

OccamRazer

June 30, 2021

Contents

Introduction	2
DeFi and Fundraising	3
Introducing OccamRazer	3
Outer World Swap Engines	5
Fixed Price Swaps	5
Price-Volume Dimension	6
Fixed	6
Parameters & Conditions	6
The Process	6
Ladder Increasing	7
Parameters & Conditions	7
The Process	7
Ladder Decreasing	7
Parameters & Conditions	7
The Process	8
LBP	8
Bi-Directional Auction Swap	8
The Process	8
Sealed-Bid Auction Swap	9
The Process	9
Modified Vickrey Sealed-Bid Auction Swap	9
The Process	9
Pool Time-in-Force Dimension	10
Global TiF parameters	10
Good-till-Expired/Filled Pools	10
Fill-or-Kill (FOK pools)	10
Partial Fill-or-Kill (PFOK pools)	11
Distribution of Unfilled Asks Dimension	11
No Pool Originator Dilution (Giveback)	11
Full Pool Originator Dilution (Distribute)	11
Liquidity Airdrop (Contribute)	11
Pool Access Dimension	12
Public (i.e. Permissionless)	12
Private	12

Pre-Market Dimension	13
Duration of the Pre-Market State	13
Acceptance of Bids	13
Tokenomics (Utility)	13
Liquidity Mining	14
Occam Association and Ecosystem Diversification	14
Project X Status	14
Motivation	15
How does it work?	15
Pool Generation	17
Pool Access	17
Referral Link Generation	17
Other Features	18
Order Routing Engine	18
Portfolio Credit Engine	18
Front-Running Prevention	18
Hidden Transactions	19
About Cardano	19

Introduction

Since inception, the success of DeFi applications has been staggering, although limited at inception, its growth has been accelerating to propel the industry around financial disintermediation to a multi-billion dollar powerhouse.

While limited initially, the DeFi market capitalization has culminated in exponential growth through the summer of 2020.

The institutional landscape of DeFi is rapidly expanding, taking over, morphing and synthesizing the institutions of traditional finance by infusing decentralized governance and permissionless access mechanics, all on-chain, all inclusive and incorruptible. The sheer potential for crowd innovation enabled by the open source nature of the bulk of the DeFi codebase is yet another major factor fueling the explosive growth of the ‘money legos’. The aforementioned, calls for an obvious conclusion: today, we are in the very early stage of the process of formation of the new institutional landscape that, for the upcoming decades, will reshape the financial system as we know it today, turning it into something very different, something inclusive, free, and efficient.

Decentralized applications, having their goal to replace key institutions comprising the landscape of the contemporary financial system, have been growing ever more sophisticated and efficient in terms of lending and borrowing mechanisms, risk management and on-chain liquidity generation. The pace at which innovations happen is higher than ever and accelerating.

DeFi and Fundraising

A particular use-case of DeFi, the AMM-powered DEXs, built mostly around the concept of bonding curves, is perfect for replicating the general dynamics of the central limit order books prevalent in the space of centralized trading platforms.

As is the case, however, with traditional order books, AMM requires initial liquidity and an efficient price-discovery process to operate as intended. While a celebrated property of Uniswap-type AMM protocols is their ability to offer liquidity at any price level, there is little added value to this when the project is new, and its fair value is really anyone's guess as is the case with projects that attempt to raise funds in an AMM setting. In practice, the resulting price volatility deprives investors from capitalizing on the fundamental value of the asset, instead making, the so-called, Initial DEX Offerings a front-running game where faster bots feed slower-to-react investors and MMs with immense amounts of slippage.

It is also worth noting that IDO's price volatility is to a large extent a function of the liquidity initially available in the pool. Anything below \$80-\$120k equivalent will cause massive price swings assuming any public interest, whatsoever in the token being offered. This, in turn, results in de-facto capital requirements to the project's team, which while not being bad per-se, brings the IDO process closer to that of CEX listing in terms of its effective cost. It goes without saying that not every talented smart contract developer with a bright idea has \$100k lying idle in one's pocket.

Cardano has been advancing its technology, community and ecosystem for over several years by now. The advent of DeFi has coincided with the culminating efforts on bringing live the CCL-enabled smart contract capabilities Goguen.

This paper describes OccamRazer, a Cardano-powered project aimed at bringing the decentralized fundraising up-to speed .

