DECONSTRUCTING DECENTRALIZED EXCHANGES

Lindsay X. Lin*

INTRODUCTION

Decentralized exchanges are becoming a critical tool for purchasing and selling an increasing percentage of cryptocurrencies. The term "decentralized exchange" generally refers to distributed ledger protocols and applications that enable users to transact cryptocurrencies without the need to trust a centralized entity to be an intermediary for the trade or a custodian for their cryptocurrencies.

Decentralized exchanges provide a number of important benefits, including (1) lower counterparty risk (i.e., no need to trust a centralized exchange to secure and manage private keys),[1] (2) the potential for lower transaction fees, and (3) a more diverse array of trading pairs that can unlock access to riskier or less liquid cryptocurrencies.[2] As demand for these features increases, decentralized exchange technology may witness tremendous growth in usage, development, and adoption within the next couple of years.

Additionally, decentralized exchange usage is being fueled by concurrent regulatory and industry trends, including (1) a surge in the quantity of distinct cryptocurrencies that makes comprehensive listing impractical,[3] (2) regulatory risks of listing cryptocurrencies on centralized

* Lindsay Lin is Legal Counsel at Interstellar and Stellar Development Foundation. This writing is not legal advice and is unaffiliated with Interstellar and Stellar Development Foundation.

[1] Centralized exchanges have a history of significant security breaches, with many incidents resulting in tens or hundreds of millions of USD value of cryptocurrency stolen. *See* Julia Magas, *Crypto Exchange Hacks in Review: Proactive Steps and Expert Advice*, COINTELEGRAPH (Aug. 31, 2018), https://cointelegraph.com/news/crypto-exchange-hacks-in-review-proactive-steps-and-expert-advice.

[2] To learn more about the various benefits of decentralized exchanges, *see* Fred Ehrsam, *Why Decentralized Exchange Protocols Matter*, MEDIUM (Sept. 27, 2017), https://medium.com/@FEhrsam/why-decentralized-exchange-protocols-matter-58fb5e08b320.

[3] CoinMarketCap.com, a website that lists almost all centralized and decentralized exchange traded cryptocurrencies, displays over 1926 cryptocurrencies. Comparatively, Bittrex, the U.S. exchange with the greatest quantity of listed cryptocurrencies, lists only 207 unique

exchanges,[4] and (3) users' desire to avoid centralized exchanges' Know-Your-Customer requirements for more private and less censorable transactions.[5]

Decentralized exchanges can differ dramatically in terms of technology, trustlessness, security, legal implications, economic implications, and more. These differences render some exchanges more or less suitable for specific use cases. The goal of this Essay is to explain the architectural structure of decentralized exchanges, and the performance and security tradeoffs associated with various architectural choices. By understanding these technical differences, the reader will have a better grasp of which decentralized exchanges are optimized for which use cases.

ARCHITECTURE OF A DECENTRALIZED EXCHANGE

The term "decentralized exchange" is used colloquially to describe both blockchain-based exchange protocols, as well as applications that leverage the protocols. A decentralized exchange protocol generally describes a software program, hosted on or integrated into one or more distributed ledgers (e.g., Ethereum), that enables peer-to-peer transactions that are automatically settled on the distributed ledger.[6] Users retain sole custody of their private keys throughout the transaction process.

A decentralized exchange application builds on top of a decentralized exchange protocol, and adds an on-chain or off-chain order book database

cryptocurrencies, and Coinbase Pro only has five. *See Frequently Asked Questions*, COINMARKETCAP, https://coinmarketcap.com/faq (last visited Sept. 8, 2018); *Bitcoin Markets*, BITTREX, https://bittrex.com/home/markets (last visited Sept. 8, 2018); COINBASE PRO, https://pro.coinbase.com (last visited Sept. 8, 2018).

[4] *See* SECURITIES & EXCHANGE COMM'N DIVISIONS OF ENFORCEMENT AND TRADING AND MARKETS, STATEMENT ON POTENTIALLY UNLAWFUL ONLINE PLATFORMS FOR TRADING DIGITAL ASSETS (Mar. 7, 2018), *available at* https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading ("If a platform offers trading of digital assets that are securities and operates as an 'exchange,' as defined by the federal securities laws, then the platform must register with the SEC as a national securities exchange or be exempt from registration.").

[5] *See, e.g., Crypto Exchange ShapeShift Sees Criticism for Mandating Memberships with KYC Norms*, CCN (Sept. 7, 2018), https://www.ccn.com/crypto-exchange-shapeshift-sees-criticism-for-mandating-memberships-with-kyc-norms.

[6] In this paper, the terms "distributed ledger" and "blockchain" are used interchangeably for most instances. A distributed ledger describes a ledger (or another data structure) that is replicated and hosted among numerous independent parties wherein any changes to the ledger must be confirmed based on a consensus mechanism. A "blockchain" is a type of distributed ledger that relies on the mining of blocks. The Ethereum and Bitcoin networks have blockchains: they rely on miners to produce a series of blocks containing transaction data in order to confirm changes to the ledger. In contrast, the Stellar protocol does not involve the mining of blocks, and thus is better described as a distributed ledger protocol than as a blockchain protocol.

and a graphic user interface (GUI) and/or APIs so that the information is easily accessible.

