deFIRE
Powered by Changelly.com

Version 1: April 19, 2021

Contents

Introduction

Within the last year, worldwide events and a heightened focus on capital market instability has precipitated an explosion in blockchain activity, leading the entire digital asset market into by far its most bullish period to date. While protocols have risen and fell, one innovation remains constant—the growing and almost omnipresent role of decentralised finance, or 'DeFi', in the blockchain industry. Growing from just a handful of original projects, multiple DeFi projects are now being created on a daily basis, and billions of dollars' worth of on-chain value is being locked in various 'on-chain finance' protocols.

But despite the rapid phase-shift in decentralized technology innovation, there are still components of the blockchain markets that remain highly inefficient. This is perhaps most pronounced in the realm of exchanges, where decentralized exchange bonding curves and liquidity mining have replaced centralized exchange order books and maker rebates; but have brought with them

elevated fixed cost to users and a highly fragmented market where the concept of best execution has to be invented anew.

As a result, as an industry we have arrived at a new juncture, where for many average retail users as well as large institutional order flow originators making a decision on which exchange to use, or to provide to users, is one of the biggest barriers to entry. Absence of guarantees on the quality and speed of execution imposed by the limitations of existing solutions diverts many players away from DeFi, preventing oceans of institutional liquidity from flooding the on-chain space. It's not just a case of choosing one provider over another, either. In fact, choosing a trading venue now involves taking into account a wide range of disparate parameters. These include trading and network fees, asset liquidity, protocol incentives, and more. This complexity is multiplied in the presence of several functional layer-1 networks, assuming the absence of native cross-chain interoperability (which still today is a realistic assumption). Calculating and navigating this complex landscape requires domain expertise, heavy infrastructure, and overall, the process is highly non-trivial.

So, what is the solution? Do we build new, more efficient exchanges from scratch leveraging close to a decade of domain expertise? Or do we build routing infrastructure to aggregate and enable access to the 'cheapest depth' liquidity from multiple exchanges through a simple set of interfaces, visual and programmatic, having a depth of features capable of accomodating the demands of institutional and retail players alike? Well, deFIRE does both.

Incubated by Occam.Fi, a fintech powerhouse aimed at developing the Cardano ecosystem, in a partnership with Changelly, deFIRE aims at bringing optimal execution and liquidity services for users of Cardano's DeFi ecosystem.

Changelly has been both a leader and innovator in this space since 2015. In a sense, Changelly is in the business of cross-chain swap settlement since before there was even a DeFi industry. In this time, it has built the most popular cross-chain liquidity engine in the space. In fact, if you ever wondered when using a crypto wallet where token swaps are executed, the odds are that the answer is Changelly. With over 350 API partners, more than 100 wallets, the best execution prices, and thousands of BTC worth of average daily volume. And, of course, millions of active users.

The goal of deFIRE is to build an entirely decentralized order execution engine while retaining the cross-chain nature of order settlement and to do so in a cost-efficient manner. We have chosen to build a decentralized order router and a DEX also delivering intricate tokenomics design on top. We have chosen to build it on Ethereum, BSC and Cardano first.

But before we deep-dive into the deFIRE platform and protocol itself, let's examine exchange aggregators in greater detail.

Exchange Aggregators

Decentralized exchange (DEX) aggregators source liquidity from different DEXs, and thus offer users better token swap rates than they could get on any single DEX.

A DEX aggregator's key value proposition is the ability to offer optimal effective order execution in the shortest possible time, while presumably also optimizing gas consumption.

DEX aggregators have built the stack to optimize slippage across multiple bonding curves, swap fees and token prices, ultimately offering a better effective swap rate for users. Indeed, a swap split sourcing liquidity across several DEXs, if built right, gets a user a better price than a swap on any single exchange.

While optimal effective execution price is key, order routers also offer options to protect users from price impact, reduce the probability of failed transactions and offer various front-running prevention mechanisms.

However, despite their clear benefits, the number of high-quality DEX aggregators are few and far between. That being said, deFIRE is currently doing what few of its rivals in the space are creating a low latency decentralized order router and offering its facilities to the growing network of Cardano ecosystem-oriented institutional order flow originators and retail traders.

Execution-wise, we will connect to the deepest pools of on-chain liquidity out there and also, build one of our own.

deFIRE Details

This section provides a brief summary of the mechanics and components of the deFIRE. In particular, it describes how limit orders are created and processed in a decentralized setting and the mechanics of the smart order routing algorithm.

Limit Orders Functionality

Limit orders can be created by specifying a set of parameters including:

a) Base currency;

b) Quote currency;

c) Volume;

d) Limit price;

e) (Optional) Expiration date and time.

