IDEX: A Real-Time and High-Throughput Ethereum Smart Contract Exchange

Aurora Labs

Version 0.7.6
January 23rd 2019

Abstract

In this paper we explore IDEX, the base component of the Aurora DAO. For a complete understanding of the entire design we also suggest reading the Aurora whitepaper.

IDEX is a hybrid, semi-decentralized exchange that provides a trustless, real-time, high-throughput trading experience in conjunction with blockchain based settlement. By centrally managing trade matching and Ethereum transaction dispatch, IDEX enables users to trade continuously without waiting for transactions to mine, fill multiple orders at once, and cancel orders immediately without gas costs.

1. The Problem

On established decentralized exchanges, the improvements in security come at the expense of the user experience. Trade speeds are limited by block times, and order books update slowly and are often out of sync with the interface. Filling multiple orders simultaneously and submitting market orders is impossible, and canceling each individual order costs gas. These design flaws make the use of trading bots - a key factor in order book depth and liquidity - cost prohibitive, creating a poor user experience that ensures these alternatives won't meet the quality standard demanded by modern traders.

New relayers on 0x are addressing some of these issues, but still fall short of providing a premium user experience. Designating a specific relayer helps with order book maintenance, but eliminates all of the benefits of shared liquidity. Old orders must still be mined to completely invalidate them, and gas costs increase with each cancelled order, making bots cost prohibitive. Trading directly from the wallet gives market makers an opportunity to back out of unprofitable trades and opens up exchanges and takers to griefing attacks.

2. Our solution

IDEX addresses these issues by centralizing the non-critical components of the trading process. All transactions, such as deposits and trades, must be authorized by end users and their private key, but IDEX maintains ownership of broadcasting these authorized transactions to the network. By carefully sequencing the dispatch of these authorized transactions, IDEX provides the speed and user experience of a centralized exchange combined with the security and auditability of a decentralized exchange.

IDEX consists of a smart contract, a trading engine, and a transaction processing arbiter. The smart contract is responsible for trustlessly storing all assets and executing trade settlement, and all trades must be authorized by the user's private keys.

The IDEX smart contract has a unique design such that only the exchange is authorized to submit signed trades to the Ethereum network. This enables IDEX to control the order in which transactions are processed, separating the act of trading from final settlement. As users trade their exchange balances update in real-time, while their private keys are simultaneously used to authorize the trade in the contract. This authorization prevents users from rescinding any completed trades, and prevents IDEX from initiating any unauthorized trades.

Authorized transactions are passed to the arbiter which manages the queue of pending transactions, dispatching them in sequence to ensure that each trade is mined in the correct order and that the smart contract balances stay in sync with the exchange balances. This design allows users to trade continuously across multiple markets without waiting for transactions to mine, place true market orders and fill multiple orders at once, and cancel orders immediately and without gas costs.

