# Decentralized Exchanges (DEX)

Analyst
Mrinalini Bhutoria (Ria)
@riabhutoria

Updated
19 December 2018

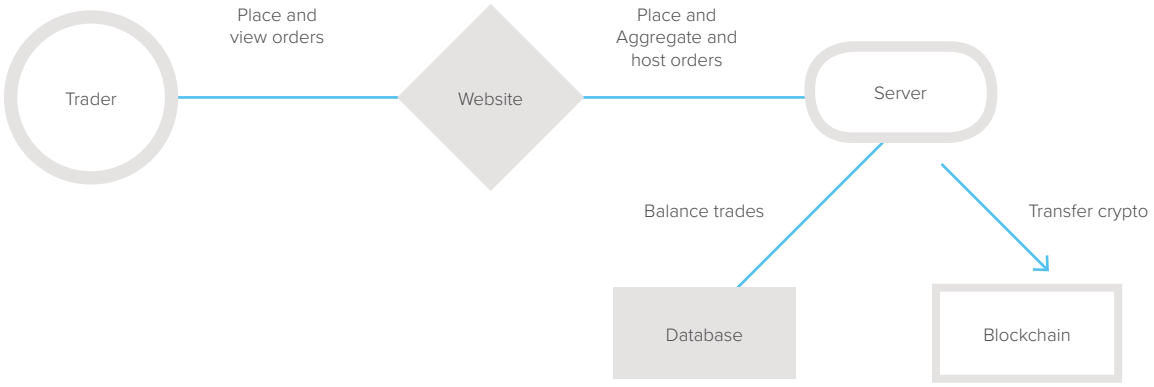
## INTRODUCTION TO DECENTRALIZED EXCHANGES

A crypto asset exchange is an electronic venue for buying and selling crypto assets. Currently, the majority of crypto asset trading occurs on centralized platforms like Coinbase, Poloniex, Binance, Bittrex, etc that collect fees for facilitating trades. Many believe that assets powered by decentralized technology should be traded on decentralized platforms. This revelation, along with several events that have degraded trust in some centralized exchanges, have led to a rise in decentralized exchanges, or DEXs.

### Centralized exchanges

Centralized crypto exchanges aggregate liquidity, custody customer assets, and execute trades. Every trade is reflected as a change in the exchange's database. Users deposit their funds into the exchange wallet address, which pools all customer assets. Trades are conducted on an IOU basis. Users do not get actual delivery of their funds until they explicitly withdraw their funds from the exchange. Centralized exchanges are fast because they are centralized and don't swap assets on-chain.

Benefits of legitimate centralized exchanges include that they offer significant liquidity (~99% of crypto trading occurs on centralized exchanges), offer fiat on-ramps, offer greater trading functionality and the ability to use sophisticated trading strategies, offer institutional support, and comply with regulations of the jurisdictions in which they reside. However, they also have some points of weakness and not all crypto exchanges have a robust infrastructure in place.




Source: rados.io/architecture-comparison-of-decentralized-exchanges/

Some or all of the funds in a centralized exchange could be stored in a "hot" wallet on the exchange's servers to facilitate quick withdrawals. Hot wallets are at greater risk of being hacked by virtue of being connected to the internet. Centralized exchanges with weak security measures and infrastructure are especially attractive targets for hackers because they collectively store large sums of customer funds, and security breaches have led to significant losses.

Table of Contents
Introduction
0x (ZRX)
IDEX (IDXM, AURA)
Sources

TOP FIVE EXCHANGE HACKS

| Exchange | Date | Amount | Token stolen |
|---|---|---|---|
| MtGox | Mar-2014 | $700,000,000 | BTC |
| Coincheck | Jan-2018 | $534,800,000 | NEM |
| BitGrail | Feb-2018 | $195,000,000 | NANO |
| Bitfinex | Aug-2016 | $72,000,000 | BTC |
| Nicehash | Dec-2017 | $60,000,000 | BTC |

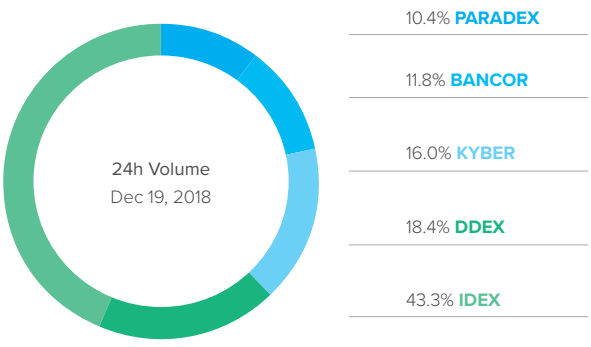
Source: rados.io/list-of-documented-exchange-hacks/

In the past couple years, centralized exchanges have also become more careful in listing assets due to regulatory uncertainty around security laws. Given the large amount of ICOs in the last couple years, people worried that tokens they purchased in an ICO would be illiquid. For these reasons, there has been heightened interest in developing decentralized platforms to address some of the drawbacks of centralized platforms.

## Decentralized exchanges

Decentralized exchanges (DEXs) are applications built on top of dApp platforms (such as Ethereum) that use smart contracts to facilitate trading. There are currently over 250 DEXs and over 30 DEX protocols. A DEX protocol is not exactly a DEX itself, but rather provides teams with the tools they need to build a DEX, so they don't need to worry about building the smart contracts needed to power their DEX. The most popular DEX protocol is 0x. The standard feature that makes DEXs "decentralized" is that they do not custody customer assets. Rather, users are responsible for holding assets in their respective wallets, which should reduce the risk of being hacked.

TOP 5 DEXS



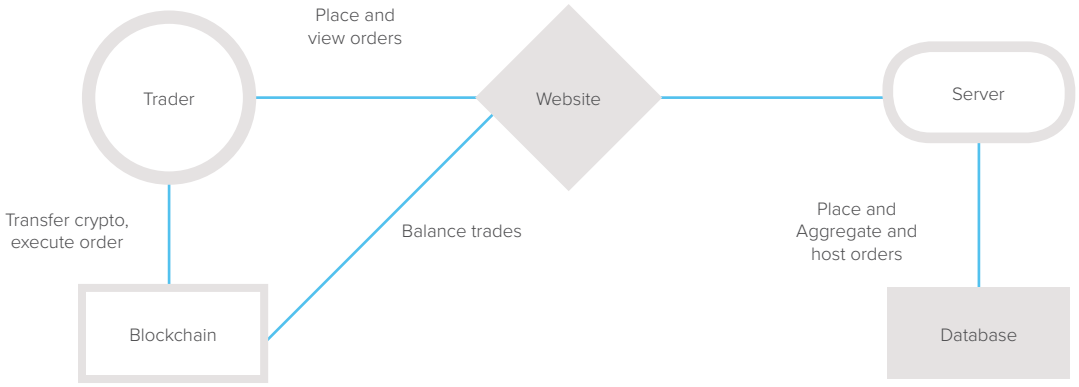

Source: dex.watch/

The key differences lie in where the orderbook is hosted, how orders are created, modified, matched, and cancelled, and how transactions are executed. This determines the architecture and where DEXs lie on the decentralization spectrum. For example, a DEX could be fully decentralized and submit every order creation, modification, cancellation, and settlement to the blockchain.

However, this is problematic due to the scalability limitations of existing blockchains because users would have to submit multiple entries to the blockchain, even for theoretically non-critical actions. As a result, very few DEXs are fully decentralized. Most DEXs have chosen to use a hybrid centralized/decentralized approach by keeping non-critical actions off-chain and critical actions on-chain.

## Off-chain orderbook & On-chain settlement

The two DEXs we discuss in this report, 0x and IDEX, both use a hybrid off-chain orderbook model with on-chain settlement. This allows users to post and modify orders in real-time - much faster than if everything had to be mined on-chain. They attempt to minimize trust in the central entity hosting the website by not giving them the power to automatically match and execute[1] trades. Rather, traders manually choose and fill orders by signing them and submitting them to the blockchain (or submitting them to a trade arbiter who submits it to the blockchain).




Source: rados.io/architecture-comparison-of-decentralized-exchanges/

0x and IDEX are different in that 0x is a base layer protocol for building DEXs and IDEX is a proprietary DEX. Because 0x is a base layer protocol, the DEXs building on top of 0x - called relayers - have some flexibility in what strategy they employ, and strategies can differ from relayer to relayer.

## General DEX Advantages

### Non-custodial

All DEXs are non-custodial, meaning that DEXs do not pool user funds in a single wallet or central server. Rather, users are in possession of their funds and grant permission to the DEX smart contracts to access their funds to facilitate trading. This eliminates the security risk of holding customer assets in a single wallet. Funds are settled in a peer-to-peer manner.

### Unique features

DEXs could enable seamless integration with other dApps built on Ethereum that require exchange functionality. For example, the 0x team has said relayers could implement KYC by integrating a provider like Polymath or Harbor to whitelist Ethereum addresses that have been through an off-chain KYC process and are permitted to trade on the platform.

Another unique feature is token abstraction, which obfuscates the conversion between different tokens for users. An example of this is Weasel, which allows ETH holders to send DAI in Status without the user having to convert from ETH to DAI. Weasel trades ETH for DAI on behalf of users through KyberNetwork.

## General DEX Challenges

### User experience

The user experience of DEXs (and most dApps in general) is still a work in progress as users have to wrap their heads around trading through a wallet rather than an exchange account, the latency associated with on-chain settlement, and more. Centralized exchanges have a familiar and relatively more easy to understand process whereas many decentralized exchanges have confusing exchange interfaces and processes that requires getting used to.

[1] The 0x protocol does allow relayers to use the closed, order-matching strategy, which is more centralized. Paradex and DDEX are relayers that use this model, but they cannot share in the 0x liquidity pool as a result and are not considered representative of the true intention of the 0x protocol.

### Smart contract bugs

Ethereum-based dApps and smart contracts are built using Solidity. However, it is widely recognized that Solidity has major design flaws and a lack of verification tools. As a result, it is possible for developers to make mistakes when deploying smart contracts, and bad actors can exploit these bugs to compromise user funds.

### Cross-blockchain functionality

Ethereum-based DEXs currently only offer the exchange of ERC-20 and/or ERC-721 tokens and do not currently offer cross chain exchange. Cross-blockchain atomic swaps could address this issue. However, decentralized exchanges that enable cross-chain trading are likely to exhibit these challenges and more. Additionally, DEXs do not offer a fiat on-ramp. Thus, users have to convert their fiat to ETH and potentially convert the ETH to the native token of the DEX (i.e. ZRX in 0x).

