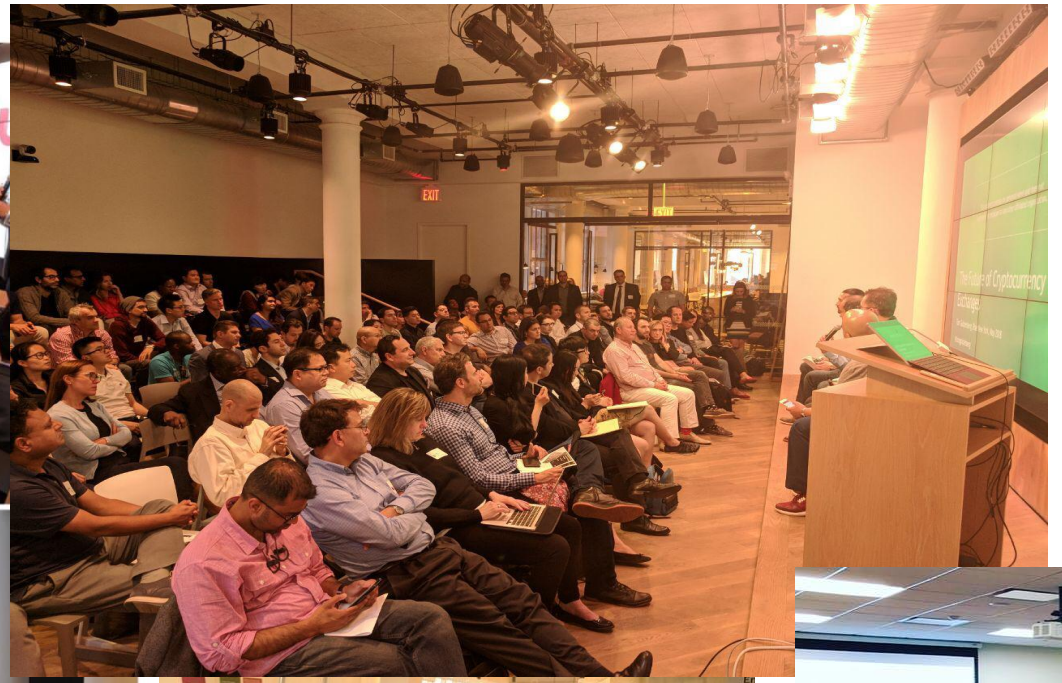
Introduction to DeFi

http://blockchainNYC.io



Welcome & Agenda

- Welcome & Introduction
- DeFi Basics and Road to DeFi
- DeFi & Institutions
- Case Study: MakerDAO
- Case Study: Uniswap with Financial Model Spreadsheet
- Case Study: Derivative Protocols Synthetix, Hegic and dYdX
- Q&A

chainhaus

Disclaimer

- Nothing else contained in this presentation should be used or construed as an offer to sell, a solicitation of an offer to buy, or a recommendation for any product. Nor is it intended as investment, tax, financial or legal advice.
- The presenter holds no view in regards to the merits or viability of the technologies presented
- The presenters are presenting in their personal capacity and do not necessarily express the views of their respective employers

chainhaus

Clemens Wan

- **Global Solution Architect** at ConsenSys with specialization in blockchain enterprise deployments, DeFi components, and Corda architecture for the past 2 years.
- 2.5 years at R3 leading global solutions architecture design and
- 6 years at Credit Suisse within Credit eTrading.
- LinkedIn: http://linkedin.com/in/clemenswan/
- Email: clemens.wan@consensys.net

CONSENSYS

Joel Aihende

- **Joel Aihende** is part of the Global Blockchain team at Accenture with the focus on advising financial services clients on platform agnostic Blockchain, DLT and Multi-Party Systems strategy & solutioning for the past 3 years.
- Responsible for Accenture's Blockchain & DLT business in Switzerland.
- Prior to that he worked in business management and software engineering in Zurich, London & Hong Kong
- LinkedIn: https://www.linkedin.com/in/joel-aihende-93b429108/
- Email: joel.aihende@accenture.com

accenture

Jamiel Sheikh

- Bio: http://jamiel.io
- LinkedIn: http://linkedin.com/in/jamiel

chainhaus

Logistics

- Hold questions till end, use “Raise Hand” button please
- Slide deck will be posted after session
- Let’s have fun!

chainhaus

What is DeFi?

