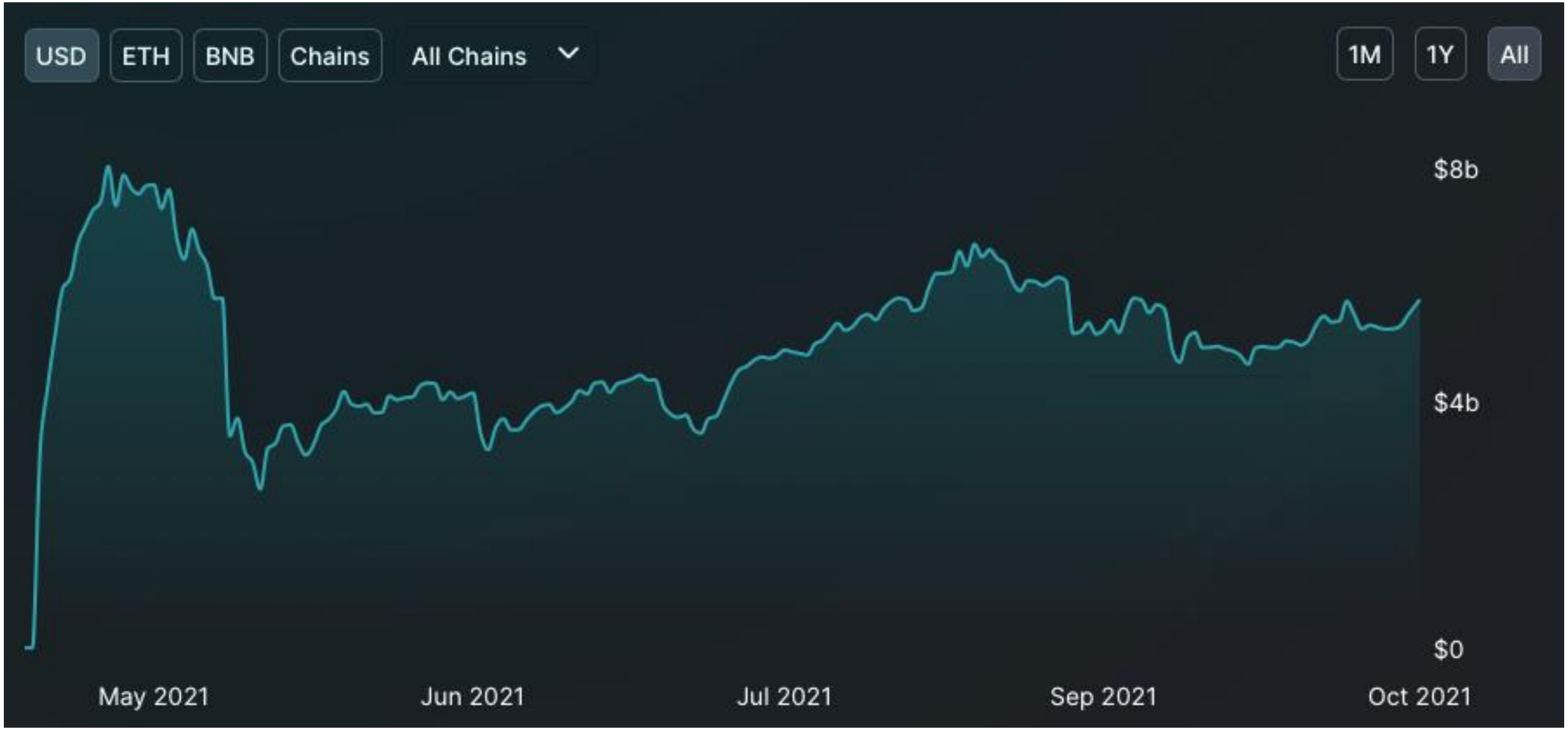
Total Value Locked (USD) in SushiSwap

PancakeSwap

PancakeSwap is another AMM-based DEX, this time deployed on the Binance Smart Chain, instead of Ethereum. PancakeSwap's core functionality is very similar to that of Uniswap, but the protocol offers some additional features in the form of:

