Axo Protocol

Whitepaper

THE NEW ERA OF TRADING

Jarek Hirniak
January 2024

This page intentionally left blank

A new standard for trading.

Fair and programmable trading protocol
for the Cardano blockchain.

White Paper v1.1

Jarek Hirniak
January 2024

This page intentionally left blank

Abstract

axo protocol is a solution to the inefficiencies and central counterparty risks of traditional centralized and decentralized protocols. By reflecting on the fundamental meaning of trading, value exchange and market forces, it proposes a series of innovative solutions, addressing them in a trustless manner.

The outlined work is the outcome of years of financial experience combined with cutting-edge research in market making and formal methods. It proposes a series of revolutionary solutions for trading, from a formal language of exchange – programmable swaps, to a unique protocol design allowing for robust and fair construction.

axo will be developed on Cardano to show the approach's potential and utilize unique Cardano security and computation paradigms. In doing so, the protocol is poised to make the entire ecosystem more efficient and provide novel revenue-generating streams. The proposed approaches will enable protocol users to take control of impermanent loss, significantly increase capital efficiency, and will render much more efficient market making and price discovery.

Building on the foundation of programmable swaps and an order execution network, the platform enables a multitude of alpha-generating products. These products could include passive investments such as indexes, through synthetics, and financial derivatives, to programmable trading strategies akin to those employed by top-performing market makers and hedge funds in traditional finance.

The platform connects investors with a wide range of investment products while enabling risk control, dynamic hedging, and adaptability to market conditions. Alongside the protocol, a signal engine architecture offering high-frequency on-chain data streams, data and tooling for back-testing is outlined.

The **axo** platform is set to decentralize and democratize access to bespoke trading tools and investments for the entire world.

1 Disclaimer

Cardano is a new, third generation blockchain, with a novel Extended Unspent Transaction Output (EUTxO) model and the Plutus smart contract programming language under active development. **axo** is a platform proposing a series of innovative and revolutionary concepts. Therefore, matters described in this white paper are subject to potential change in the future, carry unknown risks that might impact parts of the project, and create opportunities for new discoveries that could require rethinking some of the initial assumptions. We reserve the rights to adjust the plan. Any new endeavours are filled with discoveries and novel ideas, and we plan to capitalize on them and adjust to them.

Below is the vision of the **axo** platform in the long term and does not represent a feature list planned for launch.

Contents

List of Figures

List of Tables

2 Introduction

In this section, we lay the foundations for the rest of the paper, introducing fundamental financial engineering concepts, with a focus on their application in *Decentralized Finance* (DeFi). We firmly believe that DeFi is a young ecosystem that can benefit in a significant way from the application of a wealth of existing knowledge in *Quantitative Finance* (QuantFi) and the discovery of financial engineering concepts unique to the nature of DeFi and blockchain.

Let's start at the beginning – agents who create the market.

2.1 Market participants

In the context of exchanges, market participants are classified into:

- *(market) takers* – are agents who wish to exchange assets. They take liquidity away from the market by exchanging one asset for the other. They need the market to be liquid in order to guarantee that they can both exchange the assets (immediately) and at the same time that the asset price is not significantly affected by the mere fact of the exchange.
- *(market) makers* – are agents who provide liquidity to the market. In *Traditional Finance* (TradFi), market makers profit from excellent market price predictions and providing liquidity at small profits (e.g., a cent on each share). When applied to as many market participants as they do, it guarantees them a significant over day profit. In DeFi, this role is often deferred to the algorithm that models the liquidity curve, automatically updates the price, and distributes market maker rewards to the liquidity providers.

As demonstrated above, both parties are fundamental for exchange operations to function. On the one hand, without market makers, market takers would often be forced to overpay for the assets and be limited to waiting for a party willing to take the opposite side of the trade. On the other hand, without market takers, market makers would not be able to generate a steady profit.

2.2 Liquidity

We have seen in 2.1 the crucial role that market makers play in the creation of liquidity, in this section we will explore what liquidity is, and some known ways of providing it.

Liquidity is the efficiency and ease with which an asset can be converted into another one without affecting its price. In TradFi, the most liquid asset of all is fiat (cash), and among them the most liquid is USD.

In traditional finance, liquidity is provided by large and sophisticated institutions, from investment banks such as Goldman Sachs and Credit Suisse to *High-Frequency Trading* (HFT) companies such as Citadel Securities, Jane Street, and Virtu Financial.

Those sophisticated algorithms and trading strategies[1] competing against each other lead to an extreme optimisation of the market making process. Strategies are devised by world-class mathematicians and analysed for predictive capabilities. As for speed, specialised hardware such as *Field-Programmable Gate Array* (FPGA) are programmed, hardware is co-located in the exchange, the cable from the box to match making engine is measured to be the same for each co-located participant, shortest possible paths to send signal between exchanges are constructed, and much more. As a result, traditional markets have liquidity provision optimized to the physical and computational limits.

In contrast, the DeFi scenario is quite the opposite. In TradFi all mathematical models, hardware, and software are optimized to perfection, whereas in DeFi basic and simple formulas and solutions are in use. This is purely due to how young and small (in comparison to TradFi) the cryptocurrency market is, and especially DeFi.

The formula for Liquidity Provision in TradFi has geometric distribution, very well defined higher moments, and is provided in very tight ranges. Contrarily, in DeFi most liquidity formulas (such as CFMM) believe that it is as likely to buy asset X for \$20, as it is for $\$1,000,000,000$ or \$0.000001. The inefficiency of the formulas utilized in DeFi are the source of impermanent loss, capital inefficiency, inefficient and slow price discovery, and loss to both market makers and market takers.

2.3 Efficient Market Hypothesis

Efficient Market Hypothesis (EMH) is a hypothesis stipulating that asset prices in the market reflect all available information, or in other words, that the market is

- completely rational;
- that all participants have perfect access to information;
- that everyone's beliefs can be reflected in the market due to the availability of financial instruments (e.g., shorts).

However, this is often not true [122, 128, 123, 124, 125]:

- there is high asymmetry in access to information, from expensive research and terminals to advanced analytical tools;
- there is limited access to reflect the market beliefs (e.g., shorting is only available for sophisticated investors);
- agents do not act only on the information available, but also on their own personal judgement, sentiment, fear, and many other emotions;
- not all agents are able to derive as efficient conclusion from the same data;

[1] A trading algorithm is a computer program that based on the data, such as price, order book, external signals, risk-profile, execution costs, etc., decide what is the optimal portfolio to hold at any given moment and rebalance to it. Trading strategy can be that algorithm or a rigorous model followed by a trader such as in systematic trading, but can be as well non-systematic and rely much heavier on the trader's personal experience and reading of the market. TradFi market makers rely on sophisticated and usually also very fast algorithms to facilitate market making.

- agents are easily deceived by poor sources of information and market manipulation;
- inefficient and irrational methods are used to predict price movements;
- investors are prone to take decisions hindered by different biases, e.g. loss aversion in the case of trader who booked just a series of loses, confirmation bias in the case of trader who just had a successful strike, overconfidence bias where trader believes stronger in their abilities than the market data and signals, etc.
- and many more.

Taking into the account behavioral aspects of investing, 3 forms of EMH are proposed: weak, semi-strong, and strong. In the case of weak form, the market price barely reflects fundamentals and existing information. The cryptocurrency market specifically is in the weak-form of EMH due to:

- small size when compared to the size of markets in TradFi where a single company, *Apple Inc*, has larger market capitalisation than that of all crypto (on October 15, 2021), which amplifies the effects in the market;
- pricing models are flawed and lead to slower convergence on the market price, for instance by the usage of CFMM[135];
- historical reasons, where early investors, called whales, accumulated disproportional amount of wealth in comparison to other market participants, leading to a small group of agents being able to significantly move the market;
- there is an evident lack of tools to reflect market sentiment, financial derivatives are limited, and *centralized exchanges* (CEXs) are ineffectively implemented, leading often to losses on non-losing shorts, etc.;
- cryptocurrencies are extremely volatile compared to other investments, this both means that usually cryptocurrency traders are prone to accept higher level of risks, but also that they are more exposed to the impacts of their own behavior on the trading, as all the effects and biases are magnified[38, 39];
- there is a large network effect at play, where financial advice is derived from the network effect, which is often exploited by malicious parties, who instead of focusing on building fundamentally-sound products, rather focus on creating network effects;
- lack of clarity from the government on the regulation of crypto, preventing wider adoption and causing investors to include other information than financial and performance when making their predictions;
- inefficient taxation on cryptocurrency assets, which leads to agents often making sub-optimal trades (e.g., sell a portion of good positions to secure fiat for future taxes, minimize the amount of trades due to the accounting requirements, etc.);
- cryptocurrency markets are open 24/7, meaning there is an inevitable necessity for active participants to exit the market or take sub-optimal positions in it, in order to be able to sleep and fulfill their physiological needs – this is not an inane matter, as active participation in the market requires sophisticated tools and is limited

by human capabilities (e.g., active crypto traders will often set up multiple alarm clocks during the night to check on the key risk metrics and their positions);

- and many more.

2.4 Automated Market Makers & Decentralized Exchanges

AMM is the underlying protocol powering all *Decentralized exchanges* (DEXs). AMM is the autonomous market making mechanism which eliminates the need for centralized exchanges, or large single parties taking the role of liquidity provider and creating all related infrastructure themselves. AMM pulls the liquidity from the network and replaces centralized market makers with code[134].

The unique property of a DEX is that nobody owns it per se, the protocol specifies how providing liquidity and trading work. The code will be open sourced.

A vast majority of DEXs rely on CFMM to define the liquidity curve. Those are formulas that specify how transactions are performed and how the price changes in response to transactions taking place[133, 2, 3, 4].

2.5 Constant-Function Market Makers

CFMM was the first class of AMM applied to real-world financial markets. All CFMM formulas have one distinguishing feature, that is they are all equal to a constant value, for instance:

- Uniswap's CFMM is $x \cdot y = \text{const}$ [5, 6]; more specifically (including slippage) Uniswap's formula is $(R_\alpha - \Delta_\alpha)(R_\beta + \gamma\Delta_\beta) = \text{const} = k$; Uniswap's formula is used by multitude of other DEXs such as PancakeSwap;

- Bancor's CFMM is an extension of Uniswap´s formula to any number of assets N all sharing the same pool [4], also called constant mean market maker, $\prod_{i=1}^{N} x_i = \text{const}$;

- Hybrid CFMMs, which are modified in such a way as to achieve the desired properties based on the characteristics of the assets being traded.

  $An^n \sum_i x_i + D = ADn^n \mid + \frac{D^{n+1}}{n^n \prod_i x_i}$, where x are the asset reserves, n is the number of assets, D is an invariant representing the value in the reserve, and A is the "amplification coefficient", which is tuneable constant.

  This produces an effect similar to leverage, and influences the range of asset price volatility[39] (the higher the asset volatility the higher A should be set)[132].

Figure 1: Constant product AMM formula (Uniswap's model).

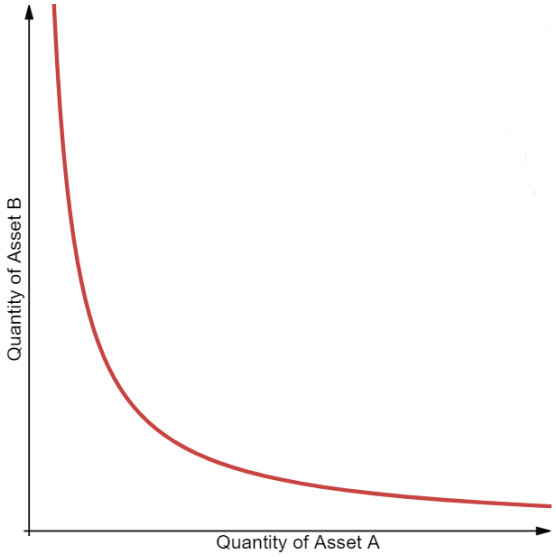


Figure 2: Constant mean AMM formula (Balancer's model).

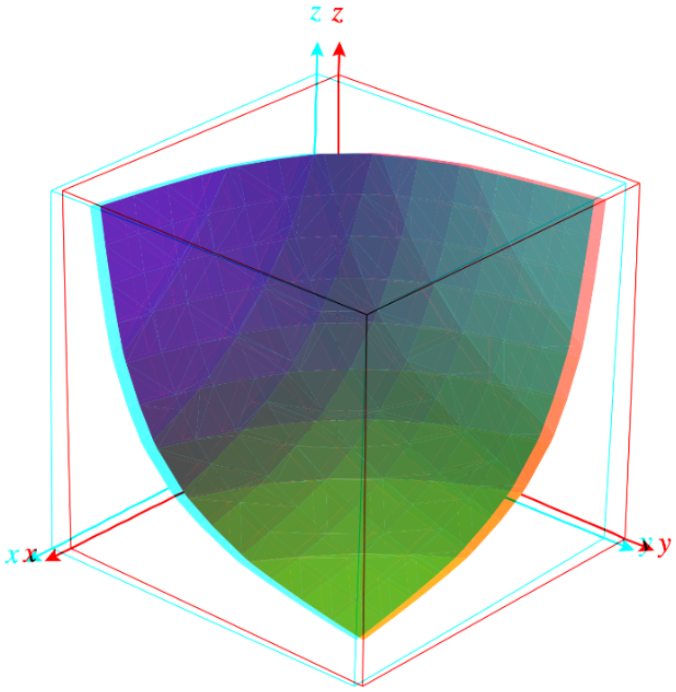
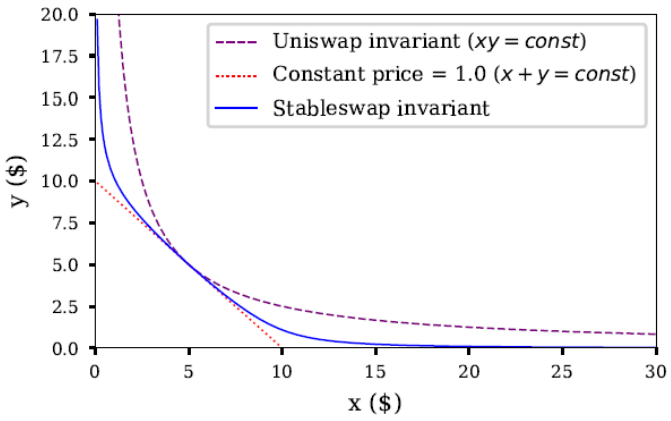


Figure 3: Hybrid CFMM of Curve's stableswap vs constant-product CFMM comparison.

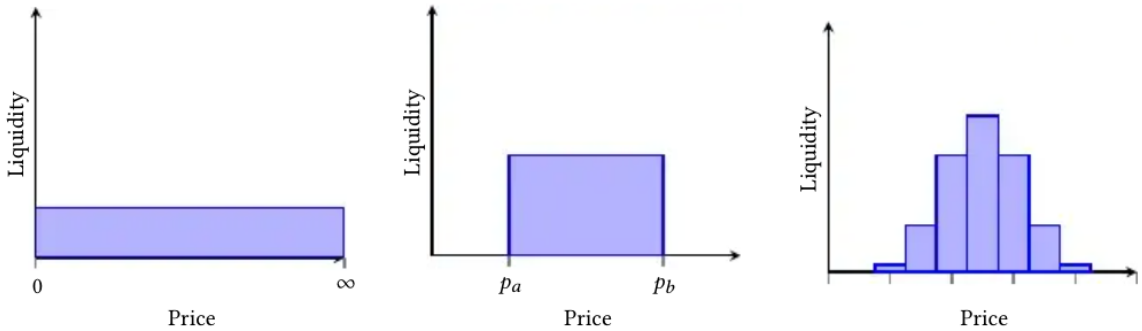


2.6 Concentrated Liquidity

In unconstrained liquidity, i.e., one provided in the full CFMM range of $(0, \infty)$ capital is highly inefficient, for instance in Uniswap the trading pair DAI / USDC assigns only 0.5% of the liquidity for the trading range between \$0.99 and \$1.01 through which majority of trading volume goes through. This basically means that 99.5% of the liquidity sits idle. Only about 0.5% of liquidity is enough to provide the same level of experience. What's more, that range of $[\$0.99, \$1.01]$ is where market makers earn the majority of their fees.

Concentrated liquidity attempts to resolve this issue by allowing market makers to specify the price ranges (indexes) between which they want to provide liquidity[7]. For instance, in the case of DAI / USDC pair, they could specify the range to be \$0.99 and \$1.01, hence concentrating the provided liquidity resulting in higher profit per unit of value locked. Furthermore, such fragmentation of the pool naturally leads to emerging properties such as geometric price distribution.

Figure 4: Convergence onto geometric price distribution of concentrated liquidity model.



(I) Uniswap v2 **(II)** A single position on $[p_a, p_b]$ **(III)** A collection of custom positions

Fragmentation leads to much more complex routing. In the case of Ethereum, where all code execution happens on-chain, with a global memory (and hence high transaction costs), this also has the inadvertent effect of increasing transaction prices. As the user has to specify the price range when creating a concentrated liquidity pool, for weakly correlated and non-correlated pairs the range will become obsolete quickly. This will

require the user to unstake their liquidity and resubmit it at the new range, spending even more gas (and hence taking away from the market making profits they generated).

In contrast to these problems on Ethereum, there is fertile ground for concentrated liquidity on Cardano. Due to the nature of the *Extended Unspent Transaction Output Model* (EUTxO) model, concentrated liquidity can be smoothly implemented in such a way that the off-chain code ensures the expensive computation can happen off-chain and only be validated by on-chain validators, resulting in no impact on transaction costs from complex routing.

That is exactly what axo achieves via its *programmable swaps*, defined in section 4, and goes one step beyond with sophisticated and dynamic liquidity pool modelling, called Algorithmic Automated Market Maker, as outlined in section 6.

2.7 Capital Efficiency ξ

Capital efficiency is a metric of how much capital is needed to generate the same level of revenue. It is easier to think of money M as stored energy that can be used to perform work, that work in turn is performed in expectation of generating revenue. Therefore, the less energy E that's required to perform the same work as W, the higher capital efficiency ξ the system has.

For instance, in subsection 2.6, we described an example of providing liquidity to DAI / USDC pair. As the used CFMM formula provides liquidity over the range of $(0, \infty)$, but 3σ of trading activity takes place within the $\$0.99, \$1.01$ range, it means that only around 0.5% of capital is used on useful work (providing liquidity in the active range), thus 99.5% is unused except for the $1-3\sigma$ case (less than 1% of all the cases). Hence, the capital efficiency of providing liquidity for the DAI / USDC pair using $x * y = k$ formula is $\xi \leq 0.5\%$. Imagine a car engine that only uses 0.5% to propel the car and loses 99.5% of fuel in unproductive energy, such as heating the engine.

This issue is prevalent across all CFMM AMM and makes *Total Value Locked* (TVL) unproductive. One of the main premises of the axo protocol design with *programmable swaps* and *Algorithmic Automated Market Making (AAMM)*, is to put capital to efficient use, the same way as TradFi market makers do.

2.8 Impermanent Loss

Impermanent loss is an integral part of all CFMM AMM and is rooted in the const $= k$ part of the equation, which entails that ratio of the assets in the pool changes with the asset price, and there is no mechanism to counter it. This means that for the majority of the trading pairs, besides special cases such as pools of all assets following the price of the same external asset (underlying) e.g., same currency stable coins, like DAI, BUSD, USDC, USDT, etc., the impermanent loss is guaranteed.

We cover impermanent loss in great detail in subsection 6.1. However, here we will just outline what causes it and what effect it has on the capital locked into an AMM protocol.

Why are we so concerned with impermanent loss? Market makers earn money by providing liquidity, usually they earn a portion of the protocol fee, equivalent to $0.1 - 0.2\%$ of the exchanged assets. This provides compensation for providing liquidity. However,

users always have the alternative of keeping their assets in their wallets instead of locking them in a liquidity pool. Now, as the asset ratios in the pools change, impermanent loss starts to occur, as summarized in Figure 5.

Figure 5: Percentage Divergence Impermanent Loss (Duplicate of Figure 17 for Easier Reading).

Percentage Divergence Loss									
Price ratio	ADA multiple	0.10	0.50	1.00	1.50	2.00	4.00	10.00	25.00
X multiple	Price	$0.20	$1.00	$2.00	$3.00	$4.00	$8.00	$20.00	$50.00
0.10	$100.00	0.0%	-25.5%	-42.5%	-51.6%	-57.4%	-69.1%	-80.2%	-87.4%
0.20	$200.00	-5.7%	-9.6%	-25.5%	-35.6%	-42.5%	-57.4%	-72.3%	-82.3%
0.50	$500.00	-25.5%	0.0%	-5.7%	-13.4%	-20.0%	-37.1%	-57.4%	-72.3%
0.80	$800.00	-37.1%	-2.7%	-0.6%	-4.7%	-9.6%	-25.5%	-47.6%	-65.3%
1.00	$1,000.00	-42.5%	-5.7%	0.0%	-2.0%	-5.7%	-20.0%	-42.5%	-61.5%
1.10	$1,100.00	-44.7%	-7.3%	-0.1%	-1.2%	-4.3%	-17.7%	-40.2%	-59.8%
1.25	$1,250.00	-47.6%	-9.6%	-0.6%	-0.4%	-2.7%	-14.8%	-37.1%	-57.4%
1.50	$1,500.00	-51.6%	-13.4%	-2.0%	0.0%	-1.0%	-10.9%	-32.6%	-53.8%
2.00	$2,000.00	-57.4%	-20.0%	-5.7%	-1.0%	0.0%	-5.7%	-25.5%	-47.6%
4.00	$4,000.00	-69.1%	-37.1%	-20.0%	-10.9%	-5.7%	0.0%	-9.6%	-31.0%
10.00	$10,000.00	-80.2%	-57.4%	-42.5%	-32.6%	-25.5%	-9.6%	0.0%	-9.6%
15.00	$15,000.00	-83.8%	-64.7%	-51.6%	-42.5%	-35.6%	-18.5%	-2.0%	-3.2%
20.00	$20,000.00	-85.9%	-69.1%	-57.4%	-49.0%	-42.5%	-25.5%	-5.7%	-0.6%
25.00	$25,000.00	-87.4%	-72.3%	-61.5%	-53.8%	-47.6%	-31.0%	-9.6%	0.0%

The main challenge is the exponential nature of impermanent loss. For small asset ratio variations, the loss is negligible, but for large shifts it easily eradicates all the profits from providing liquidity and from governance tokens earned from yield farming.

axo aims to eliminate impermanent loss completely (property derived from the protocol design), and where the user desires to provide liquidity via a specific model (even including CFMM), it provides means to statistically eliminate it as well via asset ratio management, arbitrage, and dynamic risk compensation, all outlined in subsection 6.1.