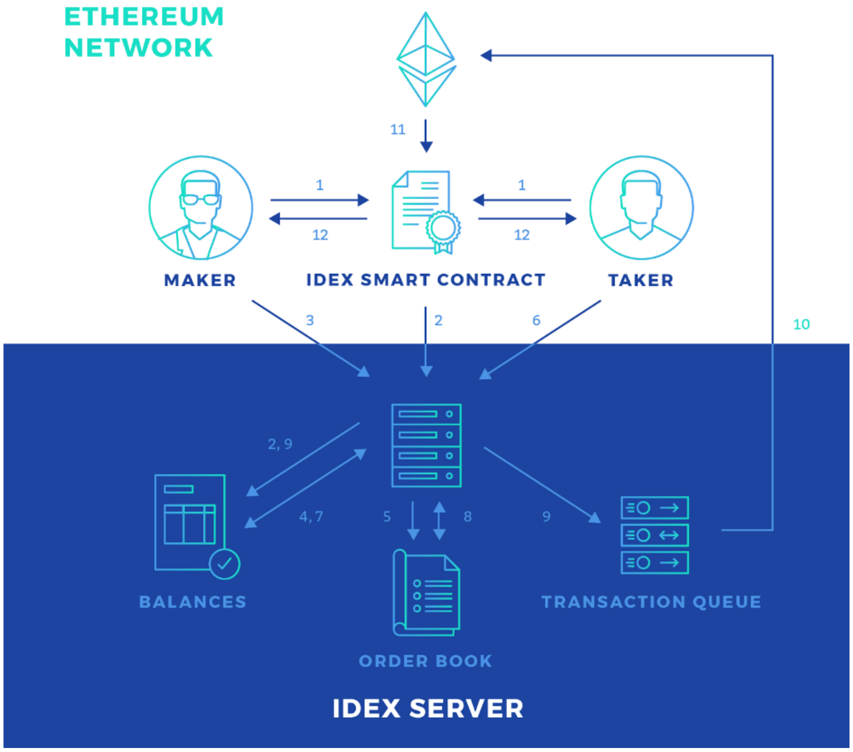


Fig. 1 - The IDEX Ecosystem

1) The maker and taker deposit their tokens into the IDEX contract.
2) The IDEX database is updated to include the customer addresses and token balances.
3) Maker creates and submits a signed order that includes the relevant trade data.
4) IDEX confirms that the maker's account has sufficient funds and that the signed transaction matches what was submitted to IDEX.
5) If all checks in part 4 pass, the order is added to the orderbook.
6) The taker submits a matching order, signing a transaction with the same price as the target order and an amount less than or equal to it.
7) IDEX confirms that the maker's account has sufficient funds and that the signed transaction matches what was submitted to IDEX.
8) If all checks in part 7 pass, the trade is marked as matched and the orderbook is updated.
9) The IDEX database is updated to reflect the new balances, and both traders can continue to make new trades based these updates. Simultaneously, the signed order is added to the queue to be broadcast to the Ethereum network for processing.
10) After all dependent trades have mined, the transaction is dispatched to the blockchain.
11) The transaction is mined and the contract balances update to reflect the trade.
12) Once the transaction has mined, the maker and taker are able to withdraw their funds.

The IDEX design addresses almost all of the challenges faced by existing decentralized exchanges.

Gas Fees for Cancels - As a general rule for DEXs, all cancelled orders must be invalidated on the blockchain, otherwise traders run the risk of others collecting old, unfavorably priced orders to be filled at a later date. Each of these cancellations costs gas. The 0x protocol includes a function to bulk cancel transactions, however the gas costs of this option scale almost linearly with the number of cancelled orders. This aspect of the protocol makes the use of trading bots cost prohibitive.

In contrast, IDEX has a specific function in the contract that allows users to invalidate ALL past order in one single transaction. Users can call this function on-demand after a series of many cancellations, while IDEX will purge cancelled orders across the entire exchange once a week. This provides a low-cost way to ensure no outdated orders can be broadcast, even in the event that IDEX is compromised. By changing the approach to how canceled transactions are invalidated IDEX has created a DEX that is friendly to trading bots.

Order Competition - the 0x protocol allows for one order to be shared across many relayers, but in the process exposes users to race conditions. If multiple traders compete for the same order at one time, one trader will be successful while the others will encounter the dreaded “bad jump destination” and wasted gas.

The preferred solution is to assign the rights to fill an order to a single relayer. Doing so prevents race conditions, but also increases the complexity of sharing liquidity. Makers can designated relayers in separate orders for the same funds, but now must manage orders on multiple exchanges. This creates a coordination challenge between the designated relayers and leads to a further escalation of order cancellation costs. Some exchanges with this approach have suggested that cancellations are not necessary as long as you trust the relayer, however this ignores the possibility of a bad actor taking control of their exchange, and the resulting product is no longer a trustless solution. Given the history of exchange security and what is at stake, any solution that relies on everyone playing fair should be approached with caution.

Market Maker Non-Compliance - trading directly from your wallet leads to a great UX for honest actors, but exposes traders to issues caused by dishonest market makers. While waiting for matched trades to mine, it’s possible for the market maker to submit a cancel or a token transfer transaction with a higher gas price and prevent the trade from settling. Market makers are incentivized to do so any time a pending trade is no longer profitable. This also opens up the exchange to griefing, and as Ethereum scales it will become cheaper to cancel matched orders and interfere with the integrity of the relayer’s orderbooks.

IDEX requires that users first deposit to the contract before trading, and users cannot withdraw until all transactions have cleared. While this may seem inconvenient, it eliminates all of the possible attacks related to rescinding orders that have already been dispatched. The IDEX contract also has an “escape hatch” that allows users to withdraw directly from the contract after a period of time, guaranteeing users access to their funds even in the event IDEX is unavailable.

Susceptible to Ethereum Backlogs - centralized exchanges have trained users to expect speed. Here traders can buy and sell the same assets in quick succession, making it possible to take advantage of quick price movements. On 0x traders must wait for previous transactions to mine before submitting another order. In the event of an Ethereum backlog this problem becomes even worse, as traders are forced to space out their orders over longer periods of time. This delay makes many otherwise profitable trading strategies untenable on these exchanges.

IDEX traders do not have to worry about any backlogs on Ethereum, as the user experience is insulated from longer settlement times. Users can trade continuously, back and forth in real-time. The IDEX balance updates immediately, while the authorized transactions are broadcast in the correct sequence for final settlement. This asynchronous design insulates IDEX traders from the current shortcoming of the Ethereum network.

