Telegram ID: @**dividik**

Email: kondensfo@mail.ru

FreeTon DEX Architecture & Design Proposal

Architecture and Economic Model for a FreeTON-based DEX

1. Analysis of Trade by Distributed Order Book vs. Liquidity Pool

This section describes the advantages and disadvantages of the two trading modes, i.e. distributed order book and liquidity pool systems and reviews the variants of each mode considered for application in the new DEX.

1.1. Trade Mode Experience and Know-How

Distributed order book systems are the traditional type of trading systems and are applied in stock exchanges, pair trade of fiat currencies and commodity trade. One of the major advantages of distributed order book systems and this mode of trade is the vast knowledge and experience accumulated in using them and virtually experiencing or addressing every possible scenario of applying and operating them. For example, high volume trades, low volume trades, application of advanced rules (e.g. "stop loss"), slow vs. rapid system reactions to trade and price setting, etc.

In comparison, liquidation pools are not commonly applied beyond their application in different cryptocurrency DEXs (such as uniswap.org and curve.fi). The vast majority of financial transactions worldwide is carried put via distributed order book trading systems, hence their reliability and stability in pair trade (such as currency pairs). On the other hand, liquidation pools are emerging in cryptocurrency trade and exchanges, where their use is relatively new though rapidly expanding. Hence, the experience of liquidation pools is relatively limited in comparison to the volume, usage and wealth of experience accumulated in platforms based on distributed order books.

1.2. Reaction, Price Setting and Trade Settlement Time

The major advantage of distributed order book systems is in the immediate reaction time and trade settling, matching in real time "sell" and "buy" orders, even the most complex and highly conditioned among them. The rapid trade in distributed order book systems results from the centralized architecture of these systems, which along with high degrees of security enable to manage funds and liquidity within a single trade ledger and carry out rapid transactions of bought/sold currencies or securities between all parties to a trade.

However, when Blockchain trade systems are considered, trade transactions are completed within relatively long periods that may change from seconds to more than 10 minutes, due to the decentralized structure of the Blockchain and the need to carry out decentralized transactions and to update the miners' ledgers. Over these relatively long periods of time, prices may drastically change and new sell/buy orders may be received, hence modifying the trade and pricing

conditions, yet not enabling traders to engage in frequent and rapid trades until their wallet balances due the completion of selling and buying tokens are settled and updated on the Blockchain. Despite the major advantages of the distributed order book architecture, the time differences between accomplishing a trade and updating the trader's wallet may be used for time-based arbitrages and strategies that can lead to substantial losses and damages to many traders.

The use of a distributed order book requires a relatively massive and intensive submission and cancellation of buy/sell orders into the Blockchain. As the ledger is updated only after a relatively long time (seconds to minutes), values of currencies may substantially change over this time and may damage a trader's position. Additionally, in order to obtain higher priority of the trade order over other orders that await their completion, the trader has to pay higher gas fees, hence increasing the transaction costs of a trade order. Therefore, if traders are interested in engaging in strategies other than long term "buy and hold" (such as swing trading or frequency trading), they should involve in provision of massive amounts of buy/sell orders, updating and cancelling trade orders due to the time difference between trade decisions (that is, trade orders) and their execution of the Blockchain.

The other approach, namely liquidation pools, does not suffer from similar shortcomings, as prices of cryptocurrencies are determined for all pairs of currencies at any time and are continuously updated due to changes in the amounts of currencies in the pool. When trade is carried out via liquidity pools, the price offered to users of the DEX (i.e. potential buyers) is determined being continuously calculated and updated in real time as a function of the amounts of the different cryptocurrencies provided, purchased from the exist in the pool.

In this respect, liquidity pools operate not as a platform for negotiating and matching between buy and sell orders until a price for the traded pair is determined, but rather as an agency that dynamically sets prices for pairs and settles buy/sell orders that are forwarded by users into the pool in determined prices.

Indeed, a distributed order book optimizes price discovery and setting in fiat trade platforms. The centralized architecture of these platforms enables optimal match between different buy/sell orders forwarded to the system and negotiation mechanism that take into account not only the amounts of currencies provided or requested and the initial prices the users determine but also the limits that they set for their trades in real time. However, in decentralized systems, such as those the utilize the Blockchain and in particular FreeTON based platforms, settlement of trade orders is impossible in time durations of micro- and milliseconds and therefore a different order-price settlement mechanism that fits to the relatively long ledger updating durations of FreeTON is required. This mechanism is provided by liquidity pools since, at any time, prices are determined via the DEX and the volumes of currencies in the pool, presented to users who wish to provide ("sell") currencies to the pool or to purchase from it ("buy"). There is no matching or negotiation between buyers and sellers, but all parties that agree to the terms of the trade virtually accept the

determined price and completion of the transactions of the currencies into and out of the pool is carried out by updating the ledger on the FreeTON Blockchain.

Buying and selling cryptocurrencies on a liquidity pool based DEX is significantly less costly than in a distributed order book DEX and requires smaller volumes of buy/sell orders. If the presented price of a currency pair matches the preferences of traders, they can create a single buy/sell order that transfers the currencies into and from the pool and updates the ledger. If traders needs to prioritize the execution of the transaction on FreeTON, they will increase the amount of gas. Since the total volume of orders that communicate with a liquidity pool DEX is significantly lower than in a distributed order book DEX, the "competition" against other transactions is lower and the amount of gas will be lower per transaction. Similarly, the trader will execute a single transaction per trade (rather than several transmitted and cancelled transaction in a distributed order book DEX), thereby the gas spent per trade is on average lower in a liquidity pool DEX than in a distributed order book DEX.

1.3. DEX Mode of Operation

The recommended mode of operation for the DEX is by establishing a liquidity pool platform to manage the trade of users. This recommendation is supported by the following arguments:

1) The development and the operation of the DEX is expected to be simpler as a liquidity pool platform rather than as a distributed order book platform – while the maximal volume of trade orders at any time is expected to be $N(N-1) \times C(C-1) \times O_n$ where:
   N – The number of users of the DEX
   C – The number of currencies traded via the DEX
   O_n – The number of trade orders of user n ($n=1,\ldots,N$)
   Then the maximal volume of trade orders at any time in a liquidity pool based DEX is $(N \cdot C)$, which is significantly lower in scale than the operation and order management in a distributed order book DEX.
2) The costs of trade for users in a liquidity pool DEX will be significantly lower than in a distributed order book DEX, thereby serving better users (who wish to trade at particular price levels presented by the DEX) and resulting in a lower volume of orders necessary to successfully "negotiate" to complete a trade over the FreeTON Blockchain. Additionally, the cost of gas will be lower for users, as prioritizing the completion of a transaction over the FreeTON Blockchain is less costly. It results from the lower scale of transactions that await their completion and the need to carry out one transaction per trade, rather than multiple transactions as in the case of trading via distributed order book DEX.
3) The time of confirming a transaction over the Blockchain may cause damages to traders on a distributed order book as the value of the currency pair may change within it, before the transaction is confirmed on the Blockchain (hence, traders are unable to sell a currency that they negotiated earlier its trade). However, in the majority of trade values, liquidity pool models

are more immunized to significant changes in the value of currencies within short times, as they base the calculation of exchange rates on the volume of tokens in the pool, which usually provides stability against dramatic changes in supply and demand.