2.9 Risk Control

Risk is inseparable from any investment, but risk control is not part of any existing AMM architecture. Risk control activities include:

- portfolio allocation that achieves the optimal expected return given fixed maximum accepted level of risk σ such as done in Markowitz's Modern Portfolio Theory (MPT)[27, 26];
- providing tools and data to the user when engaging in the market, e.g., creating liquidity pool, helping to achieve a much better outcome;
- actively calculating and monitoring risk metrics such as VaR (Value at Risk), volatility, Sharpe ratio, etc.[40, 41, 43];
- dynamically hedging the risk, e.g., buying inversely correlated assets to offset the investment risk, and updating this hedge dynamically to maintain the risk level below desired levels;

- providing risk-taker compensation, hence helping investors (e.g. market makers), to maintain risk neutral positions;
- integrate fuses and other market stress scenario control mechanisms, including offsetting sudden crashes to other parts of the network (e.g. when a rug-pull is identified, performing swaps on all other DEXs to convert and remove the risky asset from the portfolio[27]);
- provide verification of policy ids, but also trust scores, and ability to whistleblow.

We delve deeper into how the axo platform enables management of risk in section 14.

2.10 Cardano Blockchain & EUTxO Model

Cardano offers 3 major innovations, making many of the ambitious goals outlined in this paper achievable, which were previously impossible on global-shared state blockchains:

- Smart contracts are composed of on-chain validators and off-chain code; on-chain validators provide the same level of assurance as any other blockchain model, but at the same time Turing-complete off-chain code, enables performing complex and resource-consuming computation without any impact on transaction cost; this is revolutionary, as ideas such as *programmable swaps* and *algorithmic automated market maker (AAMM)* would not be possible to implement without it. What's more, on-chain validators provide full scope of smart contract security, meaning that despite the off-chain code, the entire protocol is equivalent to being fully executed on-chain as all security is achieved on-chain.
- EUTxO fragmentation and redeemer model, which provides a unique method to enable many concurrent independent actions to take place in parallel across multiple protocols; for instance, given this fragmentation and desire to arbitrage with other DEXs, this can be done simply thanks to the EUTxO model and how redeemers work.
- Hydra head – fast and isomorphic state channels allowing for straightforward usage of the same transaction settlement code in the local hydra head formation. This enables a significant performance improvement without incurring layer 2 software engineering cost.

2.11 What's Next

After having inspected the current state of AMMs and having outlined existing challenges, in the following sections we discuss the axo protocol implementation objectives that aim to address the aforementioned challenges.

3 axo Protocol Mission & Objectives

axo aims to revolutionize the world of finance by:

- providing the tools that allow everyone to create sound and efficient ways of investing;
- increasing the efficiency of the cryptocurrency market and accelerating the transition from TradFi to DeFi;
- building the foundations of the financial markets of the future.

3.1 Providing the Building Blocks of Sound and Efficient Ways of Investing to Everyone

axo will be a sound platform for developing investments with high capital efficiency and without impermanent loss. Additionally, Decisions and observations will be supported by data, market indicators and by providing a DeFi education platform.

We aim to develop a pathway for people to improve their investing skills, as well as providing tools and infrastructure for the creation of revenue such as market making, crypto indexes, synthetics, automated portfolio management strategies, and more.

3.2 Increase Market Efficiency

The axo platform improves market efficiency by allowing users to create a range of products, allowing for the expression of specific market participant sentiments, from swaps to option strategies and sophisticated automated trading strategies.

Markets that cannot be shorted are inadvertently inefficient [22, 18, 19]. This is a simple consequence of the fact that a person who believes that asset X is undervalued can buy it and hold it until the price discovery catches on, while the person convinced that the asset is overpriced cannot take a separate position (short). The person who believes asset X to be overpriced cannot simply sell it, as it only protects them from the downside risk, but does not provide a way to capitalize on their knowledge of the asset overvaluation. This results in very little incentive for discovering overpriced assets, but there's one for undervalued ones. If you can only add water to a jug, but never take away, the amount of water will inadvertently only increase. It can be even stipulated that a lot of volatility in the crypto market takes origin in this mechanic. Due to a lack of sufficient access to short instruments, the price tends to go up until it suddenly reverts to the mean, like stretching a rubber band to its limits[39].

Developing a sound system composed of all types of financial instruments, most importantly negatively correlated ones, will lead to increased market efficiency and drive it closer towards the equilibrium.

3.3 Build the Foundations for the Future Financial Markets

Last, but not least, having a trading platform with a wide range of tradeable crypto assets, indexes, derivatives, and mirrored assets, enable the development of more specialized financial platforms on top of this infrastructure layer. One example of such a layer would be the creation of a distributed hedge fund, allowing users to stake investments in automatic trading strategies and bots, providing exposure to a wide range of additional source of alpha (additional revenue compared to an index without taking additional risk).

We start our discussion of novel proposed ideas with *programmable swaps* – a combination of off-chain and on-chain code capable of performing many functionalities, from market and limit orders to executing sophisticated automated trading strategies.

4 Programmable Swaps

In this section, we introduce the concept of *programmable swaps*, swaps composed of:

- *type* - order type;
- *triggers* - specifying conditions upon which the swap is active to be executed;
- *actions* - payload definition of what action a *programmable swap* performs upon activation;
- *assets* - assets required to perform actions outlined above.

Programmable swaps provide an elegant and automated way for the execution of many order types, just to give a few examples:

- *market order* (a.k.a. *swap*) – an order that is executed immediately, exchanging one asset for another, e.g., $2 for 1 ADA; this *programmable swap* has *no triggers* hence it is always active; it has one action, exchange one asset for the other at the best immediately available market rate, and locks assets specified for the exchange.
- limit order – an order that executed at specified price or better; limit order can be executed partially; this *programmable swap* has 1 trigger - the best available price is specified by *least upper bound (LUB)* for sell orders (the lowest price at which a trader is willing to sell the asset) and *greatest lower bound (GLB)* for buy orders, the maximum price for which a buyer is willing to buy a specific asset; this *programmable swap* is composed of order type *limit-order*, LUB/GLB (for sell, buy respectively), and assets to swap;
- *weighted DCA (dollar-cost average)* is a trading strategy that exchanges at defined intervals, one asset for the other, adjusting the daily portion of exchanged assets (weight) for given market conditions (e.g., when the price rises buy less and when the price drops buy more); this *programmable swap* is composed of a time trigger defining all time indexes after which the DCA operation should be performed (e.g., daily interval). *Action*s are composed of market indicator Oracles (e.g., divergence and momentum indicators indicating local price minima and maxima), and DCA parameters (periods, the response to indicators, etc.); finally it contains USD or other assets, which we cost average into the other asset (e.g., ADA).
- engage arbitrage bots that exploit pricing inefficiencies of models used by other exchanges, to both increase the profits of arbitrage bot funders, increase the overall market efficiency and to ensure that the **axo** platform reflects the true market price, regardless of TVL (Total Value Locked);
- *dynamic liquidity provision* - is risk-controlled market making where in stable conditions and price ranges (medium price and volatility) assets are provided bidirectionally (buying and selling at the same time, i.e., taking both positions in the market around the current price and in the given spread around it), providing liquidity to the market and earning the market maker fees. What is unique about this approach is that as soon as the price of one asset (e.g., ADA) starts to quickly

rise, the *programmable swap* is converted into ADA (the asset that investor prefers to hold) and the swap is terminated. This allows the market maker the ability to earn rewards from market making, but prevents being locked out of the preferred asset as its relative price to USD starts to rise. This *programmable swap* is composed of a trigger that defines the safe trading range, once it is crossed, the programmable swap isn't executed anymore, *actions* – provide liquidity according to efficient market formula, all assets being exchanged;

- *portfolio management strategy* – a complex trading strategy defining system for performing trades, taking the market data as input and outputting the actions to rebalance the portfolio[27, 26]. This type of strategy usually employed by sophisticated traders. It allows for the implementation of systematic investment strategies. Such strategies are commonly employed by traditional market makers and hedge funds. This type of *programmable swap* is composed of triggers representing *fuses*, actions consuming a wide array of Oracle data, describing all inputs necessary for the strategy to design portfolio rebalancing decisions, the strategy definition transforming Oracle data into new portfolio balance, initial assets (e.g., ADA) to seed the trade, and a current portfolio allocation thereafter. It is worth mentioning that this type of programmable swap allows for the implementation of hedge funds on-chain by creating a market for *portfolio managers (PMs)* to develop trading strategies, and for investors to provide funds via locking them into trading strategy vaults, and paying a commission to PMs from the generated profits; this creates a unique opportunity for everyone having access to services of seasoned PMs and for users to have access to the best performing strategies in the market.

- dynamically hedge your position using derivatives/underlying/etc..

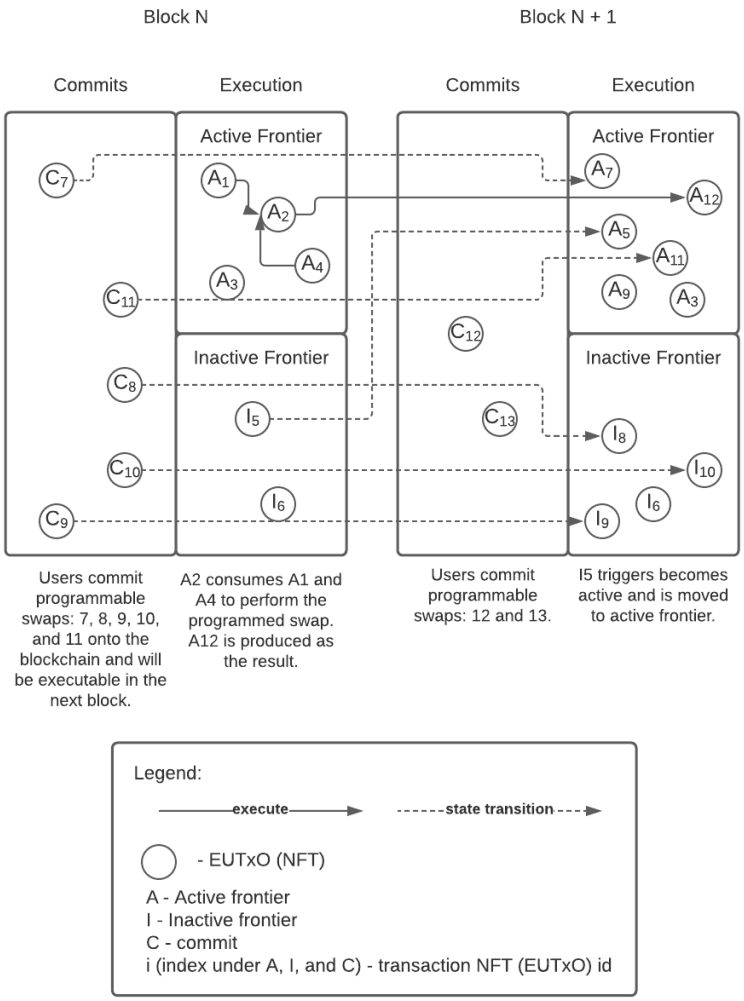
4.1 Architecture

The axo programmable swap protocol is composed of 2 parts:

- *the commit phase* – send commitment onto the blockchain to perform a certain action; each commitment can be cancelled by sending a cancel order as another programmable swap; each commitment is an NFT and can be produced in parallel using a minting policy;

- *the execution phase* – all commitments are executed against each other each block, resulting in trades happening; due to high fragmentation and optimized routing, transactions take much less memory and can be efficiently managed.

Figure 6: axo programmable swap protocol execution stages.



4.2 Commit Phase

All *programmable swaps* are submitted onto the blockchain by minting NFTs representing the programmable swap and all internal information. *Minting* is an action that is perfectly parallelizable (see *parallelism) – NFTs are picked from the user´s wallet to mint commitment and as many NFTs as the memory pool allows. These can be minted in parallel each block cycle.

Now, all commitments represent intents to perform certain actions given specific market conditions (triggers). All commitments are separated into 2 types: - *active frontier* – *programmable swaps* with all triggers active, hence executable this block cycle; - *inactive frontier* – *programmable swaps* with at least one trigger not-active, hence not executable this block cycle.

As axo *programmable swap protocol* uses hydra heads to scale the number of transactions, it is worth describing the consequences of this beautifully simple, fragmented design. All EUTxOs present in *active frontier* can be moved to the hydra head for execution and once

executed, back to layer 1 to settle the trades on the base layer. As each *programmable swap* is the smallest possible intent, it presents the most optimal exchange of information between layers.

What's more, this design means that even when executed on layer 1, much less memory needs to go into all trades. The minimum possible amount of information is expanded in the execution of *programmable swaps*, hence the memory used and cost is minimal as well. Traditional AMM models, with a single EUTxO representing the entire liquidity for a given pair, need to be included in all transactions, leading to large transaction sizes, and hence larger costs and lower total throughput (or TPS - transactions per second).

4.3 Execution Phase

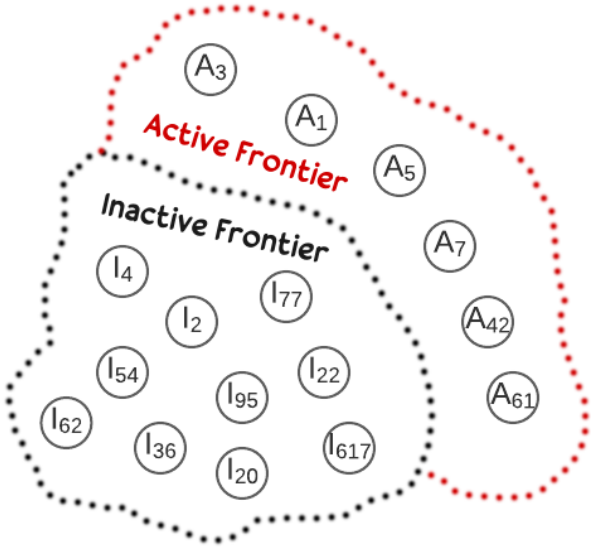
After *commits* are submitted onto the blockchain in the form of *Non-Fungible Tokens* (NFTs), they enter the execution pool. The execution pool is composed of 2 disjoint groups:

- active frontier $\mathbb{A}$ - the set of all *programmable swaps* schedulable in the current block, defined as $\mathbb{A}$ - the set of all *programmable swaps* of which all triggers are all active, defined as $\mathbb{A}(b) := \{s \in S \mid \|\text{active\_triggers}(s,b)\| = \|\text{triggers}(s,b)\|\} = \{s \in S \mid \|\text{inactive\_triggers}(s,b)\| = 0\}$;
- inactive frontier $\mathbb{I}$ - the set of all *programmable swaps* of which at least one trigger is inactive, defined as $\mathbb{I}(b) := \{s \in S \mid \|\text{active\_triggers}(s,b)\| < \|\text{triggers}(s,b)\|\} = \{s \in S \mid \|\text{inactive\_triggers}(s,b)\| > 0\}$

where

- b - block id;
- s - programmable swap;
- $\mathbb{S} := \mathbb{A} \cup \mathbb{I}$ - set of all committed programmable swaps;
- active_triggers(s,b), inactive_triggers(s,b), triggers(s,b) - functions that return correspondingly all active, inactive, and just all the triggers for the given swap s during the block b.

Figure 7: Active and inactive frontiers.



The Cardano blockchain architecture specifies the smart contract architecture of:

- on-chain validators – scripts validating that the submitted transaction, with specified input and output EUTxOs, can be executed; this part is executed on-chain by block producing nodes;
- off-chain code – *Decentralized Application* (dApp)'s code, responsible for all platform functionality and most importantly, preparation of the transaction to be submitted onto the blockchain, to be validated and executed by validators, and confirming the desired state transition.

Cardano's blockchain design makes it very straightforward to implement complex off-chain logic, in the case of **axo** it is this *order matching engine* responsible for executing all *programmable swaps* according to their specification and the on-chain state.

Such off-chain component requires:

- *Plutus Application Backend* (PAB) (or its equivalent) to interact with Cardano nodes and a smart contract enabled wallet via *dApp connectors*;
- smart contract enabled wallet (Cardano wallet capable of storing dApp endpoints and interacting in the smart contract execution);
- Cardano node to monitor and query the blockchain.

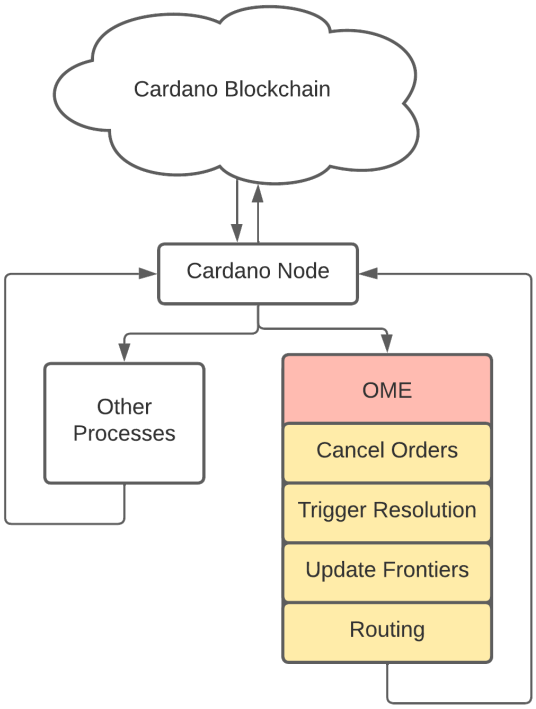
From the point of view of **axo** protocol implementation, this architecture is highly beneficial, as it allows for development of an advanced *order matching engine*, as outlined in the below section, subsection 4.4, and expanded in full detail in section 5.

4.4 axo Execution Pipeline

axo execution engine takes a look at the latest snapshot of the blockchain *layer 1* and then in order:

- processes *cancel order* requests and cancels all non-EOL (end of life) *programmable swaps*;
- partitions the set of all *programmable swaps* $\mathbb{S}$ into the active frontier $\mathbb{A}$ and inactive frontier $\mathbb{I}$;

Figure 8: axo protocol (off-chain order matching engine) execution pipeline.



4.5 Scalability

The process of minting NFTs can be done completely in parallel (see *parallelism). Hence, it is possible to create a programmable swap, and interact with the axo protocol, with minimal risk of delays and requirement for sequencing. NFT minting is parallelizable. Once minted, NFTs storing the programmable swap code and assets required to transact are ready to interact with the market. Hence, the commitment phase achieves the highest level of concurrency possible (full parallelism).

On the other hand, in the execution phase, multiple EUTxOs can be matched against many other EUTxOs, meaning that we need to implement an efficient routing mechanism. This is explained in detail in section 5. Due to optimal EUTxO fragmentation and graph-based execution scheduling, it results in the most scalable routing mechanism possible (limit of which is defined by Amdahl's law).

The proposed scaling design is not only an elegant solution to the *concurrency challenge*, stemming from the lack of global memory (distributed state) and the ability to spend only once each EUTxO per block, but also one resulting in a much smaller memory footprint as only the information required for the execution of the order goes into the transaction. This is the opposite of the popular *Uniswap*-style designs, which in the context of the

EUTxO model, leads to including all available information for the given liquidity pool into a transaction (which is the least memory-efficient solution possible).

4.6 Memory Requirements

The Cardano protocol requires a payment of $a \cdot \text{size}(\text{tx}) + b$ where a is proportionality constant representing the cost of a unit of storage and b is a minimum payable fee (introduced with the primary goal of preventing *Distributed Denial of Service (Attack)* (DDoS) attacks)[129]. Therefore, it is important and beneficial to all axo protocol participants for all transactions sizes to be minimal.

In centralized liquidity models (the ones relying on single EUTxOs), the total amount of memory required for the transaction is high. All of that centralized information is included in every transaction that interacts with the EUTxO that stores the liquidity pool information.

In contrast, the axo protocol, does quite the opposite. Instead of including all existing information as centralized EUTxO liquidity models do, only the bare minimum required information is included. The axo protocol is composed of highly fragmented programmable swaps and as those are matched with each other, only the information required to perform the action is stored in all. The consequence of this is much smaller transaction size requirements.

4.7 EOL of Programmable Swaps

Once all tasks outlined in the programmable swaps are done, it reaches its *EOL* – end of life. This means that the programmable swap can be destroyed and is no longer needed. There are two conditions for termination of programmable swaps: *cancel order* (order to cancel existing programmable swap) and *end of life (EOL)* (when the programmable swap has completed its task).

When this happens, a final transaction is performed where:

- all assets in the programmable swap are returned to the wallet from which they originated;
- a receipt NFT is minted and sent alongside.

4.7.1 NFT Receipt

NFT receipt is an NFT containing the information about how the trade was executed and might contain a graphical visualisation of the performed tasks, for instance:

- market orders (swaps) and limit orders will just include information about the execution price and time;
- *Dollar-Cost Averaging* (DCA) would contain a record of all buy orders, assuming DCA is executed daily over a period of 30 days, that would contain 30 records similar to market order / limit order outlined above;

- liquidity pool fragment minting using one of the available formulas and parametrisation (stochastic models) will contain the pictorial representation of the model (distribution, its moments, and sensitivity to market dynamics), etc.

NFT receipts will fulfill 2 important roles:

- *book-keeping* – providing information to the user about how the orders were executed;
- Profit & Loss *(P&L) tracking* – tracking performance of the executed strategies;
- *collectibles* – best trades (achievements), first trade to exchange some newly listed asset, etc.

4.8 Theoretical Model Performance Characteristics

The proposed, commit-phase solution maximises concurrency and provides means to achieve high throughput. This is parallelization, commit-phase submissions are performed in parallel, subsection 4.2, and the optimal fragmentation of EUTxO information in the execution phase, subsection 4.3.

The proposed solution allows for full parallelism during minting commit-phase NFTs of programmable swaps. This in the result achieves the highest score using Amdahl's law metric. This further leads to improved ability to parallelize transations and reduce *memory footprint* on both layer 1 and 2. The burden of work is off-loaded to order matchmaking engine, which by doing so, is able to implement *Domain-Specific Language* (DSL) for *programmable swaps*, and provide a novel utility to the universe of DEXs.