Overall, a decentralized exchange application can be broken down into the following components:

1. The blockchain platform & technical implementation
2. The counterparty discovery mechanism
3. The order matching algorithm
4. The transaction settlement protocol

A decentralized exchange application may not be fully decentralized in all four components. Note that for many decentralized exchange applications, one or more components may be off-chain/centralized, or otherwise feature economic incentives which would promote a tendency towards centralization.

We will discuss each of these components and provide examples of how some decentralized exchange protocols implement these components.

1. Platform & Technical Compatibility

Most decentralized exchange protocols generally operate with tokens that feature the same technical implementation and are on the same distributed ledger platform. For example, AirSwap,[7] EtherDelta,[8] and 0x[9] are independent protocols that are operable only with standardized ERC-20 tokens on the Ethereum blockchain. Beyond Ethereum, Stellar's decentralized exchange is operable with tokens issued on the Stellar network,[10] and BitShares' OpenLedger DEX is operable only with tokens issued on the BitShares blockchain platform.[11] Off-chain cryptocurrencies and assets could also be traded through the Stellar decentralized exchange or OpenLedger DEX if an "anchor" issues tokens onto the network that represent ownership of a defined unit of the off-chain cryptocurrency.[12] However, this requires users to trust that the anchor has sufficient reserves of the off-chain cryptocurrency to satisfy all redemptions of the tokens.

[7] AIRSWAP, https://www.airswap.io (last visited Sept. 8, 2018).

[8] ETHERDELTA, https://www.etherdelta.com (last visited Sept. 8, 2018).

[9] 0X, https://0xproject.com (last visited Sept. 8, 2018).

[10] *Distributed Exchange*, STELLAR, https://www.stellar.org/developers/guides/concepts/exchange.html (last visited Sept. 8, 2018).

[11] OPENLEDGER, https://openledger.io (last visited Sept. 8, 2018).

[12] *See Anchors, trust, and credit*, STELLAR, https://www.stellar.org/how-it-works/stellar-basics/explainers/#Anchors_trust_and_credit (last visited Sept. 8, 2018).

A few decentralized exchanges are beginning to use atomic swaps to enable users to atomically[13] trade cryptocurrencies that exist on different blockchain networks (e.g. exchanging Bitcoin for Dogecoin, cryptocurrencies from separate blockchains). However, atomic swaps still require that the transacted cryptocurrencies adhere to certain common technical standards. For example, in BarterDEX, a cross-chain decentralized exchange that enables users to transact cryptocurrencies from different blockchains, atomic swaps are only available for cryptocurrencies from blockchains that have implemented features that mirror the Bitcoin reference implementation, such as BIP65 (Check LockTime Verify) and other standard Bitcoin API methods.[14] In practicality, this means that cryptocurrencies that were built off the Bitcoin reference implementation, such as Litecoin and Dogecoin, or cryptocurrencies that forked from Bitcoin, such as Bitcoin Cash and Bitcoin Gold, will be the easiest to make compatible for atomic swaps with Bitcoin.

Cross-chain swap technologies like PolkaDot[15] and Cosmos[16] are also building tools and protocols that could eventually be integrated into decentralized exchange applications that can atomically swap tokens from different blockchains. However, given the current latency of most cross-chain atomic swaps (with transaction confirmations dependent on the confirmation times of both cryptocurrencies' underlying blockchains), most popular decentralized exchange applications currently focus exclusively on token trading within one chain. As PolkaDot, Cosmos, and other interchain swap tools and protocols are refined and developed in conjunction with Lightning,[17] Raiden,[18] and other transaction performance-enhancing upgrades, some day users may enjoy liquid and low latency cross-chain decentralized exchanges.

[13] The traditional challenge of trading across different blockchains is that a user would need to trust her counterparty: once user sends Blockchain A Crypto to the counterparty's address on Blockchain A, she would need to trust the counterparty to send Blockchain B Crypto to her address on Blockchain B. A centralized party could help intermediate these transactions, but in the decentralized exchange landscape, the most trustless solution would be an atomic swap. An "atomic" transaction is a type of transaction with a binary outcome that either (1) all operations in the transaction are fully executed, or (2) no part of the transaction is executed. In the context of two parties transacting cryptocurrencies across different blockchains, an atomic transaction ensures that either all necessary operations in the transaction are settled in both blockchains, or that no operations are settled in either blockchain. This reduces the risk that one party sends Blockchain A Crypto to the other party, but never receives Blockchain B Crypto in return.

[14] *See Frequently Asked Questions — BarterDEX 0.1a2 documentation*, BARTERDEX, https://barterdex.readthedocs.io/en/latest/faq.html (last visited Sept. 8, 2018).

[15] POLKADOT, https://polkadot.network (last visited Sept. 8, 2018).

[16] COSMOS, https://cosmos.network (last visited Sept. 8, 2018).

[17] LIGHTNING NETWORK, https://lightning.network (last visited Sept. 8, 2018).

[18] RAIDEN NETWORK, https://raiden.network (last visited Sept. 8, 2018).

2. Counterparty Discovery Mechanisms

Counterparty discovery mechanisms enable buyers to discover sellers who are willing to execute transactions on mutually acceptable terms. On traditional cryptocurrency exchanges such as Binance, Bittrex, and Kraken, users have the option of submitting both market orders and limit orders, and these orders are automatically matched with unidentified counterparties using the exchange's central limit order book which aggregates all user orders.