1.4. Support of Multi-Platform Exchanges

The exchange of currencies on multiple Blockchains requires establishment of an exchange system that supports the transfer of assets between separate chains in a decentralized manner. To accomplish this aim, two possible solutions can be carried out:

1) Development of atomic swaps between networks – this mode of asset transfer between chains is based on integration of the Lightning network that enables transfer of assets off chains. The network opens a channel for the swap for a time defined by the smart contract and the terms dictate the completion of two sided asset transfer from one chain to another and vice versa.
2) Development of cross-chain bridges in which one asset is "frozen" on the first chain until the other asset is released on the second chain. Once the transaction of the second asset is completed, the first asset is released on the first chain. THORChain implements a solution that is based on cross-chain bridges for cryptocurrency transfers between chains.[1] As of Nov. 2020 FreeTON does have an operable solution either for atomic swaps or cross-chain bridges. However, contests to develop such solutions will continue.[2]

From analysis of the technical terrain, cross-chains provide a simpler solution for connecting multiple chains into the DEX and supporting swaps between them. Despite major development efforts, atomic swaps were not largely applied for supporting multiple Blockchains, with the exception of Decred. Therefore, following FreeTON's development of cross-chain bridges and atomic swap solutions is highly recommended, as this field is expected to yield new possibilities in the upcoming months. Nonetheless, at the current state of the technology application of cross-chains is more mature and widespread and is recommended for carrying out cross-chain operations in the DEX.[3]

[1] See https://medium.com/thorchain/why-cross-chain-bridges-are-superior-to-atomic-swaps-aebde263103c
[2] https://forum.freeton.org/t/contest-atomic-swaps-on-free-ton-31-august-2020-20-september-2020/2508
[3] See also https://www.researchgate.net/publication/329301079_Atomic_Cross-Chain_Swaps/fulltext/5c00a4b892851c63cab055fe/Atomic-Cross-Chain-Swaps.pdf

2. Proposed Architecture of the DEX

2.1. Principals of the DEX Architecture

Following the analysis of the different configurations and alternatives brought above, the proposed architecture of the DEX is based on the following principles:

1) The DEX will operate a liquidity pool platform and will not include a distribute order book platform.
2) The DEX will operate cross-chain bridges to support trades via multiple chains.
3) The exchanges will be carried out in a decentralized manner without support of an underlying token to carry out the exchanges from one cryptocurrency to another.
4) The price setting for cryptocurrency pairs is based on an economic model that implements the best practices of Uniswap and Curve (among other DEXs and their pricing models) and improves them.

The users are divided to:

- Market makers – users that provide liquidity by transferring their tokens (of different cryptocurrencies) into the pool, usually for a sale opportunity.
- Traders – users who provide sell/buy orders for their currencies by swapping them with other currencies at a given price (currency pair trade).

The DEX will integrate the following components to enable a continuous, safe and user-friendly trade and use of its platform:

- Poolbase – a non-custodian platform for generating pools of cryptocurrencies in a non-custodian manner. This component of the platform will manage the holdings of each market maker and will continuously calculate their relative shares in the pool, as more currencies are pulled from the pool due to trades or provided to it due to trade and additional liquidity provided by other market makers. Additionally, Poolbase will distribute the relative share of the commission from each trade dedicated to market makers that provide liquidity to the pool of the purchased currency.
- Pricesage – the price discovery, calculation and presentation of currency pair values for trade. Pricesage will operate with a Curve-like economic algorithm for pricing of each traded currency against the other traded currencies (see Section 3).
- Tradebase – the platform for communicating with traders, that is receiving their trade orders, settling their payment for pool-originated purchased currencies and receiving the payment for it and updating the amounts of the purchased and paid-for currencies in the Poolbase.
- FreeTON – the Blockchain will serve as the main network for managing the ledger of currencies and for carrying out secure transactions between wallets of traders and pools to complete the pair trade in which they are involved. FreeTON will also provide a secure

communications channel for traders providing their buy/sell orders via the Tradebase platform and for market makers providing liquidity to the pool via the Poolbase platform.

- Lightning – the Lightning network will serve as a platform for cross-chain transactions. As the volume of currency trade dramatically increases, the scope of traded cryptocurrencies increases too, suggesting that their spread on networks other than FreeTON (such as the Bitcoin and the Ether networks) is an increasingly difficult challenge for pair trade, where the two currencies are managed on different networks. Additionally, when a DEX offers a broader range for currencies in trade, it attracts more users that seek more diverse opportunities for trading and investment and its competitive position in the DEX market improves. The implementation of Lightning for cross-chain, on- and off-chain swaps (including, for example, Lightning Radar and Lightning Loop) will increase the number of currencies and liquidity pools traded and managed in the DEX by offering non-custodial bridges for on- and off-chain trades.