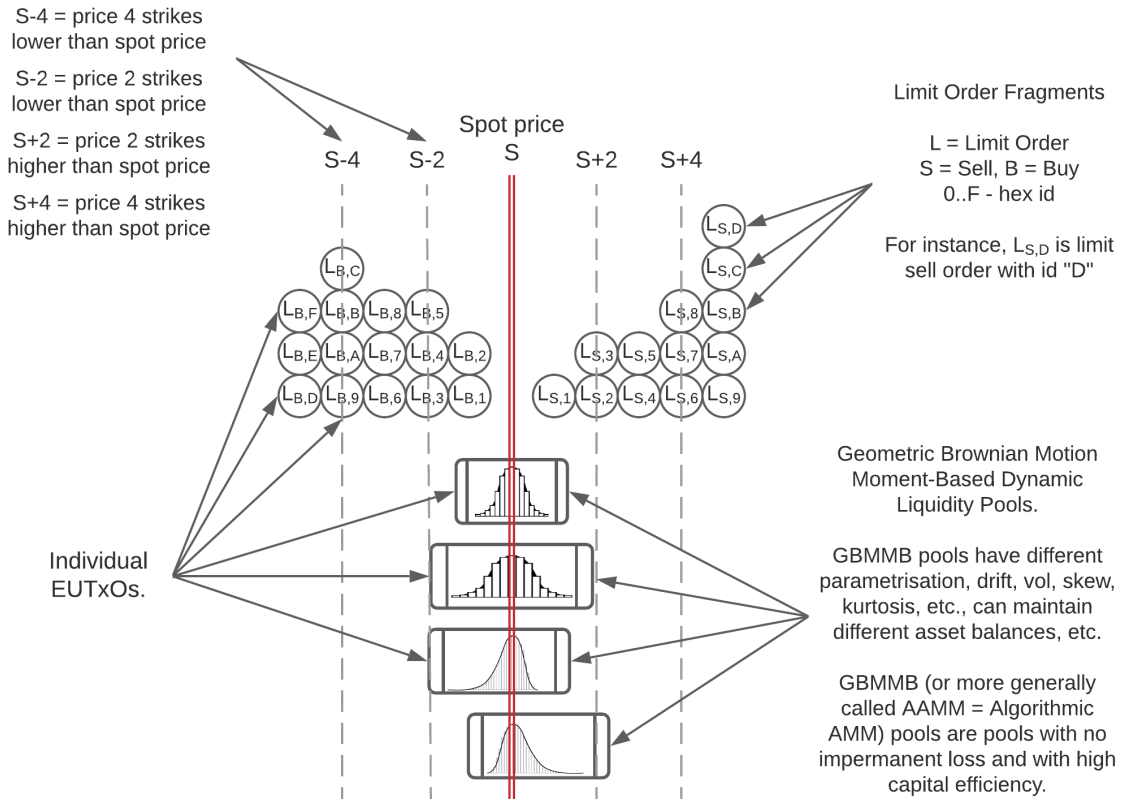
4.9 Fragments Matching

The automated and algorithmic execution offered by *programmable swaps* is fully executed on-chain. There are no links to external APIs, there is no external software that has access to the contracts, there is no critical component stored *off-chain*. It is worth noting that in Cardano's on-chain validator and off-chain code programming model, while the off-chain component is responsible for selecting EUTxOs for the transaction, the actual execution still happens on-chain. This means that the model offered by the **axo** protocol is not only self-contained, but more importantly, it is trustless and implemented using smart contracts.

In this section, we explore further how the fragments are matched against each other and how fairness and security are achieved.

We are going to explore fragmented liquidity pools, without explanation of what *Algorithmic Automated Market Making (AAMM)* is or how it works, which we will explain in detail in section 6. Here, we use the same model as in section 6, namely the fragmented liquidity model, but focus on the execution, trustlessness, and safety.

Figure 9: Fragmented (virtual) liquidity pool's initial state $\mathbb{S}_0$.



We start with fragmented liquidity pool[2] initial state $\mathbb{S}_0$.

Each bubble above is a separate EUTxO, as defined by an NFT minted in the *commit phase*. In the example below we used limit orders (circles) and *AAMM* fragments (AMM liquidity pools automatically and algorithmically adjusting to the market conditions).

We'll discuss 3 execution examples:

- market order matched by limit order;
- market order matched by *AAMM* liquidity pool;
- limit order matched by limit order on the opposite side of the order book.

4.9.1 Market Order Matched by Limit Order

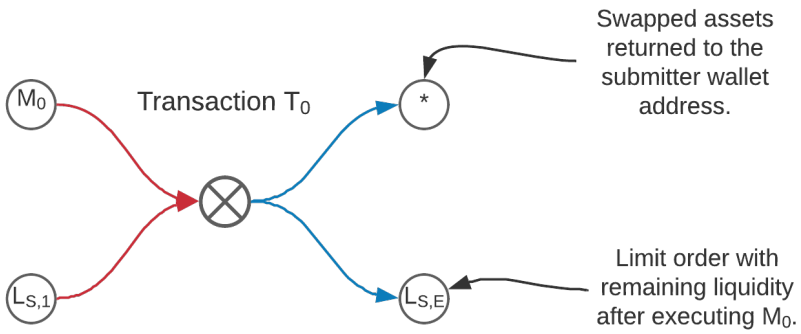
Let's assume market order M_0 being committed in the previous block $\mathbb{B}_{-1}$.The Market order is executed as long as there is liquidity, at the best available price. In this example, let's assume that the best available price is provided by limit order $L_{S,1}$ and that the amount of assets being sold by $L_{S,1}$ is sufficient to cover the entire M_0 (if it wouldn't simply the next best available limit order or *AAMM* would be used, whichever provides the best price).

[2]Fragmented liquidity pool can also be called virtual due to the fact that it is not a pool, but multiple fragments (separate EUTxOs) from which properties a liquidity pool naturally emerges (by liquidity pool we mean here pooled resources that give the impression of the market being liquid.

Now, a transaction T_0 is submitted that uses both M_0 and $L_{S,1}$ as input EUTxOs and creates as output:

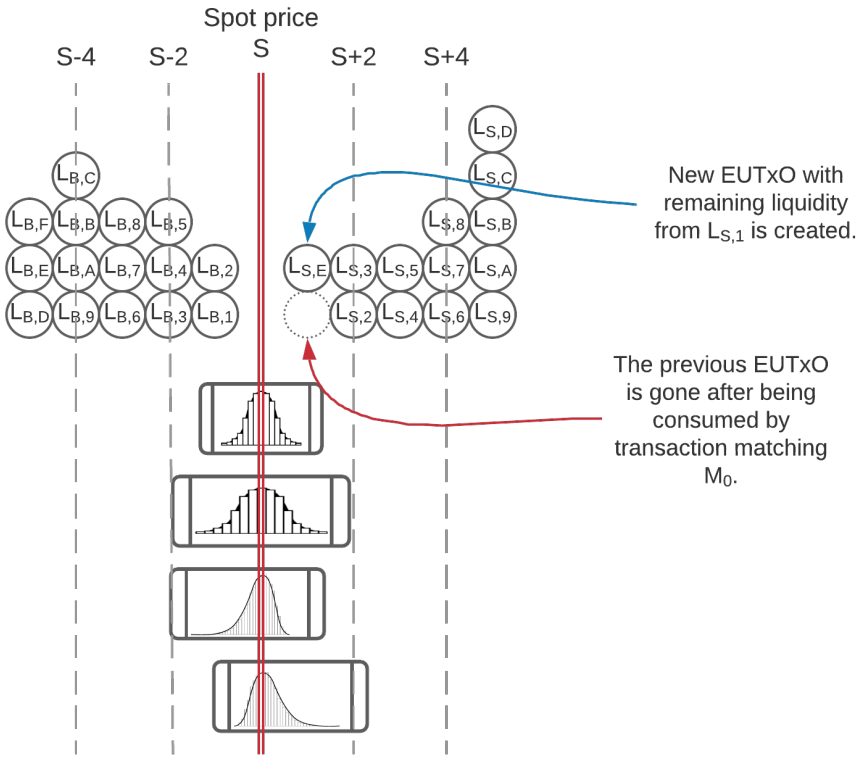
- EUTxO with swapped assets, spendable by the agent that submitted M_0 (hence swapped assets are directly sent to that user´s wallet);
- a new EUTxO with remaining assets from $L_{S,1}$ after executing M_0.

Figure 10: Transaction executing M_0 using $L_{S,1}$.



After executing T_0 the state of the fragmented liquidity pool is as below:

Figure 11: State of the fragmented liquidity pool after executing T_0.



As we can see $L_{S,1}$ and M_0 are spent, $L_{S,E}$ with remaining liquidity is created and * the result of market order (swap) is returned to the wallet of the M_0 submitter[3]

The presented approach has multiple benefits:

- thanks to *commit phase* the transaction M_0 is submitted without any delays and bereft of concurrency issues immediately onto the ledger;
- off-chain components match $L_{S,1}$ with M_0, which provides the best execution price;
- the transaction created by off-chain match making engine has minimum possible size, only EUTxO with the market order (swap) is consumed and only single EUTxO providing liquidity. In contrast to entire liquidity pools stored in a single EUTxO (the biggest possible footprint of transaction memory per transaction) it offers the highest possible optimisation. In a sense, this is not much different from a regular transaction on the Cardano blockchain, which automatically allows high scalability of axo on layer 1; this cost memory size minimisation means that market taker pays the smallest possible transaction fee for having their transaction executed;
- limit order is free of impermanent loss and represents the price the user wants to get for the exchanged assets, plus provides market maker fees to the limit order owner;
- *programmable swaps* allow for additional parameters to be specified in a limit order, e.g., to be executed at $S + 1$ price, as opposed to fixed price, this price is moving with the market price, offering constant market making opportunities until resource exhaustion.

From the security point of view:

- sell limit order $L_{S,1}$ is only spendable at the preset price of $S + 1$ in this example, hence there is no other way to redeem this EUTxO than at this price;
- market order M_0 is guaranteed to be executed at the best market price by the transaction input of the transaction at the current market price plus/minus accepted volatility: $S \mp \sigma$.

4.9.2 Market Order Matched by *AAMM*-LP

Let's assume market order M_1 being committed in the previous block $\mathbb{B}_{-1}$. Market order is executed as long as there is any liquidity, at the best available price, same as in the previous example, subsubsection 4.9.1, however now the best available price is provided by *Algorithmic Automated Market Maker (AAMM)* A_3.

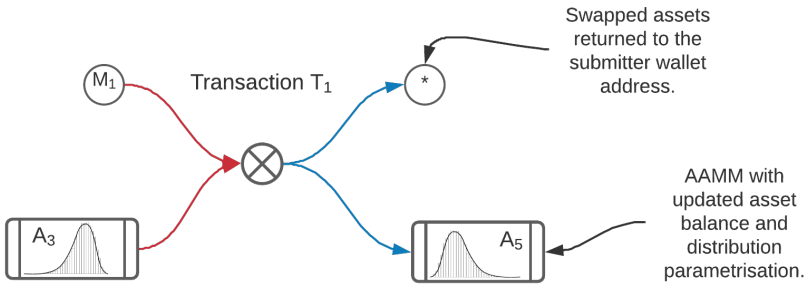
Now, a transaction T_1 is submitted that uses both M_1 and A_3 as input EUTxOs and creates as output:

- EUTxO with swapped assets, spendable by the agent that submitted M_1 (hence swapped assets are directly sent to that user´s wallet);

[3]The assets are not sent per se, simply the output is only spendable by the creator of M_0 wallet address, which is the EUTxO-native way of returning assets.

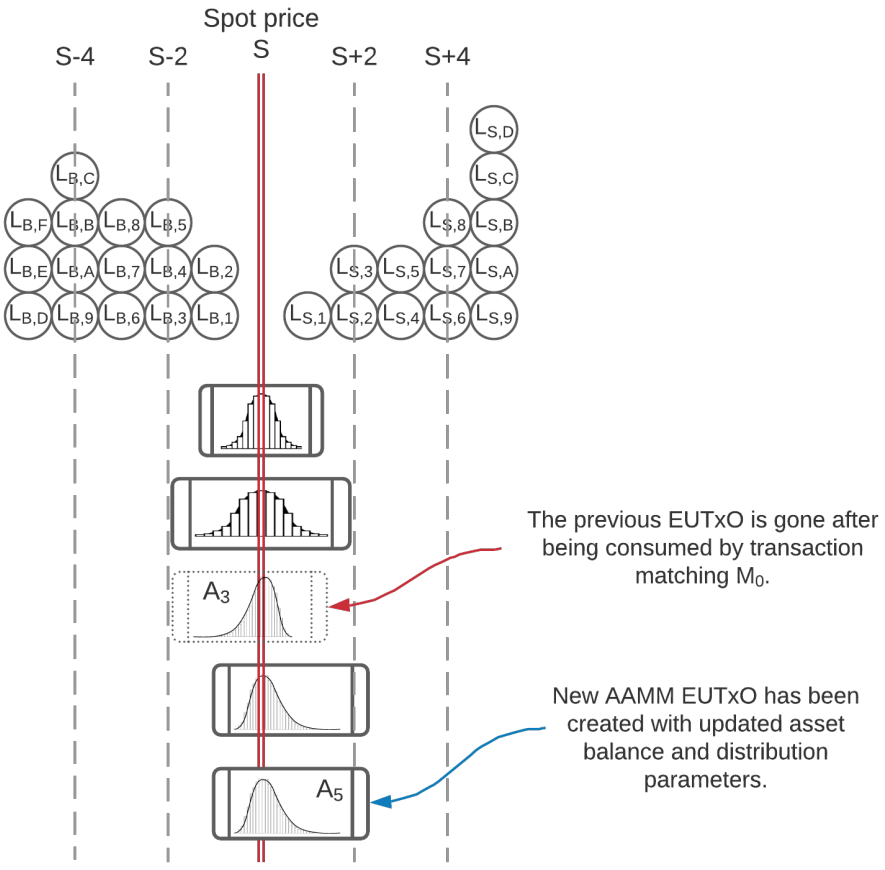
- a new EUTxO with updated assets and distribution A_5.

Figure 12: Transaction executing M_1 using A_3.



After executing T_1, the state of the fragmented liquidity pool is as below:

Figure 13: State of the fragmented liquidity pool after executing T_1.



We can see that A_3 and M_1 are spent, A_5 with updated asset balance and distribution model has been created and $*$ the result of market order (swap) is returned to the wallet of the M_1 submitter.

The presented approach has multiple benefits:

- thanks to *commit phase*, the transaction M_1 is submitted without any delays and no concurrency issues, immediately onto the ledger (this is the same as for the previous example, and is an invariant that holds regardless of the transaction type);
- off-chain components match A_3 with M_1 which provides the best execution price;
- the transaction created by the off-chain match making engine has the minimum possible size, only the EUTxO with the market order (swap) is consumed and with only a single EUTxO providing liquidity. In contrast to entire liquidity pools stored in a single EUTxO (the biggest possible footprint of transaction memory per transaction), it offers the highest possible optimisation, this is the same as a regular transaction on the Cardano blockchain. which allows high scalability of the axo Protocol on layer 1; this cost memory size minimisation means that the market taker pays the smallest possible transaction fee for having their transaction executed;
- *Algorithmic Automated Market Maker (AAMM)* is a unique model that collapses the provided range to the true geometric price distribution of the asset, hence is free of impermanent loss and represents the price that the user wants to get for the exchanged assets, plus provides market maker fees to the *AAMM* liquidity fragment owner[4];
- *programmable swaps* and liquidity pool moment-based distribution allows for smooth adjusting based on market conditions and the pool composition, providing continuous liquidity at the true market price plus minus volatility $S \mp \sigma$, for all requests coming at the prices close enough to the true market price, or better.

From the security point of view:

- stochastic liquidity pool (AAMM) A_3 provides liquidity at the present geometric distribution around mean S and within the volatility σ, further precised by the higher moments of the distribution (skew, kurtosis, etc.), hence there is no other way to redeem this EUTxO than at the fair and efficient market price plus/minus market volatility σ;
- market order M_1 is executed at the best market price by the transaction input of the transaction at the current market price plus/minus accepted volatility: $S \mp \sigma$.

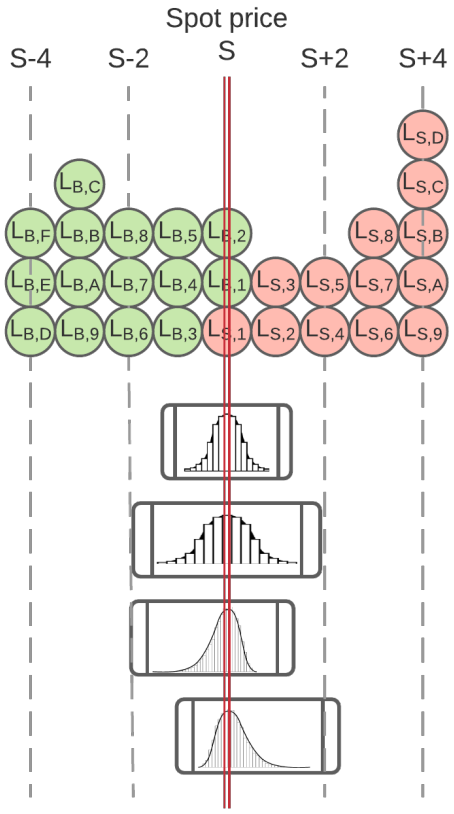
4.9.3 Limit Order Matched by the Order Book

The final example deals with limit orders matching each other, this happens when the order book sides cross over (that is if there is a buy order with the price equal or greater than the cheapest sell order), i.e.

$$\exists_{b \in \mathbb{I}_b, s \in \mathbb{I}_s} L_b.\text{price} \geq L_s.\text{price}$$

[4]As identified by the wallet which minted the liquidity fragment.

Figure 14: Order book crossover.

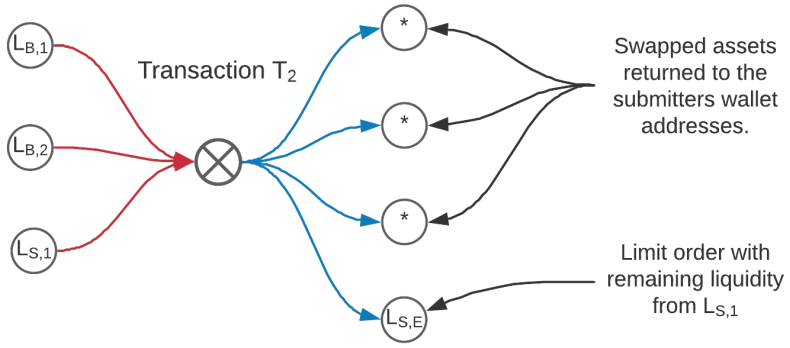


In the figure provided, the following 3 limit orders cross over: $L_{B,1}$.price = $L_{B,2}$.price = $L_{S,1}$.price. That means they should execute immediately among each other. They provide liquidity to each other, and in this case the total volume of $L_{S,1}$.volume > $L_{B,1}$.volume + $L_{B,2}$.volume meaning that both $L_{B,1}$ and $L_{B,2}$ will be executed completely and the remaining liquidity of $L_{S,1}$ will return as a fragment to the virtual liquidity pool.

Now, a transaction T_2 is submitted that uses $L_{B,1}$, $L_{B,2}$, and $L_{S,1}$ as input EUTxOs and creates as output:

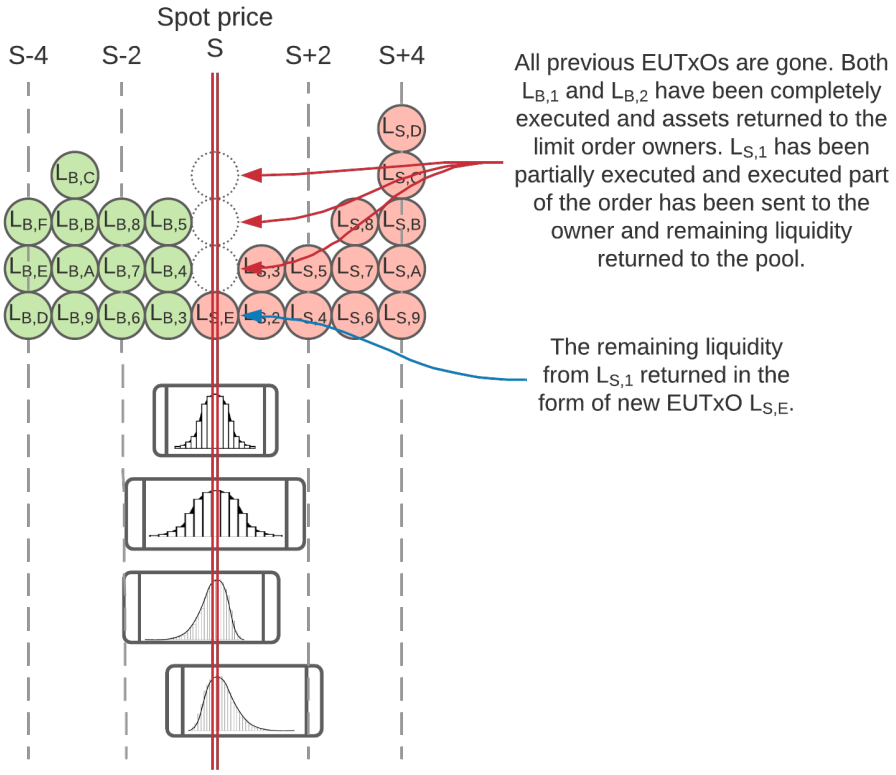
- 3 EUTxOs with swapped assets, spendable by agents that submitted by $L_{B,1}$, $L_{B,2}$, and $L_{S,1}$ respectively (hence swapped assets are directly sent to that user´s wallet);
- a new EUTxO with remaining assets from $L_{S,1}$ after executing $L_{B,1}$ and $L_{B,2}$.

Figure 15: Transaction matching 3 order book transactions: $L_{B,1}$, $L_{B,2}$, and $L_{S,1}$.



After executing T_2 the state of the fragmented liquidity pool is as below:

Figure 16: State of the fragmented liquidity pool after executing T_2.



We can see that all $L_{B,1}$, $L_{B,2}$, and $L_{S,1}$ are all spent, $L_{S,E}$ with remaining liquidity is created and * the results of limit orders are returned to the corresponding wallet owners.