By infusing the existing decentralized applications with sheer volumes of on- and cross-chain liquidity we empower a better, more inclusive, and freer tomorrow of financial services.

Introducing OccamRazer

OccamRazer has been built with the Cardano ecosystem in mind as the key fundraising vehicle and catalyst for the yet-to-emerge Cardano DApp universe. There are a number of, what we believe represent, killer features of OccamRazer. These stem either from the cross-chain nature of the solution we propose, our intelligent governance layer design, the width and depth of services that are untied under the Occam umbrella, compliance and regulatory toolbox we offer or the sheer size and weight of the Cardano ecosystem. Let us elaborate upon these dimensions in turn.

OccamRazer is a feature-rich protocol sufficiently flexible to accommodate most fundraising profiles. We cover:

1. Fixed price mechanics,
2. Dynamic ascending or descending price mechanics,
3. IDO-type bonding curve fundraising,
4. Auction mechanics for projects with non-standard value propositions,
5. Private and public pools for seed funding and more public offerings,
6. Various governance features for community rating projects,
7. A number of community engagement mechanics like bounty hunting, referral system, and community missions,
8. Front-running prevention measures and transaction mixing for privacy-valuing investors and sensitive deals,
9. Many other features which are elaborate upon below.

Apart from being an elaborate protocol with a rich set of product features, Occam takes compliance seriously even in the permissionless setting. We believe that the range of instruments that we will enable decentralized trading in will to a large extent define our community footprint. Achieving compliance within a permissionless setting requires a rich regtech toolbox. In particular:

1. Optional KYC-filter on participating investors,
2. A set of KYT features and blockchain intelligence tools to prevent ‘bad’ coins from flowing into the system,
3. DAO-governed project Due Diligence tools,
4. Partnerships with regulated tokenization service providers to enable tokenized securities trading in a compliant, yet permissionless setting.

OccamRazer ecosystem is more than merely a DEX, a money market protocol, or a crowdfunding platform. We are building a layer of DApps enabling all the key financial services united by an intelligently designed governance layer¹. Being a part of this ecosystem, the Razer project benefits from a number of key mechanics enabled by the interactions with the other components of the Occam ecosystem:

1. Automated participation, alarms,

¹The key mechanics, services and products are elaborated upon in this document as well as in the OccamRazer solution and the Occam tokenomics paper.

2. Continuous ecosystem diversification across the universe of high quality projects,
3. Best-in-breed liquidity enabling tools and order-routing software enabling ease of participation,
4. A number of benefits to the holders of the OCC, the Occam ecosystem token,
5. Fast and cheap transactions within a cross-chain environment.

Finally, as a project building on top Cardano, OccamRazer brings a lot of benefits to Cardano, while synergistically benefiting itself from Cardano's strong community:

1. Unilateral community support and Association backing
2. Fundraising engine for Cardano CCL
3. Design enabling deepest pools of DeFi liquidity
4. Capitalizing on untapped pools of idle ADA liquidity

This section has coined a number of aspiring concepts. The following sections elaborate upon how we plan on delivering those.

Outer World Swap Engines

To put it simply, the Swap Engine is a kind of protocol that is aimed at providing liquidity at some price levels. AMM-based DEXs are designed to provide liquidity at any price level, gradually increasing the slippage with the order size. It is continuous and the priority is given on a temporal basis. In other words, orders submitted earlier (or those that pay higher gas fees) are treated first. As elaborated upon above, traditional AMM-based protocols are ill-suited for decentralized initial offerings.

In this paper, we introduce a family of protocols, continuous and discrete in nature, that would fill the niche and offer smart-contract vehicles designed for various fundraising use-cases, private and public, over- and under-subscribed, fungible and otherwise.

Fixed Price Swaps

In the simplest case, fixed price swaps are defined by the 'infinitely' elastic supply curve - all the allocated supply is guaranteed to be offered at a specific price. This mechanism per se has a number of advantages when compared to IDOs:

1. It is far less capital demanding;

2. It explicitly minimizes volatility;
3. When expanded and enhanced, it offers high degree of flexibility in designing the fundraising process;
4. It allows for good-incentive-setting tokenomics tailored to the process of fundraising.

