Foundations of FinTech

Decentralized Finance (DeFi) – II

Eshwar Venugopal

Centralized Exchanges (CEXs)

- Centralized exchanges are counterparts of security exchanges (NYSE, NASDAQ, etc.) in the crypto world.
- A simple interface to exchange fiat currency for crypto tokens.
- CEXs require identity disclosure – must adhere to KYC and AML laws (compliant onboarding)
- Charge fees for trading
- Can be expensive (can time consuming) for projects to list their tokens
- Has an established fait on-ramp: connection with banks for deposits and withdrawals
- E.g., Binance, Coinbase, Kraken, FTX, etc.

Centralized Exchanges (CEXs)

- Most CEXs allow for market and limit orders
- Handle a large number of transactions
- Trades are routed via internal networks
- Extremely fast execution rates

- Does not allow swapping tokens
- Transactions are executed as IOUs and settlement follows immediately after that.
- Owned and managed by single entity
- Censorship is centralized

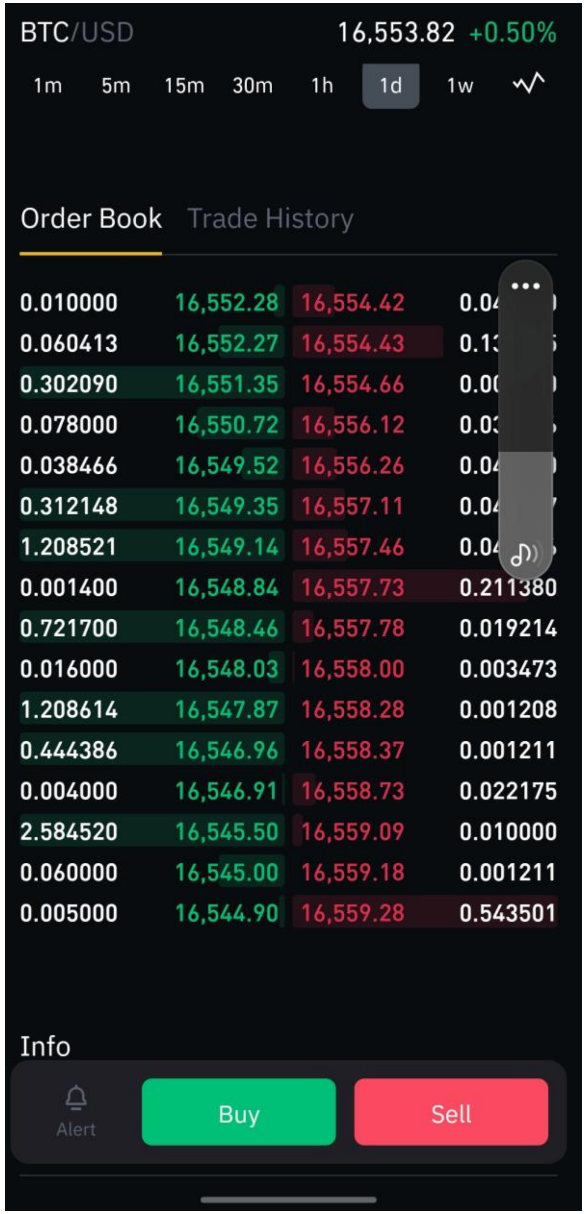
Centralized Exchanges (CEXs)

Just like security exchanges:

- Price discovery, trade matching, and settlement are facilitated by the CEX.
- Custody of the asset is handled by CEX
  - Unless the user explicitly transfers the asset out of the exchange provided wallet
- Private keys of the wallet are maintained by CEXs
- Single point of failure in case of breaches
- Currently, CEXs can and do use customer funds to finance other activities (FTX, Coinbase, etc.)

Centralized Exchanges (CEXs)

- Centralized exchanges *deploy order books to operate.*
- Prices are determined by bids and asks (supply & demand)
- Most exchanges *employ 'market markers'* to support the market during volatile times.
    - During illiquid times, market makers play a crucial role by providing liquidity
    - Market makers could potentially off-load their positions later on for a profit.



BTC/USD 16,553.82 +0.50%

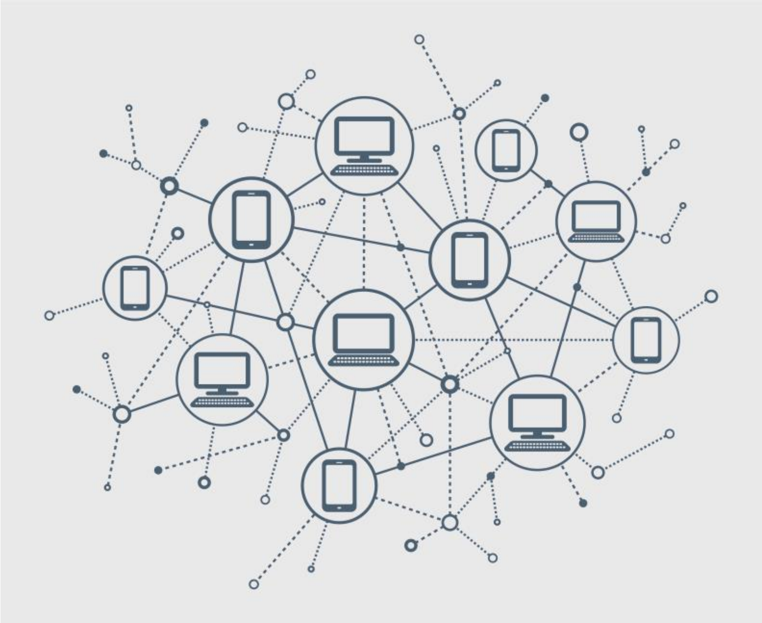
0.010000	16,552.28	16,554.42	0.04[illegible]0
0.060413	16,552.27	16,554.43	0.13[illegible]5
0.302090	16,551.35	16,554.66	0.00[illegible]0
0.078000	16,550.72	16,556.12	0.03[illegible]5
0.038466	16,549.52	16,556.26	0.04[illegible]0
0.312148	16,549.35	16,557.11	0.04[illegible]7
1.208521	16,549.14	16,557.46	0.04[illegible]5
0.001400	16,548.84	16,557.73	0.211380
0.721700	16,548.46	16,557.78	0.019214
0.016000	16,548.03	16,558.00	0.003473
1.208614	16,547.87	16,558.28	0.001208
0.444386	16,546.96	16,558.37	0.001211
0.004000	16,546.91	16,558.73	0.022175
2.584520	16,545.50	16,559.09	0.010000
0.060000	16,545.00	16,559.18	0.001211
0.005000	16,544.90	16,559.28	0.543501