### DDoS and DNS attacks

In theory, one of the major advantages of dApps running on blockchain technology is zero-downtime. However, the existence of centralized components prevents dApps from realizing this objective. The more centralized a DEX, the higher its risk of being the target of a DDoS (distributed denial of service) or DNS (domain name service) attack on its central servers. This is also a risk with centralized exchanges. A DDoS attack happens when servers are overloaded with traffic from multiple sources that makes online services unavailable. A DNS attack happens when an attacker gains control of a website's DNS server and redirects visitors to a malicious website that can compromise user information and/or funds.

EtherDelta was the subject of a DNS attack in December 2017. The attacker did not gain control of the exchange's smart contracts, but was able to take over its DNS server for a few hours. Visitors who used the site during the attack might have sent funds to the attacker. It was reported that about $250,000 worth of ETH and an unknown amount of other ERC-20 tokens were sent to the attacker.

### Regulation

When the first DEXs went live, people assumed their benefits would include censorship resistance and no KYC, unlike their centralized counterparts. However, in recent months, we have come to discover that if any component of a DEX is centralized, it can be subject to regulation. Recent comments from regulators also show that DEXs that are fully decentralized could still be subject to regulation if lawmakers believe that they facilitate the trading of security tokens, or regulated options or derivatives.

In November 2018, The SEC charged former CEO of Etherdelta (Zachary Coburn) for violating federal securities regulations (Exchange Act Section 5) by operating an unregistered securities exchange. According to the SEC, Etherdelta qualified as an exchange because it operated as a marketplace for bringing together the orders of multiple buyers and sellers in tokens that included securities. However, due to lack of concrete guidance at this point, it is very challenging to know what the SEC does and doesn't consider to be a security, so DEXs could be unknowingly violating securities regulations.

Some DEXs are trying to avoid listing any assets regulators would consider to be securities to avoid having to register as a national securities exchange. Alternatively, if a DEX does offer tokens that might be classified as securities, the only way to qualify for an exemption would be to register as an ATS. If a DEX is fully decentralized (on-chain orderbook, non-custodial, no trade execution) and offers securities tokens, it would be more difficult for regulators to enforce exchange laws, because there is no central point of contact.

Others are taking a proactive approach and implementing KYC/AML processes to comply with money laundering and sanctions regulations (IDEX). 0x has also said that relayers could restrict trading in certain tokens ("permissioned tokens") to users to those who have completed an off-chain KYC/AML process through entities like Harbor and Polymath.

### On-chain settlement and cancellation

The latency and cost associated with the Ethereum blockchain creates challenges for DEXs using on-chain settlement and on-chain cancellation.

- **Trading strategies** - Many DEXs do not yet support sophisticated exchange functions such as margin trading[2], stop-loss orders, high frequency trading, or other trading strategies because they are limited by slow on-chain settlement and/or on-chain cancellation. IDEX claims it improves upon this by keeping cancellations and execution separate from trade settlements and cancellations via a trade arbiter.
- **Arbitrage** - DEXs with on-chain order cancellation are more exposed to in-market arbitrage opportunities because users cannot quickly cancel stale orders in response to market fluctuations.
- **Race conditions** - On-chain settlement and/or on-chain cancellation also exposes users to risks such as frontrunning, trade collisions or maker griefing.

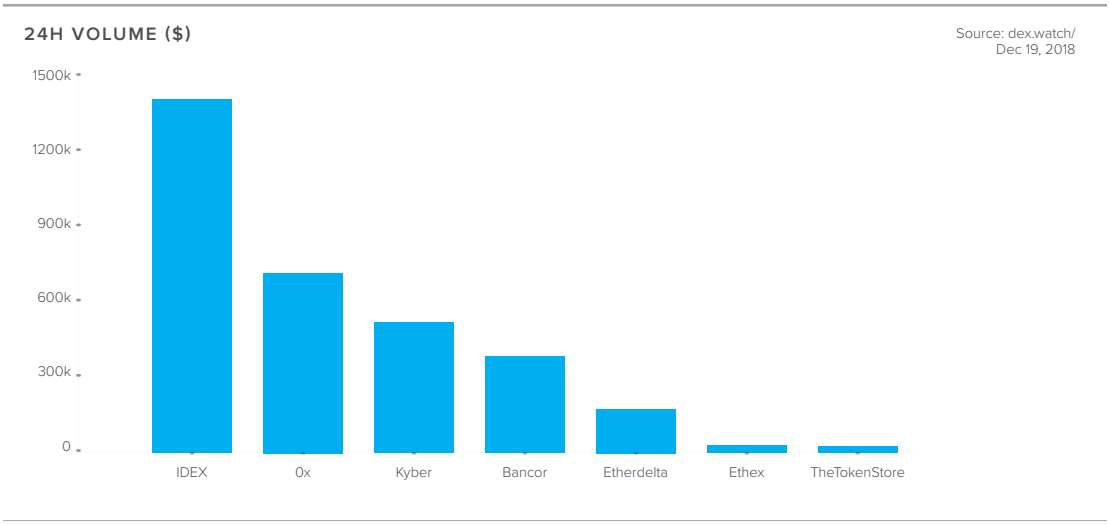
### Liquidity

DEXs currently have inadequate liquidity in a classic case of the chicken-or-the-egg. Traders are attracted to platforms that offer liquidity but platforms need traders to aggregate liquidity. In the last 24 hours as of this writing, the top five DEXs had about $3.2 million in volume (30,700 ETH) versus $7.5 billion in combined volume on the top 5 centralized exchanges. However, DEXs are still in their infancy, and liquidity could increase if/when DEXs address the challenges outlined here.

## Remarks

Today's DEXs seek to address perhaps the most important problem in crypto trading - custody of user funds. However, they have not yet perfected the solution and have simultaneously introduced a plethora of new dangers that need to be addressed before they can begin to compete and coexist with their centralized counterparts. It could be the case that users initially use DEXs to trade in the long tail of tokens that do not meet the listing standards of centralized exchanges, while users use centralized exchanges to trade in primary crypto assets. But this is also in question given most DEXs are not fully decentralized, making them as vulnerable to regulators enforcing securities laws as centralized exchanges.

In the 0x and IDEX sections below, we discuss the structure of these two DEXs in greater detail and explain how they are attempting to address some of the challenges outlined above. 0x is the most popular DEX protocol and IDEX is one of the most popular DEXs, by volume.




[2] Bamboo Relay, Star Bit, Amadeus are a few relayers that allow users to lend and borrow tokens by integrating a protocol called b0x.

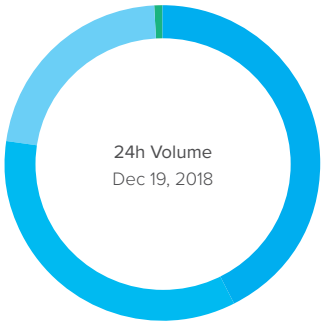
# 0x (ZRX)

## OVERVIEW

0x is an open protocol for exchanging ERC-20 tokens on the Ethereum blockchain using an off-chain order relay and on-chain settlement strategy. It's native token, ZRX, is used for trading fees and ultimately, governance. 0x is a public system of smart contracts with a formalized message schema that outlines how an order should be structured. 0x is not a decentralized exchange itself[3], but rather democratizes the process of *building* a decentralized exchange. The founders believe the true value lies in equipping teams with the tools, libraries and smart contracts needed to build for-profit relayers (0x's version of DEXs) and creating a global pool of shared liquidity. Thus, 0x is to relayers what Ethereum is to dApps - a platform to build upon.

After spending time with dApp teams building on Ethereum, Will Warren and Amir Bandeali, co-founders of 0x, identified a key problem - multiple dApps would require exchange functionality and were building one-off exchanges with one-off tokens that were not interoperable. In December 2016, 0x pivoted to developing open DEX infrastructure that anyone could build on or plug into. 0x was built with the intention to address the fragmented ecosystem of dApps and DEXs, combine liquidity to create a global liquidity pool, and automate trades on behalf of users by allowing smart contracts to execute trades automatically with a single line of solidity code.

There are currently sixteen relayers built or building on 0x. The top three relayers by 24-hour volume are DDEX, Paradex, and Radar Relay. Additionally, there are nineteen projects using the 0x protocol, many of which are in the DeFi ecosystem, including District0x, Maker, Dharma, and Melonport. 0x launched version 1 of the protocol on the Ethereum mainnet in August 2017, a few days before launching the ZRX token sale. It launched version 2 in May 2018.




Source: 0xtracker.com/relayers

### Team

**Founders**
Will Warren (CEO), Amir Bandeali (CTO), Fabio Berger, Leonid Logvinov, Alex Xu (14 total team members)

**Advisors**
Fred Ehrsam (CEO of Coinbase), Olaf Carlson-Wee, Joey Krug, Linda Xie (Co-founder of Scalar Capital)

**Investors**
Pantera, Polychain Capital, Blockchain Capital, JenAdvisors, Fintech Blockchain Group

[3] The 0x protocol does allow relayers to use the closed, order-matching strategy, which is more centralized. Paradex and DDEX are relayers that use this model, but they cannot share in the 0x liquidity pool as a result and are not considered representative of the true intention of the 0x protocol.

### Token sale

0x raised $24 million in its token sale on August 15, 2017. Tokens were sold to those who registered to participate in the token sale through a smart contract that executed The Genesis Trade - a huge sell order for 50% of the total supply of ZRX tokens (500 million tokens) distributed to ~12,000 people that registered.

0x has a fixed supply of 1 billion ZRX tokens. The distribution of ZRX tokens is: 70% to crowd sale investors, 18% to the Foundation, 10% to the founding team, and 2% to advisors. The lockup period for founders, advisors, and staff was over a period of three years with a schedule to release 25% following the sale and 25% after each subsequent year in monthly installments. New staff has a 4 year vesting schedule with a one year cliff.

### Token function

The ZRX token has two connected functions. At its core, ZRX is meant to be a governance token. While it is not currently being used in a formal governance process, the team is working towards implementing a fully decentralized governance process via liquid democracy. In order to achieve distribution of the ZRX tokens to key stakeholders, specifically relayers and traders, relayers using an open orderbook strategy must collect trading fees in ZRX tokens. Relayers using an order-matching strategy can collect fees in ZRX tokens, but it is not mandatory.

### Off-chain order relay/On-chain settlement

The 0x protocol uses the off chain orderbook/on-chain settlement model. In this model, users compile the parameters of a trade into a message or a packet of data that they cryptographically sign with their private key but do not broadcast to the blockchain. Rather, they either send the message to a specified counterparty directly (point to point order)[4] or send it to a relayer to include in their orderbook (broadcast order). While relayers have access to cryptographically signed messages, they cannot touch user funds - they are non-custodial.