IDEX is currently the most advanced DEX on the market. However, in order to compete with and displace centralized exchanges, IDEX must be able to match and exceed the transaction throughput of these less secure alternatives. In the case of IDEX, the Ethereum blockchain is the limiting factor. By combining our innovative design with a sidechain, IDEX will scale to process the necessary number of transactions and eventually render centralized exchanges obsolete.

3. Team

We have a qualified team with a healthy mix of business and development experience.

Alex Wearn - CEO (https://www.linkedin.com/in/alexwearn/)
Alex is an expert at leading teams in the design and delivery of software products. He has managed a wide range of operations, marketing, and sales analytics products for Amazon, Adobe, and IBM, and most recently led a product management team in re-platforming their application to operate on a private Ethereum blockchain (project still in stealth mode). Alex is a graduate of the Kellogg MMM program, a dual MBA in Finance and Operations and MS in Design and Innovation.

Phil Wearn - COO (https://www.linkedin.com/in/philwearn/)
Phil is a Co-founder of EtherEx and has been building blockchain based companies since the time when Ethereum was little more than a white paper. While developing EtherEx he identified the pressing need for a high performance decentralized exchange protocol, an insight which served as the basis for IDEX. Phil has a background in aerospace engineering.

Jason Ahmad - CTO (https://www.linkedin.com/in/jason-ahmad/) Jason has spent his career leading product and engineering teams in the creation of world class software. A two-time venture backed founder, his last company, Epoxy, was successfully acquired in 2016. A Stanford CS graduate, Jason brings his expertise and knowledge to lead the engineering team of Aurora.

Brian Fernalld - Full Stack Developer (https://www.linkedin.com/in/brianfernalld/)
Brian is a full stack developer with over 10 years experience in startups. In addition to engineering, Brian has worked for many years in the fields of blockchain technology, product management, marketing, and design. Brian uses his passion for fintech and blockchain technology to build the best user experiences possible.

4. Aurora

IDEX is the first product of the Aurora DAO, a suite of DAPPs and protocols that make up a distributed banking and financial network. The components of Aurora support the boreal, a stablecoin, and together enable global banking in the new currency. Revenue from the various components of Aurora will be used both to expand boreal banking and to provide economic incentives that ensure that Aurora runs as designed. More information about Aurora, including the whitepaper, can be found here.

5. Aurora (AURA) Token

All fees from IDEX are remitted to the Aurora reserves. As the reserves grow Aurora can increase the value of outstanding loans, generating additional revenue for the Aurora network. Fees from the Aurora banking system will then flow back to those who stake the AURA token and provide the economic foundation that holds Aurora together.

Aurora has its own native network token, AURA, that aligns the interests of Aurora users and operators. All of the revenue from Aurora is used to compensate those who stake their AURA and provide security for the Aurora network. AURA staking aligns the economic interests of the operators with the health of the network, and makes it extremely costly for any would be attacker to disrupt operations.

6. AURA Token Details

Supply: 1,000,000,000
50% will be used to help accelerate adoption of the Aurora network. Of the total amount of AURA tokens, 40% will be used to help subsidize the growth of Aurora by distributing AURA to users and community members through programs such as market maker rewards, marketing campaigns, and air drops. The remaining 10% will be given out proportionally to individuals who purchase IDEX memberships.
The remaining 50% of AURA will be used as follows:

- 25% founding team
- 10% future employee token pool
- 10% future use
- 5% businesses expenses

7. Market Maker Reward Program

Aurora is implementing a crypto rewards program, enabled by the AURA token, to encourage the creation of limit orders on IDEX. This program is designed to jump-start exchange usage and encourage the growth of liquid order books.

Market makers who place and execute limit orders on any IDEX market are eligible to receive AURA token grants. 20% of the total AURA token supply will be distributed to the community via this grant program at a rate of one percent of the total *remaining* reward tokens per month. With each additional month the number of AURA rewards will be slightly reduced, providing an incentive for market makers to join early and ensuring that the rewards program can continue indefinitely. Traders will receive AURA proportional to the fees they spend on their limit orders. For example, if three traders trade during a one month period with trader A paying 5 eth in fees, trader B paying 2 eth in fees and trader C paying 3 eth in fees, they will receive 50%, 20% and 30% of the total AURA distributed that month respectively.