In short, it is just a better fit for the general purpose fundraising process. However, it goes without saying that fundraising needs might differ per project. So do the fundraising process designs. There are a number of dimensions that need to be taken into consideration when crafting a system with sufficient flexibility to accommodate the needs of as wide of a spectrum of projects as possible. An example would be, say, NFTs or highly innovative projects with no existing market for similar tokens and therefore an undefined price.

In what follows, we introduce the family of protocols we bring to the Cardano community. These protocols vary across a number of dimensions - the price-volume relationship, the extent and nature of access barriers, the premarket settings and others. We will elaborate upon each of these in turn. The actual smart contract will contain settings for each of the aforementioned dimensions resulting in a 'lego' contract where fundraising process design can be fine-tuned to accommodate the needs of any project.

Price-Volume Dimension

Price-volume dimension refers to the functional form between the tokens sold and the price. Mind, that all pools will have a lifetime setting - there will be no infinite fundraising processes.

Fixed

Fixed Static Swap pool: a limited token supply is offered at a given price. The token sale lasts until all the allocated token supply is sold out or until the time runs out.

Parameters & Conditions

S - supply

P - price per unit

V - volume

StartDate - the starting date of the offering

EndDate - the ending date of the offering

The Process

For an order of volume V , if the remaining volume is greater than V , then the trader receives V tokens and pays a total of $P * V$. Otherwise the trader receives the remaining volume V' in the pool and pays $P * V'$.

Ladder Increasing

Token sale is executed in bulks, every new bulk arriving at a higher unit price².

Parameters & Conditions

$(S_1, P_1), (S_2, P_2), \dots, (S_k, P_k)$ - each bulk size and respective prices, while $P_1 < P_2 < \dots < P_k$

The Process

For an order of volume V the smart contract determines which bulk the trade belongs to, based on the sold amount, and then the respective price. It might happen for large trade that it belongs to more than a single bulk, then the price is calculated as volume-weighted average. For example, a large trade of volume V overlapping, say, three bulks in amount V_{k-1} with price P_{k-1} , amount V_k with price P_k , and V_{k+1} with price P_{k+1} , then the average price is $\bar{P} = (P_{k-1} * V_{k-1} + P_k * V_k + P_{k+1} * V_{k+1})/V$. For the avoidance of doubt, the pool is one-sided: only buying of tokens is allowed and hence, the price differential between the 'stairs' of the ladder cannot be exploited.

Incentivizing early participation, this mechanics has an obvious drawback: for any project that is not oversubscribed, it disincentivizes late participation and in general historically has been employed by many less than ethical projects that wanted to collect at least a part of their inflated cap.

Ladder Decreasing

Similar to its sibling described above, this mechanic implies bulk execution, where every new bulk is marked by a particular volume being purchased. However, this is where similarities end: upon the sale reaching a pre-set volume milestone, the price offered *decreases* **and** everyone who has bought in at a higher price gets an airdrop, such that their effective purchase price becomes the new (lower) or a *better price* (this latter option implies an effective discount over and above the new lower price and is economically similar to the ladder increasing).

Parameters & Conditions

²This mechanic is by far the most common in the digital asset world today - earlier investors get a better price. Those who decide to participate later down the road get a worse price - easy, sensible, but in the humble opinion of the authors of this text, lacking any imagination.

$(S_1, P_1), (S_2, P_2), \dots, (S_k, P_k)$ - each bulk size and respective prices, while $P_1 > P_2 > \dots > P_k$

The Process

The price calculation is the same as that presented in the Ladder Increasing case. Below we describe possible mechanics on how to reward early buyers.

1. When a project sells token A , the i -th bulk will contain “modified” tokens A_i .
2. When the offering ends the token A_i can be exchanged for either some amount of A (that is, token A_{k-1} is worth more in token A than token A_k), or get a price *refund* (token A_{k-1} gives more refund than token A_k).

While being more cumbersome, this model of fundraising has several desired properties and a distinct use case. It fits better for less hyped, undersubscribed and possibly undervalued projects with strong core communities.

LBP

Adding weights to the constant product formula allows a different asset allocation than 50:50, i.e. the project does not have to provide that much quote token. Keeping the weights constant during the course of the fundraising can also create great price fluctuations. Hence, under LBP, the weights are dynamic deterministically to anticipate asset shift towards the project’s token which makes the price overall more stable and discourages malicious token hoarding.

Bi-Directional Auction Swap

Bi-directional auctions represent a hybrid model with elements of AMM-style IDOs, yet requiring no initial liquidity other than that of the token being sold. A distinct feature is a price-volume curve, shape of which is defined by the Pool Originator.

