DAOCROSS AND DAOSWAP

GP SAGGESE, PAUL SMITH

Contents

1. Introduction

DaoCross and DaoSwap constitute a decentralized protocol that facilitates on-chain ERC20 token exchange. DaoSwap provides a mechanism for efficient relative price discovery, and DaoCross enables parties to engage in zero market impact transactions with price improvement.

DaoSwap is a smart contract for performing decentralized Walrasian-style auctions at regular time intervals. The auction performs price discovery by matching supply and demand ([11]).

DaoCross is a decentralized liquidity pool that crosses buy and sell orders with respect to an external reference price, i.e., a price oracle. This allows traders to interact directly with each other and share price improvement with respect to exchanges (by trading at bid-ask midpoint). Additionally, order intentions are not publicly disclosed prior to a cross, which enables block or other high-volume traders to execute quickly with minimal market impact.

DaoSwap and DaoCross differ in how the token exchange rate is determined, but both share several common advantages:

(1) Low Cost: they are a DeFi primitive that allows trading tokens peer-to-peer without incurring spread costs
(2) Capital Efficiency: participants provide liquidity only when they wish to trade, and only in the amount they wish to trade
(3) No Impermanent Loss: liquidity providers are not exposed to the risk of impermanent loss (a form of unrealized loss that becomes realized upon withdrawing liquidity), unlike the case with other decentralized exchange protocols based on automated market makers
(4) No Intermediary Custody: exchanged tokens always remain under the control of their respective owners

Date: March 20, 2023.

(5) No Rent Extraction from High-Frequency Traders: speed alone does not confer an advantage to traders, as the discrete timing prevents predatory tactics such as front-running, limit order scalping, and spoofing, which are known issues seen with continuous limit order books
(6) Ease-of-use: the interaction between buyers and sellers occurs through smart contracts, with a website front-end available

2. Matching liquidity

Suppose there are two parties, Alice an ETH holder and Bob a BTC holder, who wish to swap tokens at a competitive rate. Suppose also that there are many additional ETH and BTC holders who may be interested in participating in a swap. How should the liquidity be pooled? At first glance, it appears that there should be a single pool of liquidity. The wrinkle manifests in determining how to express a desire to trade. A simple expression of a desire to trade is a limit order representing a commitment to trade up to q in quantity of a token at a token exchange rate up to p. But what if some parties express quantity in terms ETH and and some in terms of BTC, and some parties express limit prices in terms of ETH per BTC, while others express limit prices in terms of BTC per ETH? Under these conditions, setting a single clearing price and determining fill prioritization rules raises several questions without obvious answers.

2.1. **Breaking the symmetry.**

To simplify, we follow the practice of FX (foreign exchange) futures markets, which break the symmetry by specifying two non-interchangeable roles:

(1) a *base* currency (for quantity)
(2) a *quote* currency (for price)

The roles are expressed by writing *base currency/quote currency*, e.g., "EUR/USD".

A limit order then consists of a quantity expressed in the units of the base currency and a price expressed in terms of the quote currency (per unit or suitable multiple of base currency). See, for example, [6] (e.g., footnotes on page 25), for usage of this terminology. See [7] for how this works in practice for Euro FX contracts, where contract units are denominated in Euros and price is quoted in U.S. dollars and cents per Euro increment.

By breaking the symmetry, one may run a standard limit order book, hold a classical Walrasian-style auction, and handle size quantization effects by using one of a variety of priority rules based on quantity, price, and time.

See [4] for discussion around these variations and their effects on market quality outcomes.

On the other hand, liquidity for a pair of currencies may be split across two separate contracts, necessarily with two separate limit order books. Using our example, this would mean treating BTC/ETH and ETH/BTC as separate token pairs, even though the underlying parties and sources of liquidity are the same.

2.2. **Basket case.**

It seems plausible that by retaining the symmetry in the two-token case and instead treating a pair of tokens as a single source of liquidity, one may contrive a more efficient exchange mechanism.

This minor expansion, however, suggests widening even further the universe of eligible swaps. For example, if there are three tokens available for exchange, one could contemplate many-for-one, one-for-many, or many-for-many token swaps, all to be carried out in an atomic fashion, and perhaps with complex constraints. A toy case along these lines one may consider is as follows:

Problem 1 (Triangular liquidity)**.** *Suppose there are the following three parties:*

- *Party A, who holds* BTC *and wants* ETH
- *Party B, who holds* ETH *and wants* DAI
- *Party C, who holds* DAI *and wants* BTC

How should an auction be structured to "best" facilitate exchange?