Source: Binance Order Book, Nov 27, 2022

Decentralized Exchanges (DEXs)

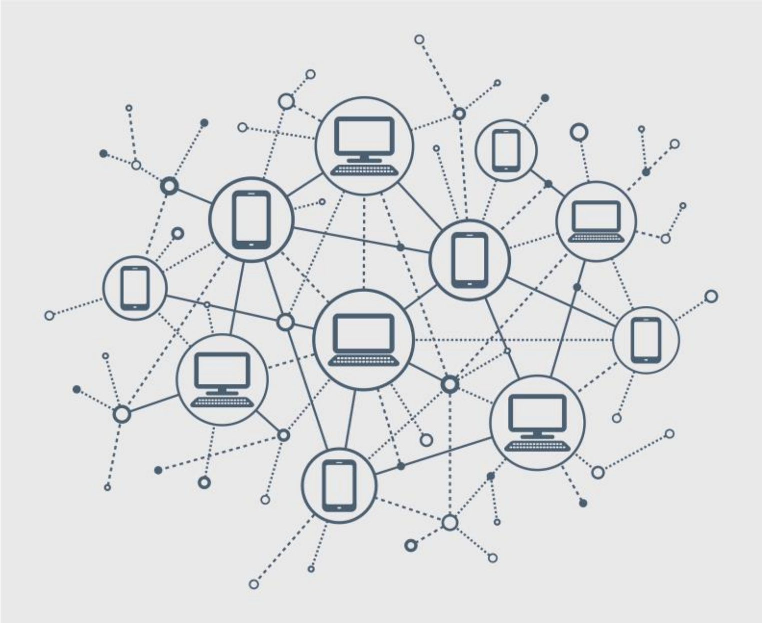
- DEXs are peer-to-peer marketplaces where traders interact *without* the need for a central third party to facilitate transactions.

- Slightly more complicated than CEXs
- Does not require identity verification
- Large number of tokens available for purchase
- Non-custodial transaction and settlement
- Wallet private keys belong to users
- Potentially lower transaction costs
- E.g., Uniswap, Curve, Pancakeswap, dYdX, etc.



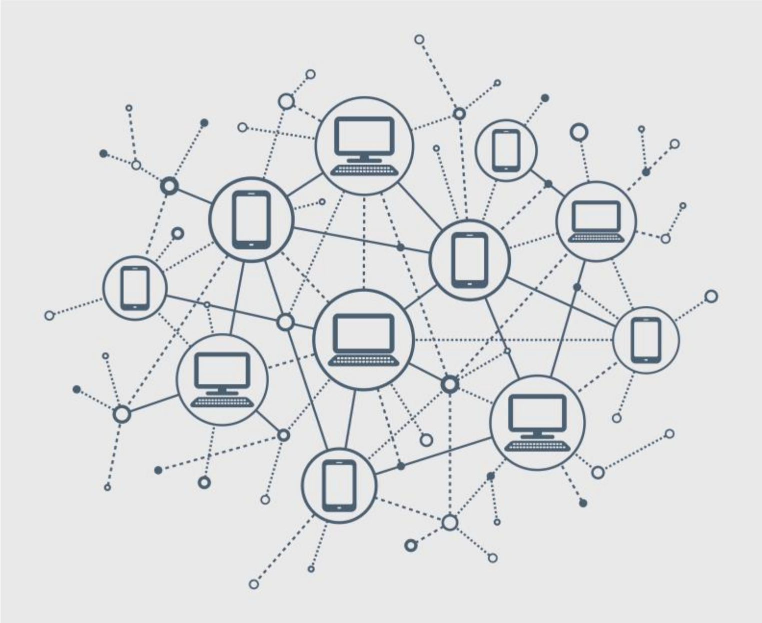
Decentralized Exchanges (DEXs)

- Does *not* have a fiat on-ramp
- Crypto-to-crypto transactions only
- Relatively slower execution times
- Potential for *slippage* is higher
  - *Slippage* is the difference between the expected price of an order and the actual execution price; often expressed in percentage.
  - Depends on the market depth
- Consumer is responsible for security



Decentralized Exchanges (DEXs)