The Process

The funds contributed are used to purchase the offered coins and thereafter automatically fill the bid side of the ‘book’. The ‘auction’ begins at a particular price, which thereafter changes as traders purchase the token moving up the price-volume curve. After the pool is sold out, or the time runs out, the project owner can proceed by either:

1. Collecting all the proceeds and the inventory of unsold tokens thereby closing the pool, or
2. Collecting a part or none of the liquidity sitting in the pool thereby re-balancing it, enabling sell orders and leaving as a full-fledged liquidity pool.

Sealed-Bid Auction Swap

As the name implies, this fundraising paradigm is conceptually very similar to the classic sealed-bid auction, however with a minor modification reflecting the fungible nature of tokens being offered.

The Process

1. The Pool Originator sets the minimum token price, and the amount of tokens to be distributed.
2. Traders thereafter commit their bids and volumes they intend to purchase. Bids are private - only the bidder knows one's own bid. Bids have to be higher or equal than the minimum price and upon submission are ordered in the ascending order.
3. Finally, the bids are filled with one large order, where all the committed supply is distributed across bidders - from the highest down until either the supply runs out or all the bids are filled.

We will abstain from economic and game-theoretical analysis of the implications of such (and the next) model of public sales and dedicate a full article to the comparison across the models we endorse. It suffices to say that it can be shown that assuming sufficient information on the side of investors, auctions in general promote more efficient resource distribution for illiquid projects with uncertain market value. We believe that the auction-based fundraising paradigm is far superior to others, assuming sufficient informational content is sufficiently widely disseminated across participants.

Modified Vickrey Sealed-Bid Auction Swap

In the spirit of Vickrey sealed-bid auction design, we propose a subtle modification to the sealed-bid auction design described above. This modification can potentially have far reaching implications for the auction dynamics and we will abstain from making this smart contract available to a wider public limiting the participants to a limited community strata that we believe possess sufficient expertise. The said modification is that the price paid by every participant upon filling the bids is the average price across the winning bids.

The Process

Suppose that the winning bids are $(V_1, P_1), (V_2, P_2), \dots, (V_k, P_k)$, i.e. $V_1 + V_2 + \dots + V_k = V$

1. The first bidder with a bid V_1, P_1 receives V_1 tokens with volume-weighted average price across all other winning bids, i.e. $\frac{(V_2 * P_2 + V_3 * P_3 + \dots + V_k * P_k)}{(V_2 + V_3 + \dots + V_k)}$

2. The second bidder with bid (V_2, P_2) , receives V_2 tokens with volume-weighted average price across all winning bids with lower bid price, i.e.
$$\frac{(V_3 * P_3 + V_4 * P_4 + \dots + V_k * P_k)}{(V_3 + V_4 + \dots + V_k)}$$
3. The k -th bidder (i.e. the last) with bid (V_k, P_k) receives V_k tokens with price P_k .

Pool Time-in-Force Dimension

The Time-in-Force (TiF) settings enable Pool Originators to condition the ‘success’ of the token sale upon reaching a particular bid volume threshold. By default any pool has a limited lifetime. The TiF dimension adds a volume condition atop. If the volume condition is not met during the lifetime of the pool, tokens and contributed funds return to their respective owners. If the specified minimum volume is filled, a swap takes place in accordance with the rules specified in the Price-Volume dimension. The distribution of unfilled asks dimension elaborated upon below describes what happens assuming partial fill above the volume threshold.

Global TiF parameters

These parameters are enforced system wide (where applicable) and can be changed by a community vote on the DAO stage of the protocol:

1. Note, that for the obvious purposes, we introduce a global parameter enforced for every token sale, the MFOK (Minimum Fill-or-Kill). This metric refers to the minimal fill ratio for the allocated token supply that is required for the token sale to be deemed successful. It will stand at 10%. Should a token sale not reach this volume threshold, the contributions will be refunded.
2. Likewise, token sale duration cannot exceed 30 calendar days.

Good-till-Expired/Filled Pools

In this type of pools no volume milestone is specified. In other words, the ‘Success’ condition is set at any level (above 10% FOK default) of bid volume reached within the pre-specified time period or until the entire supply offered is bought out.

