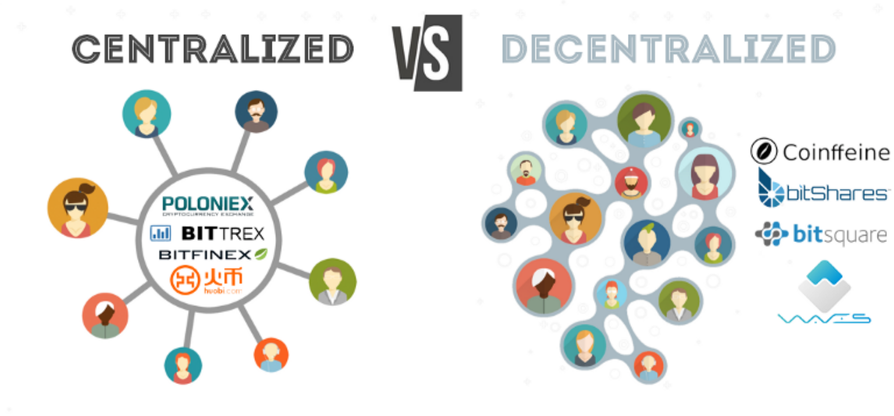
Gary Basin Follow
Digging into crypto. Ran an algo trading firm.
Jun 21 · 11 min read

The State of Decentralized Exchanges

Starting late last year, I've been taking a closer look at the cryptocurrency (aka crypto) landscape. Given the nine years I've spent running an algorithmic hedge fund, I'm naturally drawn to the dynamics of crypto trading. Since I'm not a crypto true believer, I expect to have a fresh perspective on any new trading technologies. ICO scams aside, there are some interesting innovations occurring in the space. Particularly new is the concept of a *decentralized exchange*.



Source: https://bisq.network/

The core value proposition of a decentralized exchange (DEX), and what makes them interesting, is allowing for counterparties to find each other and trade *directly on-chain*, thereby not being dependent on a centralized trading exchange and taking on the associated custody risks. By making trades that settle directly on-chain, you avoid moving your crypto into an exchange wallet and facing the risk of a hack or theft.

Because cryptocurrencies are bearer instruments, exchanges holding large sums effectively become honeypots. At current exchange rates, over USD $15 billion has been stolen from over a dozen different exchanges.

The different flavors of DEXs

The purest form of decentralized exchange is a fully decentralized on-chain model using Ethereum. The Maker team runs one called OasisDEX. Being completely on-chain, all orders interact with each other directly through the blockchain. This makes it fully decentralized, but also expensive and slow. Everything from canceling orders, to transferring crypto, requires paying gas on Ethereum and waiting for block confirmations—at least a few minutes, sometimes hours. Aside from cost and speed issues, this is also vulnerable to front-running. You can see when someone is trying to execute against an order as their message shows up in the Ethereum mempool (pending transactions) and you can get ahead of it by spending more gas to be mined first.

To improve user experience, specifically focusing on costless and faster order placement as well as alleviating front-running issues, a hybrid on-chain/off-chain model has emerged. Basically, you run an order book off-chain, have the "exchange" sign matches (when a *taker* tries to trade with a resting *maker* order) to ensure price-time priority, and then send them to settle in the "settlement smart contract".

This preserves the non-custodial aspect of trading crypto. You never have to leave your tokens sitting on an exchange, but allows for a smoother trading experience that feels more comparable to trading on a centralized exchange. This means traderst still rely on a trusted third party to maintain the order book, but that's a much smaller risk relative to the custodial risk of transferring crypto into a centralized exchange's wallet.

IDEX is one of the leaders in this space.