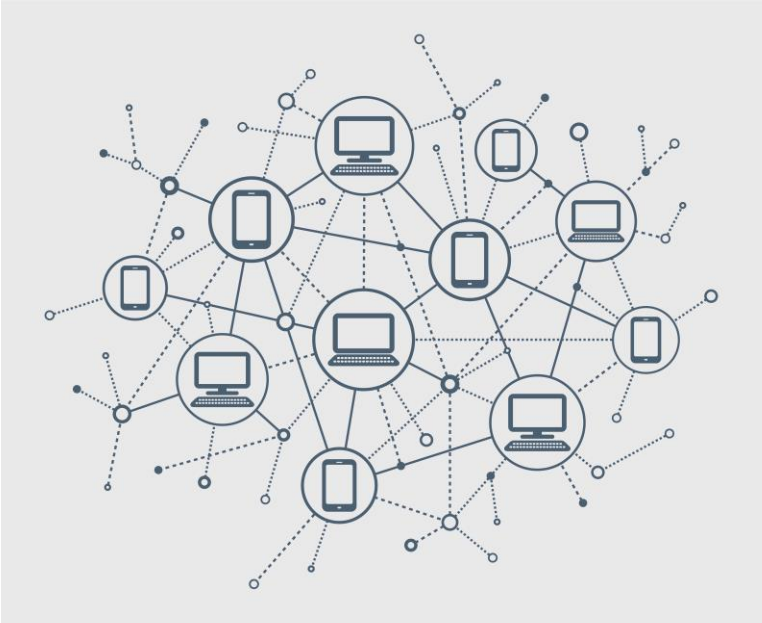
- EtherDelta (https://etherdelta.com) was the first DEX build
- Uniswap is the most popular DEX
  - Built in 2018 on Ethereum with funding from Ethereum Foundation
  - Compatible with ERC-20 token standard and existing wallet infrastructure.
  - Open-source project that was built on Vyper
  - V2 and V3 are written in Solidity



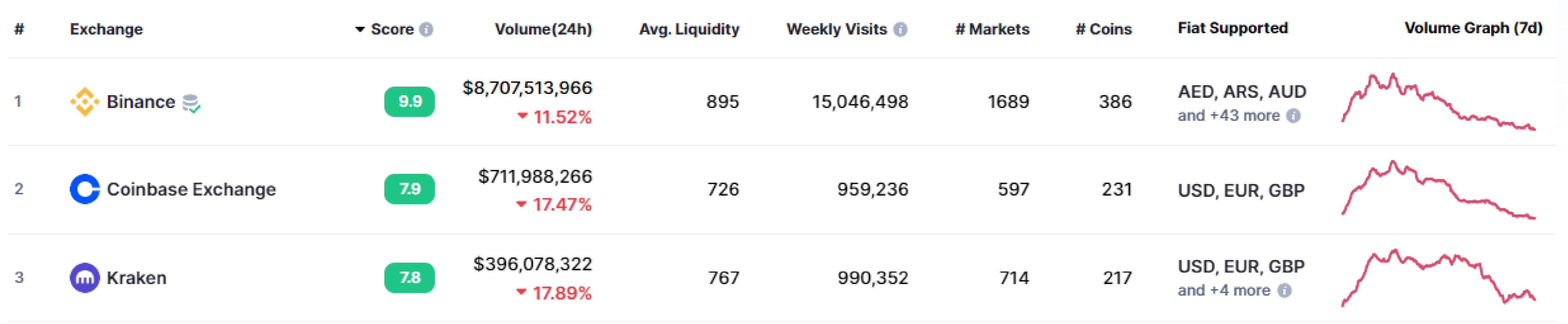
- Now, have many DEXs and recently DEX aggregators also
  - DEX aggregator is a decentralized exchange platform that searches your choice of token pair across all exchanges to provide the best possible price.

Decentralized Exchanges (DEXs)

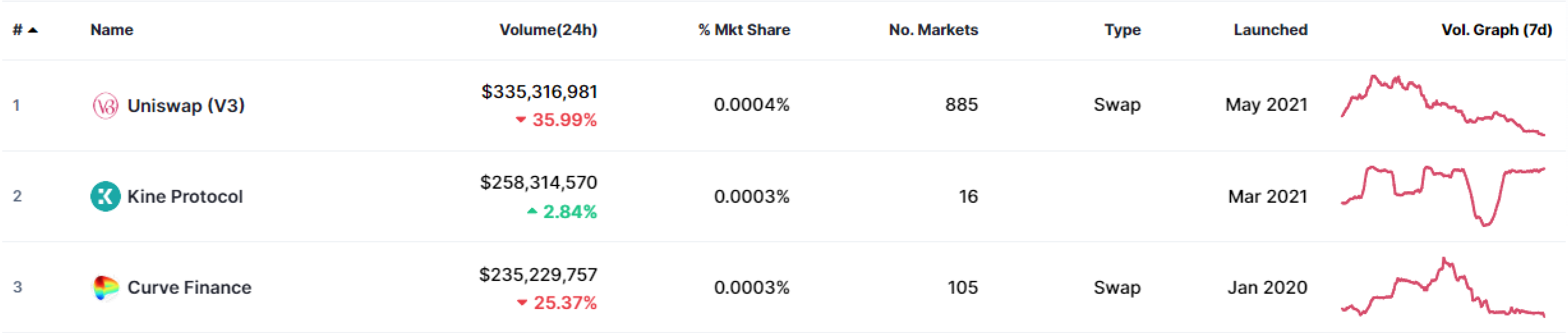
- Blockchains and Smart contracts help with *transactions execution and settlement.*
- One of three mechanisms were used for price discovery:
  - DEX Order book
    - On-chain
    - Off-chain
  - DEX aggregator
  - Automated Market Maker (becoming the most popular method)



CEXs vs DEXs



#	Exchange	Score	Volume(24h)	Avg. Liquidity	Weekly Visits	# Markets	# Coins	Fiat Supported	Volume Graph (7d)
1	Binance	9.9	$8,707,513,966 ▼ 11.52%	895	15,046,498	1689	386	AED, ARS, AUD and +43 more	
2	Coinbase Exchange	7.9	$711,988,266 ▼ 17.47%	726	959,236	597	231	USD, EUR, GBP	
3	Kraken	7.8	$396,078,322 ▼ 17.89%	767	990,352	714	217	USD, EUR, GBP and +4 more	