- A lottery
- A Prediction Market
- NFT Markets
- Initial Farm Offering

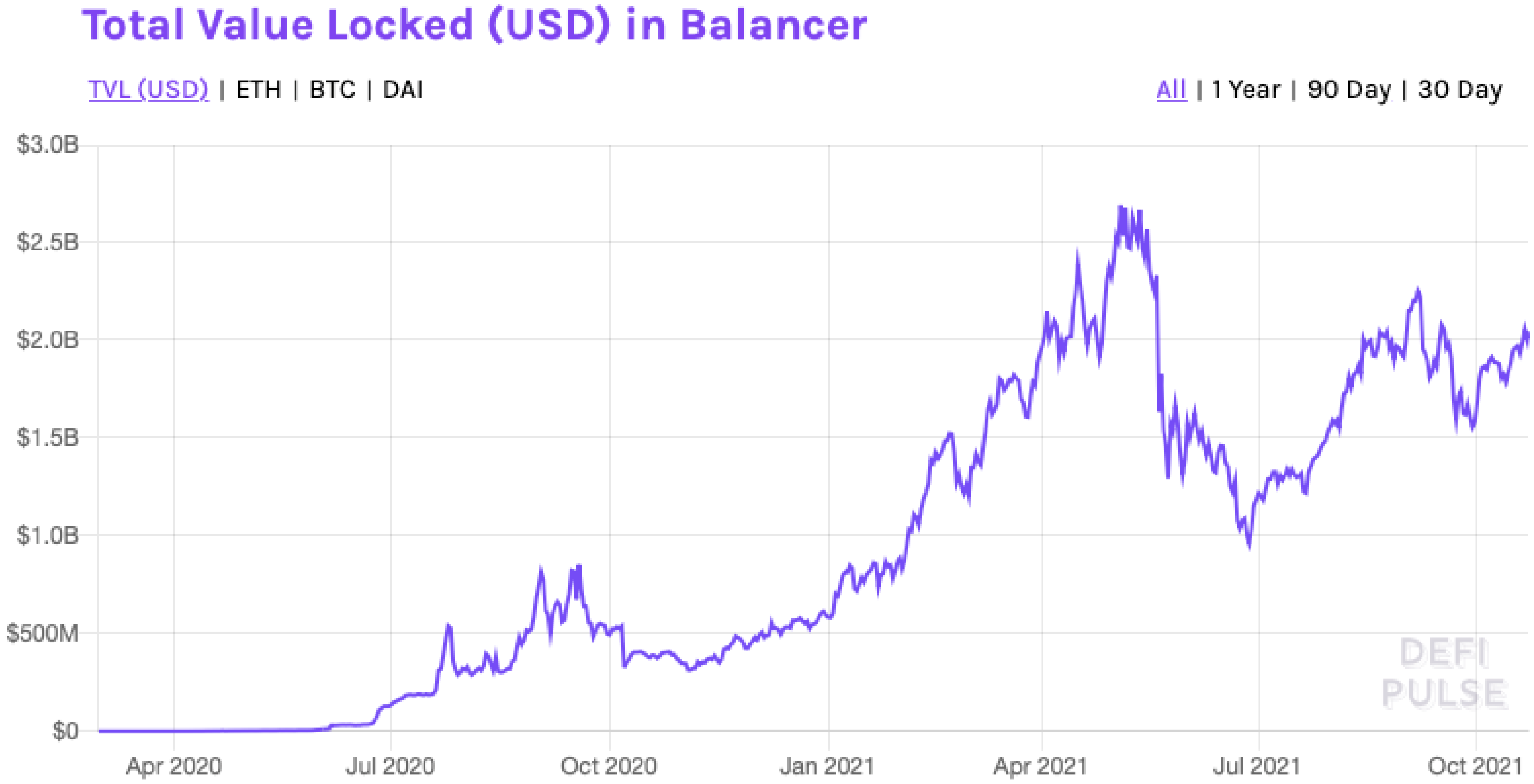
PancakeSwap TVL



Balancer

- Balancer is a portfolio manager, in addition to being an AMM-based DEX
- As we will discuss in the following, Balancer utilizes a special product formula that facilitates multi-asset pools. Creators set customized fee ranges for the pools they create.
- There are also different pools deepening on who can add liquidity.
  - **Public pools** – where anyone can add liquidity, within fixed parameters.
  - **Private pools** – Where only the owner can add liquidity and modify the parameters.
  - **Smart pools** – Where anyone can add liquidity and parameters can be changed on an ongoing basis.
- Balancer has also introduced new ways for token sales through Liquidity Bootstrapping Pools.

Balancer TVL



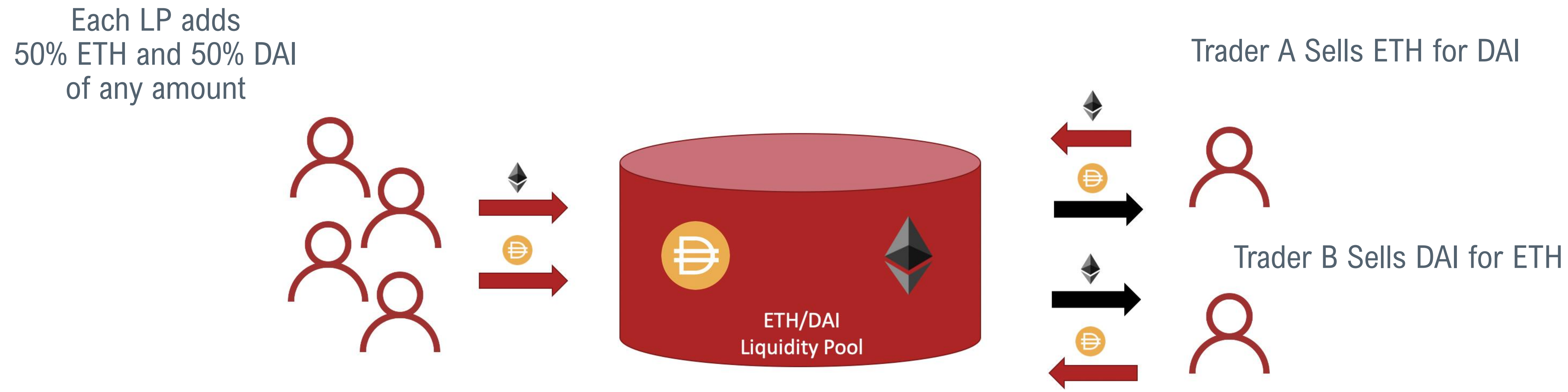
Total Value Locked (USD) in Balancer

Session 4.1: Decentralized Exchanges

4. Advanced Topics on DEXes

Visualisation of Liquidity Pools

- As we have established, liquidity pools are smart contracts that hold two or more tokens and act as reserves.
- Instead of trading with one another, users trade with the liquidity pool, at a rate determined by the AMM.



Overview of AMM Formulas and Characteristics

- As we have established, AMMs are algorithms or mathematical functions that determine token prices
- Some of the most popular AMM algorithms include:
  - Constant Product Formula
  - Constant Sum Formula
  - Stableswap Invariant (Curve.fi)
  - Constant Mean Formula
  - hybrid CFMM
- Each comes with its own advantages and disadvantages.
- The underlying innovation is providing a deterministic model for asset pricing.
- Also integral is the concept of a bonding curve that defines the relationship between price and token supply

The Constant Product Formula

- The constant product formula is the most popular one, used in Uniswap and Bancor.
- Its simplified version is the following:

