Abstract

In the first few years of Ethereum ecosystem's development,@vbuterin crystallized the following predictions about the paradigm of decentralized trading:

1. Path independent markets (i.e. AMMs) are core to bootstrapping permissionless, 24/7 price discovery.
2. Arbitrage profits in these markets are captured by miners (i.e. MEV).
3. Specialized venues for large trades will arise to address inefficiency.
4. Hybrid market designs will include asynchronous trading and redistributing arbitrage profits.

In Q2 2022, we briefly review Vitalik's four ongoing predictions with respect to the current state of decentralized exchanges, 5 years later. We introduce the Integral system as the first in-production market design to preliminarily fulfill Vitalik's not yet realized predictions about the future of liquidity on-chain (#3

, #4

). We outline Integral's design choices which yield beneficial properties from being an asynchronous market, including: risk reduction and MEV resistance, capital efficiency for market makers, and achieving a zero-impact execution price for traders. We finish with a discussion of ongoing challenges and open design questions, on which we welcome constructive community engagement, as we continue to work towards Vitalik's vision of mature on-chain markets.

Introduction

Five years ago, in June 2017, Vitalik Buterin discussed the merits and robustness properties of what we now know as Automated Market Makers (AMMs) towards permissionless, always available trading venues with path independent market states. His proposal outlined what he saw as the future for on-chain trading, and specifically how he envisioned price discovery and liquidity to develop on Ethereum. In Q2 2022, two big predictions about (1) price discovery and (2) arbitrage profits, have been definitively validated by AMMs such as Uniswap, and the rise of Miner Extractable Value (MEV), respectively.

Today we first review Vitalik's additional hunches about the frontier of longer-term development of liquidity on-chain, in the lens of what our team has been observing on-chain and building towards at Integral (integral.link). We also introduce our preliminary design to address the challenges Vitalik named, and discuss ongoing challenges and future work where we welcome constructive community engagement.

A couple of 2017 Vitalik's predictions for liquidity on-chain are yet-to-be realized:

VB Prediction 3: Market makers [AMMs] would likely be inefficient for fulfilling large trades

, hence specialized venues for large trades will arise.

Today: Market makers coordinate liquidity via liquidity mining incentive programs in order to make large trades first possible (availability) and hopefully at a reduced price impact (depth). It follows that a fundamental issue is inefficient liquidity utilization: for the market maker to fill trades of certain size, it needs to maintain a large liquidity reserve, which becomes inefficient if large trades are infrequent. Ways to address this issue include boosting depth or driving capital efficiency: i.e. Curve Finance and Uniswap v3 (through the Concentrated Liquidity mechanism).

VB Prediction 4: Expect to see a class of "hybrid semi-automated market makers that have the same guaranteed-liquidity properties" and additional properties, namely:

(a) asynchronous trading and

(b) aiding in redistribution of arbitrage profits from miners to operators (i.e. market makers)

Today: MEV affects trading on Ethereum, where about 90% or more of arbitrage profits go directly to miners. This constitutes a tax on the other trading participants: (i) market makers (AMM LPs) via impermanent loss risk and (ii) organic traders via frontrunning risk. To date, nearly all on-Ethereum trades by volume settle synchronously (atomically), either directly or indirectly (via flow through aggregators).

Enter Integral:

At Integral, our design extends the AMM architecture to focus on market depth rather than primary price discovery. The solution allows traders/LPs to swap/deposit/withdraw to a two-asset pool, thru a two-phase asynchronous trading process:

(i) Commitment: declare an action in a delay infrastructure by time-locking the associated asset(s) for a duration time t.

(ii) Delayed Execution: settle the resulting action against the pool, after t has elapsed in the delay infrastructure, at its corresponding external TWAP oracle, and a flat price curve.

Practically, Integral is the first design and production implementation system, to our knowledge, to address both of Vitalik's two aforementioned predictions on liquidity.

Design Properties:

Our system yields the following system properties and desirable consequences:

1. Asynchronous

: Firstly, due to its two phases, swapping is no longer an atomic activity, which makes the entire act asynchronous: non-composable with respect to atomic on-chain activities.

1. Swaps require proof of asset (for time t)

: as a corollary of (1), swaps must take real asset commitment, therefore actions relying on composing other atomic primitives (i.e. flash loans) where assets are "called-in" for less than time t are incompatible with the natural timeline of a swap.