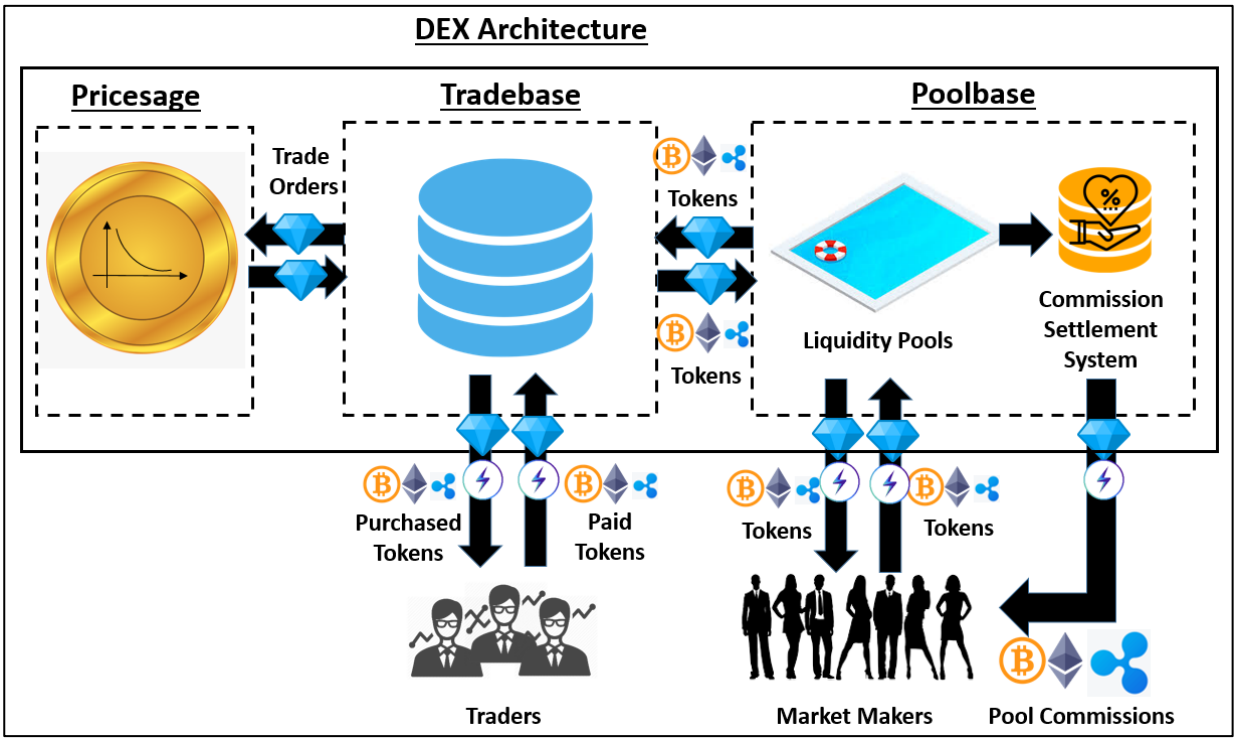


Fig. 1: Description of the architecture and currency flows

2.2. Description of Currency Flows in the System

The DEX system, as described in Fig. 1, works as follows: Market makers who are willing to provide liquidity to the liquidity pools (different currencies) connect to the Poolbase module are transfer the amounts of currencies to the pools via FreeTON in a non-custodial mode. In the case that funds are transferred via different chains (cross-chain transfers), the amounts will be transferred via swap bridges that are provided by the Lightning network. Similarly, funds can be withdrawn by the market makers from the liquidity pools via FreeTON and, if needed, by conducting cross-chain swaps via Lightning.

Traders that accept the prices of currencies presented by the DEX (and calculated by the Pricesage module), conduct trade orders via FreeTON and transfer funds in purchasing currency.

The amount is transferred to the Tradebase module that handles trade orders. The Tradebase module then transfers the purchasing currency to the liquidity pool and in returns withdraws the equivalent amount (minus the commission) from the liquidity pool of the purchased currency. The amount of the purchased currency is transferred to the trader's wallet and the commission for the trade is distributed between the market makers that contributed liquidity to the liquidity pool of the purchased currency via the commission settlement module. In parallel, the trade order and data on updated total amounts in the liquidity pools of the purchasing currency and the purchased currency are sent to the Pricesage and the prices of the currencies are updated as the trade is concluded. The Lightning network also supports cross-chain trades through its swap bridges, as in the case of market makers.

2.3. Detailed technical specification of the proposed implementation with the justification of the selected approach: smart contracts, integration layer, interfaces

The Lightning Network for creating off-chain smart contracts will be based on LND. LND enables creating Hash Time-Locked Contracts (HTLCs) that enable generation and delivery of transactions without a direct channel between sender and recipient. NLD creates a routing architecture and automatically transfers the transactions via multiple hops. By doing so, the Lightning Network serves as an interconnected financial system and enables transactions and exchange between tokens on different chains (cross-chain swaps) through its HTLCs.

To carry out the complete structure and solution, the integration layer of the DEX will include the following technologies:

- FreeTON will serve as the Blockchain network of the DEX
- Proposed application of a multisig (multi signature) wallet to facilitate the adoption and use of the DEX by larger and commercial entities, rather than by small users. A solution proposed for supporting the creation and management of multisig wallets on FreeTON is TONOS-CLI.[4]
- Funds will be kept via the application of Lightning by Hash Time-Locked Contracts (HTLCs) in the ownership of their holders (though "frozen" to enable the completion of the trade ordered by their holders) in a non custodial way.
- Swap bridges between pairs of currencies will be conducted over the Lightning network to assure the completion of the trade by its HTLCs and to provide an off-chain and cross-chain solution for trades (for example, trading BTC for ETH, etc.). The proposed swap bridges will work as submarine swaps - on-chain to off-chain swaps and vice versa that connect as bridges between Lightning and the Blockchain.
- Support for non-custody exchange of any tokens within the target network via application of Lightning network submarine swaps - the submarine swaps are implemented by

[4] See explanation how TONOS-CLI can be installed and operated on FreeTON at: https://docs.ton.dev/86757ecb2/v/0/p/94921e-multisignature-wallet-management-in-tonos-cli

integrating them via REDSHIFT RADAR[5] as trustless and non-custodial swap bridges with relative ease. Other DEXs that are built upon the Lightning network and the REDSHIFT RADAR are Boltz, SparkSwap and others.[6] This solution of swap bridges built on submarine swaps on Lightning will also support non-custodial provisions of liquidity from external Blockchains by forming Hash Time-Locked Contracts (HTLCs) on the funds added to the liquidity pools and "freezing" funds for the pair trade via application of Hash Time-Locked Contracts (HTLCs) on trade orders when currencies sold are managed on external chains.[7]

- Liquidity pools will be used for providing the liquidity necessary to complete the exchanges and trades. The pricing mechanism and model as presented in section 3 below and the order management system (i.e. Tradebase and Pricesage) have to be developed and integrated. Transfer of funds to- and pulling funds from the liquidity pools by market makers (the Poolbase model) can be based on web based and mobile based interfaces that dedicate funds via Lightning to the pool and transfer funds (where needed) to and from the owner's wallet on FreeTON via TONOS CLI.
- The commission sharing mechanism between market makers (a part of the Poolbase module) has to be developed as described in the model in section 1.3 above.