> *"Unlike EtherDelta, however, IDEX acts as an arbiter for every trade, meaning that the IDEX smart contracts validate transactions before submitting them to the Ethereum network. This serves a couple of functions. First, it allows IDEX to quality control orders, making sure that every trade*

> *is valid before executing it and keeping a queue of transactions to streamline processing. Second, IDEX can update account balances off-chain after they submit a transaction, allowing for the convenience of a centralized exchange without sacrificing security. Generally, IDEX seems to process orders more quickly and efficiently than EtherDelta. It lags less than EtherDelta, but it's still beholden to the Ethereum Network like its counterpart."*

> *Source: https://coincentral.com/off-races-finding-best-decentralized-exchange/*

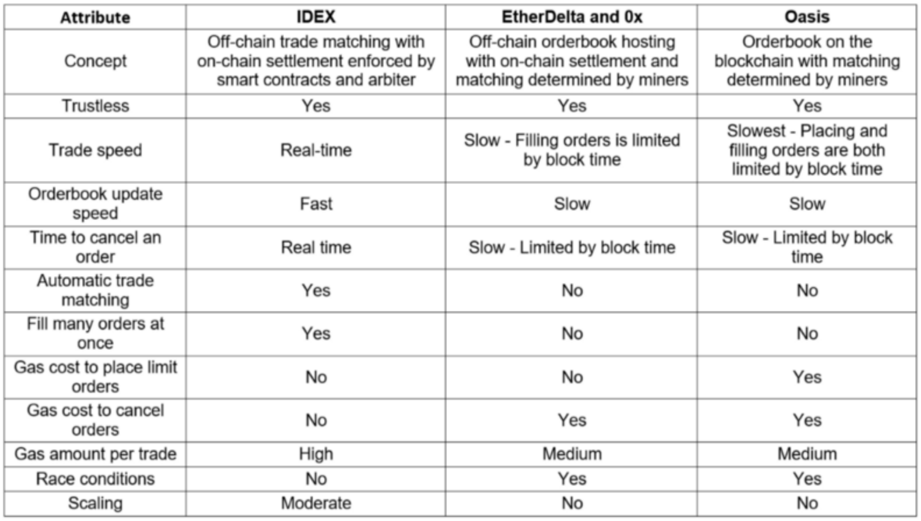
0x Project is creating an ecosystem of decentralized exchanges with their open-source protocol (a good overview can be found here). Unfortunately, in the current implementation the system is plagued with weaknesses that are likely preventing widespread adoption. There is no way to guarantee that a resting order (a *maker*) is still active at any given time, as the maker can withdraw their tokens from the smart contract. Even with their "matching model", where the relayers sign all orders before submitting them for matching, there is a chance of front running by the relayer itself. Some amount of centralized trust is necessary with current technology.

There are several proposed solutions for DEX front-running and performance issues. The 0x team has a good description of a few they are exploring. One class of approaches involves a trader placing collateral into a smart contract without publicly revealing the specifics of their intent. 0x proposes a "Commit Reveal" system where a hidden commitment to trade is made along with a deposit which is lost if the trade is not followed through (settled). The exchange smart contract could then only allow for takers that follow this pre-commitment process. Since the specific order being matched against is hidden (through encryption), and only revealed after the commitment is mined (the taker sends another transaction which has the full information of the trade along with a secret that proves they made the commitment), outside observers and relayers can't front-run the taker's intention. Nevertheless, this doesn't prevent multiple takers from trying to execute against the maker, nor does it alleviate the lack of price-time priority inherent to interacting with smart contracts on a distributed blockchain. This results in wasted gas fees and additional delays for trading.

Another variation relying on collateral is a system like the one proposed by altcoin.io. Specifically, see the description of their Plasma DEX. Once someone has locked up some amount of collateral, e.g. Ether, in a smart contract, you can allow them to take all sorts of actions either on-chain, in a sidechain, or a centralized off-chain system. A partially decentralized implementation of this would be something like a smart contract that locks up some amount of collateral and then have a centralized off-chain matching engine which allows for low latency trading of a variety of assets. Settlement can still occur on-chain, but doesn't have to be in real-time. As long as losses from the off-chain trading do not exceed the collateral amount, the cost of a failure to deliver can be taken out of the relevant party's deposited collateral. You can even extend this approach to trade derivatives on arbitrary underlying assets, as marketprotocol.io is working on.