While there may be other use cases and even demand for such auctions, unfortunately, the problem in general is NP-complete (e.g., [12]), which is a significant limiting factor in terms of feasibility and auction expense.

3. Protocol Introduction

In the previous section, we discussed the notions of base currency and quote currency from foreign exchange. Here we extend them to tokens.

Definition 2 (Base/quote tokens)**.** *A token (ordered) pair consists of a* base token *and a* quote token*. The shorthand notation for expressing the pair is* base token/quote token *(e.g., "*BTC/ETH*"), and as such indicates the respective roles of the tokens.*

By convention, quantity *to exchange is expressed in terms of the base token, and* price *is a token exchange rate expressed in terms of the quote token per unit of base token (or multiple thereof).*

By way of example, in the pair BTC/ETH, BTC is the base token and ETH is the quote token. Interest to trade is expressed in terms of orders with BTC as base token and ETH as quote token:

- Quantity q is in terms of the base token (buy/sell a certain amount of BTC)
- Limit price is in terms of the quote token (buy/sell BTC with a limit price of p BTC per ETH)
- A "buy" order represents a commitment to purchase the base token ("BTC") and pay with the quote token ("ETH")
- A "sell" order represents a commitment to sell the base token ("BTC") and receive the quote token ("ETH").

A party who places a "buy" order must have the quote token ("BTC") in custody, i.e., in its wallet. A party who places a "sell" order must have the base token ("ETH") in custody.

3.1. Order attributes.

A DaoCross or DaoSwap order must have the following attributes:

(1) Base token
(2) Quote token
(3) Action (buy/sell)
(4) Quantity
(5) Limit price
(6) Timestamp
(7) Deposit address

We have discussed attributes 1-5 in some detail.

The 6th attribute (timestamp) is used to determine eligibility in a swap or cross and can play a role in order fill priority.

The 7th attribute (deposit address) enables one to use multiple wallets to facilitate account management. For example, a miner may have a supply of BTC collected and held in one wallet which it would like to systematically diversify into ETH and perhaps other tokens. In specifying a deposit address, it may use a separate wallet to collect incoming ETH.

3.2. DaoCross reference price.

DaoCross relies on a *price oracle* for determining the effective token exchange rate in a cross. The price oracle may come from a lit exchange, centralized or decentralized, or even on-chain automated market makers such as Uniswap ([2, §2.2]).

The case of using an automated market maker as a price oracle is relatively straightforward, provided there is an automated market maker trading the target currency pair with sufficient liquidity.

To use an exchange as a price reference, we must consider some additional steps. First, exchanges typically use a dollar stablecoin (e.g., USDC, USDT) as the quote currency and all other currencies

as base currencies. Our example of BTC/ETH would be considered a cross pair in the world of traditional finance. Because most cross pairs are not traded directly on exchanges, we must derive a clearing price from pairs involving stablecoins.

Example 3 (Lit exchange bid-ask midpoint reference price)**.** *Let* $\text{bid}_{\text{BTC}}, \text{ask}_{\text{BTC}}$ *be stablecoin-denominated top-of-book bid-ask prices for* BTC *(e.g., expressed in* USDC*), and* $\text{bid}_{\text{ETH}}, \text{ask}_{\text{ETH}}$ *be the analogous prices for* ETH*. Then, a commitment to buy one* BTC *and pay* ETH *would clear at a midpoint price of*

$$\text{BTC/ETH}_{\text{midpoint}} = \frac{\text{bid}_{\text{BTC}} + \text{ask}_{\text{BTC}}}{\text{bid}_{\text{ETH}} + \text{ask}_{\text{ETH}}}$$

expressed in BTC per ETH. Note that if the dollar price of BTH is significantly more than the dollar price of ETH, then this price implies paying many multiples of ETH for BTC (as is the case at the time of this writing).