Interfaces between the technologies integrated in this architecture:

1) A user interface for traders: this web and mobile interface will present the traded pair prices at any time, the volumes of trade and will provide a possibility for traders to indicate the currency that they want to sell and the amount dedicated, the exchange rate, the target currency that they want to buy and the amount sold to them upon completion of the trade (after commission). The traders will be provided with the default amount of gas to be paid and can increase it to increase the priority of completing the transaction. After completion of the transactions of the pair trade, traders will be notified upon it.
2) A user interface for the market makers: this this web and mobile interface will present the currencies traded in the pool and the estimated profits that they can yield for the currency and the amount that they wish to dedicate to the pool based on the trades of the last 24 hours. This estimation can provide quantitative support to the decision of market makers to join the liquidity pools with their holdings and facilitates FOMO (fear-of-missing-out potential profits by not joining the liquidity pools of the DEX). The market makers then confirm the currencies and amounts in their holdings to be dedicated to the liquidity pools and confirm their actions. After creating the smart contract on Lightning, market makers will be notified about the dedication of their funds to the liquidity pools.

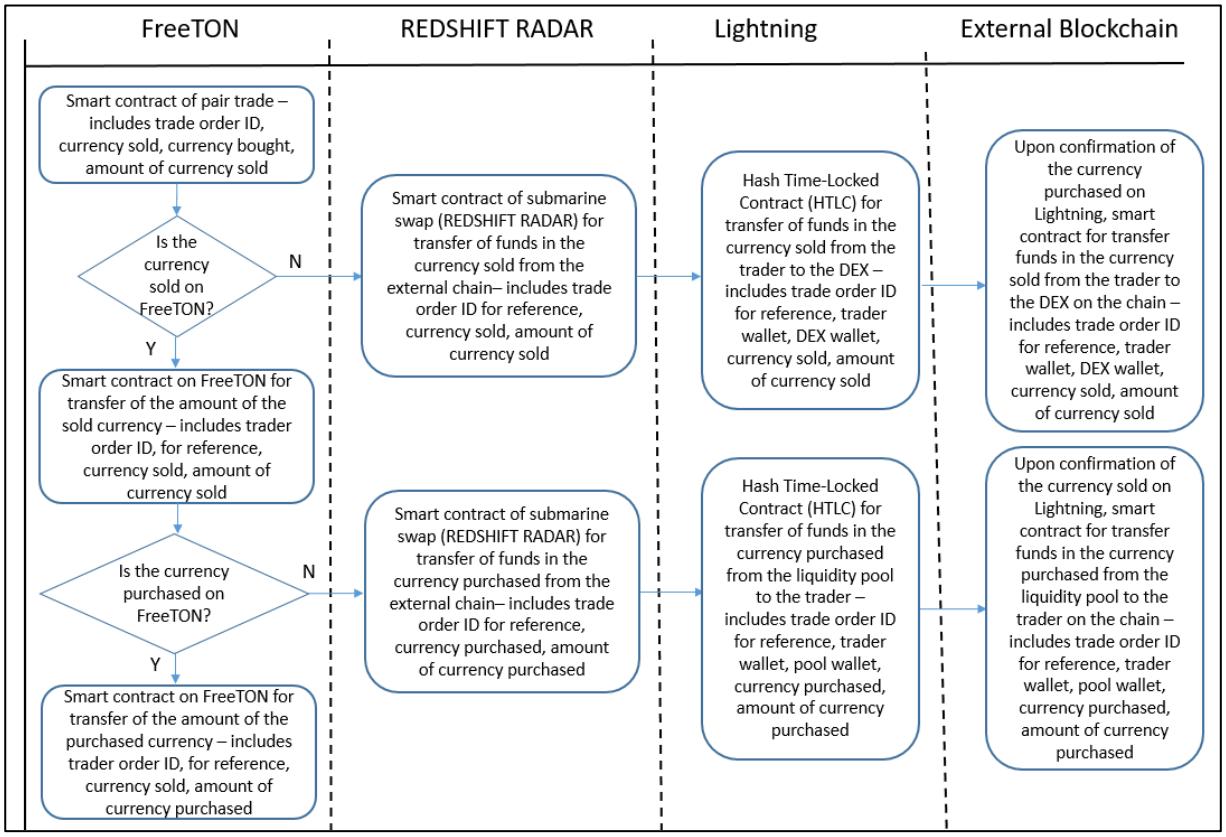
[5] https://redshift.radar.tech/
[6] See https://wiki.ion.radar.tech/tutorials/lightning-exchanges#trustless-noncustodial-exchanges
[7] The integration of the REDSHIFT RADAR platform and explanation of the exchange of smart contracts on the Lightning network and its api are brought in: https://github.com/RadarTech/redshift-widget-wrapper

3) Price update interface between Tradebase and Pricesage – the completed trade transactions along with the data on the pair of the amounts received into and issued from the liquidity pools of the currencies will be transferred from the Tradebase into the Pricesage. Upon receipt of such a transaction in the Pricesage module, the meaning is that the amounts of the pair of currencies has changed and their pair prices should be recalculated according to the model in section 3. Pricesage will add the transaction of the trade into its database of historical trades and prices and will send a message with the newly calculated currency pair prices to the Tradebase in order to present the current pair prices.
4) Liquidity pool update interface between Tradebase and Poolbase – when traders accept the prices of a pair of currencies, they send trade orders via the Tradebase module. Once a trade order is accepted, the Tradebase will send the transaction to pull the necessary amount of the purchased currency from its liquidity pool while transferring the amount accepted from the trade into the liquidity pool of the sold currency. Poolbase will then generate transactions on FreeTON or on the Lighting network (in case of cross-chain trade of currencies from different Blockchains) and will operate submarine swaps if needed to complete the trade. Then, Poolbase will spread the profits from the commissions to all the market makers, as presented in the model in section 1.3.