Most decentralized exchanges also have order books. These order books may exist on-chain, hosted on a distributed ledger, or off-chain, hosted by third parties. Most decentralized order books display the separate orders of each counterparty, rather than the aggregated orders of all counterparties. Users normally will need to identify a particular order, and thus a particular counterparty, in order to trade.

Some decentralized exchanges do not have order books and instead feature a reserve-based model. A reserve provides a supply and demand of various tokens that are readily available to be executed based on the reserve's quoted buy and sell prices for that token. These reserves are created by on-chain smart contracts that enforce the trade execution and settlement process. The trade price may also be programmatically determined by a smart contract.

For the rest of this Essay, the term "Maker" will refer to the party that provides an order, and the term "Taker" will refer to the party that fills it.

On-chain order book

On-chain order books are hosted directly on the distributed ledger: all orders are submitted to the distributed ledger network and are confirmed by the network. Anyone can host and access a copy of the order book, and anyone may submit their own orders to be included in the order book as long as the distributed ledger is public.

Examples of on-chain order books include the Bitshares and Stellar decentralized exchanges. In the Stellar network, users submit orders which are hosted on a persistent and public on-chain order book in the Stellar distributed ledger. Information about this order book is broadcast to all Stellar validator nodes and is viewable by the public. When two orders intersect in price, the trade is automatically executed and settled by the

Stellar network.[19] The BitShares decentralized exchange operates under a similar model, but for the BitShares blockchain and network.[20]

Benefits:

a. **Less censorable:** There is lower reliance on a centralized party to host and operate the order book. There may be a centralized GUI for the order book, but any independent party would be able to create separate GUIs and populate it with the on-chain data.[21] Assuming that hosting and operating of the order book is distributed across independent, non-colluding validator nodes, there is no centralized point of attack, compromise, or liability that would result in the order book being shut down or specific orders being restricted by a centralized party.[22]

b. **Less trust required:** Decentralized, on-chain order book hosting means that one does not need to trust centralized, off-chain actors to accurately and reliably publish or broadcast order books.

Trade-offs:

a. **Order book inherits performance, cost, and security characteristics of the underlying blockchain:** The speed and cost of submitting or removing an offer on an on-chain order book are limited by of the speed and cost of interacting with the underlying blockchain. Users must pay for each order book update on the network, wait for the network to reach consensus on their updates,

[19] *Distributed Exchange*, *supra* note 10.

[20] *See Decentralized Exchange*, BITSHARES, http://docs.bitshares.org/bitshares/user/dex.html (last visited Oct. 22, 2018).

[21] For example, StellarX, Stellarport, and StellarTerm are all user interfaces that display and interact with the same Stellar network on-chain order book. *See* STELLARX, https://www.stellarx.com (last visited Sept. 8, 2018); STELLARTERM, https://stellarterm.com (last visited Sept. 6, 2018); STELLARPORT, https://stellarport.io (last visited Sept. 8, 2018).

[22] In contrast to off-chain order books, on-chain order books have no central entity operating it, meaning that it may be difficult for a user, regulatory agency, or governmental body to assign legal and regulatory liability and carry out enforcement actions. Given the diffusion of liability across the network, and difficulty of taking down the order book, on-chain order books may be less prone to government censorship. However, on-chain order books do still carry some government censorship risk. A centralized party, e.g. a government, could order those it governs to cease transactions with cryptocurrency addresses that are linked to prohibited parties. In fact, the OFAC sanctions list has expanded to include cryptocurrency addresses. *See* Andrew E. Bigart, Christopher L. Boone & D. E. (Ed) Wilson, Jr., *Cryptocurrency Addresses on OFAC Sanctions List*, VENABLE (Mar. 27, 2018), https://www.lexology.com/library/detail.aspx?g=c09a5983-f72f-46b9-84a3-b8997e5f013f. Therefore, if an order book permits you to see the public address of the counterparty, some parties may be restricted from taking certain orders. Additionally, miners and validators could choose (or be forced) to ignore transactions submitted from certain addresses, essentially censoring those transactions.

and then wait for secure confirmation of the updates. If the blockchain is compromised by an attack,[23] the order book may be compromised. Therefore, slower and higher fee blockchains are less favorable for hosting a user-friendly on-chain order book.

b. **Slower updates:** In the absence of second-layer technologies like the Lightning Network or Raiden Network, on-chain order books are generally updated based on the information contained in the latest block or ledger. This creates latency which could range from minutes to seconds depending on the platform. In contrast, off-chain order books can support almost-instantaneous updates given that most only need to alter a centralized database to reflect the update.

c. **Stale orders:** On-chain decentralized exchanges generally support resting orders, where the desired price and quantity have been fixed by the Maker upon creation of an offer. In a resting order, the offer must be proactively canceled by the Maker if she no longer wishes to trade on those terms if, for example, the price has changed dramatically. Since updates to on-chain order books can have delays due to the speed of transaction validations of the underlying network, on-chain order books could create an environment where resting orders are exploited when there is high price volatility. However, as usage of on-chain order books grows, we expect to see growth and adoption of trading tools (such as trading bots[24]) to help users programmatically automate the submission and cancellation of order upon market price changes.

Off-chain order books

Off-chain order books are order books that are hosted by a centralized entity outside of a distributed ledger. The centralized entity helps parties discover other parties who make offers on the asset and can restrict access to view or submit to the order book.