Routing

Furthermore, one can specify whether an order is submitted to a single exchange of their choice or to multiple exchanges (either a number of user-defined or all). One may choose a single or several venues if they receive certain preferential treatment if their orders are routed there (see Guaranteed Prioritization belo). In this latter case, the algorithm will either split the order (depending on the size) and submit it to multiple exchanges or would find the exchange where the best execution conditions exist for that particular order.

Fill-or-Kill

Also, traders will be able to select whether the order is reverted if it is partially filled - for example, if only 30% (or 90% for that matter) of the order volume is executed (disregarding the number of exchanges) then the transaction is reverted (a Time-in-Force option applied to an order known as Fill-or-Kill).

Lit and Dark Books

In addition, by the very nature of the technology the order information will be stored on-chain (for which the trader incurs a fee), however the trader may choose whether that order information is visible (easily parsable) or hidden (hashed). Effectively, traders who choose to hide their orders form a type of a dark pool and their orders can be referred to as a variation of an Iceberg Order, which are highly sought among institutions.

Front-Running Prevention

In order to prevent front running in a decentralized setting, a gas threshold for each transaction is established and submitting an order with gas set higher than this threshold will be rejected. The threshold is computed and set intra-day, at high frequency utilizing a set of proprietary algorithms.

Guaranteed Prioritization

An algorithm allowing order guaranteed prioritization of order execution is in place. All orders routed to a designated DEX by the order router will be executed with priority as the threshold discussed in the previous section is elevated.

Order Routing Mechanics

Core

In general, the smart order routing (SOR) algorithm aims to optimize the execution quality of relatively large orders by dividing them into multiple ones and submitting them to a set of "whitelisted" exchanges (see the tokenomics section for definition of whitelisting). The router calculates which exchanges present the most favorable trading conditions in terms of liquidity (taking into account gas cost estimates as well). In essence the core of the SOR functions as follows:

Parameters and assumptions:

1. V - order volume (size);
2. s - order parts;
3. n - DEXs;
4. Input asset - the asset which is provided in order to obtain the output asset;

5. Output asset;

The order volume V is split $V_0 = 0, V_1 = V/s, ..., V_s = V$. Then for each DEX it is calculated $s + 1$ - the output asset amount from each V_i amount of input asset amount. A $n \times (s + 1)$ matrix M is generated, where the rows represent the DEXs and the columns represent the volume intervals. Since in each DEX the gas cost of the trade is expected to be independent of the volume, an array G_i of length n representing the gas cost is generated - that is the gas cost of a trade of size 100,000 USDC would be the same for that of 1,000 USDC size. A distribution has to be found $a_1, ..., a_n$ such that $a_1 + ... + a_n = V$ and the average token price (quantity) is minimized (in case of sale):

$$\frac{V + G}{Q}$$

where G is the sum of $G_i$such that $a_i \neq 0$ and Q is the sum $M_{i,a_i * s/V}$ over all i - that is, the output asset amount. This optimization problem is solved dynamically, by gradually calculating the values $f(m, i)$ - best average price in the case of sale of $i * V/s$ input asset and utilizing DEXs from the m first rows. For $m = 0$ it follows that:

$$f(0, 0) = 0, f(0, 1) = (V_1 + G_0)/M_{0,1}, ..., f(0, s) = V_s + G_0/M_{0,s}$$

Furthermore, $h(k, m)$ is saved which represents the amount of the output asset corresponding to the best average price $f(m, i)$. Suppose that all these values have been calculated for the first k rows of the matrix. Next the $k+1$-th row can be derived as follows:

$$f(k + 1, m) = min(b_0, b_1, ..., b_m)$$

where b_j represents the best average price for input asset volume V_m to $k + 1$-th DEX. Then:

$$b_0 = f(k, m)$$

For $j \neq 0$

$$b_j = \frac{f(k, m - j) * h(k, m - j) + G_{k+1} + V_j}{h(k, m - j) + M_{k+1,j}}$$

This provides a new $n(s + 1)$ matrix and the desired is the bottom right corner of the matrix - i.e. the total volume V and all DEXs considered.

Order Execution Quality Optimizer

The explanation above describes the case of trading a single asset directly for another asset - e.g. ETH to USDC. However, further execution quality improvements can be achieved when also considering multi-leg trade—for example, from

ETH to wBTC and finally to USDC. The mechanics of the Order Execution Quality Optimizer (OEQO) will be introduced in the supporting documentation to this brief whitepaper.

Tokenomics

The following sections will describe the tokenomics of the deFIRE ecosystem and in particular, the role CWAP token plays in setting 'right' economic incentives. At its core, deFIRE provides its patented technology of ultra-low latency order routing. The robust internal matching engine system provides unmatched speed and access to deep cross-venue liquidity for every actor involved in the ecosystem.

What does the deFIRE ecosystem look like? The easiest way to understand it is through actors involved, token flows between them and what each of them has to do with CWAP, deFIRE's native token. Ready? Let's go.