The presented approach has multiple benefits:

- as before, thanks to the *commit phase* design, all $L_{B,1}$, $L_{B,2}$, and $L_{S,1}$ could be submitted at block $\mathbb{B}_{-1}$ and executed at block $\mathbb{B}_0$ right away, without any concurrency and memory related issues;

- off-chain components match $L_{B,1}$, $L_{B,2}$, and $L_{S,1}$ together, which provides the best execution price for all 3 orders;
- the transaction created by the off-chain match making engine has the minimum possible size, only EUTxOs with the required assets and data are consumed, with only a single EUTxO providing liquidity. In contrast to entire liquidity pools stored in a single EUTxO (the biggest possible footprint of transaction memory per transaction), it offers the highest possible optimisation. In a sense, this is not much different from a regular transaction on the Cardano blockchain, which automatically allows high scalability of **axo** on layer 1; this cost memory size minimisation means that market taker pays the smallest possible transaction fee for having their transaction executed;
- limit order is free of impermanent loss and represents the price the user wants to get for the exchanged assets, plus provides market maker fees to the limit order owner;
- *programmable swaps* allow for additional parameters in a limit order to be specified, e.g., to be executed at $S + 1$ price, as opposed to a fixed price, this price is moving with the market price, offering constant market making opportunities until resource exhaustion.

From the security point of view, sell limit order $L_{S,1}$ is only spendable in the present price of $S + 1$ in this example, hence there is no other way to redeem this EUTxO than at the set price.

4.10 Programmable Swaps Domain-Specific Language

Programmable swaps on the **axo** platform will be based on DSL, unless precluded otherwise by optimisation. This language will allow users to interface with various protocols on the **axo** platform. This language will be writing in the spirit of the functional programming pearl written by Simon Peyton Jones et al, "Composing Contracts: An Adventure in Financial Engineering" [1].

The idea behind DSL is 3-fold:

- develop a secure and easy to use DSL for defining all potential *trading strategies*;
- provide means for composing financial contracts, creating a sound financial system (you compose contracts, hence there is no material risk as in TradFi);
- be able to develop an easy GUI (Graphical User Interface) on top of it, for the most popular types of contracts, such as market orders (swaps), limit orders, DCA, etc.

Initially **axo** *programmable swap programming language* will be simple, to provide the basic functionality on the launch date. Over time it will evolve into a system that allows *Portfolio Managers* (PMs) to define sophisticated automated trading strategies, akin to hedge funds.

4.11 User Interface

The programmable swaps DSL is an advanced feature, making all *programmable swaps* features available to the users, however it is of a much higher level of complexity than should be expected for a typical user (the biggest target group).

axo platform will implement interfaces allowing users to easily specify desired *programmable swaps*, without the need to understand *programmable swaps* DSL. Hence axo will have:

- a simple market order (swap) interface for selecting the trading pair and specifying the exchanged amount;
- a simple limit order interface for specifying the price bounds and the amounts of tokens to transact;
- a simple interface for DCA specifying the interval, frequency, and methodology, etc.;
- an option strategy visualisation graph, defining the underlying *programmable swap* by moving points on the graphical representation, see subsubsection 11.3.5 for example illustrations, in those cases, strikes K, expiry date, etc. would be movable parameters and displayed in the generated graph.

What is more, based off of *programmable swaps*, DSL will allow for specification of endpoints, and thus automated generation of user interfaces.

4.12 Fundamental Building Blocks

A unique property of *programmable swaps* is their composability. Composability of financial instruments ensures a sound definition [1], protected from over leveraged and unbacked structures that often lead to economic ruin. However, *programmable swaps* composability means that they can be combined with each other, type checked, and result in new unique *programmable swaps*.

This fundamental design allows for all axo trading features to be implemented using *programmable swaps*, for instance:

- an index as a programmable swap, that includes the rules for index composition (what assets and in what amount go into the index during each rebalancing operation), and the assets that the index is composed of;
- synthetics, which might include just the rules for the asset collateralization, liquidation triggers, and the collateral;
- options and futures, which contain assets in question locked into the contract, automatically settled upon the option expiration;
- option structures that can contain just different options defined at different strikes and expires, and code that defines their composition;

- sophisticated *portfolio management strategy*, akin to those used by hedge funds, containing the assets locked for the strategy via a vault, and rebalancing rules;
- and many more, the design scales to any types of financial instruments.

Composability is the key element of functional programming and composing programmable swaps is the most functional programming way of implementing financial contracts. However, what is most important is the safety that comes from both the compilation process and inclusion of dependencies in the *programmable swap* itself, as well as the scalability of the work, where all previous work directly contributes to features built in the future.

5 axo Order Matching Engine

The axo *protocol's Order Matching Engine* is the off-chain component responsible for matching *programmable swaps* with each other according to their specification. In this section, we cover it in more detail.

5.1 Architecture

axo *Order Matching Engine* is an independent component deployed on machine with *Cardano Node*. *Cardano Node* provides the state and ability to query the blockchain, the functionality required to get the list of all existing *programmable swaps* $\mathbb{S}$ and to communicate the orders (state transition).

5.2 Routing Rules and Fairness

The engine deals with multiple types of orders such as:

- market order – execute at the immediately available price, given that within the slippage range;
- limit order – execute only if at given or better price;
- liquidity pool – providing liquidity to the market at the current price;
- DCA – slightly more sophisticated order types, in this case market order executed $\frac{T}{f}$ (where T is period and f is frequency) times over the span of the contract;
- sophisticated portfolio management strategy – composed of many conditions and rebalancing strategies.

It is clear that due to the composability of the protocol, all that is required to guarantee fairness of all *programmable swaps* is to guarantee fairness of the fundamental building blocks, e.g., DCA will be guaranteed to be fair, if its' building blocks, i.e., market orders are guaranteed to be fair. This means that in the version 1 of *programmable swaps* we only need to guarantee fairness of the fundamental building block, market orders and limit orders for all *programmable swaps*, regardless of how complex, to be fair.

The routing order to ensure fairness is as follows:

1. All *cancel order* requests are processed. This guarantees that if someone wishes to cancel their order it is done before orders are executed. This creates a potential vulnerability where a user might submit an order in one block and immediately cancel it in the next, but a fee (denominated in AXO) for order cancellation will remediate it.
2. All market orders are processed in the order of submission (*FIFO* - first in, first out). For market orders to be processed the price must be within the requested slippage.

The actions of more complex *programmable swaps* boil down to the guarantee of market orders and limit orders, thus ensuring that all *programmable swaps* are fair.

5.3 Security

The safety of *programmable swaps* is guaranteed by the conditions encoded in the *redeemer*, i.e.,

- order can only be cancelled from the wallet that created it (potentially in the future, from a wallet that contains the appropriate $handle);
- order can only be executed if there is on-chain proof that it is the best available price and within defined limits of execution, such as slippage.

Those metrics do not depend on any additional sources of security, but rather simply on the market conditions. There is no more security needed, as all required conditions are to be included within the *redeemer* and are provided already by *Cardano blockchain*.

5.4 Scalability

A naïve implementation of the order matching engine would allow for deployment of multiple instances N, all executing and submitting transactions in parallel. This would lead to unnecessary transactions spamming the mempool with requests, and inefficient use of resources. Only one transaction would be validated successfully onto the blockchain, very inefficient usage of the Cardano infrastructure.

A proposal will be created to implement a consensus mechanism between the engine nodes that elect the block leader (block leader as opposed to Cardano's slot leaders), i.e., the node responsible for submitting transactions in the next block.

A series of metrics for all engine nodes is going to be tracked, such as successful submission of all orders into the next block and in fair order, and upon any deviations the underperforming node would be automatically deprioritized from the network, and in extreme cases (e.g., submitting unfair ordering) permanently banned from the consensus circle.

The ability to disconnect nodes is going to be guaranteed by the challenge included in the nodes, which the disconnected node would not be able to acquire information required to solve.

5.5 Decentralization

The aforementioned mechanism presents a unique ability to decentralize order execution, by sharing the engine binary with *Stake Pool Operations* (SPOs). SPOs would then be able to partake in order execution and hydra head (layer 2) formation for participation in the DEX rewards.

6 Algorithmic Automated Market Making (AAMM)

Algorithmic Automated Market Making (AAMM) is a novel AMM which emerges as a property of the axo protocol in order to

- completely remove or strongly limit impermanent loss;
- increase capital efficiency by utilising the capital more efficiently and keeping it constantly at work;
- use realistic pricing and liquidity curve models, as known from QuantFi and TradFi;
- dynamically adjust to market conditions and maintain liquidity pool properties via dynamically adjusting its parameters;
- aid users in creating healthy liquidity pools and pairs;
- provide better means of price discovery;
- provide means of risk control.

Most established liquidity models do not model markets well (see model, EMH, and impermanent loss in the glossary for a detailed rundown), leading to low capital efficiency, expenditure of large amount of energy (see money ≡ energy) compared to the total value locked, and have inherent scaling limitations due to global memory limitation (akin to Ethereum´s account-based model architecture). The *AAMM* model attempts to bridge that gap by applying more financial engineering scrutiny and bespoke methodologies.

6.1 Impermanent Loss & Constant-Function Market Maker

Impermanent loss originates from the inherent inefficiency of AMM models such as CFMM AMMs. Impermanent Loss occurs when the original ratios of the assets deposited in a liquidity pool change, and the total value of the assets held by the user in the pool are less than compared to what they would be, had they been held outside of the pool. This leads to incurring what is called impermanent loss, a perceived loss due to change in ratios of assets held, due to the nature of CFMM such as UniSwap's single pair liquidity $x \cdot y = \text{const}$ or Bancor's multi-asset liquidity $\prod_{i \in \mathbb{I}} x_i = \text{const}$. For a detailed explanation on CFMM, see subsection 2.5.

For example, let's take a pair of Cardano ADA and another hypothetical Cardano-native asset X as assumption. We assume that at the time of providing liquidity to a CFMM AMM style liquidity pool the price of ADA was \$2.00 and the price of token X was $1,000.00$. The initially provided liquidity, was therefore in form of 500 ADA and 1 token X at the ratio of $1:1$.

Now, having defined our starting state when contributing liquidity to the CFMM AMM liquidity pool, we can define the impermanent loss as the result of asset ratios in the pool changing. As the assets ratios change, we incur a loss in comparison to just holding assets. The most optimistic scenario in the case of CFMM is the ratio remaining the same, and hence putting the impermanent loss at 0%. However, as soon as the ratios shift, we incur the unrealized loss, and in the extreme case of asset X increasing in price

25-times, while the price of ADA remained constant, we incur the loss of -61.5% (or the loss of $16,000$\$ given the initial investment of $2,000.00$\$. All those losses are defined in percentage-terms in Figure 17 and in absolute USD terms in Figure 18.

Figure 17: Percentage Divergence of Impermanent Loss on Initial Investment of $\$1,000.00$ at valuation of \$2.00 and 1 Token X at valuation of $\$1,000.00$.

Percentage Divergence Loss									
Price ratio	ADA multiple	0.10	0.50	1.00	1.50	2.00	4.00	10.00	25.00
X multiple	Price	$0.20	$1.00	$2.00	$3.00	$4.00	$8.00	$20.00	$50.00
0.10	$100.00	0.0%	-25.5%	-42.5%	-51.6%	-57.4%	-69.1%	-80.2%	-87.4%
0.20	$200.00	-5.7%	-9.6%	-25.5%	-35.6%	-42.5%	-57.4%	-72.3%	-82.3%
0.50	$500.00	-25.5%	0.0%	-5.7%	-13.4%	-20.0%	-37.1%	-57.4%	-72.3%
0.80	$800.00	-37.1%	-2.7%	-0.6%	-4.7%	-9.6%	-25.5%	-47.6%	-65.3%
1.00	$1,000.00	-42.5%	-5.7%	0.0%	-2.0%	-5.7%	-20.0%	-42.5%	-61.5%
1.10	$1,100.00	-44.7%	-7.3%	-0.1%	-1.2%	-4.3%	-17.7%	-40.2%	-59.8%
1.25	$1,250.00	-47.6%	-9.6%	-0.6%	-0.4%	-2.7%	-14.8%	-37.1%	-57.4%
1.50	$1,500.00	-51.6%	-13.4%	-2.0%	0.0%	-1.0%	-10.9%	-32.6%	-53.8%
2.00	$2,000.00	-57.4%	-20.0%	-5.7%	-1.0%	0.0%	-5.7%	-25.5%	-47.6%
4.00	$4,000.00	-69.1%	-37.1%	-20.0%	-10.9%	-5.7%	0.0%	-9.6%	-31.0%
10.00	$10,000.00	-80.2%	-57.4%	-42.5%	-32.6%	-25.5%	-9.6%	0.0%	-9.6%
15.00	$15,000.00	-83.8%	-64.7%	-51.6%	-42.5%	-35.6%	-18.5%	-2.0%	-3.2%
20.00	$20,000.00	-85.9%	-69.1%	-57.4%	-49.0%	-42.5%	-25.5%	-5.7%	-0.6%
25.00	$25,000.00	-87.4%	-72.3%	-61.5%	-53.8%	-47.6%	-31.0%	-9.6%	0.0%

Figure 18: Divergence of Impermanent Loss in USD on Initial Investment of $\$1,000.00$ at valuation of \$2.00 and 1 Token X at valuation of $\$1,000.00$.

Divergence loss in USD								
	$0	$1	$2	$3	$4	$8	$20	$50
$100	$0	-$153	-$468	-$825	-$1,206	-$2,835	-$8,100	-$21,938
$200	-$17	-$68	-$306	-$605	-$935	-$2,411	-$7,372	-$20,728
$500	-$153	$0	-$86	-$268	-$500	-$1,672	-$6,028	-$18,429
$800	-$334	-$35	-$11	-$109	-$270	-$1,222	-$5,143	-$16,856
$1,000	-$468	-$86	$0	-$51	-$172	-$1,000	-$4,675	-$16,000
$1,100	-$537	-$117	-$2	-$31	-$134	-$905	-$4,467	-$15,612
$1,250	-$643	-$169	-$14	-$11	-$88	-$778	-$4,179	-$15,070
$1,500	-$825	-$268	-$51	$0	-$36	-$601	-$3,754	-$14,253
$2,000	-$1,206	-$500	-$172	-$36	$0	-$343	-$3,056	-$12,858
$4,000	-$2,835	-$1,672	-$1,000	-$601	-$343	$0	-$1,351	-$9,000
$10,000	-$8,100	-$6,028	-$4,675	-$3,754	-$3,056	-$1,351	$0	-$3,377
$15,000	-$12,651	-$10,023	-$8,254	-$7,013	-$6,046	-$3,508	-$505	-$1,270
$20,000	-$17,272	-$14,175	-$12,056	-$10,546	-$9,351	-$6,111	-$1,716	-$279
$25,000	-$21,938	-$18,429	-$16,000	-$14,253	-$12,858	-$9,000	-$3,377	$0

It is worth noting that, as the name indicates, the loss is impermanent, meaning it is not yet realized. If the liquidity pool would return to the original asset ratio there would be no impermanent loss. Impermanent loss is realized in the moment of withdrawing liquidity from the pool; once withdrawn, it is realized and can never be changed. However, due to the highly volatile nature of crypto assets, keeping liquidity in the pool longer leads to an increase in impermanent loss in the majority of cases.

Hence, we observe that changing initial CFMM AMM asset ratios causes impermanent loss, but what causes the ratios to change? On the surface, the answer is simple, the price

divergence between assets being part of the pool leads to different ratios. Price itself can be modelled using Geometric Brownian Motion (GBM) with drift and volatility; as such, we can classify the below cases, in order from the worst to the best, in terms of loss due to impermanent loss:

1. A cryptocurrency asset with a fixed max supply or with a burn mechanism (the decrease or fixed supply leads to natural price appreciation over time), paired with a fiat stable coin (which aims to achieve 2-4% over year level of inflation). Such a pair is negatively correlated by design and will result in consistent loss of liquidity pair value. For a liquidity pool open for an extended period of time (multiple years), this can get very severe due to the fact that most CFMM move along a $\frac{1}{x}$ line, meaning that initially the loss is small, but then becomes very sharp. Given the nature of this pair being negatively correlated, it is bound to go to 0, accelerating along the way.

2. Cryptocurrency assets with misaligned drift[5]. For instance, a new project with a low starting price and high potential, and an established currency such as a blockchain primary asset (e.g., ADA for Cardano), with high market cap and price stability. The initial drift of the novel project and much lower market cap will lead to high misalignment, and hence getting into the far parts of $\frac{1}{x}$ impermanent loss causing curve.

3. Cryptocurrency assets with similar drift. For instance, well established projects such as Uniswap token and ETH. This kind of pair, due to relatively aligned drifts and ecosystems, means a low impermanent loss, even smaller due to the fact that $\frac{1}{x}$ gives very small impermanent loss within the local vicinity of the initial supply ratio.

4. Assets reflecting the same underlying price, for instance stable coins of the same currency, e.g., DAI, BUSD, USDC, and USDT. As those assets basically have exactly the same drift, there is no impermanent loss present, only local divergence to volatility σ between different pairs. That, combined with $\frac{1}{x}$ impermanent loss dynamics curve, means this is not noticeable, except in the case of black swan events.

6.2 Reducing Impact of Impermanent Loss

As we observed in subsection 6.1, impermanent loss comes from:

- shift in the initial ratio of tokens alongside $\frac{1}{x}$ or other liquidity making curve (change in the ratio of the provided assets);
- long time exposure allowing for significant shifts with high losses to occur;
- lack of compensation to market maker for taking on the risk of potential losses;
- lack of utilisation of external liquidity sources to rebalance internal value shift;
- inability to express the desired source and target liquidity pool asset ratios.

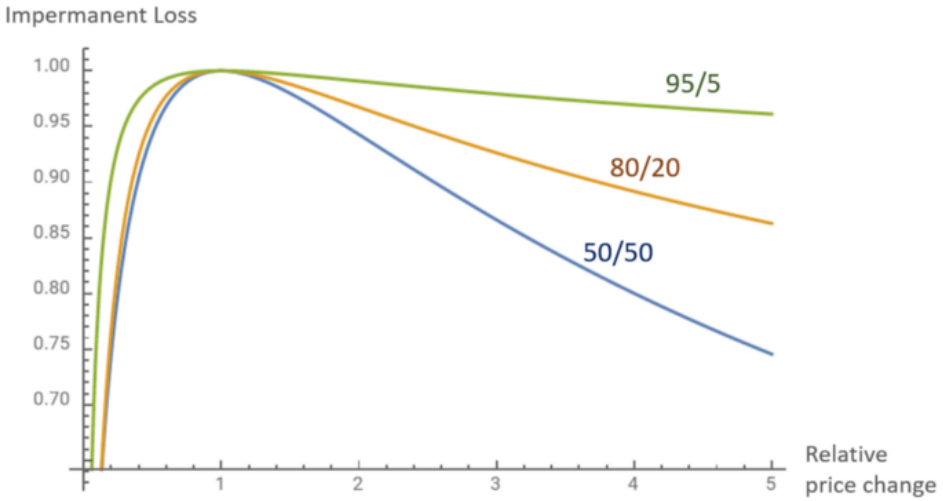
[5]Drift is the trend along which the price moves, where volatility is the local divergence from the mean.

Therefore, by addressing the above issues, one can eliminate completely the effect of impermanent loss. This is achieved by using sophisticated modeling to assess the perceived asset value and price dynamics, converging to desired assets ratios, the ability to start from the preferred liquidity pool asset ratios, and dynamic market maker reward scaling for providing liquidity in the market stress conditions, leading to a market net neutral position.

6.3 Programmable Source and Target Asset Ratios

We start by tackling the issue of changing token ratios. In the majority of CFMM AMM liquidity pools, all tokens are provided in the initial ratio of 50:50, which is the starting point that achieves the highest impermanent loss. On the opposite side, 100:0 achieves 0% impermanent loss but provides very little liquidity. The ideal system would allow the user to start with any initial liquidity and specify the desired target liquidity ratio to allow the market maker to reflect the desired outcome. For instance, start with 100% token X and using ratio shifting model end up with 80:20 of ADA to token X. The further the maintained ratio is from 50:50, the lower the impermanent loss, as shown in Figure 19.

Figure 19: Liquidity Provision Asset Ratios Impact on Impermanent Loss



Not only does this help to reduce impermanent loss and converge onto the market maker desired token allocation ratio, it also enables a series of interesting mechanisms, for instance:

- Let´s take a new project launching its token X that wants to both bound liquidity and to collect development funds. It could start with a 100% X based pool and converge on the desired liquidity ratio of 20:80 (20% token X and 80% ADA), once the pool stabilises on the 20:80 ratio, the project can withdraw 60% of liquidity in form of ADA to finance the project development. Then, we would have 20% of the initial token X provided into the smart contract and the 20% remaining after withdrawing 75% of all ADA, leaving bounded liquidity with a 50:50 ratio and the value of 40% of the initial supply.

- Balancing the risk appetite in holding the assets by using, for instance, Modern Portfolio Theory (MPT)[27, 26] or other portfolio allocation techniques, taking risk / volatility as a parameter to construct liquidity pool with the desired risk to expected revenue profile;
- By allowing every user to provide liquidity in the form of a different ratio, market participants are able to reflect their true belief about the assets provided into the liquidity pool.

6.4 Realistic Liquidity Supply Curve

As mentioned, the most popular CFMM AMM model is unrealistic and does only reflect market conditions well due to arbitrage adjusting its value to the actual market conditions. For instance, a CFMM with the formula $x * y = \text{const}$ composed of ADA and PIZZA, where the current market price of PIZZA is 10 ADA per pie, assumes that the below 3 events have exactly the same probability density (likelihood of occurring):

- PIZZA costing 0.000001 ADA;
- PIZZA costing 10 ADA; and
- PIZZA costing $1,000,000,000$ ADA.;

As we can clearly see, the above probability distribution does not reflect reality, and unnecessarily distributes TVL equally across the entire $(0, \infty)$ domain.

In QuantFi, sophisticated models have been developed to precisely define price distribution and dynamics and predict the market conditions, those methods are most often based on a *Geometric Brownian Motion (GBM)* defining stochastic process S_t, following GBM as

$$dS_t = \mu S_t dt + \sigma S_t dW_t$$

where

- W_t is Wiener process (or Brownian motion);
- μ is drift;
- σ is volatility.