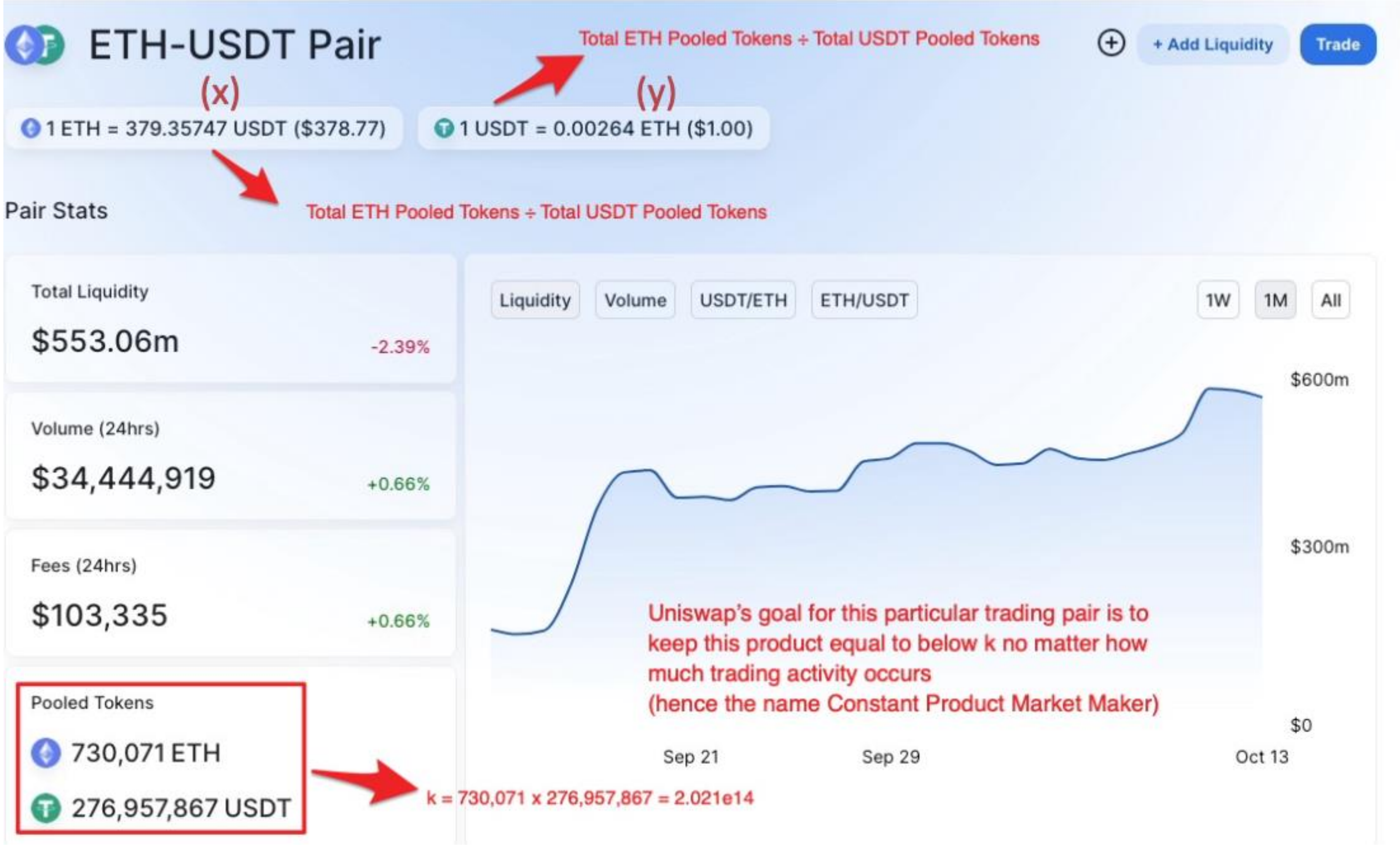
$$\boxed{k = x \times y}$$

- Where x and y are the reserves of each asset in the liquidity pool, and k their constant product.
- The formula is **constant** in that, if we assume that there are no transaction fees, all trades will shift the reserves in a way that their product (k) remains unchanged.
  - In practice, each trade increases the k **proportionally to the transaction fee and the amount traded**.
- For the sake of completeness, the full constant product formula is the following, where γ are the transaction fees, Rα and Rβ the reserves of each asset, and Δα and Δβ the change in reserves due to transactions:

$$\boxed{k = (Ra - \Delta a)(R\beta + \gamma \Delta \beta)}$$

- In our examples we will utilize its simpler version.

The Constant Product Formula



ETH-USDT Pair

Total ETH Pooled Tokens ÷ Total USDT Pooled Tokens

(x) 1 ETH = 379.35747 USDT ($378.77)

(y) 1 USDT = 0.00264 ETH ($1.00)

