PENN BLOCKCHAIN

An Overview of Decentralized Exchanges

Alex Miao

Overview

Centralized Crypto Exchanges and Their Problems

Decentralized Exchanges

- EtherDelta
- 0x Protocol
- DutchX
- Uniswap

Regulatory Challenges

Centralized Exchanges and Their Problems

Centralized Cryptocurrency Exchanges

Run by a company, users do not custody funds

Problems of Centralized Crypto Exchanges

Traders need to transfer funds to wallet custodied by exchange

- Temporarily lose ownership of cryptoassets
- Hackers can steal funds
- The exchange can do whatever it wants with your money

Problems of Centralized Crypto Exchanges

Exchanges can go down and traders temporarily don’t have access to funds

Maintenance

DoS (Denial of Service) Attacks

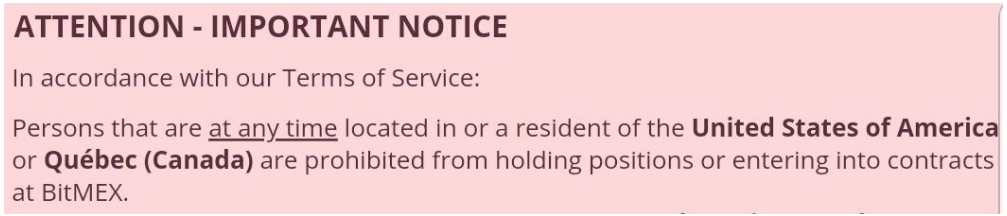
Problems of Centralized Crypto Exchanges

Require KYC/AML

- Hacker breached Binance in July 2019 and obtained KYC files of thousands of users

Subject to regional regulation

- US users cannot trade on Bitmex



Problems of Centralized Crypto Exchanges

Market Manipulation

Exchanges are incentivized to create fake liquidity to boost popularity

Wash Trading to boost volume

Problems of Centralized Crypto Exchanges

Centralized Exchanges charge exchange fees to make profit

Tier	Maker	Taker
$0-10K	0.50%	0.50%
$10-50K	0.35%	0.35%
$50 - 100K	0.15%	0.25%
$100K - 1M	0.10%	0.20%
$1 - 10M	0.08%	0.18%
$10 - 50M	0.05%	0.15%
$50 - 100M	0.00%	0.10%
$100 - 300M	0.00%	0.07%
$300 - 500M	0.00%	0.06%
$500M - 1B	0.00%	0.05%
$1B+	0.00%	0.04%

Coinbase Fees

Decentralized Exchanges

Decentralized Exchanges

Decentralized Exchanges (DEXes) are cryptocurrency exchanges that operate through smart contracts.

Users custody their own assets

DEXes may be run by a company, organization, or DAO

Ethereum has most developed DeFi ecosystem

- We will be looking only at DEXes on Ethereum

Decentralized Exchanges

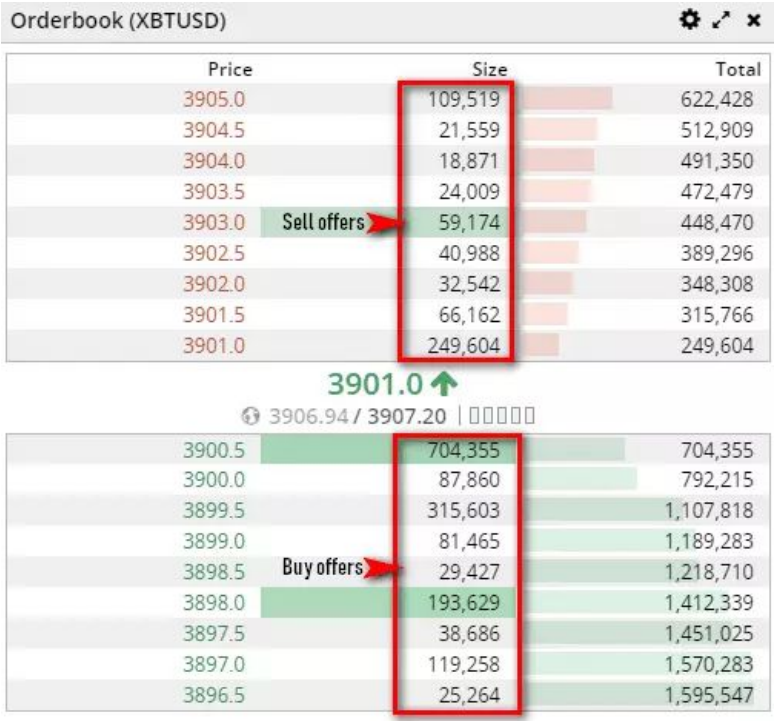
We will be taking a look at a few approaches to designing DEXes

For each, pay attention to if and how the DEX deals with

- Where assets are held
- Liquidity/Market Making
- Speed of Order Execution
- Governance

Orderbooks

Continuously updated list of buy and sell orders



ERC-20 Tokens

An interface for Ethereum Smart Contracts implementing tokens

Shared interface allows for compatibility with programs

Example: 0x Token (ZRX)

6 functions:
totalSupply(): Total supply of Token.

balanceOf(address _owner): The balance in the _owner address.