The key components of the 0x protocol include:

- **Makers:** or market maker, the party that creates, cryptographically signs, and broadcasts an order, providing liquidity.
- **Takers:** or trader, the party that fills orders created by makers.
- **Relayers:** entity that aggregates and displays orders from makers on an off-chain orderbook (a proprietary website).
- **Exchange contract:** the Ethereum contract, which settles an order by moving funds between two parties at the specified exchange rate. The contract is not controlled by anyone.

A taker executes a trade by broadcasting a cryptographically signed message using the Exchange contract. If all parameters are satisfied (i.e. the cryptographic signature is correct and both sides of the trade have sufficient funds), the transaction is added to the Ethereum mempool. The transaction is considered complete once it is included by miners in a block on the Ethereum blockchain. Funds are kept in users' Ethereum wallets until a taker fills the order, at which point, funds are exchanged in a peer-to-peer manner, bypassing third party rails.

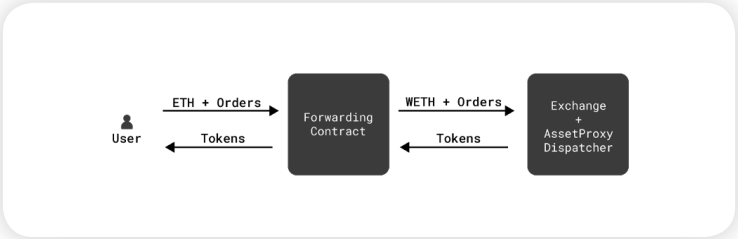
Executing a transaction requires the payment of gas fees (aka transaction fees) to miners who include transactions in a block. Unlike users of DEXs that use on-chain orderbooks, users of 0x do not pay gas fees to create or modify a transaction[5]. The current downsides of on-chain orderbooks include high latency and bloat on the blockchain because users must wait for every modification to be verified on-chain. Additionally, users must pay gas fees for every modification because it is mined on-chain. The trade-off of centrally hosted off-chain orderbooks is that they are less decentralized than on-chain models.

Relayers facilitate trade in ERC-20 tokens. Trading on relayers built on 0x requires users to "wrap" their

[4] In a point-to-point order, only the specified counterparty can fill the order.

[5] Order cancellation, on the other hand, needs to occur on chain - users need to wait for the transaction to be confirmed and must pay gas fees to do so.

ETH (or trade ETH for WETH), because ETH is not compliant with its own ERC-20 token standard. WETH is equivalent to ETH but is in a standard that is compatible with the ERC-20 tokens traded on the platform. Relayers do not charge for this, but users need to pay gas fees to "wrap" and "unwrap" ETH. In 0x v2, 0x introduced a forwarding contract, that allows dApps to abstract away the process of converting from ETH to WETH. "With the forwarding contract, users can simply send ETH and the orders they want to fill, and the forwarding contract will wrap the ETH and fill the orders in one single transaction, eliminating the need for WETH for takers."




Source: blog.0xproject.com/introducing-0x-protocol-v2-9f5bda04d38d

### 0x Components

Will Warren describes the first component of the 0x protocol as the message or order schema. Users must specify certain parameters in the message such as the expiration time, trade price, fee recipient (relayer), fee amount, counterparty (optional), etc. Users then cryptographically sign the message and create a point-to-point or broadcast order.

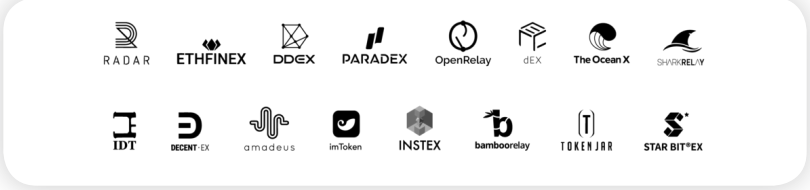
- **Point-to-point order:** In a point-to-point order a maker creates an order with a specific taker in mind and the order can only be filled by the specified taker.
- **Broadcast order:** Broadcast orders do not specify a taker address, allowing a broadcast order to be filled by anyone that happens to intercept it.

The second component is the system of 0x smart contracts, which is broken into two modules:

- **Exchange module:** The Exchange contract accepts the packets of cryptographically signed data, processes them, and settles trades on the blockchain. This contract authenticates cryptographic signatures to confirm that counterparties have the funds needed to execute a trade and ensure that an order hasn't already been filled or expired.
- **Governance module:** The second module allows the Exchange module to be upgraded over time without bringing the system to a halt and is intended to prevent hard forks of the protocol (which would create fragmented liquidity - the problem 0x wants to solve). We provide additional details in the governance section below.

## RELAYERS

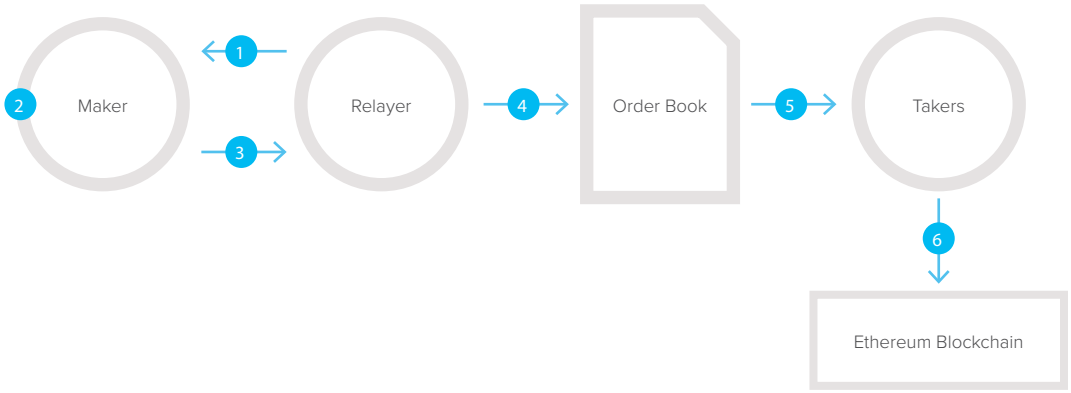
Relayers are for-profit entities that use the 0x protocol as their back-end and build proprietary user interfaces. They host an off-chain orderbook where they relay orders to users by aggregating and displaying broadcast orders, but they do not custody user assets or execute trades (unless they use an order matching strategy). They can collect fees for hosting and organizing orders on an orderbook. Relayers are incentivized to include as many orders as possible on their orderbook because they collect more fees if more trades occur.




Source: 0xproject.com/

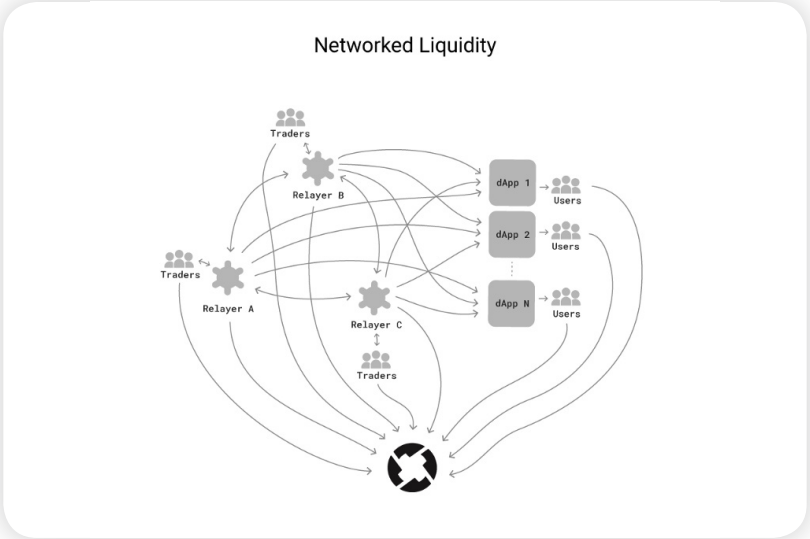
0x focuses building and maintaining the back-end system of smart contracts that power the DEXs building on top of it so relayers can focus on creating a high quality, seamless user interface and experience. This allows relayers to narrow their focus and drives competition in user experience and fees, which is theoretically good for users.

In the simplest form, if a maker accepts the fees being charged by a relayer, she can send the order to the relayer to include in the orderbook by specifying the relayer ("fee recipient") and fee (along with other parameters mentioned above) in the cryptographically signed message. The relayer checks that the fee is in line with their fee schedule and broadcasts it to their orderbook.




## Networked liquidity

One of the main goals of 0x is to create networked liquidity, which is the seamless flow of orders or transactions through a network of interconnected exchanges and dApps, resulting in a shared liquidity pool. This creates network effects via orderbook aggregation by opening up and expanding the pool of buyers and sellers for the relayers or dApps looking to bootstrap liquidity or a group of relayers agreeing to some fee sharing arrangement. Additionally, it enables fee or token abstraction, where dApps plugged into the 0x system use relayers to automatically execute token exchanges on behalf of their users. Relayers who want to share liquidity need to use the open orderbook strategy (see below) and build their interface using the 0x relayer API standard.




Source: blog.0xproject.com/front-running-griefing-and-the-perils-of-virtual-settlement-part-2-921b00109e21

### Challenges

**Trade and cancel collision.** Accidental trade collision occur when two or more parties attempt to simultaneously fill the same order i.e. the order fill attempts occur within approximately one block time of each other. Additionally, while most orders expire, accidental collisions of cancellations and trade operations can occur if a trader tries to fill an order when the maker is trying to cancel it. Cancellations are supposed to be a last resort.

**Frontrunning.** When you create, sign, and broadcast a transaction to the network, the transaction isn't immediately mined into a block. It typically sits in a mempool, or a pool of pending transactions. Anyone can see the pending transactions in the mempool. This can be exploited by traders who execute the same transaction, since it has not been settled, and pay a higher gas price so their transaction is mined into a block first.

The easiest way to avoid front-running and trade collisions is to find a counterparty ("taker") before cryptographically signing an order. Doing this prevents frontrunners from filling the order and prevents trade collisions, because the only party that can fill the order is the taker specified in the order. The downside is that the maker must find a counterparty willing to trade the exact size at the exact exchange rate and the maker must be online to negotiate with potential counterparties - she cannot "fire and forget". Further, this process does not allow for the sharing of liquidity.

## RELAYER STRATEGIES

Relayers can use an open orderbook strategy, an order matching strategy, a quote provider strategy or a reserve manager strategy. Each strategy has its pros and cons when it comes to frontrunning risks, trade collisions and networked liquidity. We discuss the most commonly used strategies - order matching and open orderbook.

The order matching strategy avoids trade collisions and frontrunning at the expense of networked liquidity. The open orderbook strategy facilitates networked liquidity but considers trade collisions and frontrunning as challenges.