Total ETH Pooled Tokens ÷ Total USDT Pooled Tokens

Pair Stats

Total Liquidity $553.06m -2.39%

Volume (24hrs) $34,444,919 +0.66%

Fees (24hrs) $103,335 +0.66%

Pooled Tokens
730,071 ETH
276,957,867 USDT

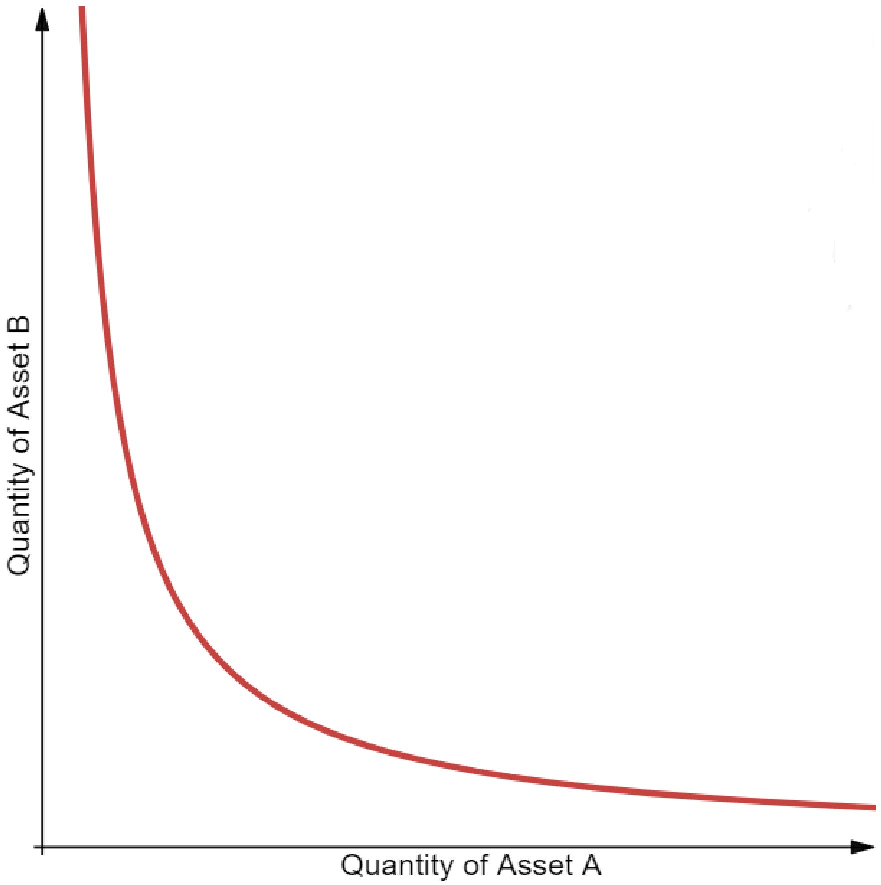
k = 730,071 x 276,957,867 = 2.021e14

Uniswap's goal for this particular trading pair is to keep this product equal to below k no matter how much trading activity occurs
(hence the name Constant Product Market Maker)

The Constant Product Formula (continued)

- Represented as a graph, the formula forms a **hyperbola**
- **Pros**:
  - Constant product formulas are preferred as they ensure sufficient liquidity for a trade, no matter what, as when the quantity of an asset approaches zero, its price approaches infinity.
  - They provide profit opportunities for arbitrageurs
- **Cons:**
  - They often result in high slippage for traders and impermanent losses for LPs

More on arbitrage and impermanent loss later

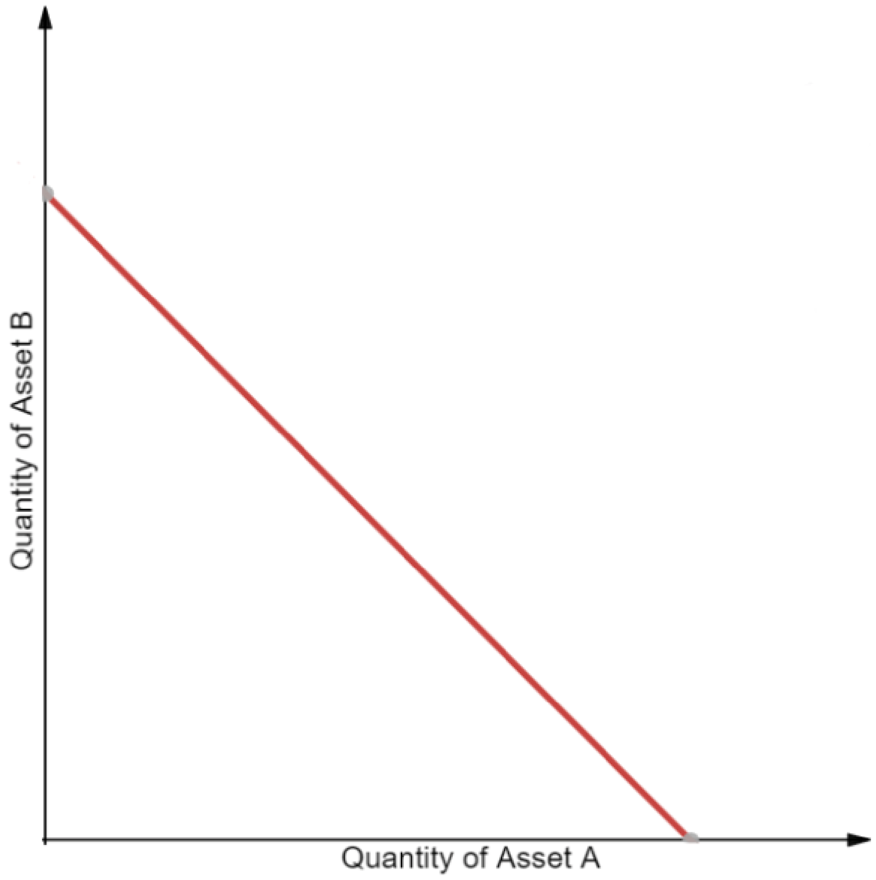


The Constant Sum formula (assuming no fees)

- The Constant Product Formula satisfies:

$$\boxed{x + y = k}$$

  - Where x, y the asset reserves and k constant.
  - It forms a **straight line**.
- **Pros:**
  - Suited for tokens with the same price
  - No slippage
- **Cons:**
  - No infinite liquidity
  - Inherently flawed as arbitrageurs would drain the entire reserves if there is a price difference between prices on the DEX and on the market.