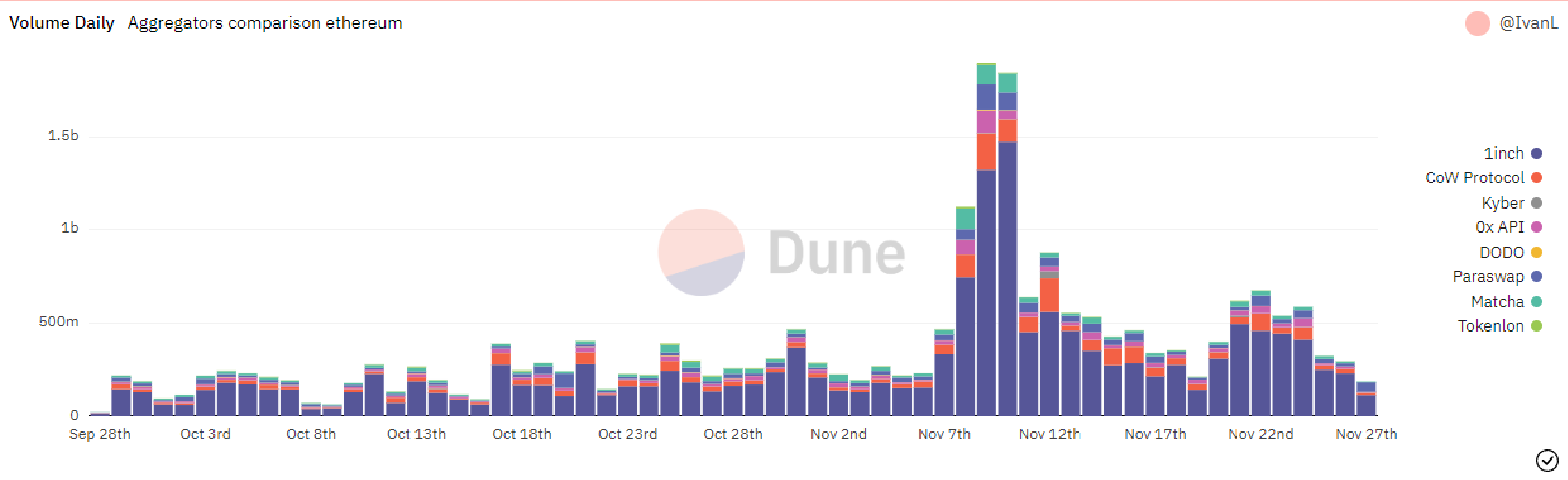


# ▲	Name	Volume(24h)	% Mkt Share	No. Markets	Type	Launched	Vol. Graph (7d)
1	Uniswap (V3)	$335,316,981 ▼ 35.99%	0.0004%	885	Swap	May 2021	
2	Kine Protocol	$258,314,570 ▲ 2.84%	0.0003%	16		Mar 2021	
3	Curve Finance	$235,229,757 ▼ 25.37%	0.0003%	105	Swap	Jan 2020	

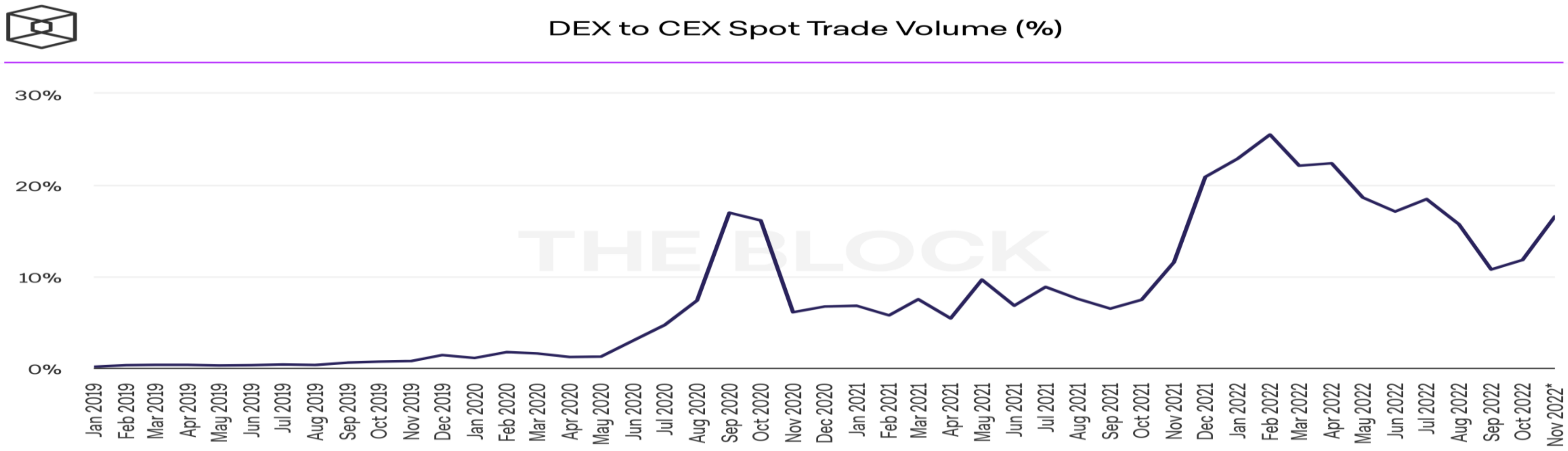
Source: https://coinmarketcap.com/rankings/exchanges/

Most trading activity is still happening in CEXs. But the recent CEX collapses have accelerated move toward DEXs