- **De**centralized **Fi**nance or “open finance” (i.e. “open source”)
- Traditional Finance.. Decentralized
- Re-interpretation & innovation
- New economic systems
- Complex & intricate

chainhaus

Why would should I care about DeFi?

- Global
- Rapid settlement
- Unbanked
- Fractional (1/10000th of a penny?)
- Lower friction
- 24/7 market
- Zero to low infrastructure costs

Use Cases

- Tokens
- ICO / STOs
- Issuance & Asset Tokenization
- Stablecoins
- Money Markets & Yield Farming
- Exchanges
- Prediction Markets
- Oracles
- Derivatives

chainhaus

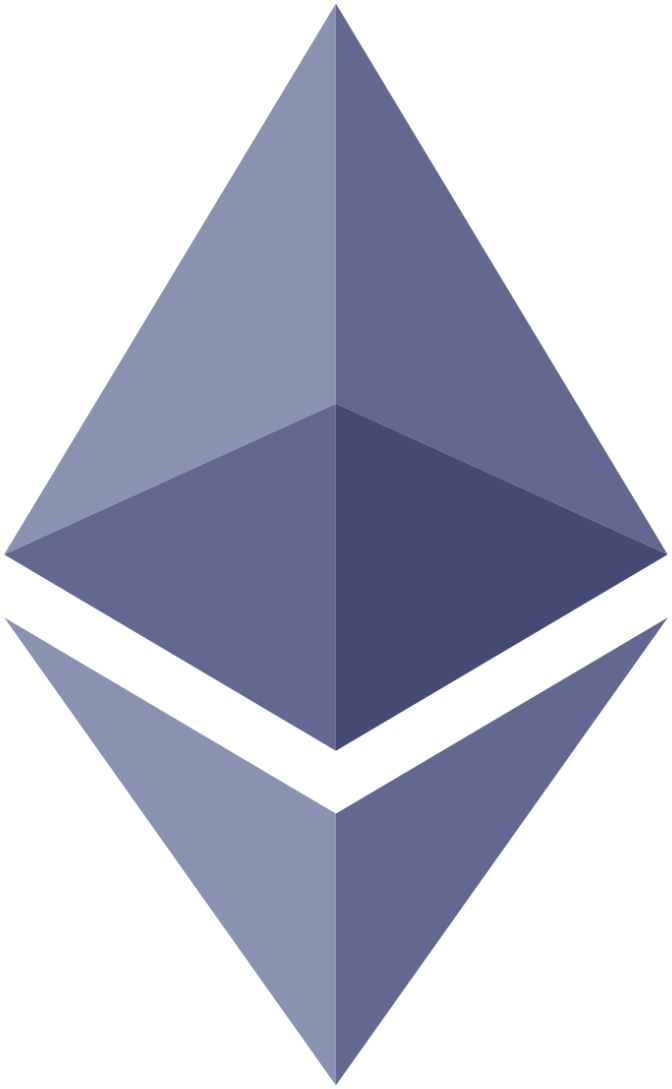
Turn back clock: Bitcoin

- Solved: Double spend
- Decentralization
  - No single point of failure
  - No single point of leverage
- Economic system of incentives / disincentives
- Blockchain
- Problem: Rigid data structure, non-Turing complete

chainhaus

Enter Ethereum

- Programmable money = defining behavior of value
  - Smart contracts
- Custom data structures
- Ether (or Eth) cryptocurrency