Front-running and price-time priority issues can be easily solved with some centralization. For example, the 0x team proposes a design that relies on a "Trade Execution Coordinator" smart contract which signs off on every attempted match. If this is done off-chain, and perhaps shared by all 0x relayers on the network, you can use it to get the kind of timing guarantees that centralized exchanges provide. Of course, this centralization is not without its potential trust, security, and obvious regulatory issues. If you're relying an off-chain TEC, you must trust the provider to act fairly—preserving price-time priority and not acting in the advantage of any specific participant. In addition, you must take the risk of the TEC being hacked or modified in a way that makes it behave unfairly. These are the problems blockchains and decentralized consensus were designed to solve, after all.

It doesn't completely defeat the purpose of a DEX—you still get on-chain settlement and therefore more control over your crypto—but it's starting to chip away at it. This is what IDEX is doing Here's a useful comparison of a few different DEX implementations:



Attribute	IDEX	EtherDelta and 0x	Oasis
Concept	Off-chain trade matching with on-chain settlement enforced by smart contracts and arbiter	Off-chain orderbook hosting with on-chain settlement and matching determined by miners	Orderbook on the blockchain with matching determined by miners
Trustless	Yes	Yes	Yes
Trade speed	Real-time	Slow - Filling orders is limited by block time	Slowest - Placing and filling orders are both limited by block time
Orderbook update speed	Fast	Slow	Slow
Time to cancel an order	Real time	Slow - Limited by block time	Slow - Limited by block time
Automatic trade matching	Yes	No	No
Fill many orders at once	Yes	No	No
Gas cost to place limit orders	No	No	Yes
Gas cost to cancel orders	No	Yes	Yes
Gas amount per trade	High	Medium	Medium
Race conditions	No	Yes	Yes
Scaling	Moderate	No	No

Source: https://medium.com/aurora-dao/introducing-idex-61af097b48ad

More specifically, IDEX combines the TEC (Trade Execution Coordinator) model with the collateral lock-up and state channel/off-chain approach.

> *"Depositing on IDEX opens a new channel hub. Each trade is equivalent to making one transaction and then immediately closing it. IDEX verifies the transaction's authenticity and updates the off-chain state while the authorized transaction is prepared for dispatch to the Ethereum network for final judgement and processing by the IDEX contract. Traders can make as many trades as they want off-chain but cannot close the channel hub (withdraw their funds) until the Ethereum state is finalized (all pending trades have mined). This design enables real-time trading while preserving all of the transparency and security of blockchain settlement."*

> *Source: https://medium.com/aurora-dao/idex-decentralized-exchange-state-channel-afca2e5809b1*

Inevitable tradeoffs?

Could there be a decentralized mechanism which is able to ensure properties like price-time priority of matches and prevention of front-running? In theory, you could use a blockchain to solve these problems.

Either the block creation time would have to be fast enough where most of these effects are minimized, or you figure out some kind of consensus mechanism which can take into account price-time priority.

You could try to develop a protocol around reaching consensus on geosynchronized timestamps of message generation and combine that with zero-knowledge proofs (ZKP) to hide each order's intentions from the nodes verifying them. The ZKP component seems possible—it's similar to the Commit Reveal mechanism proposed by 0x—but the "Proof of Timing" seems tough. Is there a way to construct a system that can prove when it—a node in the network—received a message in a tamper-proof way?

Another potential solution to front-running, and also enabling cross-chain (e.g. BTC to ETH) transactions, is the atomic swap. This is part of how altcoin.io's platform works, and as the tech becomes increasingly available (mostly blocked on level 2 tech like Lightning) it will be more widely deployed. For more, see the "Off-Chain Atomic Swaps" section in this article. In a nutshell, you create a smart contract on both chains (e.g. Bitcoin and Ethereum if the transaction is between BTC and ETH) that reference each other in a way where the counterparty can only withdraw the coin they are receiving by releasing the coin they are sending.