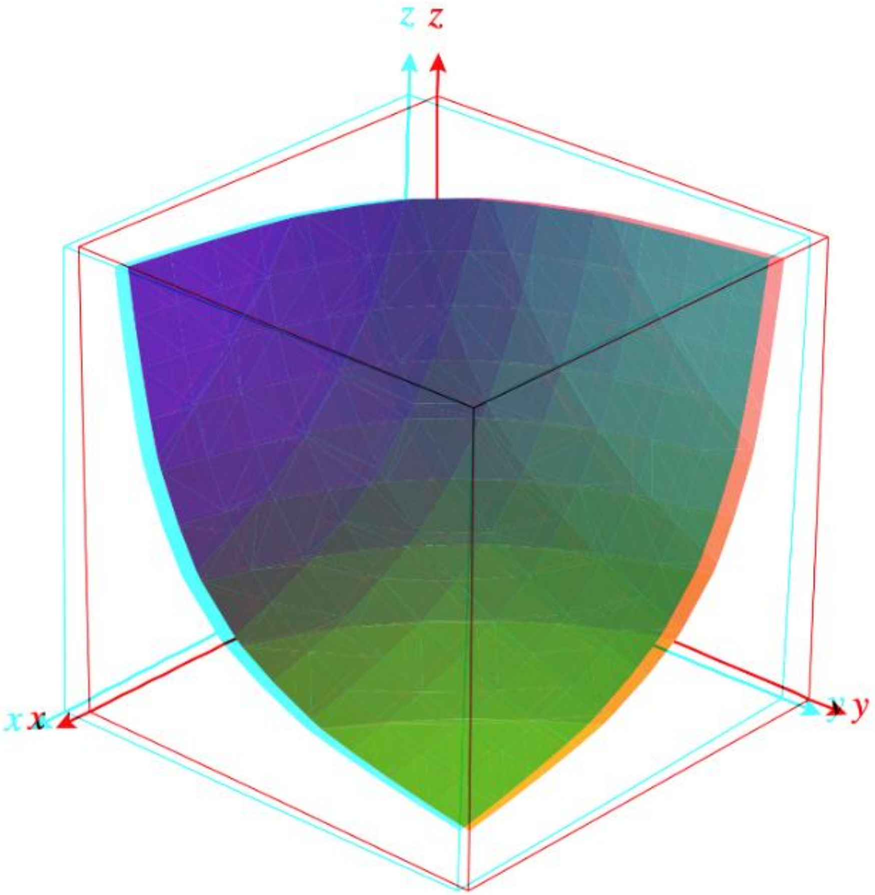


The Constant Mean Formula (assuming no fees)

- Balancer introduced a generalization of the product formula that allows for more than two assets and instead of a 50/50, any weight distribution. It is represented as:

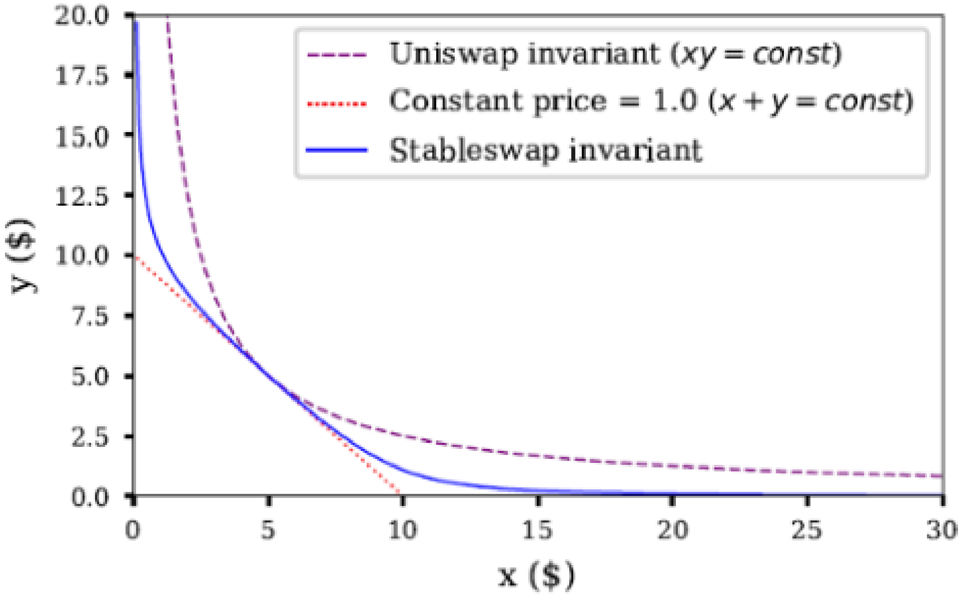
$$k = (x + y + \ldots + n)^{W} \quad or \quad \prod_{i=1}^{n} Ri^{w} = k$$

- Where R_i are the reserves of each token, w is the weight associated with each token, and k is constant
- Pros:
  - Allows for more assets
  - Allows for different weights



Hybrid Formulas

- Some protocols, with special characteristics, utilize hybrid formulas to achieve more efficient trading.
- One such protocol is Curve.fi
  - Curve utilizes a hybrid of the constant sum and product formulae
  - That is, because Curve's underlying tokens are relatively stable in value (e.g., stablecoins)
  - Trading occurs on a constant sum when the pair is balanced and on a constant product when imbalanced



$$An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

How AMMs determine prices (assuming no fees, slippage, etc.)

- We will utilize the **constant product formula:**

$$\boxed{\begin{array}{c} k = x \times y \\ where\ k = constant,\ and\ x,\ y\ the\ amount\ of\ supplied\ tokens \end{array}}$$

  - The first Liquidity Provider (LP) sets the initial exchange rate of assets in the Liquidity Pool.
  - LPs are incentivized to provide an equal value of tokens (otherwise they will lose money by arbitrageurs).
  - Suppose that the LP provides 10 Ethereum, with market value of $1,500 and 15,000 DAI (same total value):

$$\boxed{k = 10 \times 15,000 = 150,000\ (constant)}$$

- Now imagine that you wanted to trade DAI for 2 ETH. How much DAI would you have to pay?
  - You would take away 2 ETH from the pool and have to provide a proportionate amount of DAI

$$\boxed{(10-2) \times (15,000 + z) = 150,000 \Rightarrow 15,000 + z = \frac{150,000}{8} \Rightarrow 15,000 + z = 18,750 \Rightarrow z = 3,750}$$

  - You would have to pay 3,750 DAI for 2 ETH, or **on average** 1,875 DAI per ETH (in reality, the first ETH is cheaper and the second more expensive)
  - Arbitrageurs would then lower the price again by providing ETH to the pool to benefit from the difference.

Impermanent loss

- Impermanent loss is a **temporary loss** caused to a LP due to the **price volatility** of the tokens they provide
  - As AMMs lack order books and centralized parties, they rely on market forces for price discovery.
  - This means that price changes (e.g. on centralized exchanges) are not immediately reflected on AMMs.
  - As a result, there are often price discrepancies between their price on CEXes and AMMs.
  - **Arbitrageurs** discover those discrepancies and execute favorable trades (e.g., by buying low and selling high)
  - LPs suffer **impermanent losses** by being at the receiving end of the arbitrage
  - **Impermanent loss is essentially the difference between providing tokens versus holding them.**
  - The more volatile the tokens, the higher the exposure to impermanent loss.
- Why is the loss temporary or impermanent?
  - If the price of the staked tokens returns to the original price, the impermanent loss is neutralized
  - If the LP chooses to withdraw their funds, the impermanent loss is realized and becomes permanent.
- Impermanent loss can be mitigated to an extend by supplying less volatile tokens, same-pegged stablecoins, opting for one-sided liquidity pools, and by participating in uneven pools