### Order matching

An order matching model requires users to specify the taker parameter as an address controlled by the relayer. The relayer becomes a "matcher" and batch fills orders with overlapping prices. This strategy has been implemented by 0x relayers Paradex and DDEX. While the orderbook is public, only the relayer can fill orders, locking out frontrunners and preventing trade collisions. If a user fills in the taker parameter, the Exchange contract will prevent any counterparty that is not the specified taker from filling the order. This strategy allows users to "fire and forget", and implements an identical process for creating and consuming orders.

The downside to the matcher is they incur the gas costs and trades require double the gas costs relative to the open orderbook model due to the batch-fill requirement. Further, this strategy adds a degree of centralization and requires users to trust that the relayer will fill the order as specified and won't frontrun them. Finally, "in assigning each order to a specific counter party, there can be no free flow of orders and therefore no networked liquidity", which is the main problem 0x intends to solve.

### Open orderbook

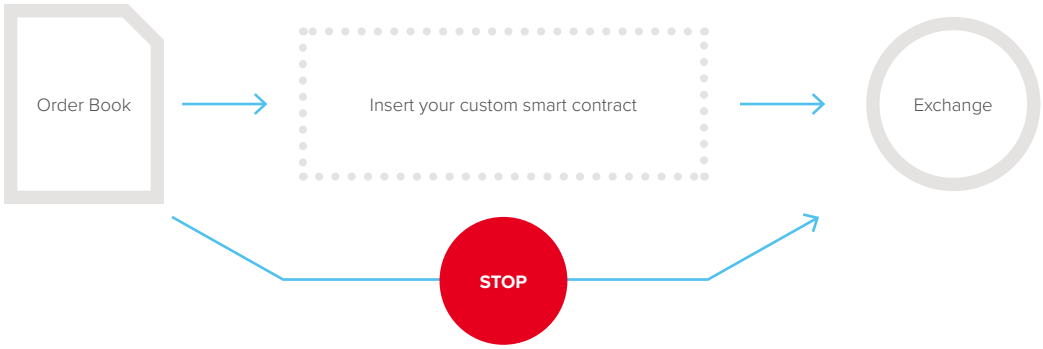
In an open orderbook strategy, users create orders without designation a taker. Relayers aggregate these orders and display them on their orderbooks. Relayers and dApps can access the liquidity of relayers that use this strategy, enforcing networked liquidity. However, trade collisions and frontrunning are risks.

Consider Maker A who creates order A and broadcasts it to Radar Relay's orderbook. Taker B finds order A and attempts to fill it by inserting it into the Exchange contract and paying 5 gwei per unit of gas. Order A gets

added to the Ethereum mempool (backlog of transactions waiting to be mined). Taker C sees Order A and that Taker B is willing to pay 5 gwei per unit of gas. Taker C decides to fill the same order, since it has not yet been settled, by paying 10 gwei per unit of gas. A miner sees that Taker C is offering to pay more per unit of gas and chooses to mine Taker C's fill of Order A, allowing Taker C to successfully frontrun Taker B and cause his transaction to fail.

### Potential solutions

One way to address frontrunning in an open orderbook model is by requiring users to specify the taker parameter as an arbitrary smart contract address that contains a set of rules. These smart contracts would sit one layer above the base 0x system of smart contracts.




Exchange will reject any attempt to bypass the smart contract specified as the taker for a given order.

Source: blog.0xproject.com/front-running-griefing-and-the-perils-of-virtual-settlement-part-2-921b00109e21

**Commit-reveal scheme.** Implementing a commit-reveal smart contract is a potential solution to frontrunning and establishing networked liquidity. A relayer using commit-reveal would host an open orderbook, but require users to set the commit-reveal smart contract as the taker. Commit-reveal breaks the transaction into two pieces - commit and reveal. In the commit phase, a taker commits to filling an order by sending a transaction to the blockchain. This transaction does not reveal the taker's intent to anyone. After this transaction is mined, the taker sends another transaction to the blockchain to fill the order with a "secret" that proves that she is in fact the taker that committed to filling the order in the first transaction.

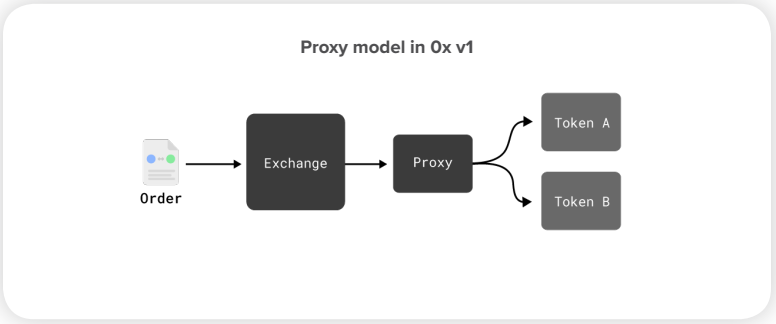
Challenges remain, including the risk of trade collisions, takers have to pay gas costs twice - once in commit and once in reveal, makers can cancel an order after the taker has executed a commit, costing the taker wasted gas fees, and takers have to wait for two transactions to be mined before the trade is executed.

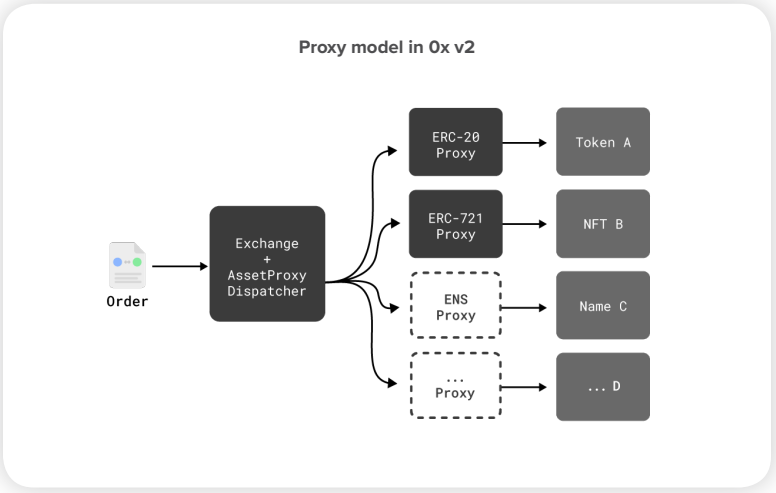
**Trade execution coordinator.** In an open orderbook strategy, the taker and Exchange contract are in charge of trade execution (most decentralized). In an order matching strategy, a matcher aggregates liquidity and executes trades. As we mentioned, this requires the user to trust that the loss of reputation is a strong enough incentive for a matcher to behave honestly, as there are no concrete slashing conditions. The 0x team suggests unbundling liquidity aggregation and trade execution by establishing a trade execution smart contract and trade execution coordinator (TEC). The TEC could be a trusted centralized entity, a trustless centralized entity, or a decentralized entity. The 0x team has said it is conducting research on each of the models and the respective trade-offs that it would need to make in centralization, censorship resistance, and user experience, but this method is one way to address race conditions while maintaining an open orderbook.

## 0X FEATURES

### New contract architecture

The 0x team rolled out a new contract architecture in v2 that makes it easier to add support for new token standards. In v1, 0x had the Exchange contract and a single Proxy contract. In order to add support for new tokens, 0x would have to keep redeploying the Proxy contract, which would force users to transition to the new Proxy contract each time. In v2, 0x can now deploy separate Asset Proxies for each new token standard. Now, every time 0x adds support for a new asset type, 0x does not need to redeploy an existing contract and force users and developers to upgrade. Currently, 0x offers support for ERC-20 and ERC-721 tokens (NFTs).




Source: blog.0xproject.com/introducing-0x-protocol-v2-9f5bda04d38d

### Gas free creation and modification

A key advantage of the off-chain orderbook (at the expense of decentralization) is that users do not need to pay gas fees to create or modify orders. On-chain orderbooks require users to submit a transaction for every change to the blockchain state - this means that users must pay gas fees to create an order that they may decide to change or cancel, which requires additional gas fees. The costs add up and is a key reason why on-chain orderbooks are not very common at this point in time.

### Token Abstraction

Aside from facilitating distributed peer-to-peer trading, another use case Will Warren (the CEO and co-founder of 0x) has spoken about extensively is the use of the 0x protocol for token abstraction. With token abstraction, dApps could convert in and out of tokens on users' behalf without users having to manually instruct the dApp to execute the conversion. Currently, in order to use a specific dApp, users have to convert from fiat to ETH to the native token of the dApp. Given the thousands of dApps on Ethereum that have their own token, token fatigue is a major problem - the additional step harms the user experience, impeding

greater user adoption. In response, the 0x has functionality that would allow dApps to include a single line of Solidity code to allow smart contracts to automatically convert in and out of tokens on behalf of users.

Consider this example: A user has to purchase GNT with ETH to use the Golem application. With 0x, the wallet of a user with ETH would see that she's attempting to use Golem and a dApp connected to 0x could execute the exchange behind the scenes without the user having to manually instruct it to do so. This functionality is not currently enabled but is something the team is working towards. The downside is that the user would still have to pay the extra gas fees for the behind-the-scenes conversion from ETH to GNT.

#### 0x Instant

According to 0x, a new functionality called 0x Instant will make it easier for businesses and dApp developers to integrate token abstraction functionality. 0x Instant is an interface built on top of 0x that allows developers to integrate automatic crypto purchasing into their app or website with a few lines of code. "Instant aggregates liquidity from 0x relayers for any ERC-20 or ERC-721 asset, calculates the best orders to fill and lets users pay for these assets with [Ether]." Currently, the main way users purchase crypto is through a centralized custodial service like Coinbase (easy but slightly risky), a centralized orderbook exchange (more challenging and potentially more risky), or a decentralized orderbook exchange (slightly less risky but most challenging). 0x Instant aims to be the option that is both less risky and less challenging. Additionally, the more dApps that integrate this functionality, the idea is that networked liquidity on 0x will grow in tandem.

At the time of writing, apps using this feature include Augur, which now allows users to easily purchase REP (Augur's native token) with their ETH, Coinbase Wallet and CoinGecko. The feature will also be useful for projects in the crypto gaming sector. For example, Gods Unchained has integrated 0x into its in-game experience and Apollo marketplace to allow users to seamlessly purchase its NFT cards and digital in-game items[6].