> *Therefore, for a trade between Alice and Bob to take place, both must submit their transaction to their respective blockchain, Alice on the Bitcoin blockchain and Bob on the Litecoin blockchain. In order for Alice to claim the 100 Litecoins sent from Bob, she must produce a number that only she knows, used to generate a cryptographic hash, therefore providing proof of payment. Similarly, in order for Bob to claim the 5 Bitcoins that was sent from Alice, he must also provide the same number, that was used to generate the cryptographic hash.*

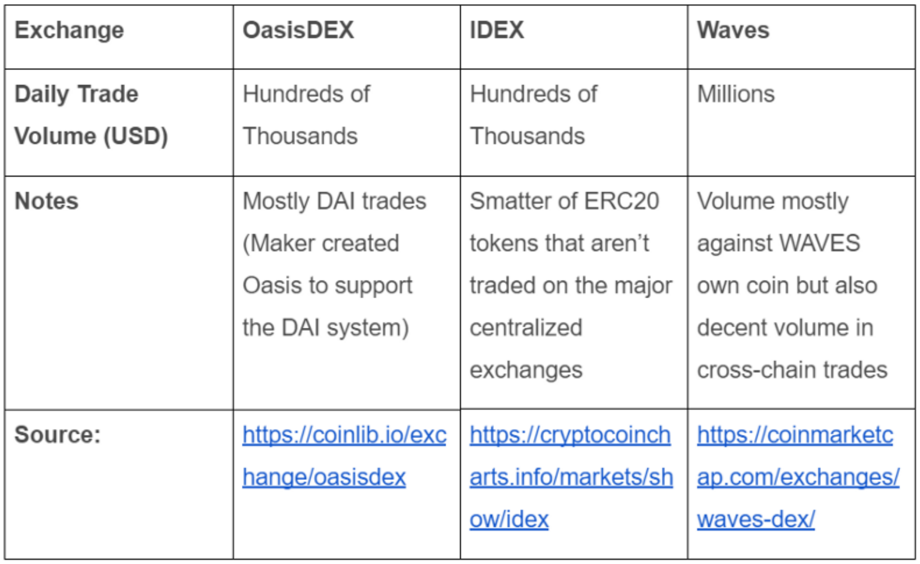
> *Source: https://www.cryptocompare.com/coins/guides/what-are-atomic-swaps/*

Atomic swaps facilitate this sort of functionality by relying on Hash Time-Locked Contracts. Effectively, if either party fails to hold up their side of the bargain within a certain period of time, the transaction “expires” and any crypto held in the contracts are returned to their respective owners.

Tough challenges ahead

How successful have DEXs been and what can we expect going forward? Volume growth has stagnated for the few 0x relayers (https://0xtracker.com/). EtherDelta seems to be running at lower volumes than it was earlier this year. Other DEXs are showing volume in the low millions with no major winners yet. This compares to USD billions in (daily) volume on centralized crypto exchanges (although much of this centralized exchange volume is likely fake. Perhaps 90% or more. This is another interesting aspect of DEXs: it’s much harder to fake activity.)