The practicality of using an on-chain or off-chain order book depends significantly on the performance of the chain. Decentralized exchanges normally do not employ on-chain order books given that every order and adjustment to an on-chain order book would require an update to the blockchain, thereby incurring transaction fees and wait time. On certain chains, transaction fees are negligible and wait times are on the order of

[23] For example, in proof of work blockchains, by a 51% attack.

[24] For example, Kelp is a trading bot that enables users to create sophisticated trading logic to interface with the Stellar decentralized exchange. *See* KELP, https://kelpbot.io (last visited Sept. 16, 2018).

seconds. Under these circumstances, an on-chain order book is practical to use for moderate volumes of intermittent orders. Comparatively, on the Ethereum blockchain, transaction fees are non-negligible and wait times are on the order of minutes.[25] Using an Ethereum on-chain order book would likely incur expensive transaction fees and debilitating wait times. For this reason, four of the most prominent decentralized exchanges in Ethereum—0x, AirSwap, EtherDelta, and IDEX—employ off-chain order books. As of October 2018, 0x, AirSwap, EtherDelta, and IDEX support ERC-20 tokens.

● In the 0x ecosystem, entities called "Relayers" host, manage, and publish off-chain order books. Makers will submit buy and sell orders directly to a Relayer, and the Relayer will aggregate all received orders into its order book. Takers discover Makers' orders by querying the Relayer's order books. Upon finding a suitable order, a Taker will fill the order by submitting information pursuant to the 0x protocol to the 0x exchange contract on the Ethereum blockchain. Given that all Relayers use the 0x protocol for settlement, a Relayer may choose to share its order books with other Relayers, thereby unlocking thicker order books and greater liquidity.[26]

● On the AirSwap platform, a Maker will submit an "intent to trade" in a certain trading pair to an entity called the "Indexer." The Indexer will aggregate information about the Makers and their intents to trade. Takers who wish to trade in a certain trading pair will query the Indexer to discover the identities of suitable Makers, using the Indexer as a counterparty discovery mechanism. Once a Taker finds a suitable Maker, they will negotiate off-chain on the terms of the trade, potentially using the input of an off-chain "Oracle" that will suggest fair pricing for the trade. Once the Maker responds with an order that is satisfactory to the Taker, the Taker will submit the order to the Ethereum blockchain.[27]

[25] As of 11:37 PM PST on October 20, 2018, the median wait time for a transaction to be included in a block on the Ethereum blockchain was 31 seconds, and the standard cost per transaction was approximately $0.02 USD, per https://ethgasstation.info. To ensure that the transaction is irreversible, many merchants require at least 10 additional blocks to be mined after the block containing the transaction. Thus, the total "safe" confirmation time would be the time it takes for a transaction to be included in a block plus the amount of time taken to mine 10 additional blocks. As of 11:45 PM PST on October 20, 2018, the total time was approximately 3 minutes. *See* https://etherscan.io/blocks to view when the previous 10 blocks were mined.

[26] Will Warren & Amir Bandeali, *0x: An open protocol for decentralized exchange on the Ethereum blockchain* (Feb. 21, 2017), *available at* https://0xproject.com/pdfs/0x_white_paper.pdf.

[27] Michael Over & Don Mosites, *Swap: A Peer-to-Peer Protocol for Trading Ethereum Tokens* (May 10, 2017), *available at* https://swap.tech/whitepaper.

● On the EtherDelta web application, in order to make or fulfill an order, Makers and Takers will deposit tokens from their Ethereum wallet into EtherDelta's on-chain smart contract. Makers will submit orders to be publicly broadcast on the EtherDelta off-chain order book, and the order book will ping the blockchain to verify that the Maker has sufficient balance deposited in the smart contract to fulfill the order. Takers will then select an order and click "Buy" on the web application, causing the EtherDelta smart contract to perform the trade.

● On the IDEX web application, in order to make or fulfill an order, users will deposit tokens from their Ethereum wallet into an IDEX smart contract. Users then use the IDEX application interface to place buy and sell orders on an off-chain order book. IDEX and EtherDelta have similar structures in that they both integrate an off-chain order book with an on-chain smart contract for settlement, but IDEX adds on a "transaction processing arbiter" that helps to manage the order of pending trades so that trades are confirmed in the correct order. Therefore, as users trade, the IDEX application interface will update their displayed balances in real-time, but the on-chain settlement may occur with a delay given that transactions are queued. By controlling the order of transactions, IDEX separates trade execution from trade settlement, facilitating a smoother user experience.[28]

There are both benefits and tradeoffs to having an off-chain order book.

Benefits:

- **Performance improvements:** Off-chain order books are better able to accommodate quick order turnover. Instead of waiting for a block to be mined and confirmed (or, alternatively, a ledger to be updated) to update the order book, off-chain services can update ledgers almost instantaneously.
- **Cost improvements:** There is no need to pay a transaction fee in order to submit or update an order.
- **Fewer blockchain-originated risks to the order book:** Given that the order books are hosted off-chain, the order books would not be vulnerable to blockchain-originated vulnerabilities such as 51% attacks (where users may reverse transactions) and front-running (where users may submit higher transaction fees for their offers to be included or updated faster than others').
- **Compatible with all ERC-20 tokens:** Any token that has the

[28] *See Guides*, IDEX, https://idex.market/guides (last visited Oct. 22, 2018).

ERC-20 technical implementation can be traded on these decentralized exchange protocols. The token does not necessarily need to be approved, audited, or reviewed by anyone to be traded.