Transfer(address _to, uint256 _value): Sends a token of _value to address_to, triggering the Transfer event.

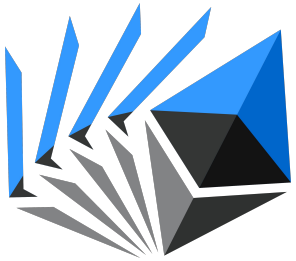
transferFrom(address _from, address _to, uint256 _value): Sends a pass from the address_from _value to address_to, triggering the Transfer event.

Approve (address _spender, uint256 _value): Approve _spender to extract a certain amount of money.

Allowance(address _owner, address _spender): Returns the amount that _spender extracted from _owner.

EtherDelta

EtherDelta



Fully on-chain exchange

Only 170 lines of code!

Contract: https://etherscan.io/address/0x8d12a197cb00d4747a1fe03395095ce2a5cc6819#code

Problems with On-Chain Orderbooks

Slow - need to wait for transaction to get confirmed on blockchain for every operation

Expensive - need to pay gas cost for transactions

Low Liquidity

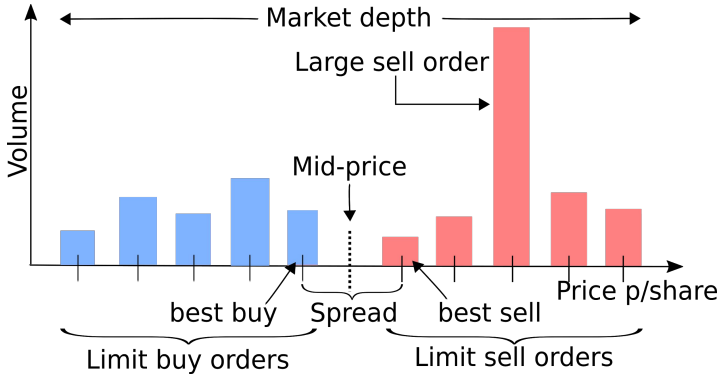
Liquidity

Traders want to be able to enter and exit positions quickly at a stable price

Liquidity is how easy it is to trade one asset for another without affecting price

Greater volume means greater liquidity

Illiquid markets are susceptible to price swings and manipulation



0x

0x Protocol

A protocol for decentralized exchanges

Released by Will Warren in Late 2016

On blockchain settlement, but off blockchain orders

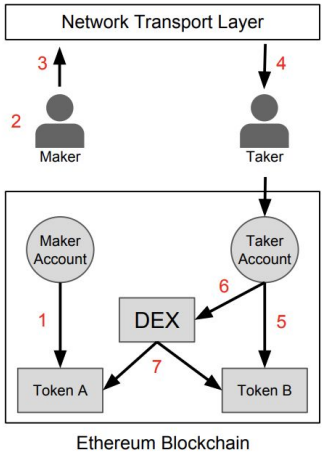
0x Protocol

Say Maker wants to sell Token A for Token B

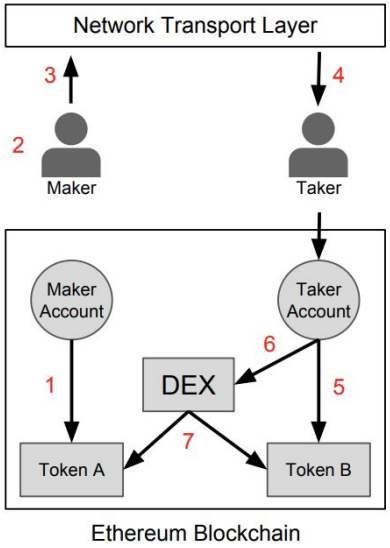
1. Maker approves (ERC-20) smart contract to access wallet of Token A

2. Maker creates order stating Token A to Token B rate, signs it with private key

3. Maker publishes order anywhere



0x Protocol



4. Some Taker sees order and wants to fill

5. Taker approves smart contract to access wallet funds of Token B

6. Taker submits order to smart contract

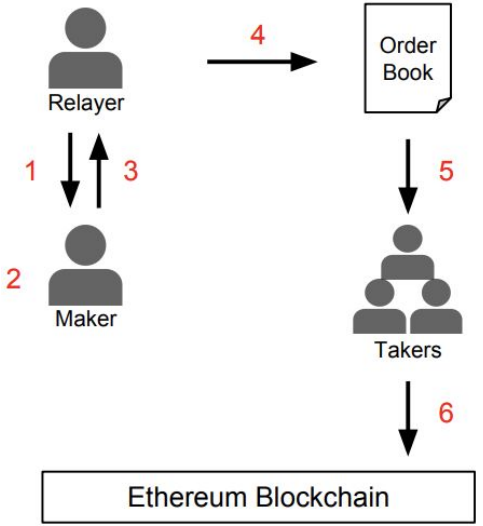
7. Contract verifies signature, checks if transaction is legal, and performs swap

0x Protocol

Where to broadcast orders?