Using stochastic processes, we can predict and model realistic price probability distribution, and create liquidity models concentrating around moving drift μ, provided in a form of oracle, and higher distribution moment:

- volatility $\sigma = \sqrt{\frac{\sum_i^N (x_i - \mu)^2}{N}}$ – expected deviation from μ;
- skew $\widetilde{\mu}_3 = \frac{\sum_i^N (X_i - \overline{X})^3}{(N-1)\cdot\sigma^3}$ - asymmetry around the mean μ;
- kurtosis $\kappa = \frac{\mu_4}{\sigma^4}$ – tailedness;

- higher moments in the case of high quality historical data available.

Figure 20: Stochastic Price Model.

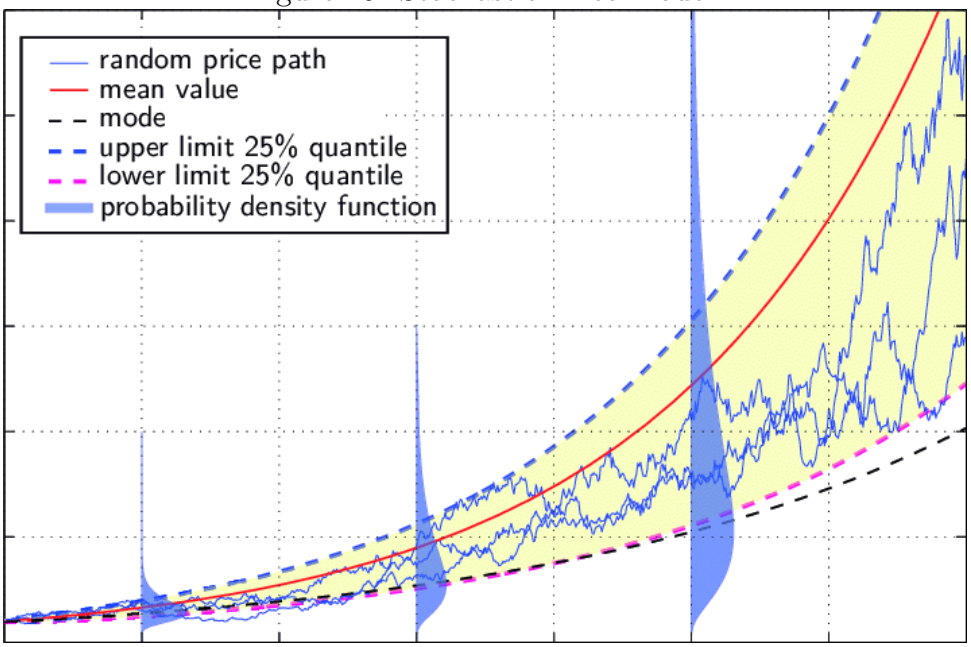
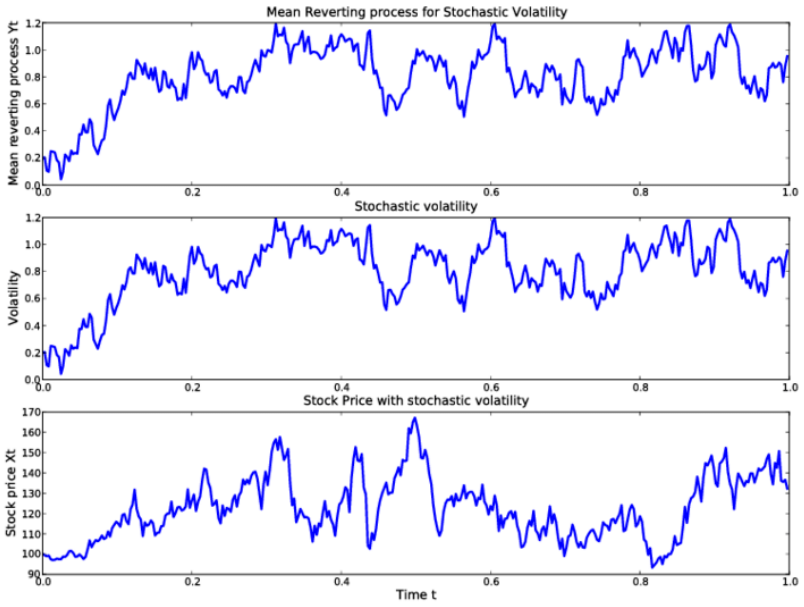


Figure 21: Stochastic Process Reversal to the Mean.



axo protocol will enable a selection of liquidity pool models:

- stochastic pool model as outlined above;

- legacy and custom formula models such as CFMM[6];
- spot pools, pools converging to specific asset ratios according to the pricing formula.

The reason for all prices to be geometric in nature is the relationship between ratios and logarithm, and ratios being how we express dynamic systems (in relation to themselves).

Unfortunately, the majority of market making formulas have a constant form such as $x * y\text{const}$, $\prod_{i \in \mathbb{I}} x_i = \text{const}$ or similar, leading to high inefficiency in the pool price discovery process. You can model any process iteratively with the worst model; given a step is small enough, it will eventually converge, but in practice it gives rise to such issues as:

- slippage – the execution moving the price significantly leading in overpaying for the transaction;
- inertia – the pool is unable to update its price due to the astronomic size of the total value locked, having single trades with very little effect on the price expressed by the pool;
- unnecessary expenditure of energy – a lot of energy is wasted where it is not needed (impossible scenarios), taking much longer to converge on the actual price. Yes, arbitrage bots fulfill a role here of price balancer between exchanges, but there is a significant lack of arbitrage between any assets other than BTC and ETH. People who exchange cryptocurrency constantly are certainly aware of these often gross pricing discrepancies for such liquid assets, as for instance Cardano on different exchanges.

axo protocol will support models suited to different cryptocurrency asset types and families of quantitative models to express the automated liquidity. The protocol will support a rich family of quantitative models for minting liquidity pools, giving information on what is the ideal pool in a given case and its parameterization, as well as allowing for dynamic on-chain updates of the liquidity pool parameters via *programmable swaps*.

6.5 Algorithmic Liquidity Pool

The ability to model the price process well, as outlined in subsection 6.4, is one important concept to reflect the price effectively, another is to react to changing market conditions. Stochastic process will be able to update its state by the usage of price oracles, while there are additional parameters we can update based on market dynamics:

- *market maker fee* – during the period of high traffic or rapidly changing price distribution, the fee collected by market maker should increase; this is a fee for

[6]Despite the fact that legacy liquidity formulas are much less effective, we predict that there might be some uses, or users who will simply want to create them, and the premise of *programmable swaps* is customizability, hence it only makes sense to include one of the most popular models as an option as well.

providing liquidity (service) in a market stress scenario and potential insurance against black swan events[7];

- *yield farming* – depending on the available liquidity in the market versus demand for the liquidity from market takers, the rewards for providing liquidity will increase in the form of **axo**. As part of its role as unit of account **axo** fees dynamically adjusts to the market conditions, incentivizing action where it is needed.

6.6 Offsetting Internal Risk with External Liquidity

Evolving market conditions might cause the liquidity pool to incur impermanent loss. The **axo** protocol reduces impermanent loss through the stochastic processes governing it. The processes dynamically adjust fees and rewards, to result in a risk neutral liquidity pool.

As pools are moved out of the true market price balance, an arbitrage bot could use this opportunity of price difference between a specific liquidity fragment on **axo** and on external DEXs, and will create transactions with it, resulting in additional revenue for **axo** market maker and at the same time reverts the fragment price mean μ to the perceived market price.

6.7 Minting Sound Liquidity Pools

It is very important for the market maker to pick assets to put into a liquidity pool that, given the pool model, will minimise any potential losses while maximising the exposure to money making opportunities. One wants a pair that is frequently exchanged, but at the same time one that is able to maintain its inherent value over time, a property that emerges from the specific assets in the pool and the model of liquidity that the pool uses. An exchange such as the **axo** platform is perfectly positioned to aid users in creation of *sound liquidity pools*.

In the majority of cases, simple CFMMs such as $x * y = \text{const}$ and the creation of negatively correlated pairs deteriorates the total pool value. The worst offenders are fiat stablecoins in pairs with cryptos. Stablecoins are by nature inflationary and crypto is in its nature deflationary. This means that the liquidity pool from day one is a bucket with a hole at the bottom through which your total rewards (rewards from providing liquidity and liquidity locked in the pool) deteriorate, or in a good case, maintain current value (which renders providing liquidity pointless).

Cardano now has a multitude of DEXs focusing on stablecoins and related liquidity pairs, while the only valuable role of stablecoins is to bridge traditional finance with the world of crypto. Once the bridge is crossed, there is very little reason to do anything with the fiat. An exception might be perhaps in the rare conditions of very soundly designed stablecoins such as Djed, which compensates swap of floatable for stable, but in the case of Djed, it only makes sense to collateralise Djed with ADA, not to create liquidity pools of Djed fiat and crypto.

[7]This fee will have mean around $\mu = 0.3\%$ similar to all other DEXs, but when the market will be inactive it will decrease to incentivize trading activity, and when the market will be overheated and risk will increase, it will be defined in such a way as to compensate the market maker for the risk taken.

axo platform will provide information to the user derived from on-chain and external data (via easy to understand user interfaces), performance metrics, aid in providing quantitative feedback on the pool parameters selected by the user, and help to optimize them to achieve the user's goals. The visual cues will be especially helpful when trying to understand the impact of parameters on the capital efficiency and the risks involved (e.g., automatically alert if the pair reserves are negatively or weakly correlated). This way market makers will be able to make far sounder decisions. The axo protocol further incentives sound liquidity nodes with platform tokens, thus rewarding sound decision making.

6.8 Fragmented Liquidity of AAMM

Each *AAMM* submission is a separate *programmable swap*, i.e., a separate EUTxO. This fragmentation achieves the highest throughput and minimal memory requirement for performing transactions. Security and soundness of the protocol is achieved via *redeemers* and *validators*.

This is in stark contrast to all other liquidity providing models, where the design of liquidity pools is very simplistic. It is easiest to design a pool with global memory, but in the case of EUTxO account model it leads to 1 transaction per block (20s), or optimization running into memory issues (16kB per transaction and 65kB per block). Doing it the optimal way, utilizing Cardano's EUTxO architecture, achieves high throughput, low transaction fees, and opens a lot of new possibilities not available to other DEXs before.

The fragmentation of the liquidity protocol leads to a series of very desirable, naturally emerging properties. If one shifts from monolithic blocks of liquidity to fragmented nodes reflecting separate market making decisions, that naturally leads to the emergence of geometric pricing models.

Uniswap v3, by introduction of concentrated liquidity and indexes, observed the same issues[7]. Users specify liquidity in the ranges they think are good market making ranges, and provide liquidity only within this range. As a result from all concentrated liquidity, a geometric pricing model emerges.

It is a natural consequence of aggregation of multiple samples, each allowing for the individual expression of market sentiment. This is due to CTL (Central Limit Theorem[8]), which states that given a large enough set of random samples, a normal distribution naturally emerges.

When we fragment the liquidity into separate nodes, all kinds of geometric distributions naturally emerge, giving very efficient and market reflective pricing and liquidity models.

When combined with the axo domain specific language , it allows for the expression of market sentiments, and an emergence of true market distribution. Maker orders in the liquidity pool express their belief of the market, and given a large enough sample, naturally reflecting market beliefs.

[8]Central Limit Theorem article on Wikipedia: https://en.wikipedia.org/wiki/Central_limit_theorem

7 Yield Curve

Yield is the product of engaging funds in a revenue producing activity, the higher capital efficiency and the lower risk the better. The Cardano protocol and axo platform have additional riskless sources of yield. We outline those yields in this section.

7.1 Yield Farming

Yield farming is providing financial incentives for users to take specific actions. On the most basic level, yield farming would aim to increase the overall market efficiency, for instance increase for pools and pairs lacking liquidity, offer higher rewards from minting scarce options and synthetics, and incentivize the creation of high-quality DeFi educational content.

7.2 ADA Staking Rewards from Smart Contracts

The architecture of Cardano's *Proof of Stake (PoS)* protocol and EUTxOs means that it is possible to delegate ADA locked into smart contracts to pools, in order to earn additional yield.

Any capital that is not actively used or required for a specific action can be delegated and earn staking rewards. Hence, it also provides a nice benchmark for all investments. If any investment is not able to generate revenue higher than the current Cardano network ROI[9], then it is not worthy of engagement in, unless it provides hedge against risk.

[9]Cardano staking reward act as network's internal risk-free rate r.

8 Emerging Properties of Programmable Swaps and AAMM

The fragmented design of programmable swaps and mechanics built into *AAMM* lead to the emergence of a series of very desirable properties:

- Fragmentation leads to geometric price distribution due to the Central-Limit Theorem applied to the sample of investors; geometric price distributions are important because they represent the market accurately, and quickly arrive at new stable states when the market conditions shift.
- Freedom from impermanent loss due to all mechanics implemented into AAMM
- High capital efficiency, meaning higher revenue generating potential on the same unit of money.
- Increased market efficiency, giving investors access to the true asset prices and a trove of investment educational content and data.
- Protocol adaptability to shifting market conditions.
- Means of risk control, helping to protect the investments made.

9 Indexes

An Index is a financial instrument representing a basket of instruments, allowing users to track the performance of a group of assets in a standardized way[8]. Index allows you to invest into the entire market, market sector, or a group of similar assets, such as DeFi projects, DEXs, NFTs, etc.

The main advantage of holding an index, as compared to single crypto assets, is that they often guarantee much more stable returns, at the efficient market rate, without too much risk exposure. Take for instance smart contract blockchains; instead of placing all bets on one horse or spreading bets according to your own metrics, one might buy shares of a smart contract top 20 index, gaining exposure to the entire smart contract market with allocation to specific assets correlated to market capitalization. As such, investors are betting on smart contracts being successful overall rather than any specific project.

In summary, the advantages of investing in an index, compared to manual portfolio management are:

- wider market exposure, increasing the market coverage and reducing volatility by the fact that basket is comoset of different assets,
- protection as in hedge against single asset failures, e.g., if one DEX fails to perform, then others in the portfolio will absorb its share, hence in that sense the risk is neutral as the index represents the entire sector.

Some of the most popular examples of indexs from the world of TradFi and DeFi include:

- S&P 500 - tracking composed 500 largest companies stocks, weighted by market capitalisation and representative of the entire US economy;
- FTSE 100 - 100 largest companies listed on the UK exchanges, weighted according to their market cap;
- (Ethereum) DeFi Pulse Index: https://www.tokensets.com/portfolio/dpi , tracking the performance of the 25 largest Ethereum DeFi projects according to the composition formula (each project capped at 25% max allocation), balanced monthly.

A good example of a similar project from the Ethereum blockchain is TokenSet, which provides indexes for a range of Ethereum blockchain tokens, e.g., DeFi Pulse Index. In this case, a trader buys a stake of the index that represents the market composition, by the capitalization for the specific group of assets (e.g., top 100 cryptocurrencies, top 25 DeFis, top 10 smart chain cryptos, etc). The index is rebalanced at a constant interval (typically 3rd week of every month) and maintains specific index properties (e.g., in the case of TokenSet they limit max position to 25%).

9.1 Index Balancing

Asset prices and market capitalization at the time of rebalancing would be ingested from on-chain Oracles, either based on:

- a centralized on-chain Oracle provider taking data from price trackers such as Coin Market Cap, CoinGecko, and such data providers as CoinAPI, or
- from purely on-chain data build using axo protocol pricing models that should reflect the true asset price on-chain in a trustless manner.

The index rebalancing can be achieved with one of many existing centralized price Oracles and the typical index rebalancing of every 3rd week of the month.

9.2 Index Categories

axo is a platfrom that allows for the deployment of the following.

- financial (fungible token) indexes - investing in fungible tokens representing different projects shares / internal currencies;
- NFT indexes - index composed of NFTs bought and sold based on the current price, valuation, and market sentiments, starting with art, but with the growth of NFTs in the future potentially also representing all the deeds stored on the blockchain;
- Cardano delegation index - an aggregated way to delegate ADA via smart contract to a portfolio of pools according to a specified condition, e.g., single stake pool operators, ecosystem developers, mission-driven pools, etc. Each pool considered for the index would need to meet the block production and reward requirements.

9.3 Cryptocurrency Index

The index protocol would consume on-chain price Oracle, reserve, and other data, according to the index specification, and each cycle (T = 6 epochs = 30 days) would rebalance the index according to the new parameters.

Moreover, CoinGecko tracks many different asset classes which is a great inspiration for potential index creation. As such, we propose the development of the below crypto indexes:

- Top 50 cryptos;
- Top 25 DeFi;
- Top 20 smart contract blockchains;
- Top 25 oracles;
- Top 25 specialized application blockchains (storage chains such as FileCoin or AR-Weave or coverage networks such as HNT);
- and others.

10 Synthetics

Mirrored (a.k.a. synthetic) assets are financial instruments deriving their value from the underlying[15, 9, 12]. The underlying can be anything from real objects such as land, art, or gold ownership to abstract such as commodities, indexes, stocks, equities, and any existing financial instrument.

The name of this asset class is derived from their functionality, i.e. mirrored implies that the asset mirrors the price behavior of its underlying asset which can be simple 1-1, but also can represent an inverted (short), where the price is followed in inverse (e.g., a loss of $10k in the underlying value is gain of $10 k in the inverted synthetic token). Synthetic, on the other hand refers to a specific way of issuance of the mirrored tokens, namely by not backing them with the actual underlying assets, but rather providing collateral acting as insurance, providing the guarantee of the price. That collateral can be auctioned at a discount to acquire back synthetic tokens and balance the value at risk requirement or liquidated at the margin being returned as collateral to the token owners.

10.1 Advantages of Using Synthetics

It's important to note a few distinguishing characteristics of synthetic instruments that (often) make them more desirable to trade than the actual underlying instruments:

- Fractional ownership: minted synthetic tokens can be fractionally traded giving access to them to low net worth individuals. Let's take as an example a stock of Berkshire Hathaway, worth at the 2021/04/27 market close $411,400.00. Creating frictionless market access, gives much more fair access for financial betterment to everyone regardless of their total net worth.
- Derivative financial instruments: synthetic tokens can use any formula to derive the price from the underlying asset, from a simple reversed token, where for the case of example, $10k loss in BTC price represents $10k gain in the reversed synthetic BTC token. This effectively provides an easy mechanism to trade short (capitalize on the knowledge of the asset being overpriced) and leads to the creation of much more efficient markets. Furthermore, derived instruments don't stop with reversed, but can be as well indexes, future contracts, options (deriving price from the Black-Scholes formula), and much more. Covered calls and puts are the easiest to implement using collateral.
- Liquidity: some assets pose a challenge to trade, e.g., physical assets or illiquid ones. Synthetic token issuance, as it only reflects the price of physical commodities, makes them easy to trade and in the case of illiquid assets, injects additional liquidity into the system via the market making incentives proportional to the risk derived from the exoticity of the underlying asset.
- No geographical boundaries: not everyone has equal access to financial markets; from the brokerage requirements to restricted trading lists and actual market frictions. A permissionless blockchain provides a platform for deployment of assets available to everyone in the world and, in combination with synthetic instruments, it gives access to trading them to a much wider audience. In turn, this creates a more even field for all traders and injects additional liquidity into the market.

- Low transaction costs: brokerages often charge significant fees for order execution. In the case of exchanges or market makers, the provided options to trade in fractional shares always come at a premium. The blockchain implementation both provides transparency of what liquidity fees are, creates a peer to peer transaction network, removing the intermediary and hence the cost, and provides much quicker settlement mechanics.

10.2 Synthetic Token Interface

Synthetic's token interface is composed of the following endpoints:

- Mint: provide collateral and the price oracle minting synthetic tokens.
- Burn: return synthetic tokens, burn them, and receive the stake of collateral represented by them.
- Trade: trade any token on the blockchain.

The critical functionality of synthetic tokens is the ingestion of asset price and the evaluation of whether the provided collateral is sufficient. If it's not, then either the synthetic tokens need to be repurchased at a premium using the collateral (which is similar to Maker's Collateralized Debt Position - CDP) or the contract must be liquidated [13, 14, 15, 16, 17, 9, 10, 11, 12].

It's worth noting that the risk can be shared among a pool of similar or even all synthetic instruments. The settlements would still reflect the price movements, but the risk can be collateralized for the system altogether. [17]:

11 Financial Derivatives

11.1 Options

An options contract is a right, but not an obligation, to buy (or sell) the underlying asset at a specific price at a specific time[25]. Options are great instruments to increase the money making potential (as it allows the trader to take a larger exposure to the price movements in the market), allow for risk control by providing inversely correlated instruments (calls/puts), allow for structuring trades to bet on specific outcomes (e.g., take limited exposure to price increase via bull spread), and provide efficiency to the market[25, 31, 32].

Options are priced using the Black-Scholes formula[25, 33]. Options derive their price from the assumption that market dynamics follow a Generalized Brownian Motion and the underlying asset volatility, free interest rate, and the option parameters themselves (type - call or put, strike price, the expiration date).

Call option price C is defined as

$$C = S_t \cdot N(d_1) - K \cdot e^{-r(T-t)} \cdot N(d_2)$$

where

- C – call option price;
- N – CDF of the normal distribution;
- S_t – current underlying price;
- K – strike price;
- r – risk-free interest rate (in the case of Cardano, this should be equal to the staking reward);
- T – expiration date, where $T - t$ is the time to expiry;
- σ – –volatility of the underlying asset;
- $d_1 = \frac{\ln(S_t/K)+(r+0.5\cdot\sigma_v^2)\cdot(T-t)}{\sigma_s\cdot\sqrt{T-t}}$;
- $d_2 = d_1 - \sigma_s \cdot \sqrt{T-t}$.

Put option price P is defined as

$$P = K \cdot e^{-r(T-t)} \cdot N(-d_2) - S_t \cdot N(-d_1)$$

where all symbols including d1 and d2 are the same.

We propose 2 option contract implementations:

- Covered options, where the option writer owns an equivalent amount of the underlying security. This means that the underlying is locked into the contract when the covered call option is minted. This provides the guarantee that the option can be exercised as per specification (according to the option type - European, American, Bermuda and the price oracle). For covered option creators, it generates income in the form of options premium.
- Collateralized option (synthetic instrument approach) where the collateral is provided to hedge the underlying volatility to around 200% the underlying value and be subject to collateral rebalancing.

