DEXs: An Analysis of AMM Alternatives

Jared Israel   Jacob Queiser

The Ohio State University

April 19, 2023

Automated Market Maker Refresher

UniswapV3

Prices are determined by a relationship between two assets in a liquidity pool.

- Bonding curves.
- Constant Product Market Maker (CPMM).
- Smart Order routers.
- And many more.

UniswapV3 marries CPMM with ticks [1]

- Ticks are price ranges liquidity providers can insert their assets in.
- Lowers slippage
- Lowers risk of impermanent loss.
- Makes things more complicated for inexperienced users.
- Ticks are fixed ranges (Still no stop-loss orders)

AMM Downsides

- Must provide liquidity to both sides.
- Pools can be volatile [1]
  - Frequent fluctuations in asset prices.
  - Requires complex calculations to determine a zero-loss liquidity position.
  - Providers will encounter more slippage.
- Impermanent Loss
  - Practically inherent with any exchange but can be mitigated.
- Must trade at market price. No deciding ...
  - Prices
  - Bids
  - Direction (movement of the market)
  - Size

Serum

Solana

Serum uses the Solana Blockchain [2]

- Proof-of-stake
- stateless = faster
- Nodes in clusters with rotating validator roles = more centralization
- cheap: a ”few cents” per transaction
- A block is mined every 400-600 ms [3]

[2]

The Serum Protocol

- Base protocol for exchanges that wish to build on Solana.
- Fully on-chain.
- Decentralized **Central Limit Order Book** (CLOB)
- No price oracles.
- Highly Composable: multiple applications can access the same liquidity.
- Non-Custodial
  - Users are responsible for their private keys
  - No custody of funds.
- uses the SRM utility token.
- Cross-chain swaps without requiring arbitrators.
- Decentralized Autonomous Organization (DAO) Governance

[3], [4]

Order Book

- Make Limit and Stop-Loss orders.
  - set price
  - set size
  - set direction
- Matching engine based on price and time priority.
- Solana allows for an efficient and high-throughput automatic matching engine.
- Market prices determined by bids/asks (like a Stock Exchange).
- Only taker fees. Makers do not pay a fee.
- Trading of custom cryptocurrency contracts also supported.

[3]–[5]

Utility Token and Staking

- SRM and MSRM (1,000,000 SRM)
- Fees for orders.
- Staked on Nodes
  - 80% towards a burn.
  - 20% redistributed to nodes.
- 10,000,000 SRM required to run a node.
- At least MSRM is also required to run a node.
- MSRM Capped at 1000
- 25,000 SRM required to participate in the DAO.
- Up to a 50% discount on fees if you stake SRM
  - 60% off fees if you stake 1 MSRM

[3]–[5]

Nodes

- Nodes receive rewards in the form of SRM for:
  - Providing insurance for cross chain swaps.
  - Optimizing throughput of the ecosystem
- Nodes are created by leaders who can receive an additional portion of the rewards.
- Penalties are also possible.

[4], [5]

Serum Cross-Chain swaps

- Parties enter smart contract with collateral.
- If one party (Bob) doesn't send their part of the exchange, the other (Alice) can open a dispute with the Smart Contract.
- Both parties send their Blockchain histories to the contract.
- Alice can receiver her swap amount, collateral, and some of Bob's collateral.
- Vice versa can occur also if Alice lied except with the swap being performed.
- If both parties behaved honestly, swap is performed and collateral is returned.

[4]

Downfall

- FTX hacked around time of its collapse.
- Hack revealed update authority keys may have been stolen, causing many exchange front-ends to migrate.
- Alameda also held complete authority in the DAO and made all the decisions, if any were made in the first place.
- Serum team has forked the code base and hopes to re-release it with improvements to the DAO system.

[6]

Airswap

Overview

- A peer-to-peer network.
- A mix of second-layer technology and smart contracts on the Etherium blockchain.
- Market participants discover others on the network and complete trustless **atomic** swaps.
- Discovery done through 1 of 3 protocols:
  - Request for Quote (RFQ)
  - LastLook
  - Over-the-counter (OTC)
- A utility token for governance only.
- Non-custodial
- No slippage.
- No front-running.
- Simple logic is gas cost-effective.

[7]

Makers

- Can form their own pricing strategies.
- Run on traditional web servers
  - HTTP
  - Websocket
- Communicate with JSON protocols (JSON-RPC)
- Their URL is registered to a Registry: an Etherium contract
  - Clients will query this.
  - The protocol therefore relies on Makers to be their own nodes in the network and be online.
  - A Maker will have to program their own orders. Can be a good and bad thing depending on who they are.

[7]

Protocols

- **Signers** cryptographically sign the terms of an order.
- **Senders** Submit the signed terms to the contract for an atomic swap.
- The Maker can be a signer and the Taker a sender, or vice-versa
- Depends on the protocol.
- Senders therefore pay for execution.
- Protocols are **off-chain** matching engines.

[7]

RFQ

- Clients (takers) request orders through HTTP or WebSocket.
- Takers are senders, Makers are signers.
- Takers can accept/reject orders.
- Protocol fee hashed into signature.
- Fee must match that of the swap smart contract.

