Gary Basin Follow
Digging into crypto. Ran an algo trading firm.
Jul 4 · 7 min read

Decentralized Exchanges — FinCEN, Payment Channels, and Custody, Oh My!

Building off my previous look into Decentralized Exchanges (DEXs), I want to dig deeper into regulatory and practical issues surrounding DEXs. There are a few questions I'm interested in answering, and my best naive guess at the answers now are not too encouraging. For one:

> ***Q. Can DEXs avoid FinCEN oversight (KYC/AML)?***

> ***A. As most of them are currently designed, possibly not.***

This section is largely about a legal question and given that I'm not an attorney you probably want to take this with a grain of salt.

One of the main touted benefits of DEXs is the ability to trade anonymously and without reliance on a third party. Unfortunately, the powers that be are strongly opposed to anonymous financial transactions. This is old news to anyone in crypto and the assumption has been that DEXs avoid this problem since there's "no one in charge". In practice, it seems like there typically is someone in charge, or at least with the capacity to shut the thing down.

Chris over at Decentralized Legal has an excellent post on this topic and I will borrow heavily from it. The first relevant question is whether tokens even count as "money" and therefore fall under money laundering surveillance infrastructure. This is a resounding yes, as clarified by FinCEN in March 2013 (emphasis mine):

> *A "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency.*

> *A "convertible virtual currency" ("CVC") is defined as virtual currency that either has an equivalent value in real currency or acts as a substitute for real currency.*[3]

> *Exchangers of CVCs subject to MSB regulation and money transmission registration are those* ***"person[s] engaged as a*** **business** ***in the exchange of virtual currency for real currency, funds, or other virtual currency."***[6] *Further, any "exchanger that (1) accepts* and *transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations."*[7]

Whether a given DEX can be classified as being engaged in the *business* of exchange, or whether it accepts and transmits crypto, becomes the critical question. What are some factors that may indicate that a DEX is in the business of exchange or is accepting and transmitting crypto? Some guesses, in ascending order of severity:

- Advertising yourself as an exchange (see: Ripple)
- Accepting deposits, holding custody of customer funds (including in a smart contract!)
- Serving as a middleman between buyers and sellers of crypto (a "dealer")
- Collecting transaction fees in order to turn a profit (i.e. running a business that profits from the trading on your platform)

These seem pretty extensive. Even worse, consider LocalBitcoins.com. LocalBitcoins functions as an offline DEX by matching crypto-to-fiat traders looking to transact in person (often with cash). Using the criteria above, you'd think it would be in the clear (their fee model charges for advertising). And yet, they have started to require KYC for larger traders on their platform. This is likely in response to enforcement actions carried out against individuals running money service businesses *through* LocalBitcoins. This latter point is key: **to the extent a given platform will evade FinCEN oversight, that doesn't exempt**

participants in the *business of trading* from having to perform KYC on their counterparties! Best case scenario, you will end up with a DEX devoid of professional liquidity providers—good luck getting much trading done that way.

How do current players in the DEX space look given this framework? As you might imagine, it's not encouraging.

Bisq is a variation on LocalBitcoins, except charging transaction fees. It seems very unlikely that they, and any major participants on their platform, won't fall under FinCEN scrutiny.

OasisDEX, the fully on-chain Ethereum DEX for DAI trading (run by Maker), and its Oasis.Direct DApp, charges no fees other than for gas and is non-custodial. It seems like they may be able to avoid scrutiny, although this won't apply to large traders on the platform.

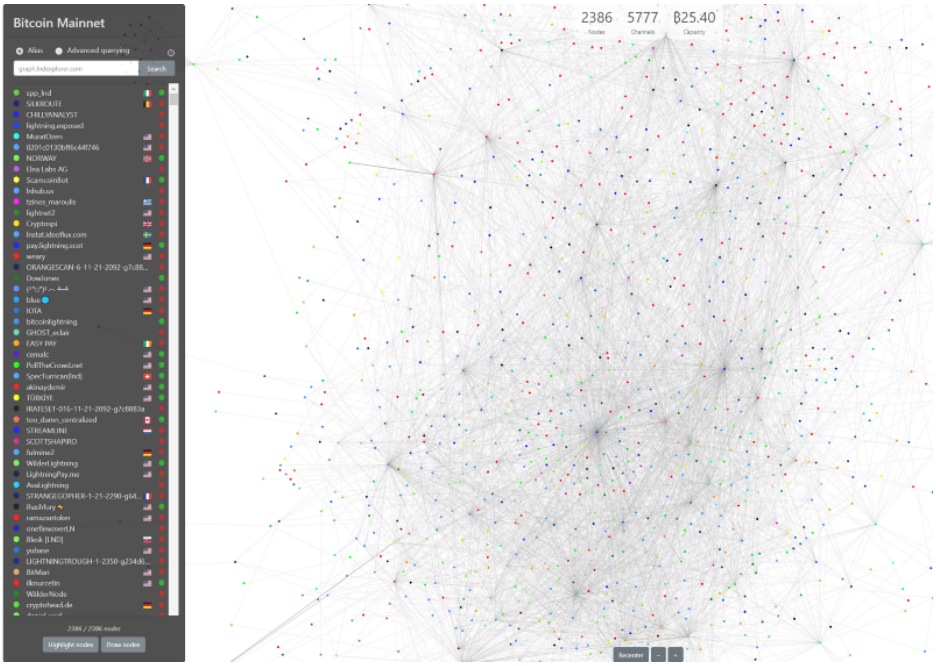
Decred has proposed creating a DEX that doesn't charge transaction fees, among other tweaks on the standard approaches. Avoiding transaction fees will help their case of not operating as a money service business. In addition, by keeping all orders on-chain they are avoiding the trap of running everything through a smart contract which would effectively be holding custody and serving as a middleman, of sorts. The latter is an approach being adopted by many DEXs (e.g. altcoin.io) in order to keep everything on-chain but achieve low latency functionality. It seems plausible that FinCEN will view these as money service businesses. Potentially this could be avoided if the sidechain component is sufficiently decentralized—I have to see any that have a plausible plan for achieving this in practice. Given the centralized smart contract which acts as the anchor onto the main chain, however, I also wouldn't be surprised if these fell under securities trading laws (to the extent they are enabling trading of securities).