Fill-or-Kill (FOK pools)

As the name suggests, if FOK is specified, the supply allocated is either filled (i.e. sold out) or the contributed funds are returned back to the investors, while the entirety of the allocated token supply remains with the Pool Originator. The ‘success’ condition here, therefore, is whether the entire allocated token supply has been filled.

Partial Fill-or-Kill (PFOK pools)

The PFOK setting allows specifying the aggregate volume of bids for tokens that have to be filled in order for the public sale to be deemed successful. If the required volume is reached, the swap of tokens is triggered. Otherwise, the tokens and proceeds are distributed back to the Pool Originator and investors respectively. A general case of FOK pools, whereby the ‘success’ condition is filling a specified fraction of the allocated token supply above the minimum 10% threshold.

Distribution of Unfilled Asks Dimension

This section addresses the design choices we have made with regard to the distributional mechanics of the unsold supply, upon completion of the token offering. All of the scenarios below imply that the volume threshold specified in the TiF settings is either met or absent.

No Pool Originator Dilution (Giveback)

This mechanics implies that all unsold tokens are returned to the Pool Originator along with the contributed funds. Traders receive their allocation of the pool’s tokens in accordance with their contribution and selected Price-Volume Dimension mechanics.

Full Pool Originator Dilution (Distribute)

This mechanics, in turn, implies a pro-rata distribution of the unsold allocated bid-side supply among the traders who have participated in the token sale. We would like to stress that affected tokens are only those of the allocated bid-side supply, not the entirety of token supply. This mechanism serves as an additional incentive for early participants.

Liquidity Airdrop (Contribute)

An important mechanic that we will introduce in the later stages of our development roadmap is the so-called *liquidity airdrop*. Certain groups of investors, traders, OCC token stakers and liquidity providers will be automatically participating in regular airdrops of unsold tokens. This feature is optional and will be incentivized by dramatically slashing the amount of OCC tokens that needs to be staked in order to open up a pool. Certain limitations will be imposed upon which projects are eligible for this. In particular, only some percent of the unsold supply can be distributed, and only projects that have raised over 50% of intended funds are eligible. The remainder (if any) of the unsold bid-side supply will be either distributed or given back.

Pool Access Dimension

The fundraising process is a subtle matter to say the least. Various projects might and will have different arrangements, especially on a pre-public stage of seed rounds. In order to reflect the intricacies embedded in this process, we develop a number of features that preclude in one way or the other a totally permissionless access to a particular pool. These settings can be specified by the Pool Originator upon setting up the pool and are not activated by default. In other words, unless specified otherwise, our pools are permissionless.

Public (i.e. Permissionless)

Public pools are opened to anyone interested in participating.

Private

Pool Originators specifying private pools have two sets of restrictions that can be imposed:

1. Access to some addresses: access is granted to anyone who satisfies a given criteria, such as:
 - a) An address associated with a verified KYC status - this feature can be useful for projects that take compliance seriously even in the entirely decentralized setting;
 - b) An address that has more than a preset amount of OCC tokens staked. This setting applies regardless of whether specified or not, unless a private Pool Originator chooses option (2) below;
 - c) Private pools can likewise be locked with passwords.
2. Access to specific addresses: access is granted to particular preset addresses and users by means of whitelisting addresses. An option that can be enabled by a Pool Originator is to allow whitelisted addresses to whitelist a limited number of other addresses. Combined with the onchain referral mechanics (to be described further) this becomes a powerful tool for community interaction.

There are certain properties and features of the protocol that interact with the private pools.

1. As mentioned above, unless the pool is locked only for the whitelisted addresses, having staked a particular amount of OCC tokens allows stakers to participate in any private pool (for details, see below).
2. Mind, that pools applying for the *Project X* status will economize a great deal on fulfilling the requirements to achieve this status if opting for a private pool rather than public (for details, see below).

3. Private pools also have certain privacy features that are not available for public Pool Originator. These include transaction mixing and specifying trees of addresses in a hierarchical deterministic setting. Enabling both of these features will guarantee that it will be unfeasible for an outside observer to decipher how many participants there have been to a private round and how much each of the participants contributed.

We believe that there are many use cases for private auctions: regulated instruments or enhanced compliance requirements on the side of the projects raising funds, new user engagement mechanics, and last but not least, they do offer a solution for a trustless participation of investment funds on the seed project stage. Also, note that projects holding ‘project X’ status are by default private and limited to stakers of the OCC token.