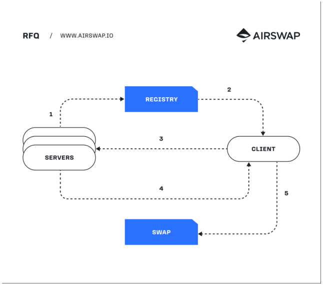


Figure: Courtesy of [7]

[7]

LastLook

- Clients (Takers) stream pricing info. from Makers.
- Takers are signers, Makers are senders.
- Makers can accept/reject orders.

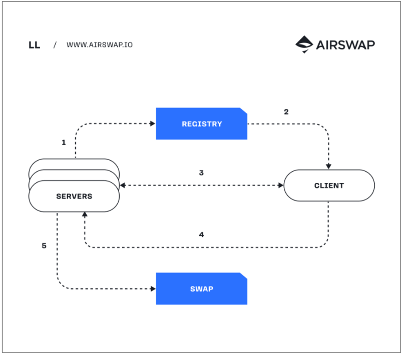


Figure: Courtesy of [7]

[7]

OTC

- More manual trading
- Prices negotiated using third party chat apps, SMS, email, etc.
- Entering a third party complicates fairness, trust, and decentralization.
- Airswap is then used to perform an atomic swap.

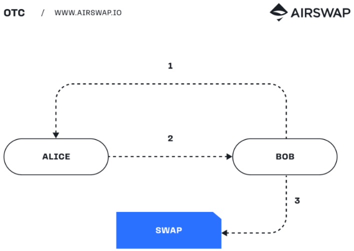


Figure: Courtesy of [7]

Gridex

What we've seen so far

AMMs:

- Low resource consumption (especially on Etherium)
- Easy to implement on chain.
- Impermanent loss, Slippage are problematic, especially on volatile pools.
- Trading not as flexible.

Order Books and P2P Systems:

- More flexible for traders.
- Lower risk of loss for liquidity providers.
- Requires additional architecture that goes beyond the blockchain.
- Or requires a specific blockchain with high throughput and low latency.
- Potential risk of fragmented liquidity (implementation dependant).

Overview of Gridex

- On the Etherium blockchain.
- Based on CLOBs.
  - **Grid Maker Order Book** (GMOB).
  - No Slippage [9]
- And a matching engine: **Grid Price Linear Movement Algorithm** (GPLM)
  - Simple and easy.
  - Reduced resource consumption on Etherium.
  - Comparable gas costs to AMMs.
- Gridex is very new. D5 began to support it just a few months ago.

[8]

GMOB

Very similar to CLOB but with some differences:

- Maker orders are bounded within a specific price range called the **resolution**.
- Orders are not instantly fulfilled like with limit orders. Rather they just add liquidity.
- Manual collection required.
- Negative fees for liquidity providers (Makers) when their order is fulfilled.

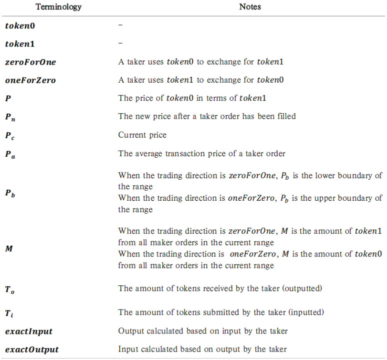
[8]

GPLM

Numerous equations the Taker has at their disposal to determine:

- Price
- Size
- Direction

they wish to trade at. These equations effect the current price of assets.

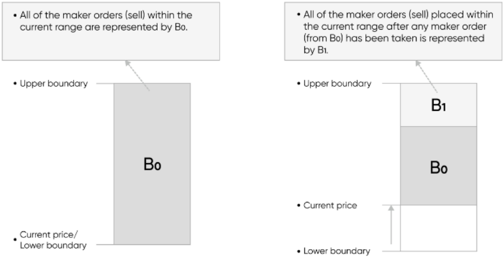


Terminology	Notes
$token0$	–
$token1$	–
$zeroForOne$	A taker uses $token0$ to exchange for $token1$
$oneForZero$	A taker uses $token1$ to exchange for $token0$
P	The price of $token0$ in terms of $token1$
P_n	The new price after a taker order has been filled
P_c	Current price
P_a	The average transaction price of a taker order
P_b	When the trading direction is $zeroForOne$, P_b is the lower boundary of the range When the trading direction is $oneForZero$, P_b is the upper boundary of the range
M	When the trading direction is $zeroForOne$, M is the amount of $token1$ from all maker orders in the current range When the trading direction is $oneForZero$, M is the amount of $token0$ from all maker orders in the current range
T_o	The amount of tokens received by the taker (outputted)
T_i	The amount of tokens submitted by the taker (inputted)
$exactInput$	Output calculated based on input by the taker
$exactOutput$	Input calculated based on output by the taker

Figure: Courtesy of [8]

GPLM

"Linear" as in price changes within a given range is linearly proportional to the taken coins.