CEXs vs DEXs



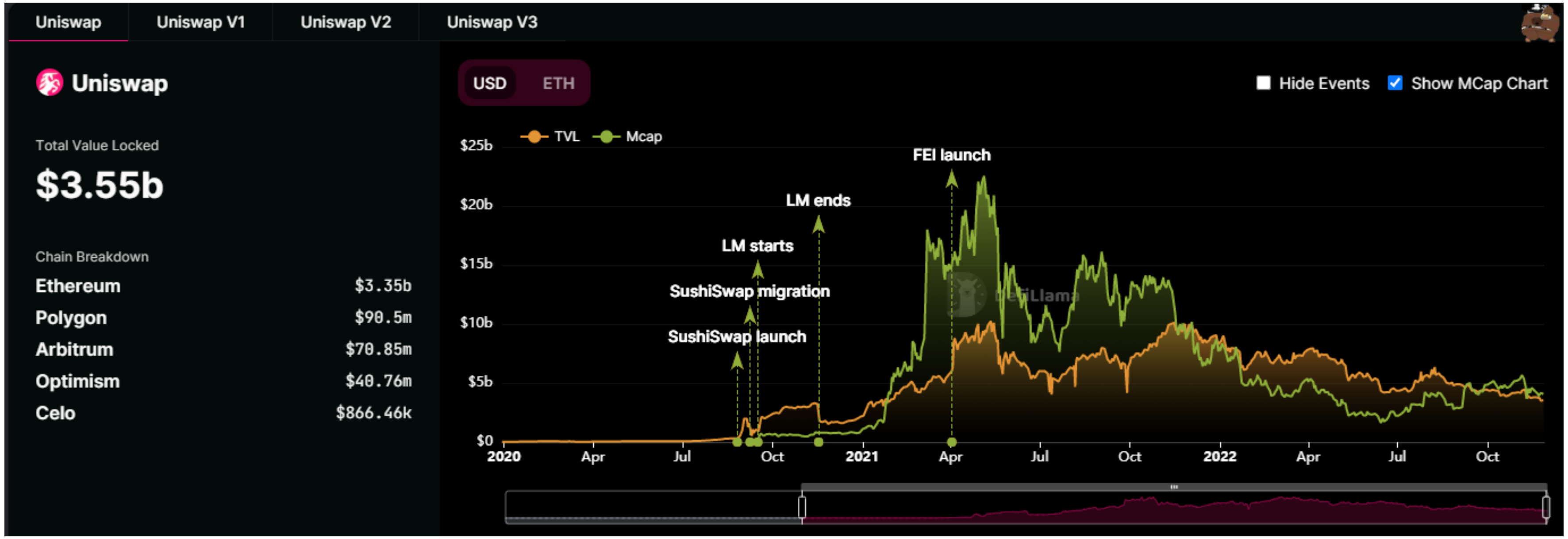
Volume Daily Aggregators comparison ethereum



DEX to CEX Spot Trade Volume (%)

SOURCE: COINGECKO
UPDATED: NOV 26, 2022

CEXs vs DEXs



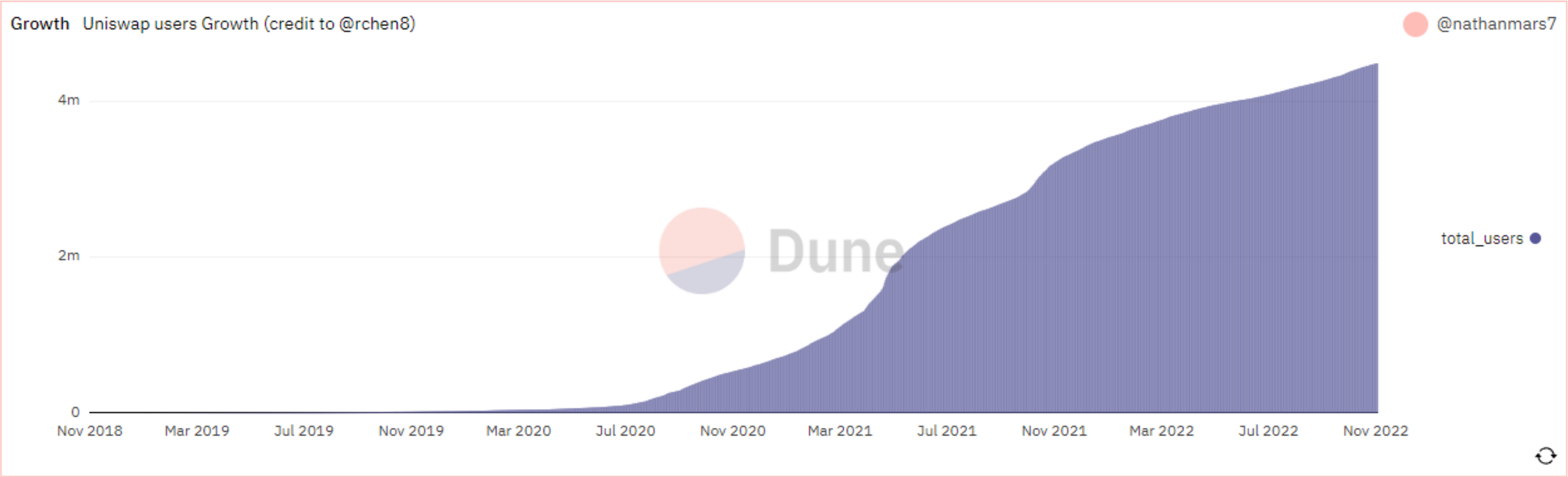
Uniswap

Total Value Locked

$3.55b

Chain Breakdown

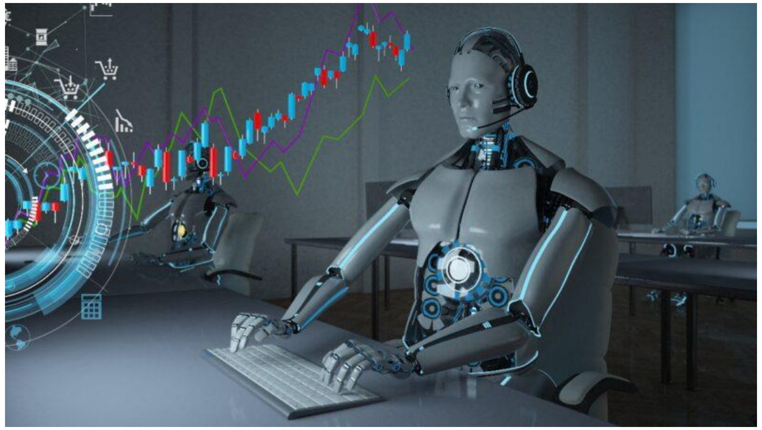
Ethereum	$3.35b
Polygon	$90.5m
Arbitrum	$70.85m
Optimism	$40.76m
Celo	$866.46k