8. Membership Sale (DVIP)

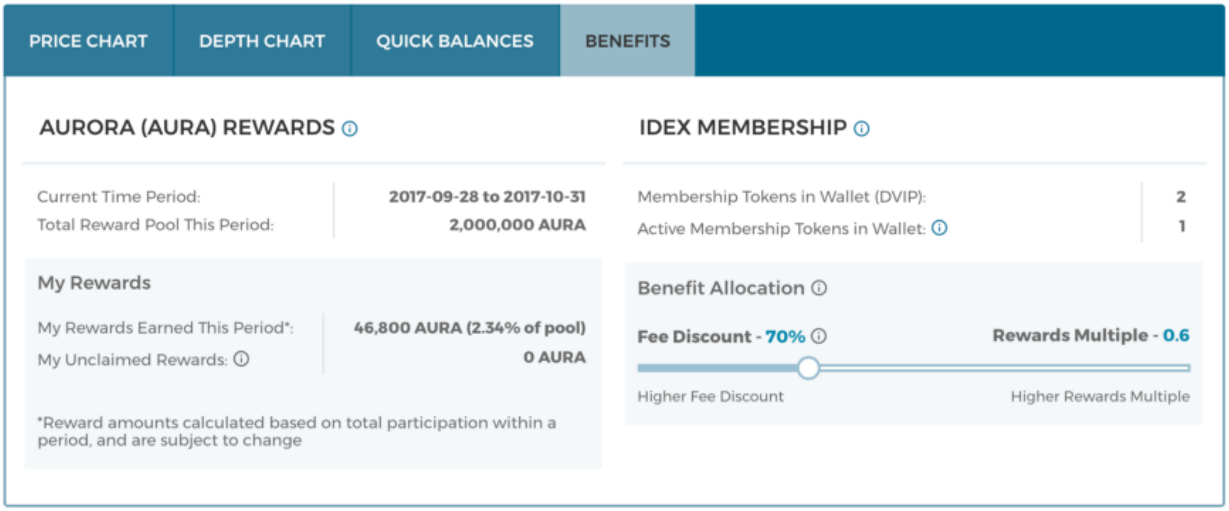
DVIP is a crypto membership that entitles the holder to free or discounted trades on IDEX until the year 2020. Approximately 2 weeks after the DVIP are distributed each holder of DVIP will be able to redeem their existing DVIP for a new membership and 50,000 AURA per DVIP. Redemption will be handled via an ethereum smart contract. A total of 2,000 DVIP exist, and Aurora Labs is selling 1,700 at the launch of the IDEX mvp.

Each full DVIP (1 DVIP) entitles the token holder to 100% of the membership rewards. DVIP is divisible to 1/100, and membership rewards are applied on a pro rata basis. Additional DVIP above one grants no further membership benefits including both trade discounts and AURA reward multipliers. The benefits are the same whether a user owns one or five DVIP.

DVIP members are able to choose from the following membership benefits:

1. Free trades and no AURA rewards
2. 2x Market Making rewards and full trade fees
3. A proportional mix of both

Membership benefits are a function of both the amount of DVIP held by the member and the choice of rewards. Membership benefits do not increase for any holdings above one full membership. Members can view and set their benefit choices using the benefits tab of the exchange.



AURORA (AURA) REWARDS ⓘ

Current Time Period: 2017-09-28 to 2017-10-31

Total Reward Pool This Period: 2,000,000 AURA

My Rewards

My Rewards Earned This Period*: 46,800 AURA (2.34% of pool)

My Unclaimed Rewards: ⓘ 0 AURA

*Reward amounts calculated based on total participation within a period, and are subject to change

IDEX MEMBERSHIP ⓘ

Membership Tokens in Wallet (DVIP): 2

Active Membership Tokens in Wallet: ⓘ 1

Benefit Allocation ⓘ

Fee Discount - 70% ⓘ

Rewards Multiple - 0.6

Fig. 2 – DVIP Benefits Allocation

The rewards multiplier and fee discount are represented by the following formulas:

Fee Discount Percentage = $(1- x) * (DVIP) * 100$
Rewards Multiplier = $((1 – DVIP) + (DVIP * x) * 2)$

x = rewards percentage; values range from zero, all fee discount, to one, all rewards multiplier
DVIP = number of active DVIP held; capped at one if holding more than one active DVIP

For example:

1. Joe has 2 DVIP
   a. If Joe sets his reward percentage to 0, he'll pay 0 trade fees and does not participate in AURA rewards
   b. If Joe sets his reward percentage to 1, he'll pay 100% of the trade fees and receive 2x market making rewards
   c. If Joe sets his reward percentage to 0.5, he'll pay 50% of the trade fees and receive 1x market making rewards
2. Jane has 0.6 DVIP
   a. If Jane sets her rewards percentage to 0, she'll pay 40% of the trade fees and does not participate in AURA rewards
   b. If Jane sets her rewards percentage to 1, she'll pay 100% of the trade fees and receive 1.6x market making rewards (1x standard rewards + 0.6x membership rewards)

c. If Jane sets her rewards percentage to 0.75, she’ll pay 85% of the trade fees and receive 1.3x market making rewards (0.85x standard rewards + (0.75*0.6=0.45x) membership rewards)