2.4. Smart contracts and their parameters

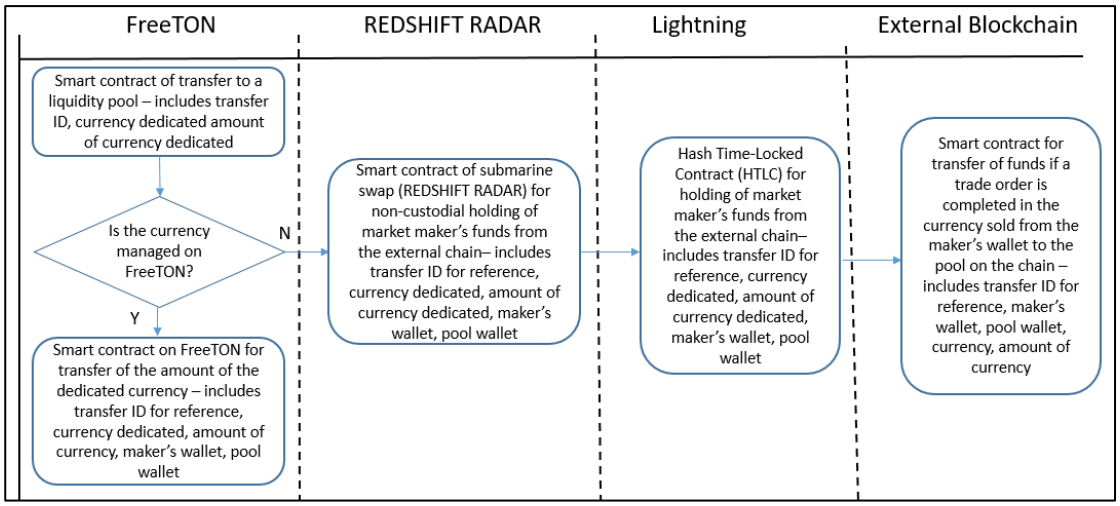
The solution and the architecture are based on integration of multiple chains via swap bridges and smart contracts as follows:

Trader <-> DEX trade orders and transactions:



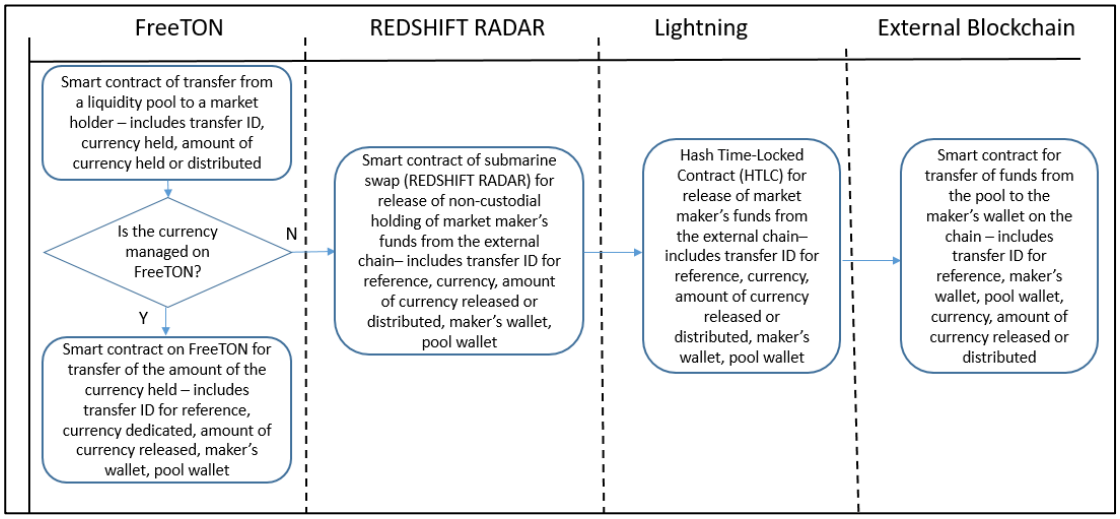
Market Maker -> DEX liquidity pool:

Funds from the market maker's holdings are dedicated to the liquidity pool as follows:



DEX liquidity pool -> Market Maker:

Funds from the market maker's holdings are withdrawn from the liquidity pool or are distributed as profits from commissions as follows:



2.5. Scalability potential for adding new tokens

The proposed architecture has major benefits for the DEX in terms of scalability and supporting additional cryptocurrencies.

First, as long as tokens are transformed on FreeTON, no scalability issues are expected as FreeTON can allegedly support over 1 million transactions per second.[8] This is a major capacity of the DEX in terms of transaction speed, larger than the speed of any other Blockchain or financial processing network.

Second, the swap bridges that are based on submarine bridges (through the REDSHIFT RADAR technology) can support any off-chain and cross-chain trade on the Lightning network. As the Lightning network will be further developed to support any necessary Blockchain via its LND platform.

Third, the use of Lightning for cross-chain swaps guarantees not only support to multitude of Blockchains, but also the completion of transactions on the Lightning Network takes between milliseconds to less than a minute.

Fourth, the Pricesage model limits the number of previous trades to be considered in price calculations. Therefore, the calculation of pair prices after each trade is completed is conducted in real time and can prevent time-based arbitrages due to the duration necessary for price updates.

2.6. Maximum utilization of the target network advantages

The FreeTON network is an excellent choice for managing the transactions of the DEX due to the high speed limit of transactions (over 1 million transactions per second). Such a speed of transactions can support huge volumes of trade, thereby the DEX can be later developed to support additional applications, such as cross-border money transactions, fiat-to-crypto and crypto-to-fiat transactions, support of derivative exchange and securities exchange, etc.

[8] See https://medium.com/@Pisha_1986/concisely-about-free-ton-concisely-about-the-future-3958719fb54e

The opening of the DEX is a first stage in fostering novel uses of financial transactions. In terms of the cross-chain solutions, the Lightning network provides an additional layer to support more complex and diverse transactions and currency trades.

2.7. Optional governance mechanism or a possibility of adding such a mechanism in the future to govern the parameters of the exchange, including but not limited to the liquidity provision and the fees

The following parameters have to considered when the governance of the DEX is formed:

1) The currencies that will be supported and traded by the DEX.
2) The DEX's growth plan and strategy in adding additional currencies to the trade.
3) The criteria that will dictate the decision whether a currency will be added to the trade or not.
4) The size of the commission charged from the trader for the trade.
5) Whether the DEX may change the commission for larger trades (i.e. less commission is charged for a large trade order).
6) The way in which the revenues from the commission will be split between the DEX and the market makers.
7) Whether the shares of the revenues from commission will be dynamically modified according to the trader order amount, trade volume, size of the liquidity pool, etc.
8) The number of past trades (h) to be determined for the pricing model, presented in section 3.
9) Whether the number of past trades (h) will be the same for each pair of currencies or be different according to the currencies, trade volumes, liquidity pool sizes, etc.

3. Economic Model of the DEX

Each transaction is charged with swap commission (usually 0.3% of the amount in swap charged from the traders). The commission is then divided between the DEX and the market makers according to the relative share of their holdings in the purchased currency:

comm – the percentage for commission from every purchase order accomplished (e.g. 0.3%).

α – the share of the commission paid to the DEX.

Vm – the value of currency m purchased by a trader.

PVm – the total value of currency m in the pool before completion of the trade.

m – the identifier of the purchased currency *m*.

MMVim - the value of currency *m* provided to the pool by market maker *i*.