11.2 Advantages of option trading on the blockchain

Usually, options are written by big institutions (e.g., banks or large market makers) and sold in bulks of options for 100 underlying shares each. Not only does this limit the liquidity and who issues the option contracts on the market, but it also limits access to buying option contracts (as they need to be bought in bulk of 100s and they carry the corresponding risk with them). Not to mention, the cryptocurrency market is much more volatile than the stock market, and taking the same exposure doesn't make sense for a lot of crypto assets.

Trading options on the blockchain provides 2 categories of benefits - to the market, by increasing its efficiency and the number of instruments that can be traded, structuring risk, hedging, and to investors, as doing so on the blockchain has a series of benefits:

- No middle man - options are minted by people on the blockchain and available to everyone else on the blockchain. Thus, the execution fees are low, and the premium is only paid for the service provided by the writer and the risk that they take;
- Fractional shares - options can be traded in much smaller units and even in fractions;
- Cheaper settlement - settlement is automatic via smart contracts;
- Full transparency - as all the information is publicly available on the blockchain.

11.3 Option Trading Strategies

We further propose composite smart contracts allowing the purchase of option trading strategies. A user would select the risk and profit profile, input strategy parameters, and the smart contract would automatically structure using the required composites for the strategy.

This adds a new innovative way of trading and makes option trading (usually very risky to novices) available in a risk controlled manner (outlying the risk at value, the best/worst potential outcomes, and for savvy traders, it just allows for an easy locking option strategy).

We outline below a dozen of the option trading strategies that we'd expect to be introduced on the axo platform as a follow up to the ability to trade options. This list should evolve in the future and additionally welcome new strategy propositions from the community, as long as they're sound and the risk is easy to understand and display.

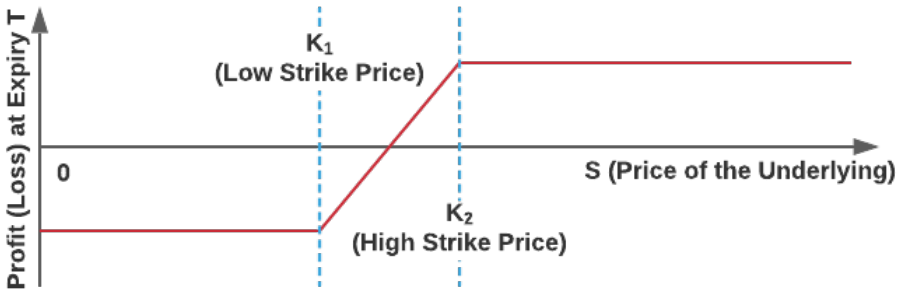
11.3.1 Bull Call Spread

Structure:

- Buy N calls, at strike price K_1 with the expiration date T;
- Sell N(the same number) calls, at strike price K_2 where $K_2 > K_1$, with expiration date T (the same expiration date).

This type of vertical spread is used when the investor is moderately bullish on the underlying asset and protects themselves from the maximal potential loss, but also caps the total profit if the contract expires above the strike price K2.

Figure 22: Bull call spread with strike prices K_1 (low strike price) and K_2 (high strike price).



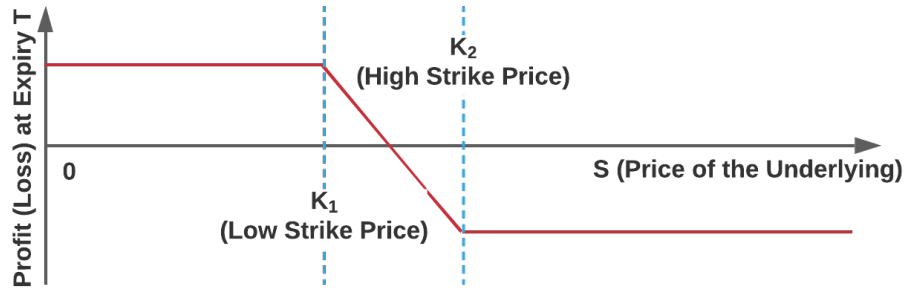
11.3.2 Bear Put Spread

Structure:

- Buy N puts, at strike price K_1 with the expiration date T;
- Sell N (the same number) puts, at strike price K_2 where $K_1 > K_2$, with expiration date T (the same expiration date).

Similar to bull call spread, bear put spread is a tool for moderately bearish investors, who wants to protect against the upside risk, and accept the potential limitation of the income if the put expires deeper into the money.

Figure 23: Bear put spread with strike prices K_1 (low strike price) and K_2 (high strike price).



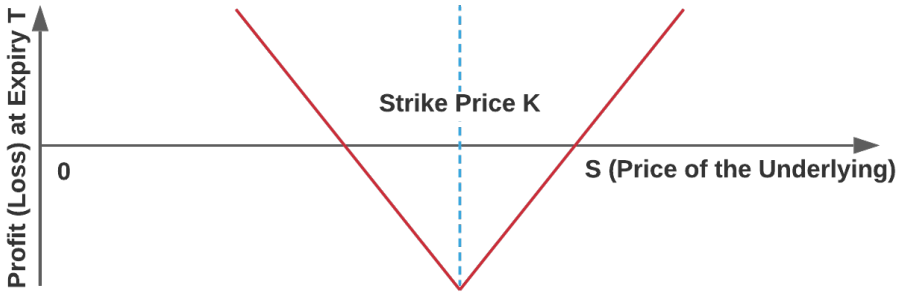
11.3.3 Long Straddle

Structure:

- Buy N calls, at strike price K with the expiration date T;
- Buy N puts, at strike price K with the expiration date T.

Long straddle does not provide risk protection, however it´s a bet on volatility, i.e., that the underlying will move significantly off the strike price K, but without knowing in which direction.

Figure 24: Long straddle with strike price K.

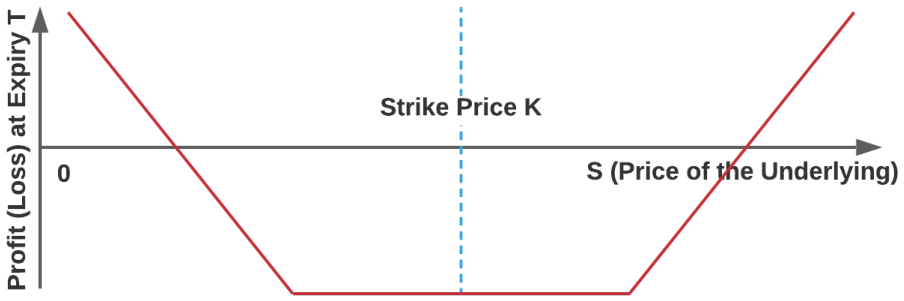


11.3.4 Long Strangle

Structure:

- Buy N out-of-the-money calls, at strike price K with the expiration date T;
- Buy N out-of-the-money puts, at strike price K with the expiration date T.

Figure 25: Long strangle with strike price K.



11.3.5 Other Option Strategies

There are many other option trading strategies that can be structured from simple call and put options, once those are available on the platform. We will provide the description on the below strategies and more in the near future.

To mention a few other option strategies:

- Short Straddle,
- Long Call Butterfly Spread,
- Barrier options,
- Long term option,
- Calendar (Time) Spread,
- Collars,
- Iron Condor,
- Iron Butterfly,
- Fig Leaf,
- Long Call spread,
- Long Put Spread,
- Short Call Spread,
- Short Put Spread,
- Double Diagonal,
- .. and many more.

12 Arbitrage

Arbitrage is the act of exploiting the market inefficiency between trading venues (exchanges). In the most simple case of the arbitrage, let's say ADA is priced at $3 at exchange A and at $2.95 at exchange B. The arbitrage bot will find this information and will attempt to buy ADA at exchange B for $2.95 and sell it immediately at exchange A at $0.05 profit per ADA. The act of arbitrage moves the price, as after the execution, the price at the exchange B will be higher (e.g., $2.98) due to purchasing the discounted ADA, and on exchange A it will be cheaper due to selling it (e.g., $2.98).

As long as there is a price difference between exchanges, so that when these trades are executed they are more profitable than the execution cost, arbitrage is possible. Arbitrage on exchanges will lead to them converging on the central limit value (true market sentiment from the aggregated exchanges) of the asset price. The arbitrageur earns profits by buying at a discount from exchange B and selling at the premium at exchange A, hence both exchange B sellers and exchange A are the source of income for the arbitrage bot.

Finally, the mentioned example is the most basic case of arbitrage (pure arbitrage), there are a multitude of arbitrage styles, including statistical, where arbitrage is based on the market movement predictions and the average expectation of reward[10]. Arbitrage leads to efficient price discovery, but at the cost of market participants (both takers and makers).

Information about the makers and takers of asset prices is spread across multiple exchanges; this leads to such gross discrepancies as the 3_{rd} largest crypto (by market cap) sometimes having 10-20 cents difference between exchanges. This gets only more extreme for smaller cap coins, as while Bitcoin, Ethereum, and to a lesser extent Cardano, are actively arbitraged, the smaller caps are deemed not worthy of running arbitrage bots.

This creates market segregation between exchanges and a lack of information flow. Arbitrage is a valuable and necessary information exchange mechanism and leads to efficient price discovery and convergence to the same price +/- delta delays on participating exchanges.

The **axo** protocol with its fragmented liquidity, where each fragment can act as supplied funds to a swap order on any Cardano-native DEX, will be able to capitalize on inefficiencies on all other exchanges. Employment of arbitrage bots in liquidity pools for ratio rebalancing and via arbitrage vaults means users can generate higher profits compared to other platforms.

In the EUTxO model and script validation mechanism model, such arbitrage can be incorporated into a liquidity protocol. It will put market makers in the role of performing additional transactions (and earning additional fees), for takers it will provide market efficient price reflecting the true market price at any given time, and for the other applications it will provide invaluable on-chain price oracle data, not approximating the true price, but having on-chain arbitrage proof of it. Such on-chain price Oracle does not have any lag, meaning it is much more efficient than any other on-chain price Oracles (it is the optimal state), only subject to lack of liquidity not allowing for convergence of price in the market.

[10] You can explore a few additional types of arbitrage by checking this Wikipedia article: https://en.wikipedia.org/wiki/Arbitrage#Types

13 Oracles

axo protocol is going to make use of oracles including pricing information and market data. A series price and trading indicators, high quality moments of distribution (based on stochastic modelling), and additional financial indicators such as Greeks (risk sensitivity parameters)[11].

[11] Greeks are a fundamental signal for trading options will eventually be available to users. You can see the list of all (financial) Greeks in Wikipedia article, here: https://en.wikipedia.org/wiki/Greeks_(finance)

14 Risk Control

Risk is an inseparable part of any investment, the most optimal trading strategy is always the one that has higher revenue generating potential, without introducing additional risk. In TradFi there is a plethora of measures to classify the level of risk such as VaR (Value at Risk), volatility or potential loses. In addition, there are mathematical tools to classify how good a given trading strategy is, taking the risk into account, such as Sharpe ratio, and there are portfolio management theories that help to optimally allocate the capital, given an acceptable level of risks, such as MPT (Modern Portfolio Theory).

The axo protocol design allows for the incorporation of risk control tool. Before we get into the solutions, we shed light on why people take risk in the first place and what the price of risk is.

14.1 Why do people take risk?

Risk implies the uncertainty of the outcome, where the outcome itself has some perceived value. In light of the volatile nature of the market, high-risk investments are usually those with the potential for high returns (although high risk does not imply high return potentials). One would expect that in an efficient market (see EMH), the price would reflect the risk involved. Unfortunately, this is often not true, owing to the inefficiencies in the market. One usually makes returns by taking the risk; hence people take risks to make profits.

Each investor may have a different risk appetite, and as such, one would construct a portfolio with an expected risk level σ acceptable to the investor. This can involve a mixture of high-risk assets, secure investments and also optimize for additional factors, e.g., asset relationships to each other in the basket (see hedge).

The fact that risk is inseparable from investing does not imply that one should do nothing about it. When actively monitored, one should adjust their position in the market due to changing conditions and reevaluate their investment.

14.2 Market Maker Risk Compensation

The axo platform will aim to use information related to risk such as *volatility* to dynamically change platform fees based on risk to market makers providing liquidity in the risky assets.

14.3 Market Maker Fuses

When providing AMM liquidity to the market, one might encounter a black swan event (highly unanticipated event), e.g., a crucial piece of information about the project might be released leading to its sudden price decline. In some cases, the initial rapid decline leads to market panic. Market panic, is the elevated level of distrust and stress in the market, leading to excessive actions (considering what caused it). The aftermath of this fear spiral, most of the time is an excessive response, which in rare cases can take entire markets

and projects down. Market safety measures and fuses help to curb the unpredictable and emotional responses, and instead allow to plan and position accordingly ahead of time.

In TradFi markets, this is often solved via implementation of *fuses*. A fuse, as the name implies, breaks during unprecedented market conditions and halts the trade, to allow the market to cool, or for the situation to be investigated.

Equivalent functionality, but in decentralized fashion, is provided by axo in programmable swap language. One can define their own fuse, which upon breaking, takes the liquidity away from the market, and further might code a more complicated response in it, for instance, by trading the risky assets for the safe one, at the same time.

However, as much as fuses are useful, they are the last resort responses reserved for serious market conditions. Under normal market stress scenarios, one would often manage portfolio and inventory risk accordingly to the market risk parameters, which in the case of axo, can be managed the same way as fuses, but under different conditions, and with gradual, rather than binary response.

14.4 Dynamic Risk Compensation

One can derive the current risk from the asset volatility (price fluctuations). Therefore, the stronger and more rapid the fluctuations, the higher the risk. We propose to dynamically adjust trading fees that go to market makers, based on volatility, to compensate for the current and implied risk level.

This is an efficient risk prevention mechanism, as it helps to cool the market, due to execution fees (going directly to market maker), compensating for on-going risk. Also, to some extent, during normal market conditions (e.g., when the volatility is not related to a big announcement where the fundamental value of the asset changed significantly, e.g., dropped to 0), this mechanism is able to put market makers in a risk neutral position (remove risk from providing liquidity).

Finally, in the extreme case, of the disclosure of new information in the market (e.g., a project turning out to be a scam and token fundamental values changing to 0 in a blink of an eye), risk management would be covered by *market maker fuses*, outlined in subsection 14.3.

Be that as it may, there is one more thing that can be done to protect market makers in the face of an extreme event, where one of the assets suddenly loses all of its value, namely arbitrage.

14.5 Token Trust Scores & Whistleblowing

All Cardano-native assets have a unique *PolicyId* which allows the unique identification of the assets. *PolicyId* is often used, on NFT trading platforms, to confirm that a specific image belongs to the official collection. That same mechanism can essentially be used for approved tokens, confirming that the token in question is an official one.

However, there is much more information that can be attached to *PolicyId* such as

- mint information (how many tokens have been minted, is the policy locked, etc.);

- information about the project (website, white paper, etc.);
- information provided by the community.

The last point, information provided by the community, can be especially effective at performing the role of project information aggregation, as users share:

- good signs about the project;
- suspicious activity;
- and even in extreme cases, whistleblow an on-going scam.

The information provided by the users could be compiled down into a trust score and provided alongside the tokens, and all objective information could be included alongside the score for each user's review.

14.6 Quantification of Risk

There are many ways to quantitatively assess the risk[131]. The most popular methods are:

- Markowitz's Modern Portfolio Theory (MPT) with the portfolio's returns defined as $\mu_p = \sum_{i=1}^{N} w_i \mu_i$ and portfolio's variance as $\sigma_p^2 = \sum_{i=1}^{N} \sum_{j=1}^{N} \sigma_{ij} w_i wj$. Portfolio might include a single liquidity pool with the desired risk profile of σ_p.
- Capital asset pricing model with $\mu_i = R_f + \beta_i(\mu_m - R_f)$ and $\beta_i = \frac{\sigma_{im}}{\sigma_m}$ where R_f is the risk-free rate of return (in the case of Cardano the current ROI on staking in a typical pool), μ_m is expected market return, β_i is the beta coefficient of asset i, and σ_{im} is covariance of asset i in the market m and σ_n is the standard deviation of such market.
- Value at Risk (VaR) which simplifies the question of potential loss compared to both above models to the question "How much can one expect to lose, given cumulative probability ζ, for the given time horizon T, defined as $F(Z(T) \leq \text{VaR}) = \zeta$, where F is cumulative distribution function, $Z(T) = S(0) - S(t)$ is the loss for an asset S at time t, and ζ is a cumulative probability function associated with threshold value VaR, on the loss distribution of $Z(t)$.
- Coherent risk measures such as CVaR (Coherent VaR), defined as $\text{CVaR} = E[Z(T) \mid Z(T) > \text{VaR}]$ and copulas.

All the above risk metrics can be used both in portfolio construction and rebalancing. It is worth noting that, for the sake of risk management, portfolio can refer to almost anything, most importantly including liquidity pool where it is used to actively balance the risk of AMM providing liquidity to the market. Note that this mechanism offers means for automated risk management (for the risk appetite defined by the user) using programmable swaps and Algorithmic AMM.

14.7 Moment Indicators

As outlined in section 6, moments of price distributions are the base for all the derived risk metrics and multiple trading indicators. As such, it is important to visualize the realized and implied volatility of the assets in the market, and both give the user visual indication of historical volatility, as well as allow them to define their own balancing mechanism in *programmable swaps* where desired. Moment based indicators provide the most verbose building components for the creation of automated risk management strategies.

15 axo Protocol Settlement Layer

axo aims to become the execution engine (settlement layer) for the financial world. *programmable swaps* will perform automated trading. We will keep all settlement on-chain, the protocol needs to solve a unique set of challenges in decentralization, memory throughput, and execution costs.

The largest DEXs, such as Uniswap, are able to reach a volume of 100,000 swaps per day, which as blockchains go is an impressive number, but this happens at a very high average execution cost, currently around 30 - 100 USD per transaction, and fades in comparison to TradFi, where millions of trades are executed every minute. We present the comparison of exchange trading volumes in Table 1.

Table 1: Exchange Amount of Transactions per Day, Week, and Month.

Exchange	Exchange Type	Average Transactions Per		
		Day	Week	Month
Uniswap v2	Ethereum DEX	50,288	352,000 [138, 139]	1,508,640?
Uniswap v3	Ethereum DEX	17,858	125,000 [138, 139]	535,740
Uniswap Total	Ethereum DEX	68,149	477,000 [138, 139]	2,044,470
SushiSwap	Ethereum DEX	17,869	125,080 [138, 139]	536,070
Binance	Crypto CEX	473,000 [141]	3,311,000	14,190,000
Nasdaq	TradFi CEX	26,390,296 [142]	131,951,480	580,586,512

15.1 axo as Scaling Layer for Cardano-native Projects

The extensible nature of *programmable swaps* and our concurrency solution reaching theoretical limits of scalability, means that in the future all Cardano-native projects will be able to utilize axo protocol to scale their own protocols. For instance, let's take minting NFTs, which currently requires all creators to prepare a scalable mint process and additionally might exceed the current mempool size (equal to 2 blocks, i.e. $2 \cdot 65$kB). This could be addressed by creating a mint contract using a programmable swap (swap X ADA for randomly selected NFT using random number generator (RNG) oracle). Such a contract would be easy to implement and could even be done using a graphical user interface (GUI). We would utilize a hydra head scaling solution and optimal concurrency, leading to the creator being able to focus on the art and community building, while outsourcing the minting process to axo protocol, where they would benefit from available scalability and low transaction costs.

This is just a single example, but we see this model extending to many more use cases.

16 High-Frequency Data Lake & Lab

Strategy development, testing, and execution requires quality sources of data.

- on-chain price oracles based on asset valuation model as outlined in section 6; those oracles will provide high quality and accurate indicators from asset price to a wide range of indicators, most importantly moment-based ones, fundamental for writing algorithmic trading strategies;
- data lab – data warehouse and live data streams interactions, generalized strategy writing API, and is a convenient way to perform backtesting and simulations.

Access to data will involve the use of AXO utility token for the higher levels of consumption.

17 On-chain Hedge Fund

axo's *programmable swaps* provide a unique mechanism for implementation of an on-chain *hedge fund*. Hedge fund refers to a pooled investment, taking advantage of sophisticated trading strategies and risk management techniques, in an attempt to improve performance above the index benchmark.

17.1 On-Chain Portfolio Managers

axo will create a market for trading strategies by enabling the publication of one's *programmable swaps* and setting a *performance based fee*, for instance 1% of all revenue generated using the strategy. PMs are going to be incentivized to create and publish trading strategies, because of the *performance based fee* they are going to be able to earn, and platform users will be incentivized to lock funds into *strategy vaults* by being able to see strategies' historical performance and PM's rankings[24, 27].

PMs via axo platform will have access to sophisticated tools such as high-frequency and quality data feeds, a backtesting platform, and a wide array of financial instruments to implement strategies, from indexes and synthetics, to financial derivatives and options strategies.

18 DeFi Education Portal

We estimate that only about 3% of cryptocurrency holders actively engage in using DeFi products. Moreover, approximately 80% of those users report that they do not understand / would like to better understand impermanent loss, capital efficiency, and how to quantitatively assess their decisions. What is more, the cryptocurrency market has one of the weakest forms of EMH.

We see it as essential, next to providing sound investment products, to provide observations and orientation (see OODA – Observe-Orient-Decide-Act loop [130] to learn more about this framework of thought) to the users of DeFi platforms, in order to be able to take better actions and to create a feedback loop by visualising the available telemetry. One of those 3 key components is the development of an incentivized DeFi educational platform.

axo is going to create a platform for users to create DeFi-related educational content. The views, engagement level, and kudos will then be used to allocate a portion of AXO tokens to articles based on their popularity and usefulness. This is going to create a financial incentive for people with experience in the field to create quality content, and share it with the community.

On top of that, axo team is going to publish a series of free articles (not participating in the outlined above token allocation) explaining many of the key concepts in DeFi.

In the future, we see the DeFi educational portal also being used for publication of market research, potentially with different funding models other than for free (the creation of high-quality research requires a lot of work, so a subscription-based model might be introduced for experienced and high-volume publishers).

Finally, throughout the axo platform, users will be able to find references to this educational content, to be able to get information when they need it the most. Some of that research will be further published by the axo team for free, based on the unique insights available to our DeFi platform, embedded in all kinds of market making, across many financial instruments.