### Unique functionality

As the 0x team continues to build out the platform, they have discussed future plans for what 0x could facilitate. Many of these ideas are tied to the process of requiring users to set the taker parameter to an arbitrary smart contract such as but not limited to the ones discussed above. This could facilitate multiple things, a few of which include:

- **Prevent front-running and trade collisions:** A relayer could require that users specify the taker as a smart contract or centralized entity that enforces certain rules around trade execution.
- **Fee sharing:** A relayer or group of relayers sharing liquidity could require users to specify the taker as a smart contract that distributes fees among a pool of relayers or dApps sharing liquidity.
- **Whitelisting addresses:** A relayer specializing in security tokens could require its users to specify a smart contract that requires the addresses trading the tokens to be registered on a whitelist of users who have undergone a KYC/AML process off-chain. Relayers could also outsource whitelist creation to entities such as Harbor or Polymath. This is also important for traditional funds that require that their counterparties go through a KYC process.

### ERC-721 token (NFT) marketplaces

In version 2.0, 0x rolled out the ability for relayers to offer ERC-721 tokens or NFTs (non-fungible tokens). One of multiple interesting relayer models Clay Robbins discusses is an ENS (Ethereum name service) Marketplace. A relayer could use the 0x Launch Kit to build a UI and ENSNifty to convert ENS domains into NFTs, thus creating a secondary marketplace for domain names similar to GoDaddy. Another interesting model he discusses is a secondary marketplace for tokenized software licenses that could allow businesses to sell licenses they don't need anymore or borrow and loan licenses they need for a certain period of time.

[6] forbes.com/sites/rebeccacampbell1/2018/12/06/0x-launches-instant-delivers-an-easy-and-flexible-way-to-buy-crypto-tokens/#68ad837f4356

## RELAYER EXAMPLES

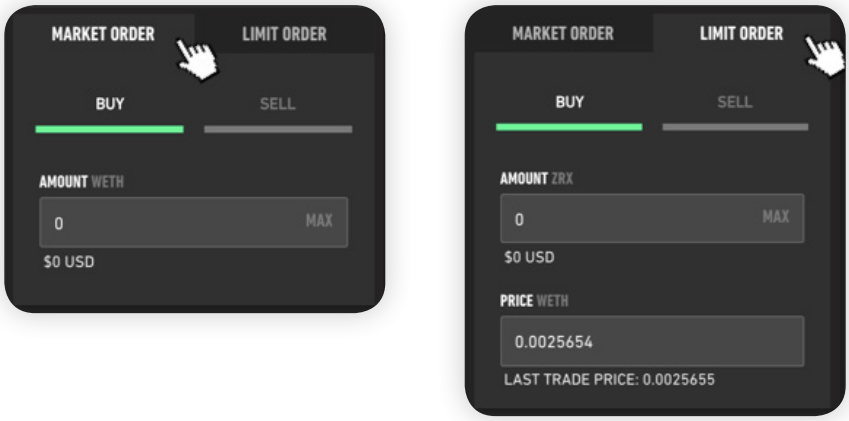
### Radar Relay

Radar Relay is the second largest relayer on the 0x network. It went live on the Ethereum mainnet in October 2017 and released version 2.0 in September 2018. Radar Relay serves users in over 150 countries, has raised two rounds of financing, and has grown to thirty team members. Radar Relay uses an open orderbook model and does not match counterparties. Relay employs a maker/taker fee model and collects fees in ZRX tokens. The team is working on implementing token abstraction in the future. Consider a taker with only ETH in her wallet who wants to fill order A. Radar Relay would convert ETH to ZRX (order B) for the amount of ZRX the taker would need to fill the order to lower the barrier to entry to using the platform.

#### Step-by-step process

Radar Relay has a how-to page that walks users through the set up and trading experience. To set up, users have to:

1. Connect their Metamask, Ledger or Trezor wallet and make sure they have some ETH.
2. Wrap their ETH to convert ETH to WETH, which adheres to the ERC-20 standard. This costs gas.
3. Enable WETH to give the smart contract permission to move funds into and out of their wallet. This costs gas.
4. Users can place market or limit orders. To make a market order, click the market order tab, choose buy or sell, enter the amount to buy or sell, and click buy or sell to complete the transaction.
5. To place a limit order, click the limit order tab, choose buy or sell, enter the amount to buy or sell and at what price, and click buy or sell to complete the transaction. In a limit buy, the trade will only execute at the specified price or below. In a limit sell, the trade will only execute at the specified price or above.




Source: radarrelay.com/how-to/

### Paradex

Paradex is the largest relayer by 24-hour trading volume on the 0x network. It does not currently serve users in the US, Canada or Japan. Paradex was acquired by Coinbase earlier this year. Unlike Radar Relay, Paradex uses an order matching strategy, which addresses the risk of trade collisions and frontrunning by unknown counterparties, at the cost of networked or shared liquidity. Users must also trust that repercussions to the Paradex and Coinbase reputation and brand is a strong enough incentive to prevent them from frontrunning.

In an order-matching model, the only piece that is decentralized is that Paradex never takes custody of user assets. However, trade execution is centralized because Paradex takes on the role of matching counterparties with one another.

Another interesting difference between Radar Relay and Paradex is that Paradex has chosen not to collect trading fees in ZRX tokens. While the original post about trading fees has been deleted, comments in reddit highlight that Paradex uses a spread-based model as compensation for providing an orderbook and

executing trades. The steps to trade in Paradex are similar to Radar Relay, except Paradex matches buyers and sellers that specify prices that overlap. Paradex and Coinbase can buy ZRX tokens to participate in governance.

## GOVERNANCE

0x is using a proxy governance system as a placeholder - a multi-sig process in which different stakeholders[7] with different interests in the protocol weigh in on protocol upgrades. Eventually, 0x plans to convert to a DAO-based governance system that would allow ZRX token holders to vote on and implement upgrades to the protocol securely without disrupting the ecosystem. For the time being, fully decentralized governance is in the research phase given the lack of study and tools for building it into smart contracts.

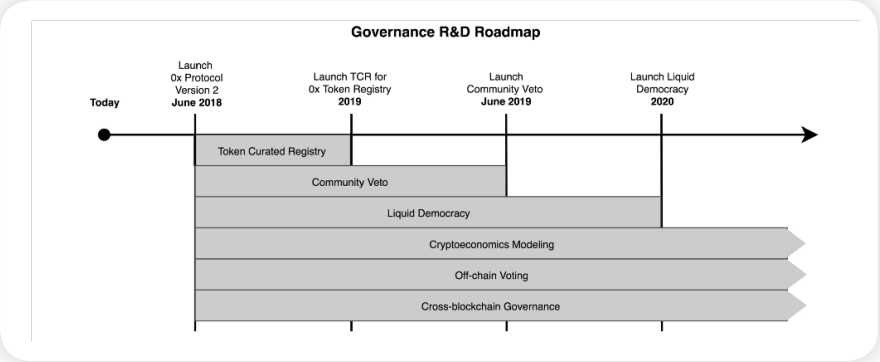
The 0x team believes that informal, opt-in upgrades would fragment the network (by creating incompatible subnetworks). Further, they believe that key stakeholders should have a say in decisions and that the process of upgrading smart contracts moving large sums of funds should be secure. In a system with formal governance, token holders would vote on whether they do or do not want to implement a specific upgrade. If enough token holders vote for an upgrade, it could theoretically be implemented without network downtime or disruption.

0x requires relayers using open orderbooks to collect trading fees in ZRX. They believe this is the most effective mechanism for getting tokens in the hands of representative stakeholders, notably, traders and relayers. Their goal was not simply to get the widest distribution, but rather to achieve wide distribution of tokens to stakeholders that have the most to lose. The main downside of using ZRX as trading fees is that users have to hold or acquire yet another token to use the platform.

A key challenge associated with token voting is that users with the most tokens will have a greater say in the decision process. However, those users qualified to make better informed decisions may not have a correspondingly large amount of tokens. In response, 0x is exploring solutions such as liquid democracy in partnership with Aragon in which token holders can delegate their tokens to people believed to be better equipped to make the right decisions.

## GOVERNANCE ROADMAP

The 0x team has shared a working governance roadmap that could change.




- **Token registry:** The first step is to create a registry. A registry provides important data on ERC-20 tokens, such as symbol, name, address, decimals. It has been centrally managed by 0x to date but they plan to move to a community managed token curated registry or TCR.
- **Community veto power:** Until a fully decentralized governance system is implemented, as a next step, 0x plans to give stakeholders the power to veto proposals submitted by the 0x team.
- **Liquid democracy:** As of now, 0x plans to implement liquid democracy as its governance process. In liquid democracy, users can delegate their votes. In the early phase of a project, they can delegate votes to core developers who have a better grasp, but can reclaim their votes as they become more educated.

[7] Who are the stakeholders in 0x protocol? Relayers, market makers, dApp developers and traders.

## Additional governance challenges

### Collecting fees in ZRX is not mandatory

A key challenge of the 0x governance system is that relayers using the order matching strategy do not need to collect fees in ZRX tokens. Paradex and DDEX[8] are two relayers using the order matching strategy. Additionally, The Block reported that some relayers offer users the option to pay fees in ZRX or in the token they're trading (The Ocean) and some relayers are not charging fees at the moment (i.e. Radar Relay and Bamboo Relay). Looking at the 'Recent Fill' in 0xtracker, none of the relayers have collected fees in ZRX recently (at the time of writing). The process of using a dApp is already difficult - users must connect a wallet, unlock tokens, wrap ETH - each of these steps must be explained and takes time to understand and get accustomed to.

The consequence of not collecting fees in ZRX is that distribution of ZRX tokens to key groups of stakeholders breaks down. Yes, relayers who don't collect ZRX fees and traders that use these relayers could buy ZRX tokens to participate in governance, but that is an assumption that has not been proven. Regardless, this brings into question the decision to require users to pay fees in ZRX. One way relayers could address this kink in the user experience is fee abstraction, where the relayer trades a user into their fee token before executing their trade. However, this might not result in the best price and users now have to cryptographically sign two messages instead of one. One way users can avoid this is buying a large amount of ZRX tokens at once.

Thus, it seems the best option for users to avoid converting in and out of ZRX manually is by using a relayer that employs the order matching strategy. The current trade-offs of using matchers include that they are more centralized and forgo shared liquidity. It will be interesting to see whether users prefer relayers that are more decentralized or relayers that offer a more seamless user experience, and how this development informs the strategy of 0x and its relayers going forward.

### Governance centralization

Paradex was acquired by Coinbase. It is possible that other centralized exchanges follow suit and acquire other relayers. While Paradex does not collect fees in ZRX, as we mentioned, with Coinbase backing it, it could still purchase a large amount of ZRX tokens to participate in governance. Similarly, other large centralized exchanges that acquire or build relayers on 0x could do the same, resulting in a handful of exchanges securing significant influence over the platform and overshadowing traders, who likely don't have the funds to secure as significant an amount of tokens as the behemoth centralized exchanges.

[8] DDEX is forking from 0x to create a new protocol called Hydro.