Impermanent loss example

○ Consider the previous example where a LP has provided 10 ETH and 15,000 DAI to a Pool

Token	Amount	Price/Unit	Total Value
ETH	10	$1,500	$30,000
DAI	15,000	$1	

- Suppose that the price of ETH **increases** from $1,500 to $1,600. This would incentivize arbitrageurs to buy the “cheaper” ETH in the pool until it there is no price discrepancy.
- They will be able to buy ~ 0.32 ETH in exchange for ~496 DAI before the price of ETH in the pool reaches $1,600 and is at equilibrium with the market (you can calculate this through the constant product formula)

○ The LP would still realize profits, but not as much as if they simply held the tokens:

If supplied to pool

Token	Amount	Price/Unit	Total Value
ETH	9.68	$1,600	$30,984
DAI	15,496	$1	

If held

Token	Amount	Price/Unit	Total Value
ETH	10	$1,600	$31,000
DAI	15,000	$1	

LP incentives: Liquidity Mining and Yield Farming

- If impermanent loss makes supplying assets to a liquidity pool less profitable that holding, then one might wonder: why even become a LP?
  - The answers is that AMMs compensate LPs in various ways for the services they provide.
  - AMMs charge a (small) swap fee for their services. Uniswap's fee is 0.3%, applicable to all trades.
  - They then use these fees to reward LPs – this is also called **Liquidity Mining**
    - 0.3% of all trade volume is distributed proportionally to all liquidity providers. By default, these fees are put back into the liquidity pool, but can be collected any any time.
  - **Yield Farming** refers to a collection of techniques that aim at maximizing yield earned. This is usually achieved by rotating between pools. There are also protocols that do that automatically (e.g., Yearn Finance)
- In addition to fees, AMMs reward their LPs in other ways too:
  - Some AMMs reward their LPs with governance tokens.
    - Governance tokens are used for voting on proposals that determine the future of the AMM.
    - Governance tokens can also be sold in the market.
    - LPs may even provide those tokens as liquidity for additional rewards from fees.
  - LPs may also be targeted by competing dApps with **airdrops**

Session 4.1: Decentralized Exchanges

5. Exotic Finance = Exotic Risks

DEX Risks

- **Hacks and Exploits:**
  - DeFi protocols are as secure as the code that supports them
  - That is code both on the level of the settlement and asset layers (Layers 1+2) as well as the protocol and application (Layers 3+4)
  - Settlement level exploits refer to security flaws of the network where the DeFi applications is deployed (e.g., Ethereum). While this kind of exploits are rarer, they are by far the most critical.
  - Protocol and application exploits refer to security flaws of the underlying infrastructure or interface of the DeFi App. Such exploits can be mitigated to an extend through auditing.
- **Loss of Private Keys:**
  - Decentralized finance is all about self-custody. Loss of private keys results in loss of funds.
  - Some solutions aim to mitigate this, such as the social recovery feature of Argent.
- **Admin Key Risk:**
  - Admin Key risk refers to the risk that the key owner(s) will modify the underlying protocols in a way that will benefit them, at the expense of the users.
  - Admin Key Risk can be mitigated :
    - Entirely by "burning" the admin keys, however no more updates can be deployed.
    - To an extend my multisignature deployments.
    - Employing a DAO controlled by a voting process.

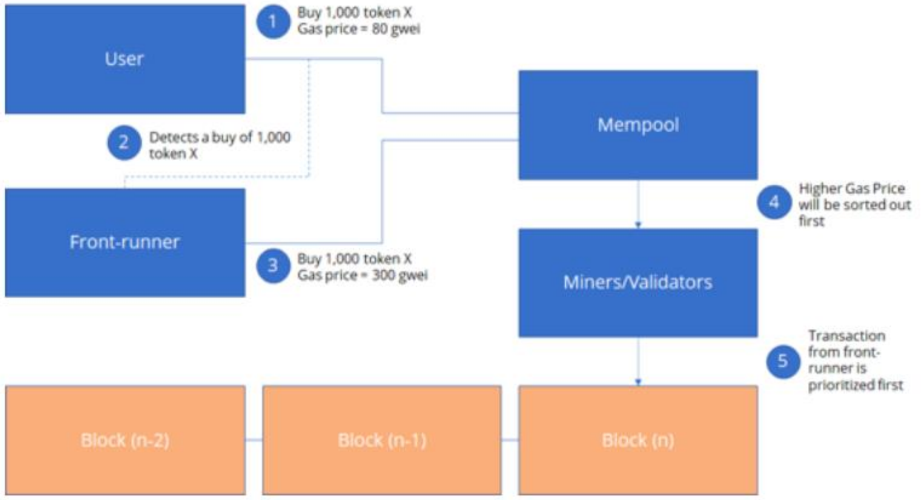
DEX Risks

- **Price Slippage:**
  - As we have established slippage refers to the difference between the expected and actual price of a trade.
  - It can be mitigated by setting limits (at the risk of the trade not being executed) or trading less volatile tokens.
  - There is a **positive relationship** between the size of the order and slippage
    - The larger the order, the larger the price slippage that a trader will incur
  - There is a **negative relationship** between the size size of the pool and slippage
    - The larger the pool the lower the price slippage
- **Front-running:**
  - DEX transactions are visible to everyone before they ”settle” on the blockchain, as they are stored in the mempool.
  - Automated systems (bots) monitor the mempool for profitable trades
  - When they identify one, they submit the same transaction, but with higher fees.
    - As miners want to maximize their profitability, they are incentivized to include the most profitable transactions in the next block, meaning the transactions with the highest fees.
  - By offering higher fees, front-runners manage to have their transactions settled first
  - Other transactions either fail or go through at a less favorable price (depending on slippage tolerance)