The remaining amount in the pool of the purchased currency *m*:

(1) PVm' = PVm – Vm

The remaining amount in the pool of the currency *g* paid by the trader to the pool for the purchase:

(2) PVg' = PVg + Vg

The amount of the purchased currency *m* paid to the trader after commission:

(3) TVm = (1-comm)·Vm

The amount of the purchased currency *m* paid to the DEX as its commission:

(4) *α·comm·Vm*

The amount of the purchased currency *m* transferred to each market maker when the purchase order is completed:

(5)

$$\frac{MMVim}{\sum_i MMVim} \cdot (1-\alpha) \cdot comm \cdot Vm$$

The pricing model is based on the Uniswap model that determines after the completion of each trade the prices of the two currencies involved in the pair trade, as the total amount of the liquidity pool decreases by the share bought by the trader and the total amount of the liquidity pool of the currency paid by the trader increases.

The Uniswap model is based on a non-linear equation as follows:

(6) PVm·PVg = K

Where *K* is a constant that results from the multiplication of the amounts in the liquidity pools of both bought and paid currencies.

Therefore, the price of currency *m* in terms of currency *g* tokens before the trade is completed:

(7)

$$p_{mg} = \frac{PV_g}{PV_m}$$

After the trade is completed, the new price of currency *m* in terms of currency *g* tokens:

(8)

$$p'_{mg} = \frac{PV'_g}{PV'_m} = \frac{PV_g + V_g}{PV_m - V_m}$$

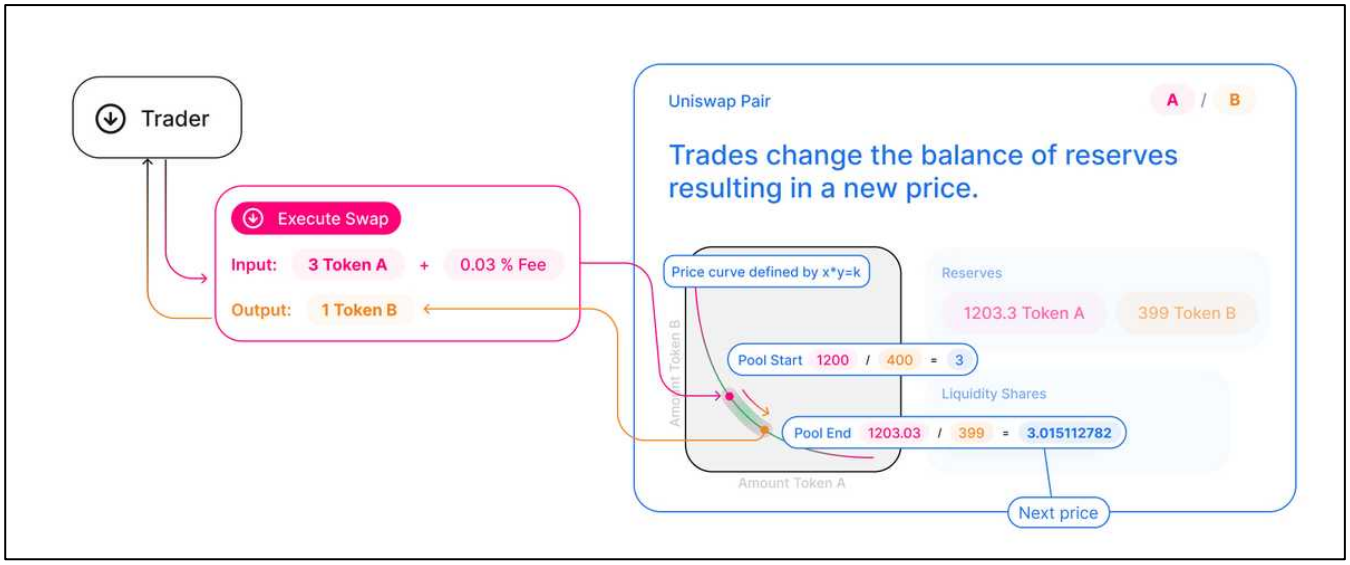


Fig. 2: Example of post-trade price setting by the Uniswap model

In order to prevent this effect of major and minor trades that can dramatically affect and modify the values of the traded pair of currencies, an improved model that includes a harnessing mechanism that tames drastic price changes (and therefore opens the trade to speculative trades and currency manipulations) is presented herein.

The proposed new model is based on moving average that utilizes exponential price factoring. By determining the price through this model, it does not take to account only the proportion between the volumes of both currencies in their liquidity pools (which is momentary and therefore can be easily manipulated through a sequence of trade orders), but also considers historical currency prices that were determined by former trades. The model includes in the pricing the currency prices at the last *h* trades (*h* is the number of harnessing periods that moderate price changes), where the "oldest" trade has a minimal effect on current currency prices and the most recent trade has a maximal impact on them.

Therefore, the model is as follows:

a. Define the value of the number of harnessing periods *h* (recommended value: *h*=5).
b. Calculate the prices of currency *m* and currency *g* after the trade is completed, as presented in (8) above. This value is defined as $p'_{mg}(t)$.
c. Retrieve the prices of the currencies in the last h trades that were completed before the current trade: $p'_{mg}(t-1)$, $p'_{mg}(t-2)$, $p'_{mg}(t-3)$, … , $p'_{mg}(t-h)$
d. Finally, define the price $p^*_{mg}(t)$ of currency *m* in terms of currency *g* tokens for the upcoming (next) trade as follows:

$$(9)\ p^*_{mg}(t) = \frac{p'_{mg}(t)\cdot e^{-1}}{\sum_{u=0}^{h} e^{-(u+1)}} + \frac{p'_{mg}(t-1)\cdot e^{-2}}{\sum_{u=0}^{h} e^{-(u+1)}} + \frac{p'_{mg}(t-2)\cdot e^{-3}}{\sum_{u=0}^{h} e^{-(u+1)}} + \frac{p'_{mg}(t-3)\cdot e^{-4}}{\sum_{u=0}^{h} e^{-(u+1)}} + \ldots + \frac{p'_{mg}(t-h)\cdot e^{-(h+1)}}{\sum_{u=0}^{h} e^{-(u+1)}}$$

The relative weight of each trade order affecting the prices of the currencies via the price setting equation (9) is as follows:

	h=1	h=2	h=3	h=4
$p'_{mg}(t)$	0.731059	0.665241	0.643914	0.636409
$p'_{mg}(t-1)$	0.268941	0.244728	0.236883	0.234122
$p'_{mg}(t-2)$		0.090031	0.087144	0.086129
$p'_{mg}(t-3)$			0.032059	0.031685
$p'_{mg}(t)-4$				0.011656

Table 1: The relative weight of the calculated price and the prices in former trade for harnessing speculative trade effects.