A Relayer aggregates orders and publishes them in a public place

Relayers essential for liquidity



0x Protocol

Maker specifies Relayer and fees in the message

Maker specifies Expiration

Maker can cancel outstanding order

Taker can specify how much to fill

https://app.radarrelay.com/ZRX/WETH

Name	Data Type	Description
`version`	`address`	Address of the Exchange smart contract.
`maker`	`address`	Address originating the order.
`tokenA`	`address`	Address of an ERC20 Token contract.
`tokenB`	`address`	Address of an ERC20 Token contract.
`valueA`	`uint256`	Total units of tokenA offered by maker.
`valueB`	`uint256`	Total units of tokenB requested by maker.
`expiration`	`uint256`	Time at which the order expires (seconds since unix epoch).
`feeRecipient`	`address`	Address of a Relayer. Receives transaction fees.
`feeA`	`uint256`	Total units of protocol token Maker pays to feeRecipient.
`feeB`	`uint256`	Total units of protocol token Taker pays to feeRecipient.
`v`	`uint8`	ECDSA signature of the above arguments.
`r`	`bytes32`	
`s`	`bytes32`	

Maker message protocol

Name	Data Type	Description
`valueFill`	`uint256`	Total units of tokenA to be filled (`valueFill` $\leq$ `valueA`).

Additional Taker field

0x Governance

0x token used to pay fees on network

Acts as governance token to vote on 0x Improvement Proposals

Goal is to hand control of the protocol over to Token holders

0x Protocols

Question: What improvements does 0x offer over EtherDelta?

Still does not handle liquidity well: https://0xtracker.com/relayers

DutchX

DutchX

Developed by Gnosis

Gnosis is an organization that develops various DeFi products on Ethereum

No Orderbook

Utilizes a Dutch Auction to sell off tokens

DutchX

Dutch Auction Mechanism

- Price starts high and goes down over time
- Bidders place bids when price is at desired value
- Auction clears at the same price for everyone (final auction price)

DutchX

Selling and bidding done in phases

Sellers deposits tokens into smart contract. If more than $1000 dollars of tokens accumulates. Auction starts at 2x price of last auction.

Prevents frontrunning since entire auction finalized at the same price

DutchX

dxDAO launched in May 2019

DAO to govern DutchX, Gnosis steps back

Reputation distributed to members

Exchange fees go to DAO members

Incentive to provide liquidity - rewarded for trades that happen

Uniswap

https://uniswap.exchange/swap

Uniswap

Created by Hayden Adams in 2018

Inspired by post about Decentralized Exchanges written by Vitalik

Uniswap

No orderbook, uses an automated market maker (AMM)

Traditionally, market makers put buys and sells at specific prices that they are willing to transact at.

Uniswap instead algorithmically determines the price of a trade

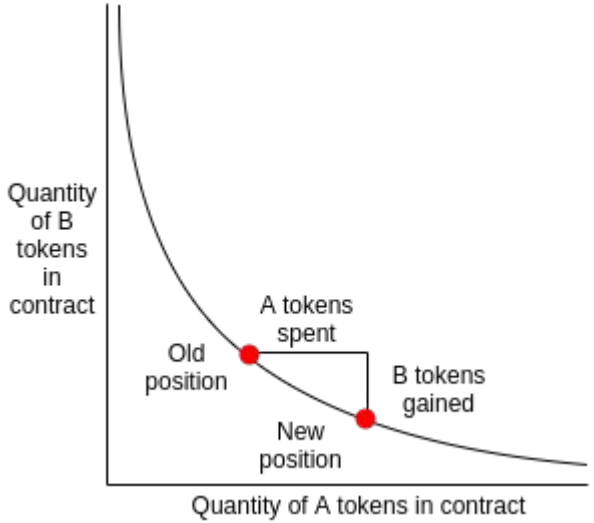
Exchange	Uniswap	EtherDelta	Bancor	Radar Relay (0x)	IDEX	Airswap
ETH to ERC20	46,000	108,000	440,000	113,000*	143,000	90,000
ERC20 to ETH	60,000	93,000	403,000	113,000*	143,000	120,000*
ERC20 to ERC20	88,000	no	538,000	113,000	no	no