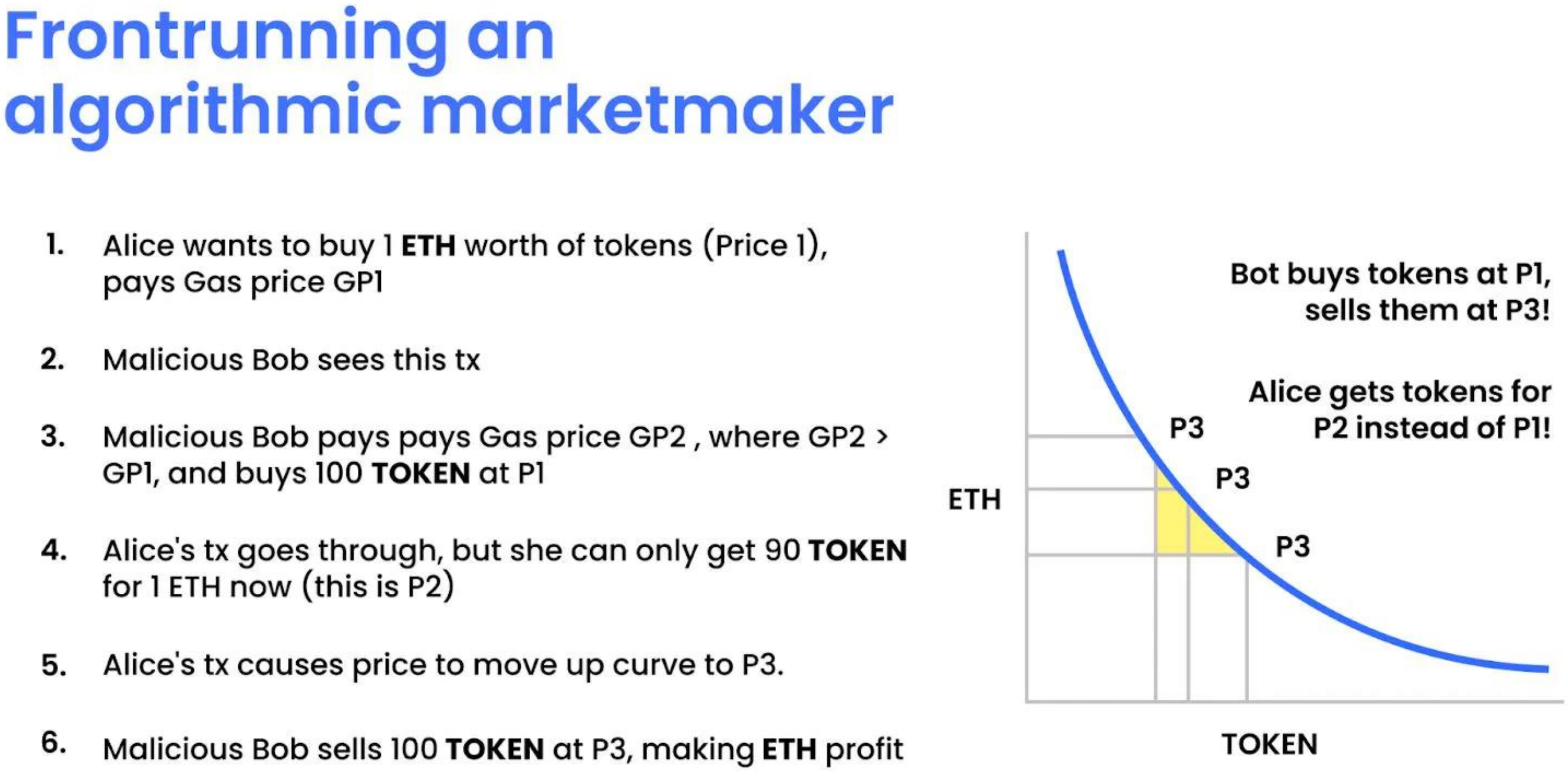
DEX Risks

Frontrunning comes in many forms:

- Displacement:
  - where a transaction B that pays higher fees is submitted in order to be executed before transaction A. This is the example of the previous slide, and what we usually mean when we talk about “Frontrunning”
- Insertion, or sandwich attack:
  - The bot detects a victim’s transaction
  - It front-runs the transaction by submitting one with a higher transaction fee (buys cheaper than the victim)
  - The victim transacts unfavorably by accepting higher slippage, thus raising the price of the token
  - The bot then back-runs the victim by immediately selling at a profit (sells for more)
- Supression:
  - Where the attacker fills-up blocks with their transactions in order to keep a specific transaction from being settled on-chain, effectively “censoring it”



Visualization of Sandwiching



Frontrunning an algorithmic marketmaker

1. Alice wants to buy 1 **ETH** worth of tokens (Price 1), pays Gas price GP1
2. Malicious Bob sees this tx
3. Malicious Bob pays pays Gas price GP2 , where GP2 > GP1, and buys 100 **TOKEN** at P1
4. Alice's tx goes through, but she can only get 90 **TOKEN** for 1 ETH now (this is P2)
5. Alice's tx causes price to move up curve to P3.
6. Malicious Bob sells 100 **TOKEN** at P3, making **ETH** profit

Bot buys tokens at P1, sells them at P3!

Alice gets tokens for P2 instead of P1!