Growth Uniswap users Growth (credit to @rchen8)

@nathanmars7

Automated Market Maker (AMM)

- DEXs ran into liquidity issues without a market maker.
- Employing a market maker in a DEX meant *executing at least two transactions to fill an order and higher transaction fees (i.e., inefficiencies)*.
- Automated Market Maker attempts to *algorithmically price* a token pair using supply & demand price and data from external sources (i.e., via Oracles)
    - Multiple formulas are available. We will use the constant product formula for illustration in this class.
- *Liquidity pools* play an important role in price discovery



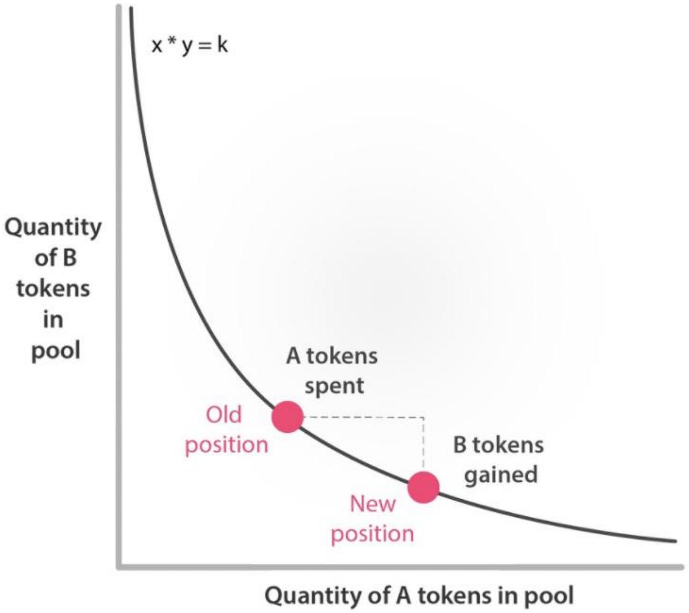


Illustration of constant product formula

Automated Market Maker (AMM)

$$Constant\ Product\ Automated\ Market\ Maker: \boldsymbol{X \times Y = K}$$

	🍇	🧀
Weight (lbs.)	1000	1000
Value	$1,000	$1,000
Price/Pound	$1	$1
Total constant quantity (K)	1,000,000	

Automated Market Maker (AMM)

$$Constant\ Product\ Automated\ Market\ Maker: \boldsymbol{X} \times \boldsymbol{Y} = \boldsymbol{K}$$

New transaction: *Sell 100 lbs. of grapes for cheese*

	🍇	🧀
Weight (lbs.)	1100.000	909.091
Value	$1,000	$1,000
Price/Pound	$0.909	$1.100
Total constant quantity	1,000,000	
Cheese received (lbs)		90.909

Automated Market Maker (AMM)

$$Constant\ Product\ Automated\ Market\ Maker\text{:}\ \boldsymbol{X \times Y = K}$$

New transaction: *Sell 50 lbs. of cheese for grapes*

	🍇	🧀
Weight (lbs.)	1042.654	959.091
Value	$1,000	$1,000
Price/Pound	$0.959	$1.043
Total constant quantity	1,000,000	
Grapes received (lbs)	57.346	

Automated Market Maker (AMM)

$$Constant\ Product\ Automated\ Market\ Maker: \boldsymbol{X \times Y = K}$$

Change out grapes and cheese for DAI and USDC: Fictional transaction

# Tokens	1042.654	959.091
Value	$1,000	$1,000
Price/Token	$0.959	$1.043
Total constant quantity	1,000,000	
DAI received	57.346	

For real transaction see: https://info.uniswap.org/#/pools/0x6c6bc977e13df9b0de53b251522280bb72383700

Liquidity pools

- Liquidity pools are essential for AMM and DEX.
- A liquidity pool is essentially a smart contract.
- Traders rely on specific pairs for swapping, lending/borrowing, etc.
- Depending on the demand, DEXs (establish) promote liquidity pools of token pairs.

- *Routing*: If a token pair demanded by a trader is not available in a DEX's liquidity pool pairs, DEXs route the order by chaining multiple pools.
  - E.g., Trader demands COMP for LOOP
  - The DEX does not have this pool but had COMP/ETH and LOOP/ETH
  - The order will first buy ETH using LOOP and use the ETH to buy COMP

Liquidity pools

In the earlier example, we established a liquidity pool when we added 1000 lbs. of grapes and cheese.

- We are the sole investors of this liquidity pool (i.e., Liquidity Provider or LP)
- We started with a 1:1 ratio of the asset value
- Attempted to maintain the ratio of asset values
- The more an asset is demanded, the supply goes down and price of that asset increases (and the price of the other asset decreases)

Liquidity pools: LP Token

- When you make your investment ($1000 of grapes and cheese), it is locked into a smart contract and a liquidity provider token (LP Token) is generated.
- The LP token gives us a claim to the proceeds of the liquidity pool.
- We receive LP token proportional to our share in the pool
- In our example we receive 100% of the LP tokens since we are the only LPs

- If we want to remove your investment from the pool, we will burn the LP token.
  - We will get the initial investment (i.e., equal value of the 2 tokens invested)
  - Plus, can accrued fees proportional to our investment

Liquidity pools: LP Token

- Traders pay a 0.3% fee for every transaction that uses the pool
- Uniswap V3 now allows for 3 types of fees
  - 0.05% - stable coin and popular stable pairs
  - 0.3% - most common standard papers
  - 1% - exotic pairs (extremely risky)

- These fees are distributed to the investors.