Trade-offs:

- **Higher degree of trust required:** Users must rely on the hosts of the off-chain order book to properly broadcast orders. These hosts could fail to accurately display and update orders, such that users would not be able to rely on them to discover counterparties. In the worst case scenario, these hosts could choose to arbitrarily censor valid orders or manipulate markets by strategically displaying inaccurate or outdated orders. Additionally, hackers could change the off-chain order book interface to manipulate users into sending cryptocurrency to the hackers' cryptocurrency accounts.[29]
- **Greater restrictions:** As a centralized entity, the operator of the off-chain order book may be subject to greater legal and regulatory requirements, such as the implementation of Know-Your-Customer requirements, obtainment of requisite authorizations and licenses needed to trade cryptocurrencies classified as securities, and the implementation of rules and policies against market manipulation.[30] While these requirements are helpful in preventing unlawful and abusive uses of the order book, these requirements may raise concerns about transaction privacy, open accessibility, and user experience.
- **Inaccurate order books:** Given that there is a mismatch in timing between a Maker's submission of an order and a Taker's fulfillment of an order, any given order displayed on an off-chain order book may be outdated by the time that the Taker wishes to fill

[29] *See* Stan Schroeder, *Cryptocurrency exchange EtherDelta got replaced with a fake site that steals your money*, MASHABLE (Dec. 21, 2017), https://mashable.com/2017/12/21/etherdelta-hacked/#5MF0H2RevqqP.

[30] For example, IDEX has announced that it has begun blocking IP addresses from certain jurisdictions and will implement know-your-customer and anti-money-laundering checks, stating that "[d]ecentralization exists on a spectrum, and unless your system or application lacks any centralized parts it can be subject to regulation." Alex Wearn, *Pragmatic Decentralization: How IDEX Will Approach Industry Regulations*, MEDIUM (Nov. 1, 2018), https://medium.com/aurora-dao/pragmatic-decentralization-how-idex-will-approach-industry-regulations-8b109212128a. Additionally, the SEC has charged the founder of EtherDelta with operating an unregistered securities exchange, claiming that "EtherDelta operated as a market place for bringing together the orders of multiple buyers and sellers in tokens that included securities as defined by Section 3(a)(10) of the [Securities Exchange Act of 1934]." *Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21(c) of the Securities Exchange Act of 1934: In the Matter of Zachary Coburn*, Release No. 84553 (Nov. 8, 2018), available at https://www.sec.gov/litigation/admin/2018/34-84553.pdf.

the order. For example, the Maker may already have withdrawn the tokens that she wanted to trade, yet her order is still posted on a Relayer. Therefore, the Taker may attempt to fill an order by submitting a transaction to the blockchain, only to realize that the order is no longer valid. This could delay the Taker and consume significant amounts of transaction fees.[31]

No (or hidden) order book: liquidity reserves

To solve the issue of low liquidity, some decentralized exchange protocols, such as KyberNetwork, Bancor, and Omega One build up and/or leverage liquidity reserves that are readily accessible when users wish to exchange tokens. The performance of these models depends on reserve depth/breadth and accurate pricing.

● In KyberNetwork, "Reserve Contributors" contribute tokens to build up "Reserves" of a variety of tokens. Each Reserve has a conversion rate for each trading pair, managed dynamically by a Reserve Manager. If a user wants to exchange token A for token B, she will send tokens to the KyberNetwork smart contract and the KyberNetwork will find her the most favorable rate, as determined by Reserve Managers. If such rate meets the user's pre-defined minimum requirements, the smart contract will send the corresponding amount of token B to the sender's pre-specified address. The user can view and approve the worst-case rate prior to sending any tokens.[32]

● In Bancor, users can exchange tokens for other tokens through smart contracts called "Smart Tokens," which store reserves of ERC-20-compliant tokens and ether. To illustrate, users who wish to exchange token A for token B would need to find a Smart Token contract holding both tokens in reserve (i.e., Smart_Token_AB). The user would send token A to Smart_Token_AB, thereby buying some number of Smart_Token_AB tokens based on token A's formulaic price. Next, the user would send the Smart_Token_AB tokens to its smart contract, thereby destroying those tokens and pulling out a number of B token based on token B's formulaic price. Prices are

[31] This occurrence is called "maker griefing." To learn more, see Iddo Bentov, Lorenz Breidenbach, Phil Daian, Ari Juels, Yunqi Li, & Xueyuan Zhao, *The Cost of Decentralization in 0x and EtherDelta*, HACKING DISTRIBUTED (Aug. 13, 2017), http://hackingdistributed.com/2017/08/13/cost-of-decent.

[32] *See Smart Contract Architecture*, KYBER NETWORK (Oct. 22, 2018), https://developer.kyber.network/docs/ArchitectureOverview/#high-level-overview.

programmatically determined through a formula that factors in the reserve supply of each token plus a constant reserve ratio.[33]

● Omega One aims to aggregate liquidity across cryptocurrency exchanges by treating the entire centralized and decentralized exchange landscape as a potential reserve. Users who want to trade token A for token B will deposit token A in the Omega One's on-chain smart contract and submit an order to trade token B subject to timing and pricing limits. Omega One will then use its own centralized and decentralized exchange accounts to purchase token B and trade it with the user's token A in a swap via the smart contract.[34]

Benefits:

- **Lower friction to trade:** The reserve model enables users to enter trades more easily given that the supply and demand sides (i.e., the reserve) have fixed terms and are readily available to trade upon those terms. This removes the potential friction involved in discovering counterparties and negotiating.