Uniswap Automated Market Maker

On-chain automated market maker

Have a smart contract that holds x amount of Token A and y amount of Token B. The contract always maintains the invariant: xy = k

The size of an order affects the price you pay



Uniswap Automated Market Maker

x - total supply of Token A.
y - total supply of Token B.
Δx - amount of A you want to sell
Δy - amount of B you want in exchange

$$x \times y = (x + \Delta x) \times (y - \Delta y)$$

$$\alpha = \frac{\Delta x}{x} \qquad x' = x + \Delta x = (1 + \alpha)x = \frac{1}{1 - \beta}x$$

$$\beta = \frac{\Delta y}{y}. \qquad y' = y - \Delta y = \frac{1}{1 + \alpha}y \quad = (1 - \beta)y$$

$$\Delta x = \frac{\beta}{1 - \beta}x$$

$$\Delta y = \frac{\alpha}{1 + \alpha}y$$

Uniswap

AMM Example:

Initial Conditions	DAI Liquidity	ETH Liquidity	Product
	100,000	1,000	100,000,000
	x	y	k

ETH Purchased	Cost per ETH	Total Cost in DAI	Premium	New DAI Liquidity	New ETH Liquidity	Product
				x	y	k
1	100.10	100.10	0.10%	100,100.10	999	100,000,000
10	101.01	1,010.10	1.01%	101,010.10	990	100,000,000
50	105.26	5,263.16	5.26%	105,263.16	950	100,000,000
100	111.11	11,111.11	11.11%	111,111.11	900	100,000,000
200	125.00	25,000.00	25.00%	125,000.00	800	100,000,000
500	200.00	100,000.00	100.00%	200,000.00	500	100,000,000
800	500.00	400,000.00	400.00%	500,000.00	200	100,000,000
999	100,000.00	99,900,000.00	99900.00%	100,000,000.00	1	100,000,000
1000	Infinity	Infinity	Infinity	Infinity	0	100,000,000

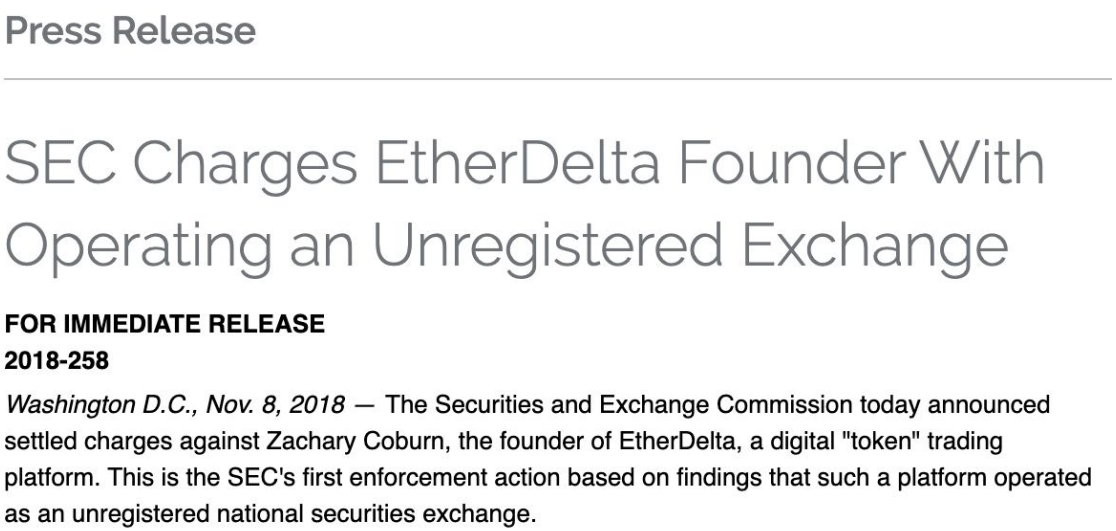
Other Decentralized Exchanges

There are tons of other DEXes out there

Regulatory Challenges

EtherDelta

Founder Zachary Coburn charged for violating Section 5 of the Exchange Act



Press Release

SEC Charges EtherDelta Founder With Operating an Unregistered Exchange

FOR IMMEDIATE RELEASE
2018-258

Washington D.C., Nov. 8, 2018 — The Securities and Exchange Commission today announced settled charges against Zachary Coburn, the founder of EtherDelta, a digital "token" trading platform. This is the SEC's first enforcement action based on findings that such a platform operated as an unregistered national securities exchange.

Securities Tokens

YouNow's Props Token was granted Reg A+ status by SEC

Can only be traded on regulated exchanges

But Props Token is also an ERC-20...