4. Position on existing DEX problems (see "Existing DEX problems to be aware of" section below) and how they are tackled in the proposed architecture

4.1. Frontrunning (flash boys 2.0 and Mooniswap vs Uniswap value proposition). If it is not possible in target blockchain (as it is), should be clearly stated why

The application of trade bots in DEXs suggests that automated and frequent trade orders cause major instabilities because of automatic identification of arbitrages. Consequently, gas prices increase for the whole Blochchain population of users as bots prioritize the completion of their transactions to engage in additional volume of trade.

Despise the severity of these concerns, these are minor concerns relatively to the potential threats of price manipulations over liquidity pool based DEXs. The price setting by the non-linear equation (see equation (6) above) and the price determination according to the momentary existence of amounts of traded currencies pre- and post-trade suggest that prices can be significantly altered, in particular in very high and very low currency price ratios. Consequently, major changes in these price ranges can achieved with relative ease but trading small amounts of one of the currencies of the pair (due to the tangent to the pricing curve that is affected by very small changes when the tangent is steep or flat).

The pricing equation (9) presents a harnessing effect on these potentially radical price changes by attributing decreasing weight to prices in former trades. Though the main component of the price setting mechanism is similar to that of Uniswap, the exponential smoothing deters massive prices changes and tames them (in particular, as the *h* factor increases) due to manipulations that are based on the amount of tokens in the liquidity pool or on timed purchased orders that dramatically affect prices.

The reduction in the supply of tokens to a liquidity pool of one of the traded currencies, due to massive purchases or market makers that withdraw their holdings in the pool may create one-sided liquidity and at the complete loss of tokens in a liquidity pool even an impairment loss. Clearly, these problems result from shortage of market makers that can drastically affect prices, as a currency is in shortage of supply.

The problems can be solved by a governance mechanism in which the DEX automatically steps in and transfers amounts of the currency in shortage into its liquidity pool, i.e. the DEX will be a major market maker if external market makers do not participate in the pool.

The funds for this governance mechanism will be transferred from a share of the DEX's revenues gained via commissions charged for each trade (see equation (4) above). Since the architecture of the DEX includes swap bridges, any funds accumulated in another currency can be exchanged to the selected currency, even in cross-chain situations and immediately be injected into the liquidity pool. This governance mechanisms with assure stability of the DEX and will prevent substantial devaluations due to momentary shortages of market makers.

4.2. Shortcomings of standard curves and its inflexible nature in liquidity based approach. These result in the issue - dilution of liquidity into several AMMs (general and specific ones with a more specific curve like Uniswap vs. Curve) which leads to non-optimal price execution

The price calculated by the Uniswap model mentioned in equation (8) above and presented in Fig. 2 is very sensitive to small changes and "flooding" the DEX with significant trade order in comparison to the size of the liquidity pool dramatically inflate value of the purchased currency, while the currency paid by the trader significantly devalues. Moreover, even relatively moderate amounts in comparison to the size of the liquidity pool can significantly affect the prices due to the non-linear curve and the tangent values at most of its range that dictates that in high exchange values small changes in the price of one currency result in major changes of the other currency and *vice versa* (see Fig. 3).

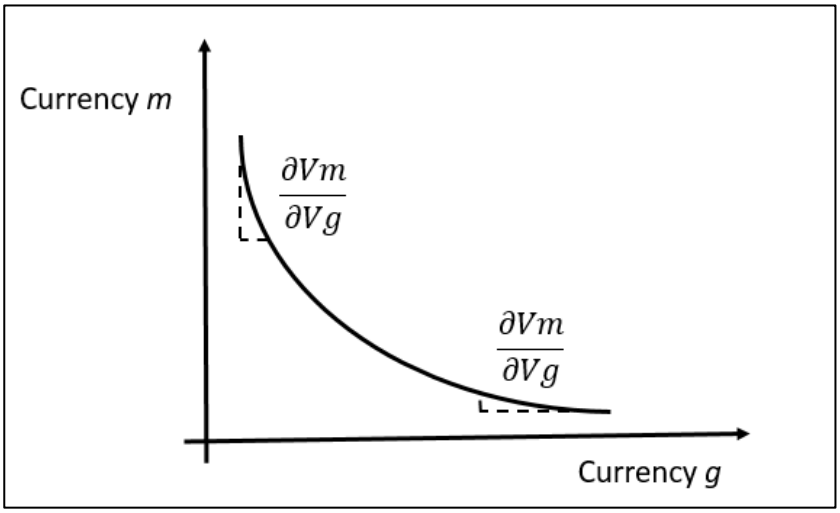


Fig. 3: Changes in the liquidity pools significantly affect currency prices.

In both models of UniSwap and Curve.fi, major and minor trades that can substantially change the values in which a pair of currencies is traded and open the trade to speculations and manipulations that are based on relatively small modifications in the amounts of currencies in smaller liquidity pools. The proposed model offers an improved solution through the harnessing mechanism that prevents drastic price changes by considering former trades and price changes (in a relatively smaller weight) in the calculation of the current currency prices.

4.3. One-sided liquidity. Impairment loss problems. The market risk of two assets in the pool is widely discussed. These problems should be somehow covered or at least mentioned for further research.

Another liquidity pool-based approach problem is the customized proportion of assets, number of assets in the pool, and metapools. How to regulate the number of assets in the pool, what is the price optimal routing, will it be available to create metapools.

When one of the currency's liquidity pool "dries" and empties due to lack of interest from market makers or heavy withdrawals of funds from the liquidity pool by the holders, the DEX may confront a situation of impairment loss. Similarly, when market makers deposit larger amounts of liquidity into the pool of one of the currency that overshadow the liquidity pools of the other currencies, the DEX may confront a one-sided liquidity problem. However, both problems have the following solutions:

1) When rational economic agents (i.e. traders and market makers) observe the price asymmetry between liquidity pools as a result of increasing the amount of one currency while the other currency remains the same, they identify the price changes in favour of the smaller pool and rush to purchase the less popular currency and dedicating larger amounts of liquidity to its pool for profit. This dynamics is based on the price setting which determines the changes in liquidity pool amounts as the basis for the new currency pair prices and hence is affected by this opportunistic profit-seeking behavior that will balance the amounts in the liquidity pools in the long-run and will provide the necessary liquidity to liquidity-seeking currencies. Importantly, even when the increases in liquidity will be relatively rapid, price changes will be gradual due to the harnessing mechanism of the price setting model, therefore assisting to stabilize the prices of less popular currencies, their demand and supply by market makers.
2) The DEX can establish a liquidity fund and dedicate a large share of its revenues to provision of liquidity when necessary to prevent impairment loss and one-sided liquidity. The currencies in the fund can be exchanged to any other currency supported by the DEX and the DEX will behave like a market maker by infusing the necessary funds into the liquidity pool in need. This measure will prevent short-term speculative operations that can largely damage the propensity of users to engage in trade or market makers to dedicate funds to particular liquidity pools.