Pre-Market Dimension

An additional number of settings can be imposed by the Pool Originator in respect to the existence of and enabled functionality during the premarket period. The options concern the timing of pool inception, pre-acceptance of bids and treatment of such.

Duration of the Pre-Market State

Pools can be opened immediately or with a delay of up to 7 days. This delay can be used by the project team to expand the community in some way, generally increase the interest in the upcoming sale (once this sale is public), generate a list of whitelisted addresses, etc.

Acceptance of Bids

Assuming that the launch of the pool is not immediate, Pool Originator has the option of enabling pre-commitment of bids. Bids in this mode are private and allow for ‘testing’ the market appetite towards the upcoming sale. In this vein, anyone is welcome to send a private transaction to the Pool Originator indicating approximate interest in the tokens offered. While such a transaction is not free, it increases the likelihood of the project owners being able to gauge the actual market appetite more accurately and to preemptively adjust the pool parameters, hence enabling more people to potentially participate.

Tokenomics (Utility)

Occam’s ecosystem is powered by the OCC token that enables a number of unique mechanics and, most importantly, powers the Occam’s governance layer. We will elaborate upon each of these dimensions below.

Liquidity Mining

Liquidity mining as a phenomenon has given a significant impetus to the DeFi ecosystem back in the memorable ‘DeFi summer’ of 2020. The concept is simple: liquidity providers are rewarded with the protocol tokens to compensate for the risk of impermanent loss they are running, locking the system in the positive feedback loop: more liquidity, more traders, more fees, more valuable protocol token attracting yet another set of market makers, etc.

Occam encourages pool participation by allocating a portion of the outstanding OCC token supply to pool participants.

Occam Association and Ecosystem Diversification

Part of the OCC held by the Occam Association will be channelled towards projects holding the status of Project X. The exact mechanics of the Occam Association will be revealed later, however, it suffices to highlight its core feature: ecosystem diversification. Stakers of the OCC token will be entitled to liquidity mining. Furthermore:

1. Any project achieving the Project X status may be entitled to a contribution of OCC tokens from the Occam Association;
2. In exchange for OCC tokens the Occam Association receives project tokens that are channeled to a dedicated closed Association pool;
3. Periodically, the liquidity tokens of this dedicated pool may be distributed to all OCC token stakers, on a pro-rata basis;
4. These liquidity tokens can be burnt for a pro-rata stake of the tokens in the pool. In other words, the mechanics of the Association pool closely resembles that of an AMM liquidity pool where OCC token stakers replace the role of liquidity providers. Another key difference is that no swaps can take place within the realm of this pool;

In this way, the broader Occam ecosystem will constantly benefit from high-quality projects making their way into the Project X marked pools.

Project X Status

Among the core protocol features is the procedure of acquiring Project X status. This procedure is the catalyst for a number of key protocol mechanics. It powers the Occam Association, continuous diversification, certain aspects of the OCC token utility and general protocol governance framework. This section is dedicated to detailing the philosophy behind this protocol design choice.

Motivation

Absent of (preferably DAO driven) rating mechanisms, permissioless systems, such as the Occam protocol, are destined to be buried under potentially malicious or otherwise unnoteworthy pools created by less than ethical or technologically meaningful projects. It goes without saying that the standardization of token issuance has made it far too simple to issue tokens. Creating a pool on our platform is likewise a simple undertaking. Project X status is fundamentally a mechanism for distinguishing legitimate projects that pass certain quality control checklists. The formation of such checklists as well as the ultimate approval will be governed by a DAO. The automatic commitment of funds from the Occam Association symbolizes the synergetic incentive structure that we hope we have achieved with the design choices made.

How does it work?

From the project side, the following actions are required:

1. Applying for the Project X status is simple. One needs to stake \$30,000 worth of OCC tokens at current market rate to initiate the procedure. The stake can be delegated. In other words, a project can ask its community to stake these tokens for the address provided. It is worth noting that:
 - a) When delegated, staked tokens can only be moved by the owner of the delegating wallet, so no scam exits can take place;
 - b) Unstaking is possible either upon denial of the Project X status or upon the completion, be it success or otherwise, of the private round.
2. Upon successfully staking the tokens, the project needs to provide (upload and has on the chain) the following information that will be thereafter available to (only) private pool participants:
 - I. Required items:
 - a) The whitepaper or an equivalent document detailing project mechanics;
 - b) The yellowpaper detailing the roadmap and details of technical execution;
 - c) The team contacts, and KYC information (the latter can be provided to a trusted third party and upon said party's confirmation can remain private);
 - d) Corporate details if the development is undertaken from under the umbrella of a legal entity (preferred);
 - e) Smart contract address;
 - f) Report from a reputable auditing firm stating that smart contract integrity, and application pentesting results, have not revealed any critical vulnerabilities;

- g) Miscellaneous project information and a plan detailing the fundraising procedure.