- All of the maker orders (sell) within the current range are represented by B_0.
- All of the maker orders (sell) placed within the current range after any maker order (from B_0) has been taken is represented by B_1.

Figure: Courtesy of [8]

[8]

GPLM

- B: Bundle of orders in this range.
- Each maker order filled by $\frac{T_o}{M}$
  - coins taken over the total amount in the pool
- Current price is adjusted.
- New bundles continue to form as Makers continue to add into the range.
- Once all bundles are filled in this range, the current price moves up into the next range's lower boundary.

[8]

Ranges, Resolutions, and Fees

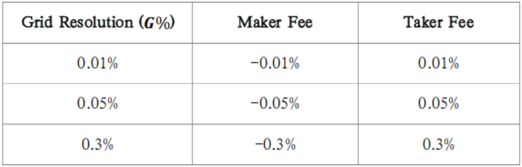
- 3 ranges initially supported
  - Any exchange can choose from these 3.
  - Wider ranges can reduce impedance loss.
  - Wider ranges can be used for volatile coins, and thinner for stable coins.
- Resolutions define a step size that can create boundary values P_b for the range at some index i:

$$P_b(i) = 1.0001^{(100G)i}$$

- Resolutions also define the fees of exchanges in that resolution, or **Grid**

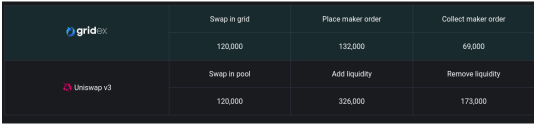
[8]

Resolutions, Fees, and Gas Costs



Grid Resolution ($G\%$)	Maker Fee	Taker Fee
0.01%	−0.01%	0.01%
0.05%	−0.05%	0.05%
0.3%	−0.3%	0.3%

Figure: Courtesy of [8]



gridex	Swap in grid	Place maker order	Collect maker order
	120,000	132,000	69,000
Uniswap v3	Swap in pool	Add liquidity	Remove liquidity
	120,000	326,000	173,000

Figure: Courtesy of [9]

Issues

- Makers submitted smaller sized orders.
- This way they could get their rewards sooner.
- Caused a chain reaction of liquidity drop.
- Caused high liquidity concentration in a price range.
- They changed the rules to give partial rewards.

[10]

Our Implementation

A Lightweight Alternative

- Secure middleman contract for token/ETH trades
- Provides quick and lightweight platform to stage trades agreed upon off chain
- Useful for pain-free trades in a non-anonymized environment (eg. friends, coworkers)
- Avoids large exchanges or unsecure middleman
- One of the two traders proposes a trade that other trader can join
- Once both have deposited, currencies are swapped securely by the contract

Demonstration

Future Work

- Working with decimals of ERC20 tokens
- Add stronger filtering/failure logic for trades
- Mitigation mechanism
- Larger digital asset support
- Implementing checks for specific tokens (simplify workflow)
- Anonymization of addresses (ZK proofs)
- Time locking/expiration
- Multiple deposits of different currencies
- Working with other networks
    - BTC using BTC Relay (http://btcrelay.org/)

References I

[1] L. Heimbach, E. Schertenleib, and R. Wattenhofer, "Risks and returns of uniswap v3 liquidity providers,", 2022, arXiv:2205.08904 [q-fin]. DOI: 10.1145/3558535.3559772. [Online]. Available: http://arxiv.org/abs/2205.08904.

[2] *Solana vs. polygon vs. ethereum – the ultimate comparison*, en-US, 2022. [Online]. Available: https://www.blockchain-council.org/blockchain/solana-vs-polygon-vs-ethereum/.

[3] K. Jayaraj, *Serum protocol: Solana defi solution you need to explore*, en-GB, 2022. [Online]. Available: https://www.coinbureau.com/review/serum-solana/.

[4] S. Foundation, *Serum whitepaper*, en-GB, 2020. [Online]. Available: https://assets.website-files.com/61382d4555f82a75dc677b6f/61384a6d5c937269dbed185c_serum_white_paper.88d98f84.pdf.

References II

[5] *Serum: A decentralized on-chain central limit order book*, en. [Online]. Available: https://consensys.net/blog/cryptoeconomic-research/serum-a-decentralized-on-chain-central-limit-order-book/.

[6] D. Nelson, *Ftx hack sparks revolution at serum dex as solana devs plot alameda's ouster*, 2022. [Online]. Available: https://www.coindesk.com/business/2022/11/12/ftx-hack-spooks-solana-defi-community-igniting-revolution-at-alameda-controlled-serum-dex/.

[7] *Airswap*, [Online]. Available: https://about.airswap.io/.

[8] *The gridex protocol*, [Online]. Available: https://www.gdx.org/gridex-whitepaper.pdf.

[9] *Gridex*, [Online]. Available: https://www.gdx.org.

References III

[10] *Our analysis of the recent crash and subsequent changes to maker reward rule*, [Online]. Available: https://blog.gdx.org/our-analysis-of-the-recent-crash-and-subsequent-changes-to-maker-reward-rules-f93a1650b573.