## CHALLENGES

### Decentralization

**Is trust still required?**

While relayers on 0x cannot custody user assets, both open and closed relayers host off-chain limit orderbooks on their central servers. Closed relayers using an order-matching strategy are further centralized in that they match and execute trades on behalf of the users. Recognizing this, Paradex has suggested that it could register as an ATS. While commit-reveal smart contracts and trade execution coordinators (TECs) have been discussed as potential solutions, they have not been tested in practice, so we cannot say with certainty that this will solve the problem or what kind of additional attack surfaces it could potentially raise. Additionally, if a centralized or semi-centralized TEC is used, users must still trust that these entities won't frontrun them.

### Race conditions

**How will the ecosystem address griefing?**

A maker can "grief" a taker by cancelling an order that a taker has attempted to fill by paying a higher gas fee. A miner scanning the mempool would choose the transaction paying a higher gas fee, causing the cancellation to settle before the trade settles. This results in a failed transaction and causes the taker to waste gas fees on a failed trade.

This has been seen in practice. Antonio Juliano, founder and CEO of dYdX, said in a tweet thread that this is a problem they've had to deal with: "about 10-20% of our trades fail because the maker cancels the order before our transaction confirms. It's much worse in times of volatility, because market makers cancel more frequently during these times."

**How will the ecosystem address frontrunning?**

As we mentioned above, there are a few ways to avoid frontrunning, each with their own trade-offs.

- **Order matching:** Relayer is the taker in all trades and matches counterparties.
  - » Trade offs: networked liquidity, plugging into other dApps and smart contracts, more centralized
- **Commit-reveal:** Taker undertakes two transactions, commit without sharing details of the transaction then reveal.
  - » Trade-offs: accidental trade collisions, longer wait time (two transactions), higher gas costs
- **Trade execution coordinator:** Unbundle liquidity aggregation function from trade execution and establish a centralized, semi-centralized, or fully decentralized TEC to execute trades.
  - » Trade-offs: introduces another step, increases complexity and centralization

Order matching is being used by some relayers but goes against the vision of 0x. The practice of setting the taker parameter to a smart contract (needed in Commit-reveal and TEC) is still new and is likely not being used and has not been tested. Therefore, it is difficult to say how effective this strategy will be at this point. Its effectiveness will determine the popularity of the open orderbook strategy and thus, success in achieving networked liquidity.

### Liquidity

**Is networked liquidity realistic?**

Skeptics don't expect networked liquidity as guaranteed to function as well as everyone hopes. There could be a scenario where one to two large relayers host the vast majority of the open relayer volume because they provide the best UX. If all relayers offer the same product, the user is likely to go to the one with the best, most seamless experience. Relayers will have to figure out how to distinguish themselves from other relayers and non-0x DEXs.

[8] DDEX is forking from 0x to create a new protocol called Hydro.

Additionally, exchanges capture market share by growing volume. Why would a big exchange, that has spent significant time and effort building up its liquidity be incentivized to share it with other relayers and dilute away a key differentiator? Smaller exchanges may be incentivized to create "shared liquidity pools" to bootstrap liquidity, but they could stop sharing liquidity once their platform achieves sufficient volume.

One case for shared liquidity is token abstraction, or the idea that dApps would rather plug into relayers that allow them to exchange tokens on behalf of users, than undergo the process of building out the functionality or require users to do it themselves. However, based on feedback from dApp developers, this is currently a tedious process and leads to worse prices for users. These are trade-offs that dApps might not want to undertake, as liquidity on the platform is also very low.

**Is it profitable to run an open orderbook relayer on 0x?**

Currently, most open orderbook relayers are not charging fees on 0x. The optimistic explanation is that relayers want to bootstrap liquidity before charging fees. The less optimistic reason is that 0x requires relayers to collect fees in ZRX, which creates a poor user experience and may deter users and dApps from using the platform.

**Can traders employ sophisticated trading strategies on 0x, as it stands?**

The short answer is no. The longer answer is that spreads (difference between bid and ask) are not great, likely because there is insufficient liquidity and because 0x requires cancellations to be verified on-chain.

**Will relayers leave 0x?**

DDEX announced on Dec 14, 2018, that they are forking the 0x protocol to create a new protocol called Hydro, which they plan to transition to once it's complete. The reasoning is that their "perspective of what's most urgent diverged" and "being on the front lines, it is painfully apparent that most DEXs today are still plagued by rudimentary problems such as order collision, frontrunning, and poor liquidity." In a nutshell, it seems that the DDEX team believes that formal governance and some other features 0x has been working on are less critical than finding solutions to these challenges. DDEX will attempt to tackle these challenges in a different way than 0x. To do so, they plan to develop "a new order schema, an engine capable of true matching, robust market orders, and a fundamentally different liquidity sharing pool." Ironically, some are questioning whether the disagreement could have been addressed if 0x had a formal governance process in place.

In the announcement, Tian Li (founder of DDEX) mentions that Hydro was initially designed to incentivize liquidity on 0x, with its own token (HOT). The whitepaper came out in January 2018. They plan to keep the name by have expanded the scope of the project. The initial plan was to use HOT for "liquidity pool membership, liquidity incentive mechanisms, and bounties for market makers", but it is unclear whether the HOT token will be used in the new protocol and, if so, in what capacity. If the team delivers a robust competitor to 0x, other relayers could choose to transition to Hydro, if their goals are better aligned with what the new protocol will offer.

## Regulation

**Will relayers be regulated?**

Relayers are central, for-profit entities building on top of the 0x protocol that have a central website. 0x has said that relayers are responsible for complying with regulations. One of the greatest advantages over centralized exchanges is their non-custodial nature. Proponents also expect DEXs to be censorship resistant and able to list assets in their early stages and avoid KYC/AML processes.

While the custody and settlement pieces of relayers are decentralized, there are other pieces that are centralized, specifically the off-chain orderbooks of all relayers and trade execution for relayers using order matching. Thus, it is very likely that relayers are not shielded from regulations, as regulators have a central point of contact to enforce exchange and anti-money laundering laws

## FINAL REMARKS

As with the other dApps and protocols we've written about, it is very early days. 0x is a project with a strong team that has held itself accountable by continuously delivering progress and improvements, and making it very easy for developers to build on and integrate into the platform. However, the regulatory landscape remains unclear and uncertain at this point, and while regulators may not be able to shut down software, they have shown that they can and will charge founders and developers who built the software.

Further, challenges around trade collision, frontrunning, griefing, governance, networked liquidity, and liquidity more generally remain unsolved. Competition in the space is also intense with DDEX splitting off to create its own open protocol and many other teams working on building the winning DEX. While the 0x team and relayers on the platform are conducting research to address these challenges, it will take time to test potential solutions and say with certainty that 0x has successfully achieved its vision to address the fragmented ecosystem of dApps and DEXs and combine liquidity to create a global liquidity pool.

# IDEX (IDXM, AURA)

## OVERVIEW

IDEX is a hybrid DEX built on the Ethereum blockchain and is the first product in the Aurora ecosystem. IDEX currently has the greatest market share (~35% using 7-day traded volume) of all existing DEXs in terms of trading volume. The exchange is described as a hybrid platform because it has both centralized and decentralized elements (though arguably more centralized than decentralized). While settlement occurs on-chain and users maintain custody of their assets (decentralized), IDEX servers currently manage the off-chain orderbook, order matching and trade execution (centralized). This allows IDEX to separate trading from settlement so that users can trade in real-time without waiting for orders to mine. Having IDEX act as trade arbiter also prevents issues such as frontrunning and trade collisions because only IDEX is authorized to dispatch trades.

Alex Wearn is the CEO and co-founder of IDEX and Aurora. Prior to Aurora/IDEX, he was at Amazon, Adobe and a marketing analytics firm. Phil Wearn is the COO. Prior to IDEX/Aurora, Phil co-founded EtherEx and has a background in aerospace engineering. Jason Ahmad is the CTO of IDEX. Development on IDEX began in November 2016, a working version of the platform was released on testnet in the summer of 2017, and the platform went live in October 2017. IDEX currently has twenty team members: 11 core members (8 developers and 3 business analysts), 5 support employees, 3 members on the token team and a couple contractors.

### What is Aurora?

Aurora is a fintech company that aims to provide a decentralized financial ecosystem. While the team is currently focused on IDEX, they plan to eventually roll out additional decentralized finance products and services. One of these products is a stable asset, boreal. Boreal is intended to be a substitute for central bank currency. It is connected to IDEX in that it will be redeemable on IDEX at its target value in lieu of trading fees (similar to Binance's BNB tokens). The idea is that traders will purchase boreal if it falls below the target value to lower overall trading costs. Eventually, Aurora intends to offer on-chain loans in boreal.

Another key product Aurora has discussed is called Snowglobe protocol, a sidechain protocol for DEXs to build on and share liquidity (similar to 0x protocol). The FAQ page says that "IDEX components will be updated to Snowglobe post launch on the mainnet" and that "Snowglobe operates as a sharded POS childchain connected to the main Ethereum chain." It is expected to have five components: "the Ethereum childchain contract for holding funds, the Snowglobe base chain, a shared distributed off-chain orderbook, and a local and global transaction dispatch arbiter."

According to Aurora's development timeline, Snowglobe's childchain architecture was supposed to go live in 3Q18, but it has not been deployed at the time of writing (Dec 2018). In a recent reddit post, Alex Wearn (CEO) said while Snowglobe has not been abandoned, the team is not actively working on it at the moment. Rather, key priorities include (1) launching a sidechain to improve scalability and reduce gas costs, (2) launch new asset types like WBTC (a proxy for BTC on the Ethereum blockchain) and security tokens, and (3) the toke staking MVP (minimum viable product).