Prediction: any DEXs still operational a few years from now that aren't doing KYC will be fully decentralized and very expensive to trade in—wide bid/ask spreads (low liquidity) and not much volume. They will be limited to people doing small infrequent transactions and hard to operate in for those in the business of providing liquidity.

> ***Q. How close are we to practically functional DEXs that are fully decentralized on-chain and could attract significant liquidity?***

> ***A. Likely years. We will need fully decentralized and scalable low latency layer 2 solutions.***

What happens when you try to keep everything on-chain and rely on atomic swaps for cross-chain trading, like with Decred's proposed approach? Currently, a core limitation of atomic swaps is their performance—they will require confirmations on both chains before a transaction has been safely cleared. Waiting several hours for a transaction to settle isn't unusual with BTC and that is a significant impediment for liquidity providers.



BTC Lightning network graph from https://graph.lndexplorer.com/

A proposed solution is the use of layer 2 state channels or sidechains, specifically to create lower latency payment channels like Lightning (for Bitcoin) and Raiden (for Ethereum). These layer 2 solutions allow for much faster and cheaper transfers but this comes with a few caveats. Principally, the transaction only happens quickly and cheaply from the

perspective of the payment network. e.g. as long as your recipient is on Lightning, they can quickly acknowledge your BTC transfer to them. This shouldn't be a major hurdle since presumably all major exchanges will want to run wallets for deposit/withdrawal on these payment networks, but this brings up another issue: limited capacity to send large amounts. Because of the mesh network design of these systems, it is likely that they won't be capable of sending relatively large amounts, like 10 BTC, any time soon. **This will substantially diminish their utility from the perspective of arbitrageurs and algorithmic liquidity providers**, without whom any given market (including DEXs) will suffer from liquidity problems.

> ***Q. Are DEXs significantly more secure than centralized exchanges will be with better custody solutions?***

> ***A. Hard to justify at this point, especially while they continue to rely on web browsers to connect wallets to the market.***

Anonymity is going to be hard to come by due to FinCEN oversight, and scalability/performance issues will continue to be a constraint for the foreseeable future, but perhaps DEXs win out due to better security? This seems increasingly implausible. To begin with, **the benefits of managing your own private keys quickly evaporate when in practice that means connecting to a DEX via some Chrome plug-in in order to make trades.** Every time you expose your wallet to the internet, you are at risk. As an active trader on a DEX, this is a huge problem. Granted, hardware wallet integrations are becoming increasingly common and alleviate some of these issues.

Nevertheless, I'd rather take my chances with a reputable centralized exchange like Coinbase—at least they have a giant team constantly improving their wallet security as well as an insurance policy on their hot wallet. Don't take this as an endorsement for Coinbase—I am agnostic—but **there are definite benefits to having a system battle tested with constant use and a critical mass of engineers working to harden it in the service of a brand's reputation.** Finally, most institutional participants, at least in the US, will be *required* to use a qualified third-party custodian. If you're giving up control of your private keys anyway, you will be less concerned over trading on a centralized exchange… especially when your custodian is owned or affiliated with the exchange.

To conclude, it seems at least for the foreseeable future DEXs will not play a significant role in the crypto trading ecosystem. Most existing and proposed designs will fall under FinCEN (AML/KYC) scrutiny, at a minimum, and likely more serious securities regulator oversight given the tendency of DEXs to trade random tokens—I believe the term of art is "shitcoins"—which will likely be classified as securities in the future. To try to avoid some of this oversight, DEXs could try to push for fully decentralized on-chain models, but due to high latency or low capacity these won't be very functional from a technological standpoint anytime soon (if ever). This will keep liquidity providers at a distance, thereby dooming these DEXs to low liquidity and being effectively useless for anything but very small trades. See OasisDEX's order books and volumes for what you can expect.

What role can we expect DEXs to play in a future crypto trading landscape? I can imagine some variation of the Bisq model—facilitating p2p crypto-to-fiat exchanges at small scale—being sustainable and useful. I suspect the battle for one of crypto's main appeals—anonymity—to be a struggle, however. I have a hunch that governments will gradually embrace cryptocurrencies but only ones that don't preserve anonymity—all transactions will need to be traceable to individual identities. More on this in a future post…