Actors

The actors of the deFIRE ecosystem are defined in relation to order flow and CWAP tokens:

1. Order flow originators: these are entities who originate order flow, and chose to trade through deFIRE. These include traders, large and small, brokers of all kinds as well as referral agents.

2. Third-party execution venues: these are the entities that deFIRE routes the orders sourced from originators to. In simpler terms, these are predominantly DEXs (or, potentially, in the future other routers).

3. Pool originators: entities that own assets that they use to list the said assets on a third-party execution venue in a permissionless setting or otherwise. Listing an asset on a DEX boils down to opening a liquidity pool, hence the name 'pool originators'.

4. deFIRE serves as a middleware between traders and other orderflow originators who seek best execution and third-party execution venues who offer liquidity against orders sent their way.

Flows and CWAP tokenomics

Liquidity Mining

Irrespective of CWAP staking, order flow originators are entitled to liquidity mining rewards on a pro-rata volume-weighted basis. In layman's terms, traders get CWAP-denominated rebates for routing orders through deFIRE.

Staking CWAP

Staking CWAP enables:

1. Order flow originators can *stake* CWAP tokens to receive referral rewards. Note, that not every CWAP staker is entitled to have referral rewards. In order to be eligible for these rewards, one needs to have staked a given amount of CWAP tokens. Tiers depend on the volume of orders originated by a given entity and amount of CWAP tokens staked. This feature mostly makes sense for those who channel third party-originated order flow towards deFIRE facilities, such as e.g. non-custodial wallets. This feature enables such entities to earn rewards for using deFIRE;

2. Additionally, *staking CWAP* irrespective of order flow origination entitles those who stake to receive trading fee redistributions on a pro-rata basis (i.e. proportional to how much one has staked compared to the total CWAP balance staked);

3. deFIRE also borrows from the industry's best practices and introduces 'HODL tax': unstaking CWAP leads to a small fee that is re-distributed across everyone who remains staked. This way, long-term staking is incentivized.

Staking CWAP is required for:

1. Order flow originators need to stake CWAP in order to make their pools eligible for order routing. Here, the thinking is that:

    i. Changelly is able to quickly attract sizable order flow through its extensive network of partners and affiliates. Therefore, there is a clear incentive for execution venues to join the Changelly ecosystem.

    ii. Changelly is able to integrate the most popular and most liquid DEXs from inception, making the system competitive from day one. Therefore, certain exclusivity will not come at the expense of worse order execution for our users.

2. Pool originators enable trading in their asset through deFIRE. Here, the logic is likewise simple: pool originators are set to be clear beneficiaries of a massive order flow brokered by deFIRE. In order to become a part of the ecosystem and capture this value, thus, these entities have to have CWAP tokens staked.

3. Perhaps the most important utility that staking order flow originating parties can derive from deFIRE has to do with price fixing. The exact mechanism is still to be specified, but so far, the working hypothesis is that it will involve CWAP token pools that will be reimbursed after adverse price movements, effectively providing a type of insurance on price fluctuation risk.

A Ecosystem-Wide View and Conclusion

From the market infrastructure perspective, deFIRE captures the middle of the order execution value chain, i.e. deFIRE is the value-generating middleman between those who seek execution and those who provide facilities for this execution to happen. The nature of value dynamics within this ecosystem flows from order flow originators to execution venues as it is up to the trading agents where they choose to send their order flow [1]. deFIRE algorithmically optimizes this selection procedure, bringing market efficiency to the wider DeFi ecosystem within given layer-1 networks.

The discussion above has focused on the preliminary view of the deFIRE tokenomics. deFIRE value offering is wider than that. We plan on deploying a game-changing DEX in the coming months. The actual parameters will be defined and calibrated in a series of blog posts that will come out as we set these parameters in stone in our smart contracts. This, however, is subject to change as we move towards decentralizing the governance of our DeFi ecosystem by introducing the deFIRE DAO, where the community of CWAP stakers will be able to introduce proposals for changing system parameters and vote upon them. More details on this will be provided as our products are released on the mainnet.

What are the Benefits to the Cardano Ecosystem?

1. Existing and those that are yet to emerge brokers of ADA and CNT order flow will have trustless execution venues. If benefits from liquidity mining and cheaper transactions on Cardano appear to be sufficiently sizable, Cardano will become the destination for a massive order flow that currently runs through other layer-1 networks.

2. Any new broker built for the Cardano ecosystem will have a built-in instant liquidity.

3. Assets issued on Cardano will gain access to instant deep liquidity.

4. DEX's built on Cardano will get access to actual orderflow.

Changelly is one of the oldest and most established cryptocurrency brands to merge forces with the Occam.fi team and ecosystem; helping to build a more efficient DeFi layer and catalyzing the liquidity of on-chain secondary markets for Cardano.

[1] This is why our tokenomics is built in a way where originators are incentivized to join our ecosystem.