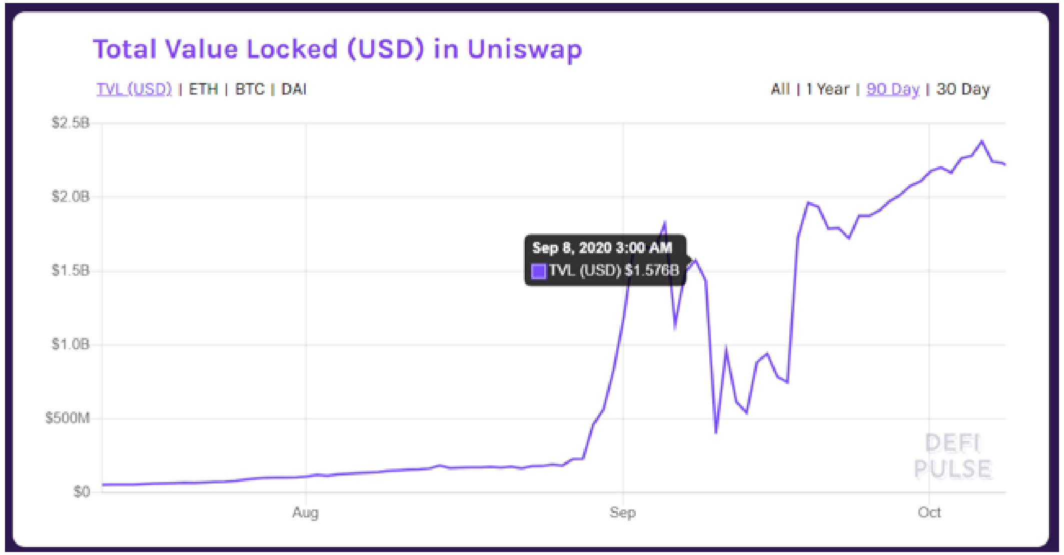
DEX Risks

- **Impermanent Loss:**
  - We have explored impermanent loss at length in the previous slides.
- **Rug Pulls:**
  - Refers to the act of maliciously removing liquidity from a pool in order to leave users holding tokens with no utility or value. Can be effectively executed for tokens that are not widely traded, especially on CEXes.
  - It is very common for malicious actors to create clone tokens that to trick users into thinking they are trading legitimate
  - This can be mitigated by research and specifically, users confirming the address of the token through multiple sources, such as various blockchain explorers, price tracking websites, and the project's official documentation.
- **Oracle Manipulation:**
  - DeFi protocols rely on oracles to receive information from the real-world. In the case of DEXes this information usually relates to token prices.
  - There is the risk that either the oracle goes bad, or its data is manipulated.
  - This can be mitigated by applications relying on reliable oracles or a plethora of oracle solutions.
  - This is part of a bigger problem in blockchain called "the oracle problem"
  - More on oracles later in the course.

DEX Risks

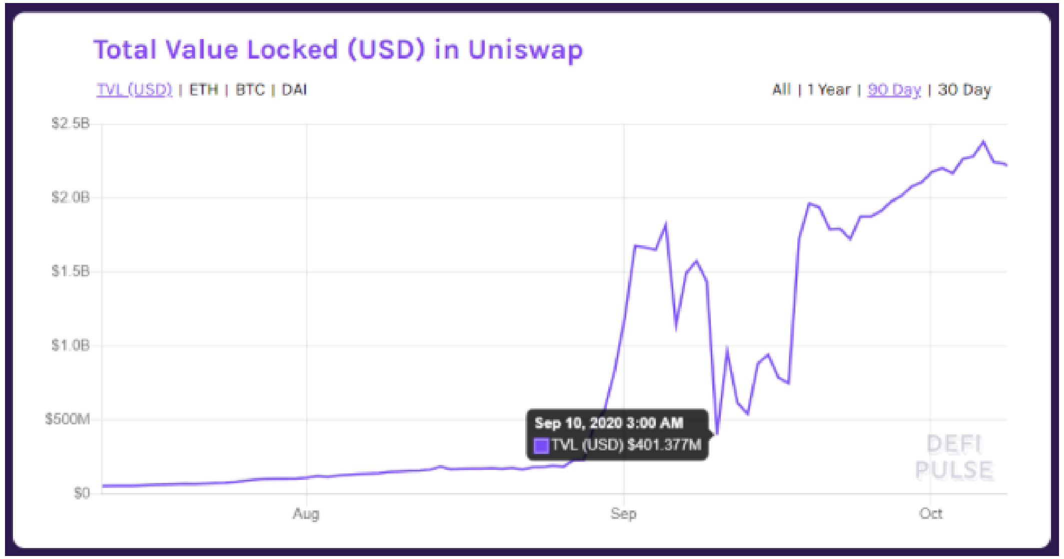
- **Vampire Attack –** A novel attack on protocols that rely on LPs for trades
  - It involves ”draining” liquidity from a DEX by incentivising LPs to move their liquidity to a competitive DEX.
- It usually conducted as follows:
  1. First the attacker incentivises LPs to stake their liquidity provider tokens to a new Platform B (clone DEX).
  2. Users of Platform A (original DEX) see the opportunity of getting more returns for their liquidity
  3. They take their liquidity out of Platform A (original) and supply it to Platform B (clone)
  4. Supplying tokens to Platform B, in exchange for rewards usually involves a token lock-up period
  5. Once enough LP tokens are attracted, the next step is for Platform B, to steal the liquidity of Platfrom A
  6. This works in practice as LP tokens are essentially the “key” or “receipt” for withdrawing and moving around the tokens provided in the Liquidity Pool
  7. The goal is to steal the liquidity and trading volume of the first DEX.
- There is also a more advanced vampire attack which also involves shorting the original DEXes tokens

Vampire Attack on Uniswap By SushiSwap



Liquidity before attack

Liquidity after attack



Source: Blaize.tech

Session 4.1: Decentralized Exchanges

6. Conclusions

Conclusions

- In this session you have learned about real and financial assets, the need for exchanges, and their breakdown based on the type and properties of the asset. You should now have an understanding of why exchanges lie at the heart of financial activity.
- You have been introduced to the concept of decentralized exchanges and learned about the market size and growth. You should now be able to delineate the basic principles that separate DEXes from their TradFi counterparts, have a good grasp of their basic functions, and be able to explain the importance of DEXes for the proliferation of DeFi as whole.
- You have also become acquainted with some notable DEXes as well as some of the more advanced aspects and principles under which they operate, such as liquidity pools and AMMs.
- Finally, you should have an understanding of the primary DEX risks.

Session 4.1: Decentralized Exchanges

7. Further Reading

Further Reading

DEXes

- No Sandwich, Please! - Popular DeFi Attack Strategy Analysis
- Demystify the dark forest on Ethereum — Sandwich Attacks
- Vampire Attack – An attack of liquidity dependent protocols
- Risks in Decentralized Finance
- Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in DEXes
- All you need to know about the Automated Market Maker (AMM)
- Constant Function Market Makers: DeFi's "Zero to One" Innovation
- Uniswap: A Good Deal for Liquidity Providers?
- On Blockchain Frontrunning
- SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols

Tip: Clicking while pressing Cltl key opens a new tab in Chrome browser on non-Apple devices

Join our discord server!

https://discord.gg/r6FrHbsfSJ

UNIVERSITY *of* NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**
Course Support: **defi@unic.ac.cy**
IT & Live Session Support: **dl.it@unic.ac.cy**