Liquidity pools: Price impact

- Assume someone deposited 500 lbs. of grapes at the start of the example and demanded cheese. *What will happen to the price of cheese?*
- *Price impact* is higher when the pools are smaller compared to the demand
- When the # investors is are low, pools tend to be smaller and price impact tend to be larger (as was the case in 2020 and 2021)

- If you are risk averse, you could invest in pools that are already large – price impact would be lower

Liquidity pools: Arbitrage Traders

- Remember that *once a liquidity pool is created the price discovery is made purely using a designated formula.*
- Such restricted pricing methodology *can lead the price of assets to diverge* from what it is outside of the pool – arbitrage opportunity
- E.g., Suppose in a BTC/ETH pool the price of ETH is pushed down because of a sudden demand for BTC.
  - In the pool, the price of 1 ETH is $1,000 and 1 BTC is $20,000
  - In Binance, the price of 1 ETH is $1,200 and 1 BTC is $18,000
  - You can deposit buy ETH from the pool and sell it to Binance for a $200 profit per coin.
- Arbitrageurs do this till the surplus is negligible (i.e., about $1,200 in the pool)

Impermanent Loss

- Impermanent loss is the *unrealized loss* that occurs when your share of the investment is not the same as your initial investment.
- When this happens, you are entitled to a larger share of the token that lost its value and a lower share of the token that gained in value
    - *Impermanent loss is paper loss in traditional terms*
- Suppose you invested $10,000 worth USDC and AAVE into a liquidity pool (1:1 value ratio).
- Assume that at the time of investment 1 USDC = $1 and 1 AAVE = $100
- A day later 1 AAVE = $110 on an exchange
- But 1 AAVE = $100 in your pool

Impermanent Loss

- Arbitrageurs will buy AAVE from the pool till the pool price reaches $110.
- *How many AAVE tokens arbitrageurs must buy to make the pool price $110?*
- Remember AMM is the constant product formula: $X \times Y \ = \ K$
    - K= 100 * 10,000 = 1,000,000
    - Ratio of AAVE to USDC price (r_0) = 100/1=100
- Initial quantities (t=0)
    - $x_0 = \sqrt{K/r_0} = \sqrt{1{,}000{,}000/100} = 100$
    - $y_0 = \sqrt{K * r_0} = \sqrt{1{,}000{,}000 * 100} = 10{,}000$
- At time t=1, the new ratio of AAVE to USDC price (r_1)=110/1=110
- Quantities at t=1
    - $x_1 = \sqrt{K/r_1} = \sqrt{1{,}000{,}000/110} = 95.346$
    - $y_1 = \sqrt{K * r_1} = \sqrt{1{,}000{,}000 * 110} = 10{,}488.088$

Impermanent Loss

- At time t=1, the new ratio of AAVE to USDC price (r_1)=110/1=110
- Quantities at t=1
  - $x_1 = \sqrt{K/r_1} = \sqrt{1{,}000{,}000/110} = 95.346$
  - $y_1 = \sqrt{K * r_1} = \sqrt{1{,}000{,}000 * 110} = 10{,}488.088$

- Arbitrageurs will pay 488.088 USDC to get (100-95.346) 4.654 AAVE at $100 to make to pool price of AAVE as $110.
- The arbitrageurs will turn around and sell this to an exchange at (4.654 AAVE *$110) $511.912 and make a profit of $23.823.

Impermanent Loss

- The liquidity provider now has $10,488.088 in USDC and AAVE(95.346*110).
- The total value of the pool is 20,976.177.
- Initial value of the pool was 20,000 (i.e., 976.177 in profit)

- But, had the LP held on to his ETH instead of investing in the pool:
  - $10,000 USDC
  - $110 * 100 AAVE = $11,000
- In other words, the investor lost $23.823 by investing in the liquidity pool.
- Investing in stable coin pools is the safer way to avoid impermanent losses.

Stablecoins

Stablecoins

- Stablecoins are the center of the DeFi space and allow you to enter the crypto world while maintaining parity with the fiat world. They are:
  - A store of value
  - A unit of account
  - A medium of exchange
- They attempt to perform the function of fiat currency in the crypto space.
- Typically, pegged 1:1 to a fiat currency
  - E.g., USDC, USDT
- Used for a variety of purposes
  - Parking assets while searching for investment opportunities
  - Pricing other token (especially in DEXs and liquidity pools)
  - Ensuring payment value (non-stable tokens fluctuate in value)
  - Lending/borrowing, insurance, etc.

Stablecoins: Types

Custodial stablecoins:

- Fiat-backed
- Crypto-backed
- Commodity-backed

- Typically issued by centralized exchanges.
- Assets are held off-chain.
- Difficult to audit

Stablecoins: Types

Decentralized stablecoins: Also referred to as algorithmic stablecoins.