19 Tokenomics

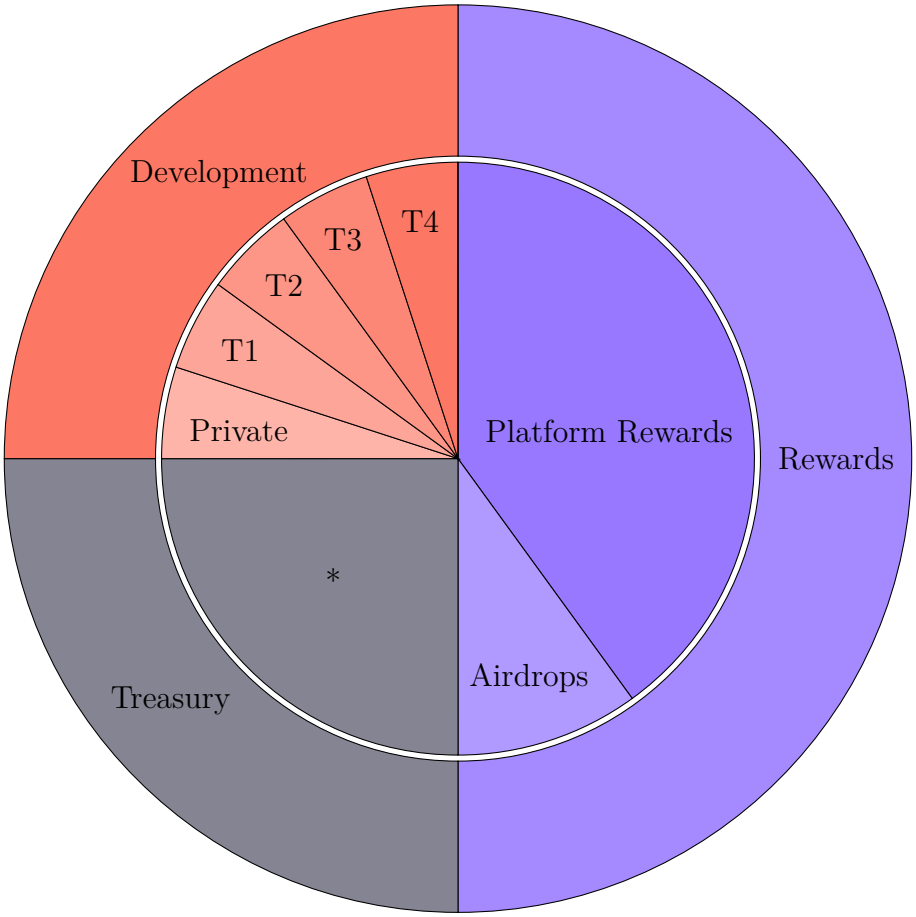
axo platform has a Cardano-native token called AXO. AXO token is the platform's governance token and enables access to certain functionalities. AXO has a fully diluted supply of 42,000,000 and approximately a 5 year gradual vesting period.

19.1 AXO Token Distribution

AXO token is allocated in the below percentages:

- 25% allocated for development; with 5% vested every year, over a total period of 4 years; and 5% separately allocated to private sale;
- 25% treasury reserves;
- 50% incentivization rewards, 40% reserved for rewards for using the platform, such as yield farming, DeFi educational content creation, etc., and 10% reserved directly for the airdrops to incentivize and reward actions outside of the mentioned ones (e.g., reward for moving liquidity from different exchange, reward for having used the platform before date X, staking to certain pools, promotion, etc.).

Figure 26: AXO token allocation.



19.2 AXO Token Vesting Schedule

AXO token has the following vesting schedules:

- development fund will vest over 4 years;
- portion of development funds reserved for the private sale will have its own discretionary vesting period;
- treasury will unlock gradually;
- platform rewards will unlock gradually to incentivize specific behaviors (providing new liquidity pairs, creating healthy liquidity, content creation, etc.); it will take multiple years for all rewards to be distributed;
- first airdrops will unlock around the platform launch to the early adopters and supporters;
- airdrops will be applied in response to specific events, it will be gradual, and only small portions will be used at times.

The initial supply will be comprised of $4,200,000$ AXO coming from the early adopter airdrop, an initial liquidity bonding, private sale, and team allocation.

19.3 AXO Token Utility

AXO token is currently designed to provide the below utility (but in the future might include additional utility):

- consumption of on-chain oracles;
- one of the rewards to DeFi educational content creators;
- access to a series of professional data;
- governance through on-chain voting via the ability to suggest changes to the protocol and create (and vote on) proposals to allocate Treasury funds for future protocol development

19.4 axo Treasury

AXO collected from protocol utilization outlined in subsection 19.3 will go into axo treasury, where they will be used (among other purposes) to:

- fund protocol development and research;
- fund the platform infrastructure;
- be distributed to the platform users in the form of incentives (once the initial 5 year supply of reward allocation is exhausted the incentives will be funded from the treasury);

- provide AXO incentives for creation of mathematically sound liquidity pools and instruments;
- be used to fund the rewards distribution for DeFi educational content writers.

Healthy inflow of AXO tokens from the protocol usage and its reinvestment into the platform will lead to a very healthy positive-feedback loop. Further, the treasury shall be managed (for instance by locking into one of programmable swaps trading strategies) to optimize its performance against the market.

Acronyms

AMM Automated Market Maker (AMM). 10, 15, 16, 18–20, 31, 43, 44, 46, 47, 65, 67, 81

CEX Centralized Exchange (CEX). 14

CFMM Constant-Function Market Maker (CFMM). 10, 13–15, 17–19, 43–47, 49, 50, 81, 84

dApp Decentralized Application (dApp). 27, 82

DCA Dollar-Cost Averaging (DCA). 29, 38, 39, 41, 78, 79

DDoS Distributed Denial of Service attack (DDoS). 29, 78

DeFi Decentralized Finance (DeFi). 12, 13, 21, 52, 54, 72, 73, 75, 81, 84, 85

DEX Decentralized Exchange (DEX). 15, 20, 30, 42, 50, 51, 54, 63, 69, 78, 80, 84

DSL Domain-Specific Language (DSL). 30, 38, 39

EMH Efficient Market Hypothesis (EMH). 13, 14, 43, 65, 72

EUTxO Extended Unspent Transaction Output Model (EUTxO). 18, 20, 27–36, 38, 51, 52, 63

FPGA Field-Programmable Gate Array (FPGA). 13

HFT High-Frequency Trading (HFT). 12

MEV Miner Extractable Value (MEV). 77

NFT Non-Fungible Token (NFT). 26, 28–30, 54, 66, 69

P&L Profit & Loss (P&L, PnL). 30, 83, 85

PAB Plutus Application Backend (PAB). 27, 83

PM Portfolio Manager (PM). 38, 71

QuantFi Quantitative Finance (QuantFi). 12, 43, 47

SPO Stake Pool Operation (SPO). 42, 84

TradFi Traditional Finance (TradFi). 12–14, 18, 21, 38, 43, 54, 65, 66, 69, 81, 83, 84

TVL Total Value Locked (TVL). 18, 47, 78, 84

Glossary

account-based model A ledger model used by Ethereum, and majority of smart contract enabled blockchains, where the global state is shared, and all operations are applied sequentially, one after the other based on tips. Due to possible impact on the ordering of transactions via tips it is prone to front-running and *Miner Extractable Value* (MEV).. 43

Amdahl's law The theoretical speedup limit in the latency of the execution of a task at fixed workload that can be expected of a system whose resources are improved, it also is used to define the theoretical limit of the system scalability due to improvements in concurrency and parallelism of the system. Amdahl's law is defined as $S_{\text{latency}}(s) = \frac{1}{(1-p)+\frac{p}{s}}$.. 28, 30, 78

arbitrage Exploiting the market inefficiency between trading venues (exchanges); in the most simple case of the arbitrage, let's say ADA is priced at $3 at exchange A and at $2.95 at exchange B. The arbitrage bot will find this information and will attempt to buy ADA at exchange B for $2.95 and sell it immediately at exchange A at $0.05 profit per ADA. The act of arbitrage moves the price, as after the execution, the price at exchange B will be higher (e.g., $2.98) due to purchasing the discounted ADA, and on exchange A it will be cheaper due to selling it (e.g., $2.98). As long as there is a price difference between exchanges, so that when these trades are executed they are more profitable than the execution cost, arbitrage is possible. Arbitrage leads to all included exchanges converging on the central limit value (true market sentiment from the aggregated exchanges) of the asset price. The arbitrageur earns profits by buying at a discount from exchange B and selling at a premium on exchange A. Hence both exchange B sellers and exchange A are the source of income for the arbitrage bot and are "victim" of the market inefficiency (in reality, they are not victims but simply prone to be scalped this way). Finally, the mentioned example is the most basic case of arbitrage (pure arbitrage). There are a multitude of arbitrage styles, including statistical, where arbitrage is based on the market movement predictions and the average expectation of reward https://en.wikipedia.org/wiki/Arbitrage#Types. Arbitrage leads to efficient price discovery, but at the cost of market participants (both takers and makers).. 23, 63, 78

Automated Market Maker (AMM) A liquidity definition as a supply formula enabling automatic (autonomous - without the presence of maker) trades, preserving certain properties such as path independence (the execution price is not depending on the history of transactions), and for trading without any active interaction from the maker party (makers provide assets into the liquidity pool which are then managed based on pool model / formula).. 76

benchmark Benchmark is an investment performance measuring tool, used to assess the allocation, risk, and return of the portfolio[29]. Benchmarks are usually constructed using unmanaged indices and exchange-traded funds (ETFs). Benchmark is selected in a way to represent asset class against which one wants to compare the outcomes.. 71

black swan event The black swan theory or theory of black swan events is a metaphor that describes an event that comes as a surprise, has a major effect, and is often inappropriately rationalized after the fact with the benefit of hindsight.. 45, 50, 65

capital efficiency Each task has many ways of being performed, one way will consume more resources (energy, time, etc.) than the other, hence the way which consumes less resources and achieves the same result is more efficient. The more efficient use of capital the better generated returns, the better user experience, and the better the actual state of the market is reflected.. 18, 21, 43, 52, 53, 72

Centralized Exchange (CEX) Classical model of an exchange where agents engage into buying and selling via the intermediary (the exchange), as opposed to DEX where investors face each other via the protocol implementation.. 76

concurrency The act of progressing on the same task by multiple agents at the same time, which implies communication between agents. Concurrency speed improvement is limited to the bottlenecks in agent communication and defined by Amdahl's law.. 77

Constant-Function Market Maker (CFMM) A liquidity provision formula that has assets on one side and a constant on the other. The most widely known CFMM is Uniswap's v1/v2 $x * y = \text{const}$ [5, 6]. The critique of this liquidity formulation include unrealistic provision range (assumption that it is equally likely to provide liquidity (make the market) when the asset that costs $20 (e.g., a pizza pie) at price of $0.000001 and $1,000,000,000. This inefficiency leads to high impermanent loss and requirement for high TVL to avoid high slippage, which leads in turn to market inefficiency and creating a huge potential for arbitrage.. 76

Decentralized Application (dApp) An application that runs on a Decentralized computing system, such as Cardano blockchain.. 76

Decentralized Exchange (DEX) Non-custodial exchange model, where trades are executed directly on the smart contract blockchain. DEX does not have intermediary, responsible for providing the service for exchanging assets, but rather it is performed in automated manner by participants providing assets for the code to access (governed by code rather than company).. 76

Decentralized Finance (DeFi) Blockchain-based form of finance, removing the need for the centralized intermediaries required to provide the service in the traditional finance, such as brokerages, exchanges, and banks. In DeFi the role of intermediary is replaced by smart contracts.. 76

Distributed Denial of Service attack (DDoS) A form of attack on the Internet infrastructure, where the attacker aims to exhaust the available resources of the target by the shere volume of the traffic created. DDoS usually results in the targeted service being unavailable for the duration of the attack.. 76

Dollar-Cost Averaging (DCA) An investment trading system employed to minimise the impact of local price fluctuations on the average buy-in-price. A person following DCA trading system would purchase the same amount of the target asset

(e.g., ADA), at equal interval (e.g., every day), for the same amount of the source currency/asset (e.g., USD). There are more sophisticated forms of DCA available, for instant, weighted DCA in which the amount bought at the equal interval (e.g., every day / week) is adjusted by the weight parameter w computed from the market indicators (e.g., divergence indicator indicating local maxima and minima). In the case, of divergence indicator, the weight w would be higher near local minima and lower at the local maxima, resulting on average in better performance of the trading system.. 76

Domain-Specific Language (DSL) A computer language specialised to a particular application domain, e.g., the language for defining axo *programmable swaps*.. 76

Efficient Market Hypothesis (EMH) A hypothesis stating that the prices in the market reflect all of the information available, in practice it is rarely true. A straightforward example is Dogecoin rising to the top 10 and firmly remaining there based on a series of tweets with no substance behind them. Even a rebuttal from the Dogecoin development team did nothing to stem the rise. The market ignored this information and irrationally valuated Dogecoin at a higher price. This does not reflect the fundamental information available in the market and is an extreme case of market inefficiency. In traditional finance, research would be published showing its shortcomings, people would evaluate the study's validity, and would short such an overvalued company. If an asset were to be severely undervalued, a leverage or long option would be bought, significantly magnifying the potential returns from the efficient use of information. Under the Efficient Market Hypothesis, assets would be priced at what they are truly worth, and there would be very little difference in the asset prices between exchanges. On the contrary, market inefficiency is such a commonly occurring phenomenon that a whole field of study is dedicated to measuring it and adjusting trading strategies based on it. Inefficiencies take root from lack of information flow between exchanges (e.g., via arbitrage) and irrational decision-making (modeled well by behavioral investing). This is not a problem without a solution, it is merely the result of the environment emerging from inefficiencies of the exchanges and the irrationality of the actors in the market.. 76

Extended Unspent Transaction Output Model (EUTxO) Accounting model used by Cardano where all assets are stored in EUTxOs (boxes) that can be spent either using private key (e.g., wallet transactions) and (Plutus) script (private key and script are locked on the box). The wallet balance is the sum of all EUTxOs that the wallet can spend. In the EUTxO model each EUTxO has to be spent when used, hence can be only used once per block (20s).. 76

Field-Programmable Gate Array (FPGA) Programmable hardware circuit composed of programmable building blocks and a hierarchy of reconfigurable interconnects allowing blocks to be wired together. FPGA is programmed in hardware description language (HDL) and once encoded behaves as an integrated circuit designed to perform a specific functionality. FPGA are used to write programs directly into silicon, significantly improving processing speed and allowing for many hardware optimisations. The only step further is ASIC (Application-Specific Integrated Circuit) which requires a fab (factory configuration to produce ICs), hence in all the

special and often changing cases, prohibitively expensive (e.g., in HFT where the algos are constantly updated and improved).. 76

front-running Process of using the existing knowledge of submitted orders (e.g., by scanning mempool) to tip the exchange / protocol, with the aim to insert your order (based on existing information) ahead of other orders, in order to capitalize on this knowledge. For instance, spot a whale swap, tip the protocol to insert transactions before in the block, buy at the cheaper price, allow the whale order to move the market (whale pays more for the order), tip for 2nd order to be placed after the whale order, sell immediately for higher price.. 77, 81

hedge Hedging is the practice of taking a position in an inversely correlated asset/market to offset the risk taken by assuming position. Hedging might take many forms, but always leads to reduction in the overall position risk. For instance, when shorting stock using options, assuming also long position in the underlying.. 54, 65

hedge fund A pooled investment fund, often trading in relatively liquid assets, and able to make extensive use of sophisticated trading, portfolio construction[24, 27], and risk management strategies in an attempt to improve performance, especially improve the performance above index benchmark, by generating alpha without taking on more risk (i.e., achieving higher Sharpe ratio).. 38, 71

High-Frequency Trading (HFT) Sophisticated algorithmic trading methodology characterized by high speeds (microsecond level), exchange co-location, high trade volumes, and high order-to-trade ratios. HFT most frequently utilizes the local market volatility and heavily relies on momentum-based indicators and derives its revenue from the trade volume and being right more often than wrong approach, compounded over millions of trades executed. HFT does not consume significant amounts of capital, nor accumulate positions, or hold portfolios overnight, and as such the results have some of the highest Sharpe ratios (reward to risk ratio) in the market. HFT is often seen as a method of providing liquidity to the market as most HFT algos will trade both sides tightly around the spot price. 76

impermanent loss Loss of capital when compared to HODLing due to inherent flaws of liquidity pool formula. The worst offenders are ironically the most popular family of constant-product pools such as Uniswap's v1/v2 $x * y = \text{const}$[5, 6]. It occurs when providing a pair of assets into a liquidity pool, as the rations of x and y change in the pool and the more the prices diverge, the bigger the impermanent loss. At some point, around the 20-50% threshold (the range is large due to inherent typical crypto volatility), actually holding the 2 separate assets outside of the pool would have been a better investment. It is made even worse by the incentivization of yield farming to create the most negatively correlated pools there are possible (completely deflationary crypto such as ADA and completely inflationary fiat such as USD). Those two assets will naturally diverge and create the impermanent loss. In a sense, there's a sizeable hole in the bucket through which the total value of your deposited funds will leak. This is made even worse by many DEXs being either only concerned with increasing the amount of transactions (in order to obtain more fees from transactions) or being completely oblivious to this obvious mathematical fact (DEX are generally built without regard to quantitative modelling). . 13, 18, 19, 21, 43–46, 53, 72, 78

index An index is a method to track (and replicate) the performance of a group of assets in a standardized way. Index typically measure the performance of a basket of assets intended to replicate a certain area of the market.. 54, 71, 80

limit order A limit order is an order to buy or sell stock at a specific price or better. A limit order ensures execution at the specified price (or better), but does not guarantee how quickly the order will be executed, or if at all. Limit orders are ideal when the primary goal is to execute at specific price, once that price is available.. 23, 29, 33, 37–39, 41

liquidity Ease of exchanging one asset for the other without affecting the asset price, at the perceived current market value. Naturally the most liquid asset category are fiat currencies, and the most liquid among them USD, which can be exchanged for many assets around the world; it is used in international settlements, and the payments performed by individual organisations, regardless how large, do not affect the price of USD.. 12, 13, 15, 18, 19, 30, 35, 43, 44, 47, 50, 51, 67, 81

liquidity pool A method of providing liquidity to the market via crowdsourcing it from among many participants into one shared pool, usually in the form of AMM.. 17, 19, 29, 32, 34, 37, 41, 43–48, 50, 51, 63, 67

market maker A party providing liquidity to the market (e.g., via liquidity pool), either by depositing assets into liquidity pool, usually constant formula pricing assets, in the case of DeFi, or via sophisticated market making tools and algos in the case of TradFi. Market makers create efficient market to transact in, ensuring good experience of market takers.. 12, 13, 17, 18, 20, 33, 35, 38, 45, 46, 49, 50, 65, 66, 81

market order A market order is an order to buy or sell a stock at the market's current best available price. A market order typically ensures an execution, but it does not guarantee a specified price. Market orders are optimal when the primary goal is to execute the trade immediately.. 29, 31, 33, 34, 38, 39, 41

market taker Any party exchanging assets on the market, and hence taking the liquidity from the market, or in other words taking the service provided by market makers. They expect the exchange prices to reflect the true prices of assets, low slippage (price change during trade execution), and ability to exchange assets on demand.. 12, 13, 33, 35, 38, 50, 81, 84

Miner Extractable Value (MEV) A measure of potential profit available to miners (validators, sequencers, etc.), arising from the ability to arbitrarily include, exclude, and re-order transactions. For instance, the existence of MEV enables front-running.. 76

model A mathematical description / definition of system, e.g., liquidity model defining how liquidity pool models market dynamics in the response to trades. However, even a poor model can be used for the purpose of modelling, but it will suffer from many inefficiencies (lagging behind the actual state, being too sensitive / having too high inertia, etc.). All CFMM AMM are poor liquidity models.. 43

money ≡ energy When modelling financial systems you can think of money as a unit of energy, same as in physics, we can think of kinetic, potential, and other energies, energy is potential to perform a certain amount of work; we can think of money in the same way. Money has potential to be applied in the market, from lending to businesses developing novel ideas, increasing market efficiency by providing liquidity to exchanges, creating information flow via arbitrage, financial analysis and research, to utilising available information to maximise returns given a specified risk appetite. Energy can be applied in many ways. If we choose a very inefficient way to do something e.g., growing tomatoes in a completely dark underground bunker, we will expend a lot of energy. In contrast, we can put them in a greenhouse or even on a balcony and make much more efficient energy use. Same in the capital markets, efficient models lead to high money utility (energy well spent towards productive work), and productive work is the work that is usually associated with rewards (e.g., business borrowing money will pay it with interest). Therefore, an efficiently allocated liquidity will work very well even with low total value locked and respond quickly to the changing market dynamics, bringing higher rewards per unit of capital.. 43

Non-Fungible Token (NFT) Is a unique and non-interchangeable unit of data (most often JSON) stored on the blockchain. NFTs are most often used to store images, and do so via 721 standard defining the JSON template. However, NFTs have many uses, such as storing wallet handles, and even could be used to store *programmable swaps* code of **axo** (the only limitation in this case being minimum ADA requirement to prevent the dusting attack).. 76

off-chain Everything that is not on-chain, most often implies off-chain code of dApp smart contracts.. 10, 18, 22, 27, 28, 30, 41, 83

off-chain code Cardano introduces the concept of Turing-complete off-chain code, that computes the necessary state update for the user taken action, and provides it to Cardano wallet for submission onto the ledger.