Here’s a comparison of the current state of a few players in the market:



Exchange	OasisDEX	IDEX	Waves
Daily Trade Volume (USD)	Hundreds of Thousands	Hundreds of Thousands	Millions
Notes	Mostly DAI trades (Maker created Oasis to support the DAI system)	Smatter of ERC20 tokens that aren’t traded on the major centralized exchanges	Volume mostly against WAVES own coin but also decent volume in cross-chain trades
Source:	https://coinlib.io/exchange/oasisdex	https://cryptocoincharts.info/markets/show/idex	https://coinmarketcap.com/exchanges/waves-dex/

Sources: https://coinlib.io/exchange/oasisdex, https://cryptocoincharts.info/markets/show/idex, https://coinmarketcap.com/exchanges/waves-dex/

For the most part, DEXs are being used to trade coins not listed on centralized exchanges. It seems odd to me that there isn’t more DEX trading of the high volume ERC20 tokens, e.g. TRX/ETH. On the other hand, I don't even see EOS listed on most of the DEXs (written while it was still trading as an ERC20 token). It's available on EtherDelta but is not especially liquid.

Is the missing factor just a few algo firms stepping up and providing liquidity in major pairs on DEXs? Currently the volumes are too low to justify the effort and risk from a profit-seeking standpoint, unless the liquidity providers are given sufficient ownership of the DEX to make it worth their while in the long run. Liquidity begets liquidity, and if the liquidity providers take the risk early on they will want the upside if the DEX takes off.

Finally, Waves seems to indicate there is demand for cross-chain trading. The success of ShapeShift validates this model as well, just need good UX. This will become far more common when atomic swaps are available for the main coins, likely later this year. Waves does it by having users of their DEX use their own multicoin wallet.

If the long-run interest in DEXs continues to be for trading coins that aren't available on centralized exchanges, the future is bleak. Anyone taking a sober look at the ICO landscape is likely to admit that the majority of offerings are little more than scams. The remaining projects may be legitimate and interesting but issue tokens that appear to be worthless (e.g. ZRX), or at best are extremely overvalued as a consequence of market hype. When the most clearly useful, and thereby valuable, tokens being traded are for discounts on trading exchanges (BNB), I can't help but be reminded of how Yahoo! reaped the rewards of the 90's dotcom bubble as all the VC money was funneled towards Yahoo ads for the new, soon-to-be-defunct, startups.

Even if DEXs continue to attract volume and liquidity, they face growing threats from regulators as well as their centralized competitors. It's only a matter of time before regulators start taking action, and you can bet that DEXs will be subject to FinCEN (KYC/AML) requirements at a minimum, and likely more elaborate registrations once the U.S. regulatory environment is clarified—perhaps even broker/dealer and ATS requirements. The savvy DEX players are thinking about this already. What this would mean for DApps and smart contracts interacting with the markets remains to be seen—it could become a full-on black market.

Some DEX providers seem to plan to argue that they are just publishing open source code and are not proprietors. As a result, they would not be subject to KYC/AML or other regulations. The lawyers I've spoken with don't seem to think this will hold up and that if there is a major loss of some sort, regulators (or civil suits) will target any and all related parties.

Finally, consider the possibility that centralized exchanges are able to solve enough of their security problems where the security/custody value proposition of DEXs becomes less impressive. More comprehensive custody solutions are in the pipeline from all major exchanges. This could alleviate most of the concerns keeping institutions and some individuals off of centralized exchanges. One of the benefits of DEXs—managing your own keys—is viewed as a cost to many market participants. Managing your own keys comes with risk and cost—ideally you can offload that to someone else and have it insured or safe enough where the risk is negligible. If most of the trading volume going forward is going to be done by institutional players rather than retail investors, it seems unlikely that institutions will want to manage their own private keys and are much more likely to outsource custody.

Closing thoughts

Decentralized exchanges are an example of a new type of trading technology facilitated by blockchains. While many players have entered the space, there is yet to be a clear winner—someone who builds a substantially successful business rather than just raising a bunch of money, at least. The challenges to improved usability are significant but perhaps surmountable. Just as with centralized exchanges, one of the big unknowns is how regulators will act. Especially with DEXs, this could make or break the space.

Please share your thoughts about DEX technology and their future!

See the follow-up post: Decentralized Exchanges—FinCEN, Payment Channels, and Custody, Oh My!

Thanks to Taylor Pearson for helping discuss and edit this piece