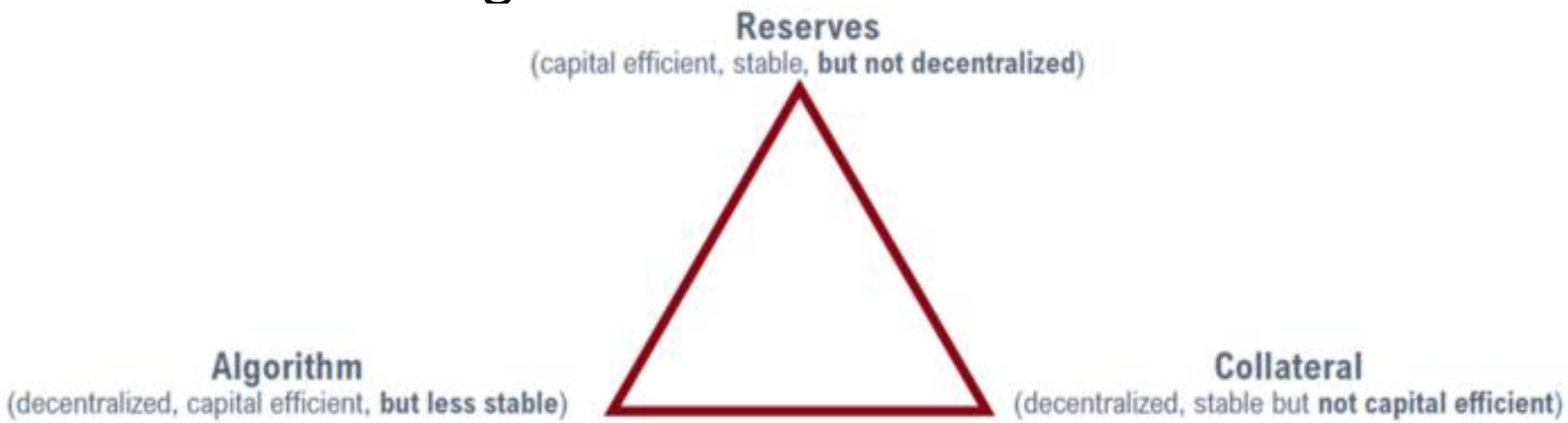
- Assets are held on-chain
- Verification of assets is easier
- Issuers must maintain enough assets for a rainy day
- As Terra/Luna fiasco showed, it is difficult to keep algorithmic coins stable during volatile times

- How do they work?
  - UST/Luna for example: https://www.youtube.com/watch?v=KqpGMoYZMhY&ab_channel=Terra

Stablecoin Trilemma

An ideal stable coin will have the following three characteristics:

- Capital efficient
- Stable
- Decentralized



Reserves
(capital efficient, stable, **but not decentralized**)

Algorithm
(decentralized, capital efficient, **but less stable**)

Collateral
(decentralized, stable but **not capital efficient**)

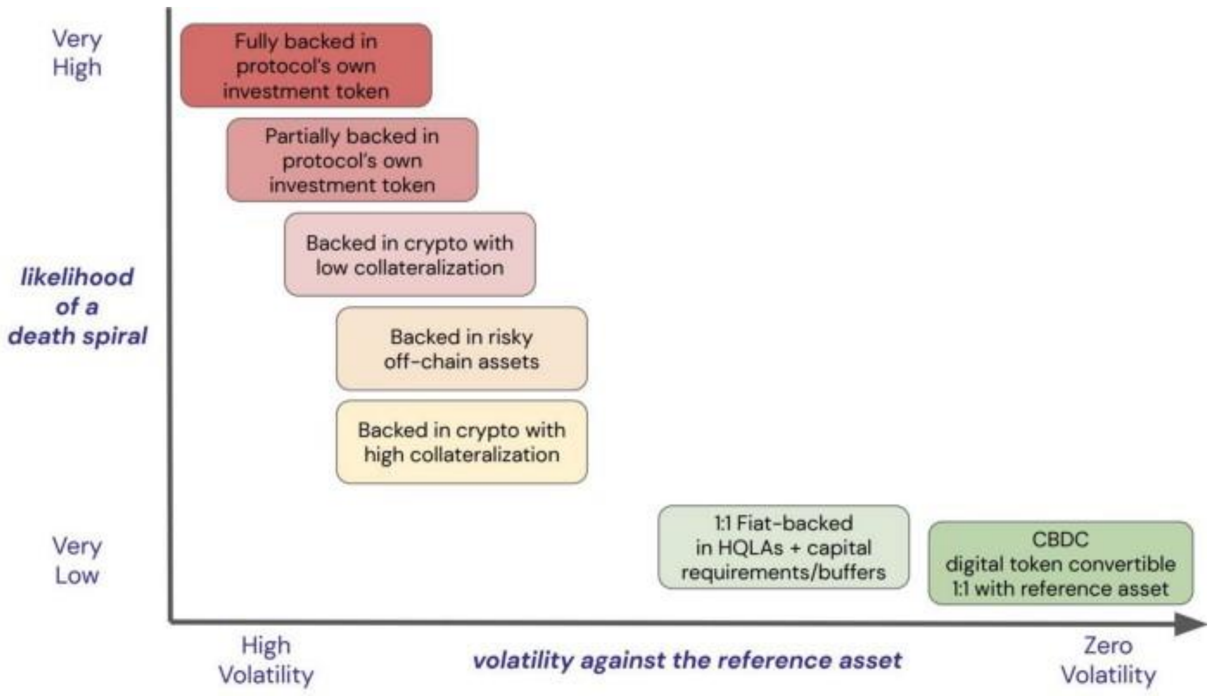
Source: WWVentures

- Most stablecoins can achieve only 2 of 3 characteristics
  - Custodial coins are reserve based
  - Collateral /crypt/commodity need over-collateralization
  - Algorithmic stablecoins are less stable

Stablecoin Trilemma

- Remember that they are attempting to ensure stability in comparison to an off-chain fiat currency!
- Naturally, private stablecoins will not be able to achieve fiat-equivalent stability

- Central Bank Digital Currencies (CBDCs) do not suffer from this issue because the reference asset is its non-digital native.


Very High
likelihood of a death spiral
Very Low
Fully backed in protocol's own investment token
Partially backed in protocol's own investment token
Backed in crypto with low collateralization
Backed in risky off-chain assets
Backed in crypto with high collateralization
1:1 Fiat-backed in HQLAs + capital requirements/buffers
CBDC digital token convertible 1:1 with reference asset
High Volatility
volatility against the reference asset
Zero Volatility

Source: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899499