In contrast to blockchains without safe off-chain component, it provides the ability to write off-chain code in any existing programming language (as long as bindings to Plutus exist, e.g., via an SDK), and provide any functionality without outsourcing the high execution cost on the users (e.g., via fee mechanism).. 18, 20, 27, 30, 82

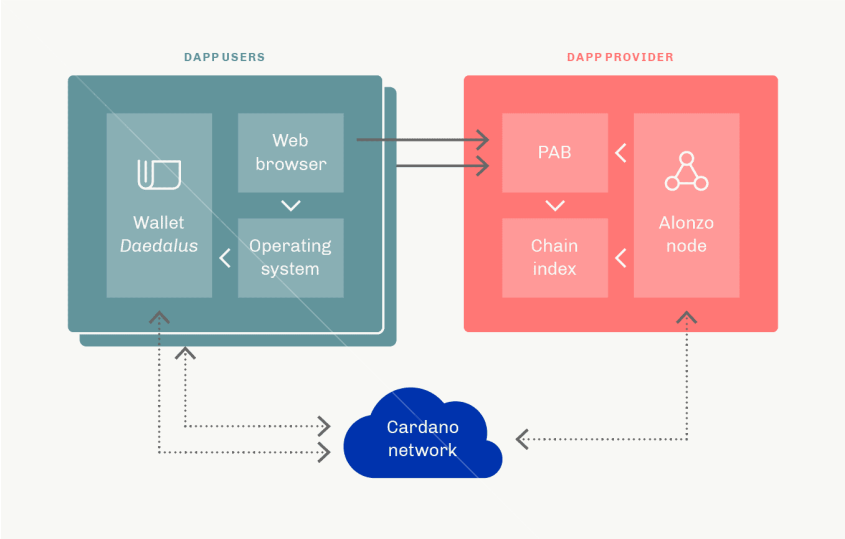
on-chain Action executed by the validator nodes or an asset stored on the ledger.. 17, 20, 22, 27, 30, 49, 51, 63, 69, 83

on-chain validator A part of smart contract code stored on Cardano ledger and used to validate submitted transactions. In contrast to other blockchains where all smart contract actions are performed on-chain, in the case of Cardano, a transaction is prepared by off-chain code and validated if it is spendable and meets all spending conditions, by block producing nodes, on layer 1.. 18, 20, 27, 30

parallelism The act of splitting a task into s, independent, subtasks, all of which can be executed independently of each other, implying that there is no communication required between agents executing the subtasks.. 25, 28, 77

Plutus Application Backend (PAB) An off-chain dev tool allowing for the interaction with smart contracts. PAB allows for interaction with external clients, such as wallet front-ends, and acts as the intermediary between Plutus application, the node, the wallet back-end, and end users. The purpose of PAB is to provide a standardised environment to run Plutus applications, with disciplined state management, discoverable interfaces by external clients (primarily wallets), track on-chain information that smart contract uses, and deal with requests such as running contract instances, forwarding user input to those instances, and notifying these instances of ledger state change events.

Figure 27: Plutus Application Back-end schematic.



. 76

Portfolio Manager (PM) An experienced professional responsible for making and carrying out investment decisions on behalf of vested individuals or institutions. Clients either invest directly into portfolio manager's investment strategies[27, 26, 29], or vest their funds with the investment institutions, that has multiple portfolio managers working for it, and managing investors' money.. 76

Profit & Loss (P&L, PnL) A financial statement summarising the revenues, costs, expenses, and losses of a given period. In trading *realized* and *unrealized* P&L is distinguished, *realized* P&L refers to closed positions, where *unrealized* P&L refers to the current profits and losses on the open positions (e.g., not matured options).. 76

Quantitative Finance (QuantFi) Statistical branch of mathematics concerned with modelling financial markets for the purpose of investment management. Quantitative finance enables modelling of complex stochastic (random processes) and building efficient models and accurate predictions. QuantFi is used heavily in TradFi in modelling markets, managing risk, making both automated and manual investment decisions, to name a few.. 76

Sharpe ratio Reward to risk (variability) ratio measuring the performance of an investment as compared to a risk-free asset, after adjusting for the risk (defined as standard deviation of the investment, i.e. volatility). The formula is named after William Sharpe, its inventor, and defined as $S_a = \frac{E[R_a - R_b]}{\sigma_a}$., where R_a is the asset return, R_b is risk-free return, $E[R_a - R_b]$ is the expected excess return, and σ_a is the standard deviation of the asset excess return. 19, 65, 80

slippage The difference between the expected execution price of a trade and the price at which the trade is actually executed. Slippage occurs most frequently in TradFi during the periods of high volatility when the price shifts quickly. In DeFi, due to inefficient liquidity provisioning methods slippage is common, for instance in, DEXs using cfmm, resulting also in a high requirement for TVL to decrease the execution costs (slippage).. 15, 41, 42, 81, 84

Stake Pool Operation (SPO) Running PoS (proof of stake) blockchain validator nodes. In the case of Cardano, it implies running block producing node connected to P2P (peer to peer) network of Cardano nodes (at the time of writing P2P feature is still under the development and relies on the central registry of relays) via SPO operated relays.

SPO upon correct registration on the ledger and depending on its total delegation and pledge, is going to be assigned the role of slot leader during each epoch. Each validated slot and block produced results in SPO rewards that are then distributed between delegators and the stake pool operator according to the pool's *fixed fee* (usually 340 ADA) and *variable fee*. Out of the profits from producing blocks, fixed_fee + variable_fee · total_rewards is allocated to SPO, and the rest is distributed among delegators, in direct proportion to delegation (e.g., if delegator provides 1% of all delegation in the pool, she will receive 1% of all remaining rewards after SPO receive its share).

SPOs receive rewards, in accordance to fixed_fee and variable_fee to cover the operation costs (including the human labor), and in the case of ISPOs and mission driven pools is a form of delegators to support specific cause and projects.

Also frequently abbreviation of Stake Pool Operator, both terms basically having the same meaning (the entity / activity of operating stake pool).. 76

Total Value Locked (TVL) Total capital amount locked into specific contract (liquidity pool). For inefficient liquidity curves such as CFMM TVL is important as it reduces the effect of slippage and volatility. However, high TVL is not only a good metric, in the case of TVL that's too high, the price will be resistant to update and present a loss for market takers and opportunity for arbitrage.. 76

trading system A trading methodology, based on market data, trader's experience, research, etc., that defines a systematic approach to take as the reaction to different market conditions. Trading systems are great in detaching emotions (which often lead to bad trades) from decision making process. System usually defines the position that the trader should take given the current market scenario, but can

be much more precise and implemented as automated trading algorithm. Trading using defined systems usually leads to better trader's performance (P&L.. 78, 79

Traditional Finance (TradFi) A phrase to contrast a traditional way of providing financial services via a centralized intermediary vs Decentralized approach of DeFi applications. TradFi represents traditional financial service providers such as brokerages, exchanges, market makers, and banks.. 76

References

[1] Simon Peyton Jones et al. Composing Contracts: An Adventure in Financial Engineering. URL: https://www.cs.tufts.edu/~nr/cs257/archive/simon-peyton-jones/contracts.pdf. Accessed on 2021/04/26.

[2] Cryptopedia. What Are Automated Market Makers? URL: https://www.gemini.com/cryptopedia/amm-what-are-automated-market-makers. Accessed on 2021/04/22.

[3] Vitalik Buterin. On Path Independence. URL: https://vitalik.ca/general/2017/06/22/marketmakers.html. Accessed on 2021/04/22.

[4] Emin Gün Sirer and Phil Daian. Bancor Is Flawed. URL: https://hackingdistributed.com/2017/06/19/bancor-is-flawed/. Accessed on 2021/04/22.

[5] Uniswap v1 Protocol Hayden Adams et al. Novembrer 2018. URL: https://docs.uniswap.org/protocol/V1/introduction. Accessed on 15/10/2021.

[6] Uniswap v2 Core Hayden Adams et al. March 2020. URL: https://uniswap.org/whitepaper.pdf. Accessed on 15/10/2021.

[7] Uniswap v3 Core Hayden Adams et al. March 2021. URL: https://uniswap.org/whitepaper-v3.pdf. Accessed on 15/10/2021.

[8] James Chen. What is an Index? URL: https://www.investopedia.com/terms/i/index.asp. Accessed on 2021/04/22.

[9] Mirror: assets reflected on the blockchain main page. URL: https://mirror.finance/. Accessed on 2021/04/22.

[10] Mirror Protocol: A trading and liquidity protocol whitepaper. URL: https://mirror.one/Mirror_Protocol_Whitepaper.pdf. Accessed on 2021/04/22.

[11] Synthetix - the derivatives liquidity protocol main page. URL: https://synthetix.io/. Accessed on 2021/04/22.

[12] Synthetix Litepaper. Version: 1.4 (March 2020). URL: https://docs.synthetix.io/litepaper. Accessed on 2021/04/22.

[13] The Maker Team. The Dai Stablecoin System. December 2017. URL: https://makerdao.com/whitepaper/DaiDec17WP.pdf. Accessed on 2021/04/27.

[14] The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. URL: https://makerdao.com/en/whitepaper/. Accessed on 2021/04/27.

[15] Mirror: Reflecting Asset Value On-Chain. URL: https://docsend.com/view/kcsm42mqiyu5t6ej. Accessed on 2021/04/27.

[16] Samuel Brooks, Anton Jurisevic, Michael Spain, Kain Warwick. Synthetix White Paper. A decentralized payment network and stable coin v0.8. URL: https://www.synthetix.io/uploads/synthetix_whitepaper.pdf. Accessed on 2021/04/27.

[17] Synthetix Litepaper. Version: 1.4 (March 2020). URL: https://docs.synthetix.io/litepaper. Accessed on 2021/04/27.

[18] Edward M. Miller. Risk, Uncertainty, and Divergence of Opinion. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.667.5934&rep=rep1&type=pdf. Accessed on 2021/04/23.

[19] Vitalik Buterin. Token sales and shorting. URL: https://ethresear.ch/t/token-sales-and-shorting/376. Accessed on 2021/04/23.

[20] Akhilesh Ganti. Covered Call. URL:https://www.investopedia.com/terms/c/coveredcall.asp. Accessed on 2021/04/23.

[21] Itamar Drechsler. Qingyi (Freda) Song Drechlser. The Shorting Premium and Asset Pricing Anomalies. URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2387099

[22] Eliezer Yudkowsky. Inadequate Equilibria - Where and How Civilizations are Stuck? URL: https://equilibriabook.com.

[23] Options Volatility & Pricing. Advanced Trading Strategies and Techniques. Sheldon Natenberg. 2nd edition.

[24] Active Portfolio Management. A Quantitative Approach for Producing Superior Returns and Controlling Risk. Richard C. Grinold, Ronald N. Khan. 2nd edition.

[25] Derivatives - Models on Models. Espen Gaarder Haug.

[26] Systematic Trading. Robert Carver.

[27] Modern Portfolio Theory and Investment Analysis. Edwin J. Elton et al. 9th edition.

[28] The xVA Challenge. Jon Gregory. 3rd edition.

[29] Econometrics. Fumio Hayashi.

[30] Principles of Professional Speculation. Victor Sperandeo.

[31] Futures Markets. Robert W. Kolb. 3rd edition.

[32] Analysis of Financial Time Series. Ruey S. Tsay. 3rd edition.

[33] Asset Price Dynamics, Volatility, and Prediction. Stephen J. Taylor.

[34] Paul Wilmott on Quantitative Finance. Paul Willmot. 2nd edition.

[35] The Alchemy of Finance. George Soros.

[36] Money Changes Everything. William N. Goetzmann.

[37] Trading Volatility, Correlation, Term Structure, and Skew. Colin Bennet.

[38] Options, Futures, and Other Derivatives. John C. Hull. 8th edition.

[39] Nonlinear Option Pricing. Julien Guyon, Pierre Henry-Labordere.

[40] Modern Investment Management. An Equilibrium Approach. BOb Litterman and the Quantitative Research Group, Goldman Sachs Asset Management.

[41] Continuous-Time Finance. Robert C. Merton. Revised edition.

[42] Pricing and Trading Interest Rate Derivatives. A Practical Guide to Swaps. J. H. M. Darbyshire. Revised edition.

[43] Derivatives demystified. A Step-by-Step Guide to Forwards, Futures, Swaps and Options. Andrew M. Chisholm. 2nd edition.

[44] The Volatility Surface. A Practitioner's Guide. Jim Gatheral.

[45] The Man Who Solved The Market. How Jim Simons Launched The Quant Revolution. Gregory Zuckerman.

[46] The Complete Guide to Option Pricing Formulas. Espen Gaarder Haug. 2nd edition.

[47] Asset Pricing. John H. Cochrane. Revised edition.

[48] Modeling Derivatives in C++. Justin London

[49] Basic Stochastic Processes. Zdzisław Brzeźniak, Tomasz Zastawniak.

[50] Stochastic Differential Equations. Bernt Oksendal.

[51] Advances in Financial Machine Learning. Marcos Lopez de Prado.

[52] Investment Science. David G. Luenberger.

[53] Fractals and Scaling in Finance. Discontinuity, Concentration, Risk. Benoit B. Mandelbrot.

[54] Finding Alphas. A Quantitative Approach to Building Trading Strategies. Igor Tulchinsky et al.

[55] Brownian Motion, Martingales, and Stochastic Calculus. Jean-François Le Gall.

[56] Credit Risk. Darrell Duffiee, Kenneth J. Singleton.

[57] Stochastic Volatility Modeling. Lorenzo Bergomi.

[58] Risk and Asset Allocation. Attilio Meucci.

[59] Dynamic Hedging. Managing Vanilla and Exotic Options. Nassim Taleb.

[60] Tail Risk Hedging. Creating Robust Portfolios for Volatile Markets. Vinner Bhansali.

[61] Modelling Extremal Events: for Insurance and Finance. Paul Embrechts et al.

[62] Statistical Consequences of Fat Tails. Real World Preasymptotics, Epistemology, and Applications. Nassim Nicholas Taleb.

[63] The Price of Fixed Income Market Volatility. Antonio Mele, Yoshiki Obayashi.

[64] Options Trading. Pricing and Volatility Strategies and Techniques. Euan Sinclair.

[65] Chaos. The Amazing Science of the Unpredictable. James Gleick.

[66] Nonlinear Dynamics and Chaos. With Applications to Physics, Biology, Chemistry, and Engineering. Steven H. Strogatz. 2nd edition.

[67] Options Volatility & Pricing. Advanced Trading Strategies and Techniques. Sheldon Natenberg. 2nd edition.

[68] Active Portfolio Management. A Quantitative Approach for Producing Superior Returns and Controlling Risk. Richard C. Grinold, Ronald N. Khan. 2nd edition.

[69] Derivatives - Models on Models. Espen Gaarder Haug.

[70] Systematic Trading. Robert Carver.

[71] Modern Portfolio Theory and Investment Analysis. Edwin J. Elton et al. 9th edition.

[72] The xVA Challenge. Jon Gregory. 3rd edition.

[73] Econometrics. Fumio Hayashi.

[74] Principles of Professional Speculation. Victor Sperandeo.

[75] Futures Markets. Robert W. Kolb. 3rd edition.

[76] Analysis of Financial Time Series. Ruey S. Tsay. 3rd edition.

[77] Asset Price Dynamics, Volatility, and Prediction. Stephen J. Taylor.

[78] Paul Wilmott on Quantitative Finance. Paul Willmot. 2nd edition.

[79] The Alchemy of FInance. George Soros.

[80] Money Changes Everything. William N. Goetzmann.

[81] Trading Volatility, Correlation, Term Structure, and Skew. Colin Bennet.

[82] Options, Futures, and Other Derivatives. John C. Hull. 8th edition.

[83] Nonlinear Option Pricing. Julien Guyon, Pierre Henry-Labordere.

[84] Modern Investment Management. An Equilibrium Approach. BOb Litterman and the Quantitative Research Group, Goldman Sachs Asset Management.

[85] Continuous-Time Finance. Robert C. Merton. Revised edition.

[86] Pricing and Trading Interest Rate Derivatives. A Practical Guide to Swaps. J. H. M. Darbyshire. Revised edition.

[87] Derivatives demystified. A Step-by-Step Guide to Forwards, Futures, Swaps and Options. Andrew M. Chisholm. 2nd edition.

[88] The Volatility Surface. A Practitioner's Guide. Jim Gatheral.

[89] The Man Who Solved The Market. How Jim Simons Launched The Quant Revolution. Gregory Zuckerman.

[90] The Complete Guide to Option Pricing Formulas. Espen Gaarder Haug. 2nd edition.

[91] Asset Pricing. John H. Cochrane. Revised edition.

[92] Modeling Derivatives in C++. Justin London

[93] Basic Stochastic Processes. Zdzisław Brzeźniak, Tomasz Zastawniak.

[94] Stochastic Differential Equations. Bernt Oksendal.

[95] Advances in Financial Machine Learning. Marcos Lopez de Prado.

[96] Investment Science. David G. Luenberger.

[97] Fractals and Scaling in Finance. Discontinuity, Concentration, Risk. Benoit B. Mandelbrot.

[98] Finding Alphas. A Quantitative Approach to Building Trading Strategies. Igor Tulchinsky et al.

[99] Brownian Motion, Martingales, and Stochastic Calculus. Jean-François Le Gall.

[100] Credit Risk. Darrell Duffiee, Kenneth J. Singleton.

[101] Stochastic Volatility Modeling. Lorenzo Bergomi.

[102] Risk and Asset Allocation. Attilio Meucci.

[103] Dynamic Hedging. Managing Vanilla and Exotic Options. Nassim Taleb.

[104] Tail Risk Hedging. Creating Robust Portfolios for Volatile Markets. Vinner Bhansali.

[105] Modelling Extremal Events: for Insurance and Finance. Paul Embrechts et al.

[106] Statistical Consequences of Fat Tails. Real World Preasymptotics, Epistemology, and Applications. Nassim Nicholas Taleb.

[107] The Price of Fixed Income Market Volatility. Antonio Mele, Yoshiki Obayashi.

[108] Options Trading. Pricing and Volatility Strategies and Techniques. Euan Sinclair.

[109] Chaos. The Amazing Science of the Unpredictable. James Gleick.

[110] Nonlinear Dynamics and Chaos. With Applications to Physics, Biology, Chemistry, and Engineering. Steven H. Strogatz. 2nd edition.

[111] Vitalik Buterin. "Let's run on-chain decentralized exchanges the way we run prediction markets" Reddit post from 2016/10/03. (The consideration of more traditional buy-side / sell-side order book model and the inception of the famous x * y = k AMM model). URL: https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way/. Accessed on 2021/04/22.

[112] Nick Johnson. Euler: The simplest exchange and currency. (Euler: e^n pricing model for providing tokens from LP. Initial price determination via distributed farm offering). URL: https://www.reddit.com/r/ethereum/comments/54l32y/euler_the_simplest_exchange_and_currency/. Accessed on 2021/04/22.

[113] Gemini market making model. (buy/sell order submission in the time-window, matching at the end of the time window, more efficient price discovery via auction system). URL: https://www.gemini.com/fees/marketplace. Accessed on 2021/04/22.

[114] Revenue equivalence. URL: https://en.wikipedia.org/wiki/Revenue_equivalence. Accessed on 2021/04/21.

[115] Vitalik Buterin. Improving front running resistance of x*y=k market makers. URL: https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281. Accessed on 2021/04/21.

[116] Decentralized exchanges research. URL: https://ethresear.ch/c/decentralized-exchanges/17. Accessed on 2021/04/21.

[117] A Practical Liquidity-Sensitive Automated Market Maker. Abraham Othman, et al. URL: https://www.cs.cmu.edu/~sandholm/liquidity-sensitive%20automated%20market%20maker.teac.pdf. Accessed on 2021/04/21.

[118] Nassim Nicholas Taleb. The Black Swan. The Impact of the Highly Improbable.

[119] George Soros. The Alchemy of Finance: The New Paradigm.

[120] Deep Thinking. Where Artificial Intelligence Ends… And Human Creativity Begins. Garry Kasparov.

[121] Antifragile. Things that Gain from Disorder. Nassim Nicholas Taleb.

[122] Quasi Rational Economics. Richard H. Thaler.

[123] behavioral Finance. Understanding the Social, Cognitive, and Economic Debates. Edwin T. Burton, Sunit N. Snah.

[124] behavioral Investing. A Practitioner's Guide to Applying behavioral Finance. James Montier.

[125] Advances in behavioral Finance. Richard H. Thaler et al.

[126] Game Theory. An Introduction. Steven Tadelis.

[127] Ultra Society. Peter Turchin.

[128] Predictably Irrational. The Hidden Forces that Shape Our Decisions. Dan Ariely.

[129] Cardano fee structure. URL: https://docs.cardano.org/explore-cardano/fee-structure. Accessed on 15/10/2021.

[130] The OODA (observe–orient–decide–act) loop. URL: https://en.wikipedia.org/wiki/OODA_loop Accessed on 15/10/2021.

[131] Sovan Mitra and Tong Ji. Risk measures in quantitative finance. Int. J. Business Continuity and Risk Management, Vol. 1, No. 2, 2010.

[132] Understanding StableSwap (Curve). URL: https://miguelmota.com/blog/understanding-stableswap-curve/. Accessed on 15/10/2021.

[133] Improved Price Oracles: Constant Function Market Makers Guillermo Angeris, Tarun Chitra. June 2020. URL: https://web.stanford.edu/~guillean/papers/constant_function_amms.pdf.

[134] Homogeneous Properties of Automated Market Makers. Johannes Jensen et al. URL: https://arxiv.org/pdf/2105.02782.pdf.

[135] Park, Andreas. The Conceptual Flaws of Constant Product Automated Market Making. August 18, 2021. URL: https://ssrn.com/abstract=3805750orhttp://dx.doi.org/10.2139/ssrn.3805750

[136] Hydra: Fast Isomorphic State Channels Manuel M. T. Chakravarty et al. URL: https://eprint.iacr.org/2020/299.pdf.

[137] Hydra PoC Source Code on GitHub URL: https://github.com/input-output-hk/hydra-poc. Accessed on 15/10/2021.

[138] Ethereum - Top Contracts and Projects by Gas, Transactions, and Users. @msilb7. URL: https://dune.xyz/msilb7/Ethereum-Top-Contracts-and-Projects-by-Usage. Accessed on 21/10/2021.

[139] Uniswap: exceeded the 100,000 transactions per day. Marco Cavicchioli. URL: https://en.cryptonomist.ch/2020/08/10/uniswap-100000-transactions-per-day/. Accessed on 21/10/2021.

[140] PancakeSwap Continues Cook Rivals as Daily Transactions Close on 2M. Martin Young. URL: https://cryptopotato.com/pancakeswap-continues-cook-rivals-as-daily-transactions-close-on-2m/ Accessed on 21/10/2021.

[141] Binance in 2021: Innovating in an Increasingly Decentralized World URL: https://www.binance.com/en/blog/421499824684901411/binance-in-2021-innovating-in-an-increasingly-decentralized-world Accessed on 21/10/2021.

[142] Nasdaq Daily Market Summary. URL: http://www.nasdaqtrader.com/Trader.aspx?id=DailyMarketSummary. Accessed on 21/10/2021.