Trade-offs:

- **Requires trust in a smart contract or third party:** The model requires a party to trust in the security, accuracy, and fairness of the smart contract or third party that is performing the reserve and/or order fulfillment functions. Given that smart contracts are complex, difficult to audit, and may have unanticipated security vulnerabilities, users could lose funds if the smart contract is hacked or misbehaves.[35] Models that rely on third parties to provide liquidity, such as KyberNetwork and Omega One, require users to trust these third parties to act reliably and fairly.
- **Uncertain pricing:** Given that there is high volatility in token prices, some models require users to trust a centralized party to provide fair and updated pricing. Meanwhile, models that rely on deterministic pricing algorithms could be easily exploited by arbitrageurs.[36]
- **Tendency to favor large reserve contributors:** Reserve

[33] *See How does a Smart Token work?*, BANCOR (Oct. 22, 2018), https://support.bancor.network/hc/en-us/articles/360000472072-How-does-a-Smart-Token-work.

[34] *See Omega One Whitepaper Version 1.26*, OMEGA ONE (Mar. 16, 2017), *available at* https://omegaone.docsend.com/view/pmvhkpy.

[35] *See, e.g.,* Jon Russel, *The crypto world's latest hack sees Bancor lose $23.5M*, TECHCRUNCH (Jul. 10, 2018), https://techcrunch.com/2018/07/10/bancor-loses-23-5m.

[36] *See, e.g.,* Emin Gün Sirer & Phil Daian, *Bancor is Flawed*, HACKING DISTRIBUTED (Jun. 19, 2017), http://hackingdistributed.com/2017/06/19/bancor-is-flawed.

models that rely on users to fund reserves may incentivize larger reserve contributors to participate more than smaller reserve contributors since lower spreads on trades will require higher volume to be profitable. In that case, users may need to depend on the participation of large reserve contributors for liquidity, leading to more centralized control of reserve supply.

- **Reserves may be available and liquid only for the most popular tokens:** Tokens that are new or exotic may not have reserves available or may have insufficient reserves to fulfill trades based on a user's desired price and quantity. Only commonly traded tokens are likely to have deep, liquid reserves.

3. Matching Mechanisms

Matching is the process through which buy orders are paired with sell orders that have mutually acceptable terms. Decentralized exchanges may feature automatic matching or require Takers to manually identify and fill an order. Automatic matching occurs when a computer algorithm is used to pair and execute buy and sell orders. "Manual" order filling is the process through which Takers identify a resting order on the order book and actively perform actions to execute that particular order.

On centralized exchanges, all user orders are aggregated, and users are able to submit market orders and limit orders. A market order is a buy or sell order that is executed instantaneously based on the current market price, and a limit order is a buy or sell order where a user will specify a maximum purchase price or minimum sale price, and will only be matched with orders that offer a price that is at or more favorable than the specified price. Market orders allow users to obtain market price for their orders without having to specify a desired price, thereby increasing the speed and ease of trade, whereas limit orders allow users to obtain market price for their orders while protecting them from trades that are less favorable than a specified minimum or maximum price.

By comparison, most non-reserve-based decentralized exchange protocols do not have market orders or limit orders. These protocols often feature manual order filling whereby Makers will submit resting orders that specify a fixed price and volume, and Takers will fill these orders based on the Makers' specified terms. Therefore, if prices of the trading assets change significantly after a Maker places an order, and the Maker does not have an opportunity to correct the price, the order may get filled at a price that is less favorable to market price. However, developers of off-chain order books, user interface applications, and bots for these protocols can implement off-chain logic that mimics automatic order filling by allowing a user to specify desired parameters off-chain, and programmatically selecting the most favorable order that meets the user's specified parameters.

Reserve-based decentralized exchange protocols may feature automatic matching services that function similar to limit orders. Prior to execution, the user may query a smart contract or an off-chain party about the reserve's current exchange rate, and some protocols have built-in guarantees that the user will receive an exchange rate that is at least as favorable as a stated exchange rate or a user's specified exchange rate.

Analyzing a decentralized exchange's order matching algorithm is important because this will affect its ease of use, ability to provide fair exchange rates, and wait time between order creation and order fulfillment (i.e., the latency of order fulfillment). Moreover, the algorithm also informs the arbitrage opportunities that could arise from manipulating the prioritization and speed of matching through mechanisms such as front-running.[37]

Manual order filling

With manual order filling, Takers must proactively find and accept a counterparty order. This mechanism introduces more latency into order filling, but generally requires less trust and provides users more control given that users do not have to rely on a centralized or smart contract-based matching algorithm.

For example, in 0x, Takers discover Makers' orders via Relayers. If a Taker wishes to accept an order, she will submit a counterorder to the Relayer and digitally sign and send the completed transaction to an on-chain smart contract that will settle the transaction. If a Maker's orders are not actively monitored, Takers could exploit stale orders upon changes in the fair market price of the underlying token. However, off-chain bots and services could help the Maker programmatically manage its orders based on market price fluctuations.

In AirSwap, users can query Indexers to find addresses of counterparties. Users must negotiate with counterparties privately to reach agreement on transaction terms and fulfill an order. This mechanism helps to protect Makers from losing money on stale orders (e.g., orders that are not reflective of current price movements).