II. Optional items:

- a) Repository with the codebase for our own inspection;
 - b) Committed investors, if any (this won't be public).
3. Upon receiving the aforementioned items, the Chair Members of the Occam Association will review them and vote for either accepting or denying it. These members are selected out of large OCC token stakers. As elaborated elsewhere in the doc, their OCC tokens can not be moved while on the board and for 6 months after they resign.
 4. Upon receiving approval, the project team can initiate the opening of a pool, provision of liquidity, etc. The pool will be opened to private participants on the date and time specified by the project team in the premarket dimension settings.
 5. Please, note that any pool holding Project X status necessarily needs to undergo the private round. In other words, the first fundraising round needs to be done through a private pool. Thereafter, it is entirely up to the project whether the team believes a public round is warranted. The pool access mechanics is elaborated upon in the relevant section below.
 6. The community is notified through in-platform notifications and email blasts about every project that gets such approval. The list of such projects will be located and highlighted on the protocol's landing page.
 7. Regardless of whether the access to the pool will be limited to only whitelisted participants or not, any such project will receive an allocation from the Occam Association. Given the mechanics of the said Association, this will serve a dual purpose of:
 - a) Exogenous diversification of the Occam ecosystem: all the OCC token stakers will be receiving regular airdrops of tokens of high quality projects. This, likewise, provides obvious utility to stake OCC tokens.
 - b) Synergetic incentives of the board of Occam Association.
 8. An endogenous diversification mechanics is also worth mentioning here: any holders of liquidity tokens and/or OCC tokens have an option to automatically reinvest the proceeds they acquire from the trading and credit market fees into the projects holding the Project X status. This is only applicable to public and private non-whitelisted pools.

Pool Generation

Anyone is free to generate a swap pool within the Occam ecosystem. This only requires burning a small amount of OCC tokens. This is done mainly to impose an additional (atop of gas fees) monetary cost against potential adversarial spam abuses. Likewise, this fits neatly the philosophy behind the tokenomics design of the general ecosystem. As specified above, applying for the Project X status requires additionally to stake a more significant amount of OCC tokens. Upon specifying pool parameters along the dimensions detailed above, the last remaining action is to deposit the pool assets - the ask side of the virtual order book.

It is also worth highlighting that generating liquidity bootstrapping pools requires depositing the bids in core platform assets.

Pool Access

Occam is a permissionless application by default. However, we do recognize the value of governance, community QA (as elaborated elsewhere in this paper) and acknowledge the need for a certain extent of quality censorship. In this spirit, there are certain restrictions on the creation and access to the swap pools that are hosted. Unless specified otherwise, access to presale (private) pools of projects carrying the Project X status is limited to the stakers of the OCC token. This works as follows:

1. Projects that undergo the due-diligence procedure of Occam Association and are, thus, awarded the Project X status, necessarily have to undergo the private round. There are two access options for them to specify, either:
 - a) Opened or closed whitelists. In this case, only the whitelisted addresses can participate and (optionally) those whitelisted by the whitelisted addresses. Note that the Occam Association address is always whitelisted.
 - b) Private and open only to stakers of OCC tokens.

Referral Link Generation

The referral system is entirely on-chain due to a lightweight smart-contract design. Furthermore, this system represents an integrated part of the token economics design - generating a referral link requires one to burn some amount of OCC (i.e. each month a payment of OCC is required in order to keep the link active). The following properties characterize the referral smart contract:

1. Referral link with certain expiration period is generated by burning a fixed amount of OCC;
2. Portion of the the liquidity mining reward generated by referred users is provided to the creator of the referral link;
3. Referred users receive a certain trading fee discount.