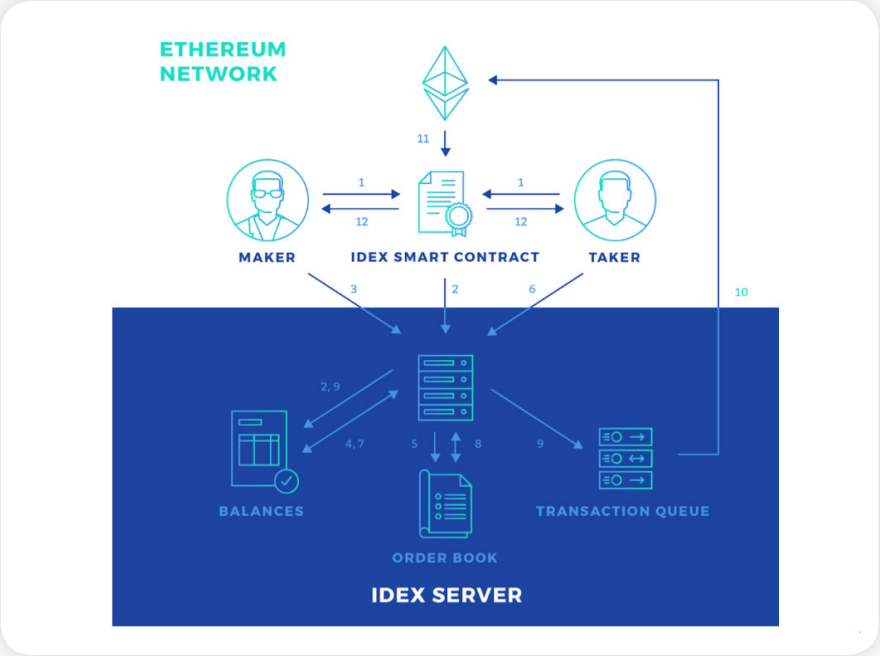
### Regulation

Until IDEX becomes fully decentralized, the team is taking steps to comply with certain regulations, recognizing that having centralized components makes them especially vulnerable to censorship. Alex Wearn recently announced that IDEX will implement KYC processes for traders on the platform and block NY IP addresses, as IDEX does not have a BitLicense, along with IPs in North Korea, Iran, Cuba, Syria, Crimea, and Washington State.

In the post, Alex Wearn acknowledges that IDEX is not exactly a “decentralized” exchange, and that it would be more accurate to classify it as a “semi-decentralized” or “non-custodial” exchange, since it is not censorship resistant and the only “decentralized” piece is its non-custodial nature.

## IDEX COMPONENTS

The main components of IDEX include the off-chain orderbook (trading engine), smart contract and transaction processing arbiter. The smart contract stores assets deposited into the contract and executes trade settlement. While it requires that all trades are signed by users’ private keys,  only IDEX is authorized to submit signed trades to be executed on the Ethereum blockchain by the smart contract.




Source: idex.market/whitepaper

In many DEXs, the taker submits the final transaction to the Ethereum blockchain to be mined. In an ideal system, the trade would settle at the same time that the taker submits it to Ethereum. However, because blocks are not mined instantly, there is a delay between a taker submitting the trade and the trade being mined, and this delay is exacerbated by network congestion on Ethereum.

What happens in practice, is that the trade is added to the Ethereum mempool (a pool of pending transactions). During this time, other traders could technically still fill the same order. This might be unintentional (trade collision) or intentional (frontrunning). Additionally, the maker or taker could cancel the order or move their funds in the time before a transaction is settled on the blockchain, causing the trade to fail. These challenges prevent traders from employing more sophisticated or high frequency trading strategies.

In response, IDEX has brought the process of trade dispatch to the exchange itself. When the maker and taker sign the transaction, their balances are updated in real-time on the exchange. However, that doesn’t necessarily mean that the trade has been mined in a block. Behind the scenes, the trade arbiter dispatches the transaction to the blockchain in the correct order that they are executed. Because the arbiter is the only one who can submit trades to the blockchain, the idea is that an honest arbiter will ensure that a given order is not mistakenly or intentionally submitted to the blockchain by multiple takers, regardless of whether they have specified higher gas fees.

[9] IDEX is not the only “de-centralized” exchange that is not fully decentralized. While “DEXs” do not custody user assets, any exchange that has an off-chain component is not fully decentralized.

### Step-by-Step Process

1. Users visit idex.market and connect their wallet to IDEX via private key, keystore file, Metamask, or Ledger.
2. Maker and taker must deposit tokens on IDEX. This requires paying a gas fee (ETH gets deposited in one transaction, but ERC-20 token deposits require two transactions).
3. After depositing tokens, a maker can create an order and sign the transaction, authorizing the smart contract to execute the future trade. IDEX reviews the order to check that the maker has sufficient funds and check that trade parameters in the signed transaction match info submitted to IDEX, then adds the order to the orderbook. The maker fee paid to IDEX is 0.1%, paid in ETH.
4. A taker sees the order and decides to fill it, signing the trade with her key, authorizing the smart contract to execute the trade. IDEX carries out the same trade parameter checks. The taker pays a 0.2% fee to IDEX in ETH.
5. Once this is complete, the off-chain orderbook is updated in real-time and takers can execute trades based on the updated off-chain balances. IDEX submits the order to the smart contract to be executed on Ethereum. While both maker and taker have authorized the smart contract to execute the trade, **IDEX is the only one that can submit the order to the contract**. The taker covers the gas fee of each trade.[10]
6. Miners mine the maker and taker transactions when they reach it in the mempool (assuming sufficient gas fees have been specified). Once the transactions are mined, the Ethereum smart contract balances are updated. This likely occurs some time after the balances are updated in the off-chain orderbook.
7. Users can withdraw their tokens if all their executed transactions have been mined.

### IDEX Features

**Maker griefing** - rescinding authorized orders. A dishonest market maker might be incentivized to cancel a pending transaction that is no longer profitable by paying a higher gas fee for an order cancellation than the taker paid for filling the order, causing the order to fail. IDEX prevents this by requiring users to deposit tokens into the smart contract before trading and users cannot withdraw tokens until trades are mined in the order they were placed. This ensures that traders don't waste gas fees on an order they're attempting to fill.

**Ethereum backlog.** Ethereum bloat prevents certain DEX users from taking advantage of quick price movements and trading strategies. IDEX users avoid the latency associated with settling trades on chain because trading on IDEX is continuous and separate from settlement. Additionally, this structure allows users to carry out limit and market orders (an order where the taker doesn't specify the price, just the quantity). While IDEX hasn't yet had any major issues keeping the off-chain orderbook in-sync with settled trades, this could pose a problem if the backlog of transactions in the Ethereum mempool significantly increases (i.e. another Cryptokitties).

**Gas free cancel & sophisticated trading strategies**. IDEX also allows users to cancel transactions without broadcasting the cancels to the blockchain. They enable this by effectively maintaining the state while the blockchain "catches up". Users can instantly trade assets they receive without having to wait for an on-chain confirm but they can't withdraw until the confirm happens. Similarly, IDEX allows users to do cancels in a similar way - by just signing a message.

In order to deploy sophisticated trading strategies or high frequency trading, trades must settle instantly or near-instantly. IDEX's model is more conducive to trading strategies than most other DEXs due to the separation of trading from settlement.

## ROAD TO DECENTRALIZATION

While certain functions are currently centralized, IDEX plans to gradually transition to staking model to achieve full decentralization where all elements are distributed. Users will stake AURA tokens in order to participate in securing the network and receive a portion of trading fees collected on IDEX as compensation. Key motivations for decentralization are to address the risks of DDOS attacks to which central servers are vulnerable and achieve censorship resistance. IDEX will roll out the staking function in multiple stages.

[10] According to the FAQ page, trades on IDEX cost ~140K gas, which is ~1.5x higher than gas costs on EtherDelta and slightly higher than gas costs on 0x. IDEX sets the gas price to Ethgasstation's "fast" setting +2. The taker cannot adjust the gas.

The idea is that users will download an IDEX client that connects to a network of nodes that run certain functions that are currently centrally managed by IDEX, such as serving the trade history, coordinating submission to the contract, and providing a distributed orderbook.

### Tier 3: Trade History

As it stands, IDEX's central servers provide trade history to users. As the history of mined trades is tracked on the Ethereum blockchain, IDEX plans to shift to a model where AURA staking nodes download the data from the Ethereum blockchain and provide it to the IDEX client. In this model, IDEX will require staking nodes to send IDEX a hash of the downloaded history, which it will verify. If IDEX servers find that the hashes don't match, the node will be blacklisted. Stakers will be rewarded in fees (collected in ETH) proportional to their stake and uptime. Tier 3 stakers will have to stake a minimum of 10,000 AURA individually or as a pool. IDEX will initially reward AURA stakers 25% of fees collected on IDEX.

### Tier 2: Transaction Arbiter

The arbiter submits approved trades to be mined on the blockchain in the correct order. Currently, IDEX is the centralized trade arbiter and users have to trust that IDEX won't frontrun them. The incentive for IDEX to behave honestly is loss of reputation and users, financial loss and regulatory action.

IDEX wants to move to a model where an arbiter and validator are randomly chosen each period from the pool of staking nodes, with the likelihood of being chosen proportional to stake as a percent of total. The arbiter compiles and signs approved trades and the chosen validator verifies the transaction before the arbiter submits it to the blockchain. Minimum staking requirements for tier 2 stakers will be higher than for tier 3. IDEX will distribute 33% of fees as rewards to Tier 2 stakers.

### Tier 1: Distributed Orderbook

Currently, IDEX has an off-chain orderbook hosted centrally on its servers. Tier 1 will have a different staking structure, with 20 to 50 "masternodes" to reduce the latency and UX trade-offs currently associated with a fully distributed orderbook. The main responsibility of Tier 1 masternodes will be hosting a distributed orderbook. Additionally, these nodes will be in charge of tracking the real-time balances of users, matching orders, and verifying signed transactions before they reach the arbiter. Tier 1 stakers will have a higher minimum staking requirement but will also receive a higher payout for the work they provide.

## DECENTRALIZATION CHALLENGES

**Slashing conditions.** If the stakers in Tier 3 try to cheat the system, IDEX says their existing wallet address will be blacklisted, but has not specified if they will lose some portion of their AURA stake. If the only negative consequence is blacklisting a wallet address, the staker can just create another wallet address to partake in staking and continue to act maliciously.

If arbiters and/or validators in Tier 2 or the masternodes in Tier 1 behave maliciously (i.e. by censoring transactions or frontrunning users), IDEX says they will lose some portion AURA staked[11]. As in Tier 3, it is unclear if these slashing conditions will be sufficient to prevent stakers from cheating the system.

**Masternodes.** Further, the masternode structure has been criticized as being too centralized in other projects that have employed it (Dash). Additionally, IDEX has not yet laid out how the masternodes will be chosen, how long they will hold their position as masternode, or whether they will be banned from participating as a masternode if they behave maliciously.

**Timeline.** Initially, IDEX said staking would go live by 3Q18. As of the last post on the subject (September 2018), they said the alpha version of AURA staking would go live in the next few months, subject to delays. In a more recent post, Alex Wearn says "most everyone acknowledges that "DEXs" with on-chain orderbooks are

[11] IDEX has not yet defined how much AURA they would lose.