On EtherDelta, Makers will post resting orders onto the order book, specifying a desired price and quantity for a trade. A Taker must manually select a Maker's order from the order book and submit the order on the web

[37] For example, on networks with public order books, some users may be able to pay more to obtain a faster transaction confirmation, and some outdated offers may be swiped by frontrunners before makers can cancel or edit the offer in manual order filling.

application. Even if there are buy and sell orders that intersect on their desired terms, EtherDelta will not automatically match and execute these orders. The absence of an automatic order matching creates more latency and friction, given that Takers must manually identify suitable trades. However, no central party is needed to fairly and reliably match orders.

Automated order filling

With automated order filling, an algorithm will match orders automatically. Automated order filling reduces the amount of user time and effort needed to identify suitable trades, thereby reducing order filling latency. However, this approach requires users to trust the matching mechanism to execute securely and provide them a favorable price.

Decentralized exchanges employing liquidity reserves have automated order filling. In KyberNetwork, Reserve Managers feed dynamic exchange rates into the KyberNetwork smart contract and orders are filled at the current exchange rate. In Bancor, orders are fulfilled automatically based on a deterministic pricing formula built into the smart contract. In Omega One, orders are fulfilled automatically based on the best rate found across multiple exchanges.

IDEX is a non-reserve-based decentralized exchange that employs automated order filling. On IDEX, users may submit limit and market orders because the application has built-in off-chain order matching algorithm that helps match orders on the off-chain order book. The user will be matched with the most favorable order that is available on the order books, provided that it is more favorable than the user’s stated baseline price. This off-chain matching logic significantly improves the user experience; at the same time, users must trust IDEX’s order matching algorithm to fairly and reliably match orders.

On the Stellar decentralized exchange protocol, users may also submit limit orders to the on-chain order book. The Stellar decentralized exchange has an on-chain order matching algorithm that matches orders based on a first-in-price, first-in-time principle: orders are automatically filled such that, when an acceptable counterorder is found, the earliest submitted order made will be filled. The on-chain order matching algorithm is built into the Stellar network protocol, meaning that there is no need to trust a centralized party to perform the order matching.

4. Transaction Settlement

All decentralized exchanges feature on-chain settlement. On-chain settlement is a necessary element that enables users to eliminate the need to trust a centralized party (such as a centralized exchange) to control user assets, settle trades, and ensure that account balances are correct. On-chain settlement helps users publicly verify on the ledger that their trades were settled according to their desired terms.

The performance of any decentralized exchange is limited, at the very minimum, by the latency involved in securely confirming a transaction on the underlying chain. Therefore, the speed of confirming a transaction in a distributed ledger network is the bottleneck for decentralized exchanges.

Some distributed ledgers feature significantly higher latency than others. A secure settlement confirmation on the Bitcoin network may take hours, whereas a secure confirmation on Ethereum generally takes minutes under current limitations.[38] Confirmations on certain more recent platforms can require a few seconds.[39] Therefore, the final settlement time would depend heavily on the confirmation latency of the underlying chain.

DIFFERENT EXCHANGES, DIFFERENT USE CASES

Each decentralized exchange presents a different array of latency, security, liquidity, privacy, interoperability, and trust tradeoffs. Therefore, different exchanges will excel in different use cases and requirements.

Access

First and foremost, different decentralized exchanges offer access to different cryptocurrencies.

Many cryptocurrencies issued in 2017 and 2018 are ERC-20 tokens; in order to purchase these tokens, one must use an decentralized exchange protocol that is compatible with the ERC-20 technical standard, such as 0x or IDEX. Similarly, as some new ICOs are held on competing platforms such as Stellar and Waves, one may be pushed to use their respective decentralized exchanges to transact tokens issued on those platforms.

Security

With respect to the technical security of Ethereum smart contract-based exchange protocols, the smart contract driving the exchange protocol may be vulnerable to accidents and security vulnerabilities. The degree to which a smart contract will function as intended and will not be vulnerable to

[38] The speed of confirmation is influenced by both the volume of network activity and the transaction fee that the user chooses to pay. A user may elect to pay a higher transaction fee so that her transaction is prioritized by miners and is processed faster.

[39] By contrast, centralized exchanges can perform arbitrarily fast transactions, limited by the speed of updating their centralized database infrastructures rather than limited by the delay of confirming distributed ledger transactions.

exploits remains somewhat uncertain given the difficulty of thoroughly auditing Ethereum's Turing-complete smart contracts. By contrast, distributed ledgers with on-chain native decentralized exchange functionality should in theory have significantly lower attack surface given that protocols are more thoroughly audited and require network consensus to change and exploit.

The security of a decentralized exchange is limited also to the security of the underlying distributed ledger. For example, if a proof of work blockchain is attacked, such as through a "51 percent" attack, settled transactions may be reversed despite a large number of block confirmations. Under any consensus mechanism, the network's validator nodes could also collude to "fork" to an alternate state of transactions (and orders, in the case of an on-chain order book), adopt a technical standard that is incompatible to the decentralized exchange protocol, censor (i.e. ignore) orders submitted by certain addresses, modify order settlement, matching, and reserve smart contracts, and more. Therefore, the ultimate security of a decentralized exchange is dependent on the security of the underlying distributed ledger.

Transactions that require strong security conditions should be settled using thoroughly audited smart contracts and distributed ledger platforms with a consistent history of guaranteed functionality.