Other Features

The setting of a fully fledged ecosystem of financial services enables a rich set of interactions on the governance, ecosystem mechanics and tokenomics layers. We believe that these features set the Occam ecosystem far apart from the existing industry peers. Albeit, necessarily running the risk of overcomplicating the system, we have ventured into outlining a number of unique interaction mechanics that, we believe, will be synergetic for the ecosystem at large.

Order Routing Engine

Any core asset from the built-on-top DEX can be invested into any fundraising campaign in one click. Transactions are processed in atomic fashion, i.e. either both legs of the transaction are executed or neither is. For example, if one holds any core asset or any asset that is traded against any core asset, one can use this to invest in any eligible token sale regardless of what assets are selected by the Pool Originator as eligible for contribution.

The transaction path selected by order routing smart contract can be optimized for speed or cost of execution.

Portfolio Credit Engine

An extension of the previous idea, one can use credit market mechanics available for beta and sigma pools in order to get exposure to the fundraising campaign while sustaining one's exposure to one of the desired core assets. In order to accomplish this, one borrows one core asset against the collateral of the existing asset and subsequently invests the borrowed asset into a fundraising pool. This way, the exposure to the asset used as collateral remains with the investor, while the borrowed asset is divested into a volatile new token. Obviously, this system works best assuming that one of the core assets (that being borrowed or that being used as a collateral) is a stable coin. Transaction is likewise atomic.

Front-Running Prevention

Blockchain transactions are processed in blocks and pending transactions are public, as a result frontrunning is easier to execute. In the same block the order of transactions is determined by the gas price, thus favoring bigger players who can pay higher gas fees. To make the playground fairer for all participants, we offer the following mechanics:

In a block all the orders coming to the pool will be saved and executed at the same price. For example, in the case of Ladder Increasing swap pool, if there are two orders from the same block, but one in bulk (S_1, P_1) and the other in bulk (S_2, P_2) then both will be executed at a price $\frac{(S_1 * P_1 + S_2 * P_2)}{(S_1 + S_2)}$.

Hidden Transactions

In general, the transactions on public blockchains are visible to anyone, however nowadays it is possible to conceal the information in the transactions. The two most common techniques are Commit reveal scheme and Zero-knowledge proof. This feature can be thought of as another measure against frontrunning, especially when one would like to execute unusually large orders (similar to one of the reasons why dark pools exist on centralized venues). This feature also enables Sealed Bid Auctions.

About Cardano

Cardano is an open platform that seeks to provide economic identity to the billions who lack it by providing decentralised applications to manage identity, value, and governance. Cardano's aim is to become a blockchain based social financial operating system for billions of users as well as a comprehensive solution for enterprise adoption. The team's vision is to bring a new standard in technology – open and inclusive – to challenge the old and activate a new age of sustainable, globally- distributed innovation. This vision is supported by a vibrant community of over 1 million members.

All developments of the Cardano ecosystem are driven by IOHK - one of world's most experienced blockchain researchers and developers who have produced over 90 academic articles (most of which peer-reviewed) over the past few years. The development approach is evidence-based - researched, challenged, mathematically modeled and rigorously tested before specified with a codebase offering an unrivaled level of assurance. Effectively Cardano is a third-generation blockchain engineered to solve the fundamental challenges of blockchain systems - efficiency, scalability, and sustainability.

The upcoming launch of KEVM (K Ethereum Virtual Machine) enables full smart contract functionality that in turn activates three parallel and massive flows towards the Cardano ecosystem:

1. Firstly, activate the transition of dApps (e.g. DeFi) from legacy blockchain-based (e.g. Ethereum) to Cardano. This is enabled by full backward compatibility with Ethereum - i.e. developers can write dApps in Solidity which are then compiled into EVM bytecode and then run on KEVM. Furthermore, this is the first step towards Cardano's strive for ultimate interoperability - the IELE VM, which will allow smart contracts to be written for Cardano in the world's most popular, non-blockchain, development languages.
2. Secondly, release the unbounded flow of initiatives and ideas (now over 3,000 projects) that have been brewing for the past few years, such as SingularityNET who demand for next-level scalability, flexibility, and security. Furthermore, these projects will be aided by ease of development

by using “Marlowe” - interface allowing easier development of smart contracts as well as robust on-chain governance, and a protocol’s design geared towards protecting privacy rights of users, while also taking into account the needs of regulators

3. Lastly, open an entire universe of unique use-cases for Cardano’s native token (ADA) that has so far been a pool of idle on-chain liquidity.