chainhaus

Use Case #1: Raising Capital – ICO / STO

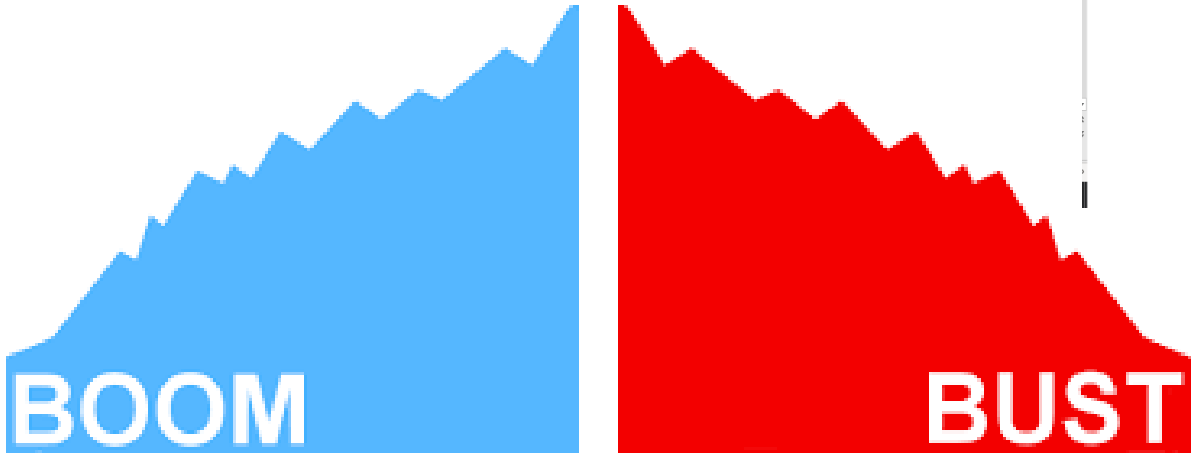
- Initial Coin Offering (Crowdfunding)
- Issue tokens to raise capital for projects
- Allocation Table

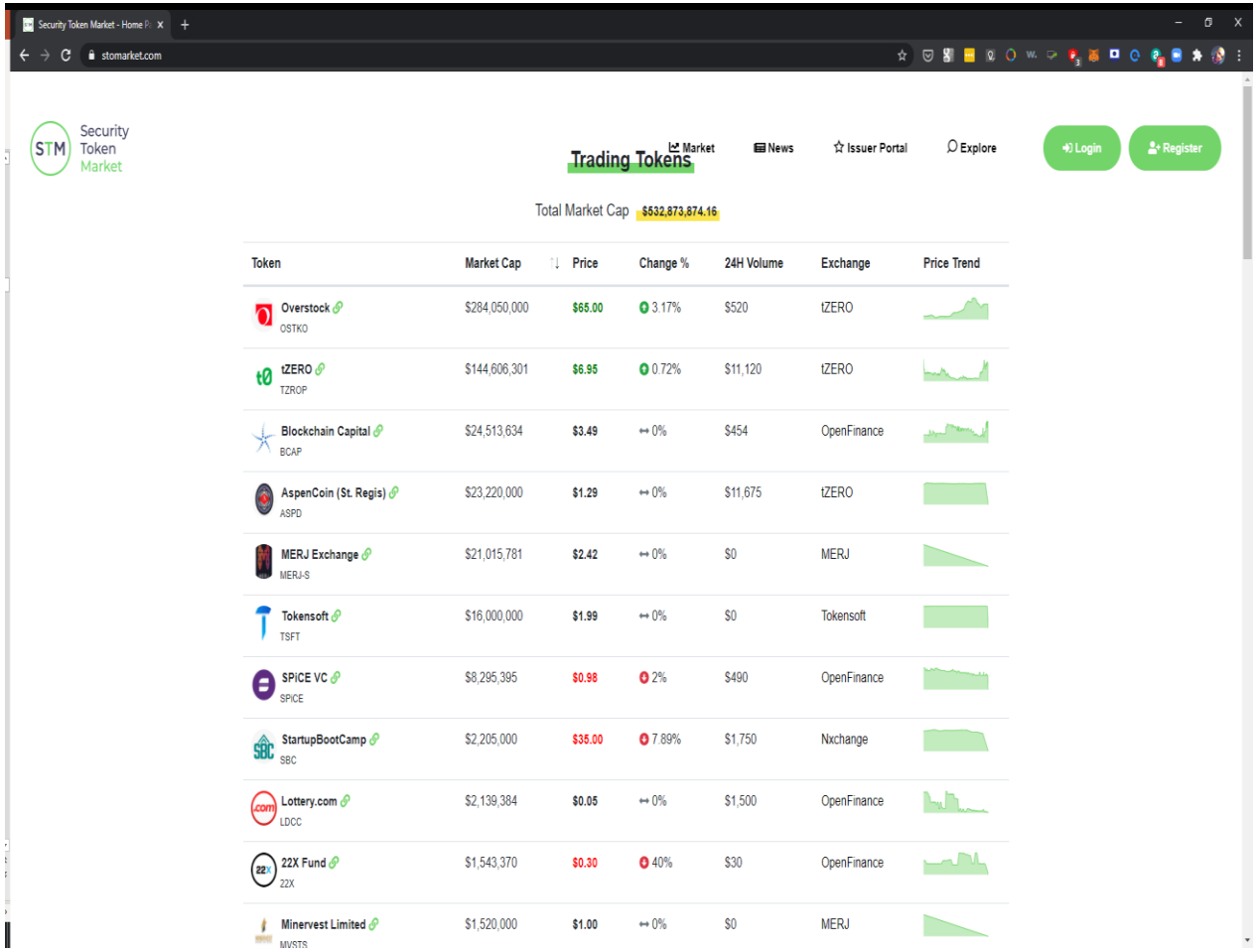
Account (Address)	Tokens
09a…82b (Bob)	200,000
4fb…aa2 (Alice)	350,000
…	100,000
…	358