4.4. Another liquidity pool-based approach problem is the customized proportion of assets, number of assets in the pool, and metapools. How to regulate the number of assets in the pool, what is the price optimal routing, will it be available to create metapools.

At this stage, when the dynamics of the behavior of both traders and market makers is unknown and their behavior to price changes that are dictated by the pricing model should be observed, it is too early to set mega-pools. Rather, at the first stage of its operation, the DEX should support a limited amount of currencies for trade. At the second stage, the number of traded currencies should gradually be expanded and the success of attracting market makers to dedicate funds to the new liquidity pools should be examined. Only after collecting sufficient data on trades, participation in liquidity pools and price changes and gaining sufficient experience in conventional currency pair trades, the DEX should decide whether to expand to mega-pools.

4.5. Orderbook-based exchanges should state clearly how the on-chain order book is maintained and how its scalability issue is resolved. It is naive to state that transactional expenditures would stay at an effective zero level, so it has to be covered.

The proposed architecture is based on liquidity pools and not on order book. Distributed order book systems are the traditional type of trading systems and are applied in stock exchanges, pair trade of fiat currencies and commodity trade. One of the major advantages of distributed order book systems and this mode of trade is the vast knowledge and experience accumulated in using them and virtually experiencing or addressing every possible scenario of applying and operating them. For example, high volume trades, low volume trades, application of advanced rules (e.g. "stop loss"), slow vs. rapid system reactions to trade and price setting, etc.

In comparison, liquidation pools are not commonly applied beyond their application in different cryptocurrency DEXs (such as uniswap.org and curve.fi). The vast majority of financial transactions worldwide is carried put via distributed order book trading systems, hence their reliability and stability in pair trade (such as currency pairs). On the other hand, liquidation pools are emerging in cryptocurrency trade and exchanges, where their use is relatively new though rapidly expanding. Hence, the experience of liquidation pools is relatively limited in comparison to the volume, usage and wealth of experience accumulated in platforms based on distributed order books.

The major advantage of distributed order book systems is in the immediate reaction time and trade settling, matching in real time "sell" and "buy" orders, even the most complex and highly conditioned among them. The rapid trade in distributed order book systems results from the centralized architecture of these systems, which along with high degrees of security enable to manage funds and liquidity within a single trade ledger and carry out rapid transactions of bought/sold currencies or securities between all parties to a trade.

However, when Blockchain trade systems are considered, trade transactions are completed within relatively long periods that may change from seconds to more than 10 minutes, due to the decentralized structure of the Blockchain and the need to carry out decentralized transactions and to update the miners' ledgers. Over these relatively long periods of time, prices may drastically change and new sell/buy orders may be received, hence modifying the trade and pricing conditions, yet not enabling traders to engage in frequent and rapid trades until their wallet balances due the completion of selling and buying tokens are settled and updated on the Blockchain. Despite the major advantages of the distributed order book architecture, the time differences between accomplishing a trade and updating the trader's wallet may be used for time-based arbitrages and strategies that can lead to substantial losses and damages to many traders.

The use of a distributed order book requires a relatively massive and intensive submission and cancellation of buy/sell orders into the Blockchain. As the ledger is updated only after a relatively long time (seconds to minutes), values of currencies may substantially change over this time and may damage a trader's position. Additionally, in order to obtain higher priority of the trade

order over other orders that await their completion, the trader has to pay higher gas fees, hence increasing the transaction costs of a trade order. Therefore, if traders are interested in engaging in strategies other than long term "buy and hold" (such as swing trading or frequency trading), they should involve in provision of massive amounts of buy/sell orders, updating and cancelling trade orders due to the time difference between trade decisions (that is, trade orders) and their execution of the Blockchain.

The other approach, namely liquidation pools, does not suffer from similar shortcomings, as prices of cryptocurrencies are determined for all pairs of currencies at any time and are continuously updated due to changes in the amounts of currencies in the pool. When trade is carried out via liquidity pools, the price offered to users of the DEX (i.e. potential buyers) is determined being continuously calculated and updated in real time as a function of the amounts of the different cryptocurrencies provided, purchased from the exist in the pool.

In this respect, liquidity pools operate not as a platform for negotiating and matching between buy and sell orders until a price for the traded pair is determined, but rather as an agency that dynamically sets prices for pairs and settles buy/sell orders that are forwarded by users into the pool in determined prices.

Indeed, a distributed order book optimizes price discovery and setting in fiat trade platforms. The centralized architecture of these platforms enables optimal match between different buy/sell orders forwarded to the system and negotiation mechanism that take into account not only the amounts of currencies provided or requested and the initial prices the users determine but also the limits that they set for their trades in real time. However, in decentralized systems, such as those the utilize the Blockchain and in particular FreeTON based platforms, settlement of trade orders is impossible in time durations of micro- and milliseconds and therefore a different order-price settlement mechanism that fits to the relatively long ledger updating durations of FreeTON is required. This mechanism is provided by liquidity pools since, at any time, prices are determined via the DEX and the volumes of currencies in the pool, presented to users who wish to provide ("sell") currencies to the pool or to purchase from it ("buy"). There is no matching or negotiation between buyers and sellers, but all parties that agree to the terms of the trade virtually accept the determined price and completion of the transactions of the currencies into and out of the pool is carried out by updating the ledger on the FreeTON Blockchain.

Buying and selling cryptocurrencies on a liquidity pool based DEX is significantly less costly than in a distributed order book DEX and requires smaller volumes of buy/sell orders. If the presented price of a currency pair matches the preferences of traders, they can create a single buy/sell order that transfers the currencies into and from the pool and updates the ledger. If traders needs to prioritize the execution of the transaction on FreeTON, they will increase the amount of gas. Since the total volume of orders that communicate with a liquidity pool DEX is significantly lower than in a distributed order book DEX, the "competition" against other transactions is lower and the amount of gas will be lower per transaction. Similarly, the trader will

execute a single transaction per trade (rather than several transmitted and cancelled transaction in a distributed order book DEX), thereby the gas spent per trade is on average lower in a liquidity pool DEX than in a distributed order book DEX.