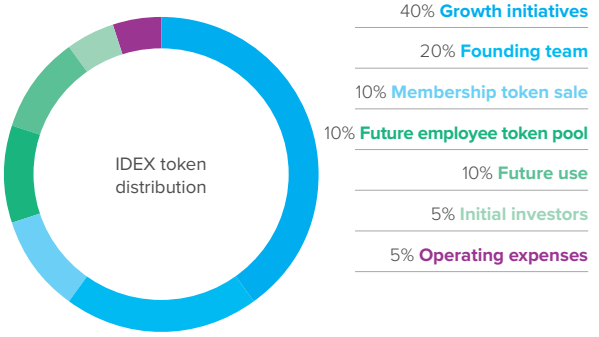
currently impractical, while other changes would make the UX too complex for anyone but advanced users." Based on this post, it is unclear if IDEX has chosen to slow down the process of decentralizing everything until latency, gas, and scaling problems on Ethereum are addressed.

## TOKENS AND TOKEN FUNCTION

IDEX currently has two tokens - IDXM and AURA. IDEX describes IDXM as a "membership token". They sold 2,000 IDXM tokens following the launch of the platform. The key motivation behind IDXM was to raise funds to grow the team and platform. Additionally, it was used to attract users to the network as one IDXM token equates to three years of free trade (through 2020) for the maker or taker. Additionally, IDXM token holders are rewarded AURA tokens at twice the rate of non-IDXM holders to participate in the future staking process. While the free trade benefit will expire in 2020, the AURA reward rate for IDXM holders will continue.

**AURA** is a staking token that IDEX plans to use in the future, decentralized version of IDEX. AURA has a fixed supply of 1 billion, with 50% distributed publicly to potential stakers. IDEX distributed the first 10% (100 million tokens) to IDXM holders. 20% of the tokens reserved for public distribution (200 million tokens) will be used to support boreal banking. 20% (200 million tokens) is being distributed in slow, monthly installments to active traders on IDEX in proportion to their trading volume, with monthly payouts equal to 1% of the remaining tokens in this bucket (i.e. 2 million in month 1, 1.98 million in month 2, etc.). The more that users trade, the more AURA tokens they will receive. The incentive to stake AURA tokens in tiers 1 through 3 is that stakers will receive a portion of trading fees collected on IDEX.

The remaining 50% will be used as follows: 20% to the founding team, 10% in future employee token pool, 10% future use, 5% initial investors, and 5% business expenses. The allocation proportions could change as IDEX has changed different components of its staking process as it nears the alpha. Currently AURA is only available for trading on IDEX, but the team announced that that alpha release of AURA staking will occur on January 8, 2019.




Source: coincentral.com/introducing-aura-staking-token-securing-idexs-future/

**Boreal** is the stablecoin that Aurora plans to roll out in the future. The mechanics of boreal are still a work in progress, but IDEX has said that it could back boreal with revenues collected on IDEX. Additionally, IDEX has said it would use boreal as the underlying asset used to provide loans on the blockchain, as more solutions around decentralized credit and identity as proxies for credit scores emerge.

## CHALLENGES AND UNANSWERED QUESTIONS

### Central servers

How can bad actors exploit IDEX's central servers?

As we mentioned in our introduction, the existence of centralized components puts dApps at risk of experiencing downtime. The more centralized a DEX, the higher its risk of being the target of a DDoS (distributed denial of service) attack that disrupts the normal traffic of a targeted server by flooding the server

with illegitimate traffic. In fact, IDEX experienced a DDoS attack in January 2018 during which time the website was inaccessible to users. While IDEX stated that user funds were safe in the smart contract during the attack, it took IDEX multiple hours to recover.

### Regulation

**How could IDEX be regulated?**

We've established that most components of IDEX are not decentralized. Until (if) IDEX successfully decentralizes these components, there is significant risk that regulators could shut down IDEX's central off-chain order-book and servers if they believe the exchange is in violation of securities regulations. IDEX's CEO recently announced that IDEX will block NY IP addresses (as it doesn't have a BitLicense) and implement KYC processes to comply with regulators, acknowledging that centralized components of the exchange put it at risk of being regulated and censored.

### Decentralization

**Is IDEX really decentralized?**

After examining the exchange, it is clear that IDEX is more centralized than it is decentralized. The only component that is currently decentralized is custody - IDEX's central servers do not custody user assets. Recognizing this fact, the team has also begun to refer to IDEX as a "non-custodial" exchange rather than a decentralized exchange. Because it has components that are centralized, the team also made the decision to comply with KYC regulations and block New York IP addresses, which received some backlash from the community who believed IDEX to be decentralized.

**Will staking, as IDEX describes it, successfully decentralize IDEX's operations?**

While IDEX has plans to become fully decentralized, it is still too early to tell if the plan will work as intended. IDEX is distributing AURA to traders on its platform, proportional to how much volume they trade so that heavy traders aggregate more AURA tokens. Additionally, as it stands, IDEX will impose a minimum staking requirement that increases with each Tier (10K for Tier 3). What we don't know is if there are any safeguards in place that prevents a small group of people from holding a large portion of tokens. If not, then the new model might not be as decentralized as people expect it to be.

**Is full decentralization of IDEX feasible or realistic?**

The execution risk of what IDEX is trying to accomplish in terms of fully decentralizing IDEX and building a decentralized ecosystem (which we have not extensively covered here as it is still very early days for the other products) seems like it is fairly high. It is a multi-step, multi-year process, and each component depends on the success of the prior component, most notably the success of AURA staking and the fully decentralized version of IDEX. Additionally, it is difficult to know whether IDEX will be able to preserve the real-time trading and seamless user experience in the fully decentralized version.

## FINAL REMARKS

IDEX is viewed as one of the most flexible and versatile DEXs that also offers users an experience that is most similar to a centralized exchange. This is also made evident based on its market share of DEX trading volume (30-35%). However, this is because IDEX is one of the most centralized of the DEXs. To address that, IDEX has stated that it is on a path to gradual decentralization. However, it is taking longer than expected to roll out the first components of the plan, AURA staking[13], and the plan is subject to change: "Due to the complex and ever-changing nature of blockchain technology, all information in this post is subject to change as the infrastructure is built and optimized." Till then, IDEX will have to deal with the regulatory and security challenges of being mostly centralized.

[12] IDEX has blocked NY IP addresses at the time of writing.

[13] AURA staking was originally slated to go live in 3Q18. On December 17, 2018, Alex Wearn (CEO) said the Aura staking alpha will go live on January 8, 2019.

## Disclosures

This report has been prepared solely for informative purposes and should not be the basis for making investment decisions or be construed as a recommendation to engage in investment transactions or be taken to suggest an investment strategy in respect of any financial instruments or the issuers thereof. This report has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research under the Market Abuse Regulation (EU) No 596/2014. Reports issued by Circle Internet Financial Limited ("Circle") or its affiliates are not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services and are not recommendations to buy, sell, or hold any asset. The information contained in this report is based on sources considered to be reliable, but not guaranteed, to be accurate or complete. Any opinions or estimates expressed herein reflect a judgment made as of this date, and are subject to change without notice. Circle will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents. Circle and its affiliates hold positions in digital assets and may now or in the future hold a position in the subject of this research.


**0x Sources**

github.com/ConsenSys/0x-review/blob/master/report/3_general_findings.md

medium.com/the-block-crypto/block-by-block-cryptocurrency-exchanges-867862226e4a

blog.0xproject.com/front-running-griefing-and-the-perils-of-virtual-settlement-part-1-8554ab283e97

blog.0xproject.com/front-running-griefing-and-the-perils-of-virtual-settlement-part-2-921b00109e21

blog.0xproject.com/governance-in-0x-protocol-86779ae5809e

blog.0xproject.com/introducing-0x-protocol-v2-9f5bda04d38d

blog.0xproject.com/22-ideas-to-explore-with-0x-4d551c10dd4e

blog.0xproject.com/ecosystem-update-ddex-and-the-0x-roadmap-5d201cafa133

medium.com/radarrelay/radar-relay-regulatory-strategy-update-3bd0d61add43

tokeneconomy.co/token-economy-50-paradox-d8f2270c0dce

www.reddit.com/r/0xProject/comments/7um7dw/confirmed_paradex_not_using_zrx_token_for_fees_or/

www.reddit.com/r/0xProject/comments/8d675w/pros_and_cons_of_different_0x_relayers_radar/

medium.com/hydro-protocol/why-we-are-forking-0x-97dc48ee0426

medium.com/@trenton.v/analysis-hydro-forking-0x-3d6faa9f4c2

0xtracker.com/relayers

**IDEX Sources**

collaborate.thebkp.com/project/TL/document/9/version/10/

www.youtube.com/watch?v=4ZOxmeDHsKc&list=WL&index=7&t=0s

www.youtube.com/watch?v=NwsxV2c2vPg&index=7&list=WL

www.youtube.com/watch?time_continue=2&v=3DWO82crisI

idex.market/static/IDEX-Whitepaper-V0.7.5.pdf

medium.com/aurora-dao/the-aura-token-share-in-the-success-of-idex-and-aurora-cf4212ba2e2a

medium.com/aurora-dao/introducing-idex-61af097b48ad

medium.com/aurora-dao/aura-staking-pos-earn-trade-fees-36319229ceae

medium.com/aurora-dao/how-to-deposit-and-withdraw-from-idex-e277f0237405

medium.com/aurora-dao/aura-idxm-the-tokens-of-idex-aurora-explained-f7794d453654

medium.com/aurora-dao/pragmatic-decentralization-how-idex-will-approach-industry-regulations-8b109212128a

medium.com/aurora-dao/idex-joins-wbtc-wrapped-bitcoin-initiative-to-bring-btc-to-ethereum-e9925d17a34b

medium.com/aurora-dao/idex-q3-recap-product-updates-integrations-media-more-87bda4a5cadf

idex.market/faq

idex.market/static/IDEX-Whitepaper-V0.7.5.pdf

www.reddit.com/r/auroradao/comments/a445ac/aura_dao_and_the_future_of_idex/

www.reddit.com/r/auroradao/comments/a543ez/calculating_payouts_on_current_volume/

**Other**

blog.hacken.io/decentralized-and-centralized-exchanges-advantages-vs-disadvantages-aa9a27da4584

www.luno.com/help/en/articles/1000168409-how-does-a-limit-order-work-and-what-are-maker-and-taker-orders

blog.ethfinex.com/challenges-of-decentralised-exchange-d553f479bda5/

medium.com/qurrex/decentralization-of-cryptoexchanges-why-dex-is-beginning-but-not-yet-winning-2be9be6fb90f

rados.io/list-of-documented-exchange-hacks/

github.com/distribuyed/index

github.com/evbots/dex-protocols

www.coindesk.com/decentralized-exchange-crypto-dex

coincenter.org/entry/what-is-a-decentralized-exchange

http://hackingdistributed.com/2017/08/13/cost-of-decent/

blog.sendwyre.com/wyre-talks-getting-100m-users-including-grandma-trading-on-a-dex-d9865e6714e3

dex.watch/