In general, DaoCross may use the following reference price for a base/quote token pair, where the bids and asks come from a lit exchange and are expressed in terms of stablecoin prices:

$$\frac{\text{bid}_{\text{quote token}} + \text{ask}_{\text{quote token}}}{\text{bid}_{\text{base token}} + \text{ask}_{\text{base token}}} \tag{1}$$

When using either an on-chain price oracle or an exchange as a price oracle, it is possible to perform a time or volume weighted average of prices so as to avoid extreme price variations and to mitigate the risk and effects of any market manipulation attemps.

3.3. **Order crossing.** At regular time intervals, order submissions are cut off and reference prices are determined. An element of randomness is used to determine order cutoff times and reference price cutoff times in order to mitigate manipulative behaviors.

An order is eligible for matching if its timestamp is within the cutoff window and if the external reference price does not exceed its limit price.

Except on occasions where eligible buy/sell volume is perfectly matched, not all orders can be fully crossed. There are also discretization effects to consider arising from discrete order sizes and a discrete price grid [5][§3.2.1]. See [4] for a discussion of the trade-offs surrounding different prioritization rule choices. See [10] for the prioritization rules used by one of Morgan Stanley's equity liquidity pools.

3.3.1. *Priority rules.* DaoCross prioritizes fills according to:

- Volume (higher volume comes first in priority)
- Price (higher limit price breaks volume ties)
- Timestamp (earlier timestamp breaks ties in volume and price)

If, in the unlikely scenario that all three of these parameters perfectly agree, a certain priority is not guaranteed.

3.3.2. *Matching algorithm.* The mechanism for matching eligible buy and sell orders consists of two priority queues, one for eligible buy orders and one for eligible sell orders. Priority is determined according to the volume/price/timestamp priority rules introduced above. Top-of-queue orders are compared, and the lesser of the two volumes is fully filled. Once an order is fully filled at the established reference price. One an order is fully filled, it is removed from the priority queue. The procedure continues until one of the two priority queues is empty.

3.3.3. *Computational complexity.* Let n denote the sum (or max) of the number of eligible buy and sell orders. Priority queue construction occurs in $O(n)$ time, order removal costs $O(n \log n)$, and order remove occurs $O(n)$ times. So, the computational time complexity of the task is $O(n \log n)$. Memory requirements are $O(n)$.

3.3.4. *DaoSwap variant.* The mechanics for DaoSwap are similar to those above, with the primary difference being that an auction is used to determine a single clearing price. Variations in prioritization rules also possible.

4. Example

References

[1] Hayden Adams, *Uniswap Whitepaper* (2018).

[2] Hayden Adams, Noah Zinsmeister, and Dan Robinson, *Uniswap v2 Core* (March 2020), available at `https://uniswap.org/whitepaper.pdf`.

[3] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson, *Uniswap v3 Core* (March 2021), available at `https://uniswap.org/whitepaper-v3.pdf`.

[4] Alejandro Bernales, Daniel Ladley, Evangelos Litos, and Marcela Valenzuela, *Alternative Execution Priority Rules in Dark Pools* (July 22, 2022), available at `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4169352`.

[5] Jean-Philippe Bouchaud, Julius Bonart, Jonathan Donier, and Martin Gould, *Trades, Quotes and Prices* (2018).

[6] CME Group, *2023 FX Product Guide*, available at `https://www.cmegroup.com/trading/fx/files/fx-product-guide-2023-us.pdf`.

[7] _____, *Euro FX Futures - Contract Specs*, available at `https://www.cmegroup.com/markets/fx/g10/euro-fx.contractSpecs.html`.

[8] Robin Hanson, *Combinatorial Information Market Design*, Information Systems Frontiers **5** (2003), 107-119, available at `https://doi.org/10.1023/A:1022058209073`.

[9] Morgan Stanley, *Morgan Stanley Dark Pools*, available at `https://www.morganstanley.com/disclosures/morgan-stanley-dark-pools`.

[10] _____, *MS Pool ATS-N Filings*, available at `https://www.sec.gov/cgi-bin/browse-edgar?action=getcompany&filenum=013-00117&owner=exclude&count=40`.

[11] *Walrasian auction*, available at `https://en.wikipedia.org/wiki/Walrasian_auction`.

[12] Mu Xia, Jan Stallaert, and Andrew B. Whinston, *Solving the combinatorial double auction problem*, Journal of Operation Research **164** (2005), 239-251, available at `https://www.sciencedirect.com/science/article/abs/pii/S0377221703008981?via%3Dihub`.