Liquidity

Many new cryptocurrencies may only be available for purchase or sale through decentralized exchanges, given that centralized exchanges have been slow to list new tokens due to regulatory risk. Therefore, many cryptocurrencies may only be attainable and tradable over decentralized exchanges. However, a decentralized exchange would not be practically useful for users if it did not have robust order books or other mechanisms that enable users to transact cryptocurrencies without significant price slippage.

The use of interoperable decentralized exchange protocols enable applications that use the same protocol to be able to pool together liquidity for "networked liquidity." For example, Relayers built on 0x may pool together their order books to build a thicker order book. Any token issued on the Stellar platform can be exchanged with any other token issued on Stellar, generating a network-wide order book. While liquidity on decentralized exchanges is currently significantly lower than on popular centralized exchanges, interoperable protocols will hopefully spur greater networked liquidity.

Latency

The latency of a decentralized exchange depends on the speed of the underlying distributed ledger. For example, if it takes 3 minutes to confirm one transaction in Ethereum, then an order would be settled in 3 minutes at a minimum given that the ultimate settlement of a trade must be on-chain. This latency will likely improve as the Ethereum network adopts new technologies to increase throughput and lower validation time.

Some distributed ledger networks permit significantly faster on-chain settlements due to the use of different consensus mechanisms. For example, an order or settlement on Stellar can be securely confirmed in 5 seconds due to the speed of the Stellar Consensus Protocol. The on-chain order books on Stellar would be slower to update than the off-chain order books on Ethereum-based decentralized exchanges, but third parties could eventually develop off-chain order books for the Stellar decentralized exchange, as well.

Even the lowest latency decentralized exchanges currently cannot compete with the near-instantaneous settlement speeds of centralized exchanges. For users who engage in high-frequency trading activities, centralized exchanges such as Coinbase Pro, Bittrex, Kraken, and Poloniex may still be the best choice, given that market orders can potentially be placed and settled in seconds. Moreover, until the stable release of cross-chain atomic swaps, centralized exchanges are still the best platforms for trades swapping tokens that were issued across multiple chains.

Cost

The cost of using a decentralized exchange application includes the costs of (1) fees to the decentralized exchange application, (2) fees of making and/or taking orders, (3) fees involved in interacting with any smart contracts enabling the decentralized exchange protocol, and (4) fees involved in settling a transaction to the distributed ledger. These costs may include blockchain network transaction costs (e.g. using ETH for transaction fees for settling a transaction on the Ethereum) or fees for using a certain protocol (e.g. paying ZRX tokens to 0x Relayers for trading fees). Settlement on some blockchains may cost more than a settlement on others.

Whereas centralized exchanges tend to charge fees that are a percentage of the total transaction size, the cost of using a decentralized exchange tends to be fixed per transaction: a high-value transaction would incur the same fees as a microtransaction. Therefore, those who are submitting high-value transactions may save transaction fees by using a decentralized exchange.

Trust Level

Different decentralized exchange applications require different levels of user trust. Users may need to trust: (1) the decentralized exchange application creator and operator to perform activities such as hosting and publishing order books or performing order matching, (2) the underlying decentralized exchange protocol, including relevant smart contracts, and (3) the security, miners, and validators of the underlying distributed ledger. Users must trust each part of the exchange application stack to perform its job fairly, reliably, and securely. If any part of the stack fails, users may be unable to reliably and securely submit and fill orders, match with orders that meet their specified criteria, and confirm the settlement of trades. Moreover, users may find that trusted parties could censor some of their transactions or act in a self-interested manner to the users' detriment.

Some users may want to minimize trust in the decentralized exchange application layer: therefore, they would want to minimize reliance on the application to host and publish order books and/or perform order matching. Therefore, these users may choose applications that have on-chain order books. They may also choose applications that do not have automatic order matching.

Some users may want to minimize trust in the decentralized exchange protocol by making sure that the protocol has a minimal attack surface. These users may choose to only interface with highly audited protocols such as 0x protocol, or an on-chain, difficult-to-modify protocol such as the Stellar protocol.

Lastly, some users may want to minimize trust in the security, miners, and validators of the underlying distributed ledger. Different users will have different opinions on which distributed ledgers have the most favorable, trust-minimized characteristics; factors such as the ledger's security and exploits history, audit history, consensus mechanism, governance mechanisms, and distribution of miners and nodes could all contribute to this calculus.

Practically speaking, many users may not be overly concerned about trusting decentralized exchanges given that users do not relinquish control over their private keys. Ultimately, most users may prefer a better user experience rather than optimizing for trust minimization. Users must decide on the level of trust that is necessary for their personal use cases for a decentralized exchange.

CONCLUSION

The term "decentralized exchange" encompasses diverse applications and protocols that differ in architecture, but all enable users to transact cryptocurrencies without relinquishing control over their private keys to an intermediary.

Decentralized exchanges are still in an early development stage; their higher trade latency, lower liquidity, and less intuitive user interfaces make them less attractive for mainstream retail users. However, as centralized exchanges continue to experience security exploits and delay the listing of new cryptocurrencies, more users will elect to adopt decentralized exchanges despite their high friction. It is worthwhile to invest in the development and growth of the decentralized exchange ecosystem to promote liquidity in an increasingly diverse token ecosystem, greater user control of cryptocurrencies, more privacy features, and lower risk of censorship.