1. Frontrunning is cost prohibitive

: as a corollary of (2), adversarial frontrunning techniques are rendered far more expensive by magnitudes.

1. Mitigated impermanent loss

: via external oracle, the protocol adjusts its internal price state lazily without the requirement of trading to convey price updates. This eliminates the systemic role of arbitrageurs' profit in typical AMMs, and its resulting impermanent loss on LPs. In practice, an oracle may not reflect the true price in a timely fashion (lagged updates), hence the delay infrastructure requirement ensures that oracle updates are always completed (catch-up) before trades are executed.

1. MEV resistance

: following from (2,3,4), the design reduces endogenous value that can be extracted from the system by miners (i.e. MEV).

1. Zero price-impact swaps, size independence

: the system employs a flat pricing curve, which enables the market maker to support large trades at zero price impact with only limited asset reserves. This enables swaps to execute at the TWAP oracle benchmark, independent of the swap size, up to the asset reserve limitation.

1. Liquidity Efficient

: as a corollary of (6), the system is capital efficient compared to constant function market makers (CFMMs).

Design Challenges:

However, despite our system's benefits, we witness significant open-ended challenges that we believe future market designers will continue to face:

i. Always or Eventual Availability?

As a corollary of market depth benefits stated in (4,6,7), one drawback is that the system liquidity is available only within a defined price range. Hence, the property of "guaranteed asset availability at all times" is not satisfied for the system unlike for instance the typical AMM; it is possible that during a particular period, trade flows are skewed meaning the pool is imbalanced with only practical availability for one-sided asset liquidity (e.g. the reserve proportions are 99% ETH and 1% USDC). Our current understanding is to rely on trade flows being balanced in the long run at the limit, meaning "eventual" availability in the case of pool skew towards one side. This is however a fuzzy and dissatisfying solution given we relax the guaranteed swap availability of the two pool assets, compared to typical AMMs. Accordingly, we see the question of designing an "always" vs "eventual" solution, as one that spans an availability spectrum.

ii. Trading Incentives for availability?

Towards creating stronger eventual availability as discussed in (i), our preliminary attempts to address the pool imbalance issue (hence availability) include:

- Incentives (i.e. native governance token rewards) for external participants to balance the pool.
- Recommending/nudging or even constraining LP deposits/withdrawals to an asset ratio that is helping the pool towards balance (for instance, when the pool is at a relative surplus of token A and shortage of token B, then incentivize or force deposit in higher value of B and lower value of A, and withdrawal in higher value of A and lower value of B).

We view these as reductive to trading incentives, in the sense that its an exogenous reward structure that encourages

trading in a particular direction and discourages trading in the other.

iii. How will Synchronous users experience Asynchronous infra?

As a corollary of (1) asynchronous workflow, the ability for atomic pass-through trade flow interfaces (such as aggregator smart contract routers) to interact with the system is currently limited without further re-design or workarounds. This requires either:

a. UX Evolution: a combination of users and front-ends adapt and adopt asynchronous processes, though unpopular now.

b. Synchronous Transferability of Asynchronous Outputs: The system could be extended to allow immediate synchronous rehypothecation of a user's ongoing asynchronous swap in the delay infrastructure of duration t. They thereby are issued an IOU (promise) that can be presented later to collect the final result of a future swap settlement. This IOU may be implemented in form of tokens or NFT, which can then be used in further atomic markets or operations and further traded/collateralized.

Looking Forward:

Now in Q2 2022, we genuinely believe we have reached the frontier of what 2017 Vitalik's foresight has outlined for a DeFi on Ethereum. Beyond his remaining hunches and predictions are now the open waters the Integral product and research teams are sailing into. We share what we have built, with the intention to begin open discussion, and collect critique and feedback, as a culmination of a cycle of building in public. We believe other systems designers and researchers in this space can learn from the designs/solutions we have tried (and are trying), and critique our approaches. We welcome those who are committed to face the ongoing open challenges, to join us together (especially on the challenges we have outlined above). At this point there are a multitude of open topics & questions for Ethereum that both encase DeFi, but also extend through it (e.g. MEV), which we believe are best solved as a series of collaborative critiques and experiments.

Contact Us:

We share what we have built, with the intention to begin open discussion, and collect critique and feedback, as a culmination of a cycle of building in public. We would love to hear thoughts and feedback here. Alternatively, you can find us on Twitter at IntegralHQ.

[Apologies for the broken links due to 2-link limit.]