chainhaus

ICO Boom/Bust

- Regulatory guidance enters 2017-2018
- ICO scams 90%+
- Registered ICOs => STOs

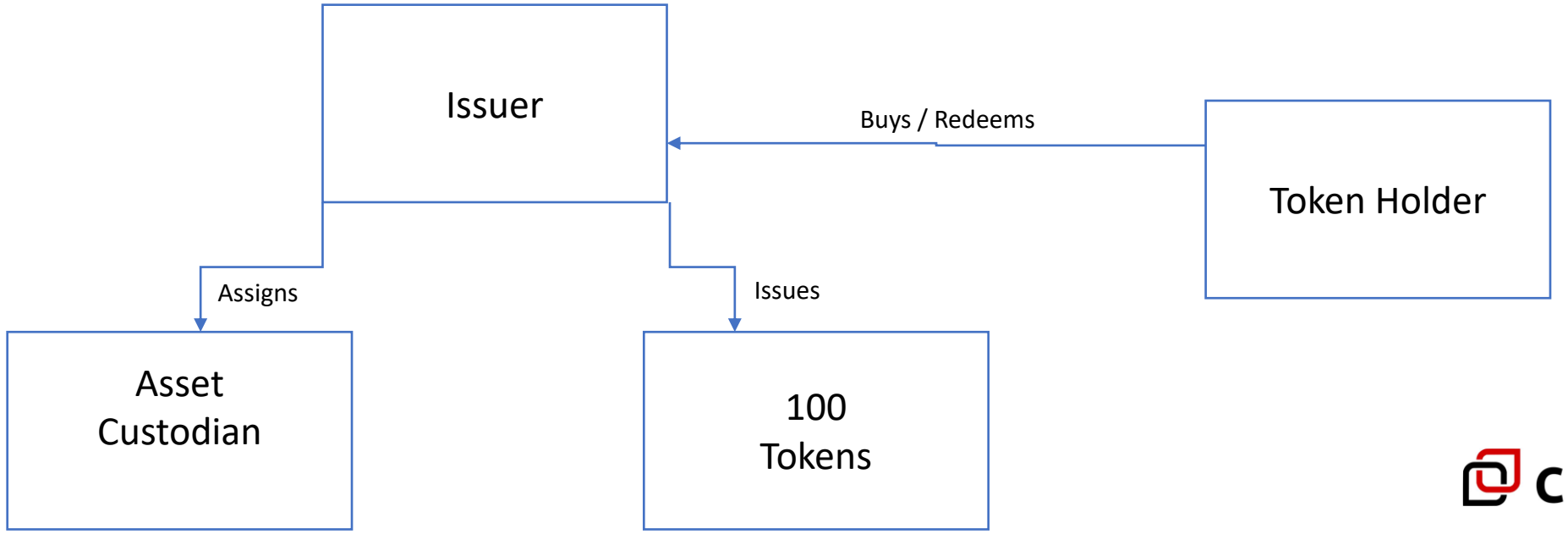




chainhaus

Use Case #2: Asset Tokenization

- Gold, Oil (Fungible)
- Real Estate (Non-Fungible)
- Token represents ownership / rights against the asset



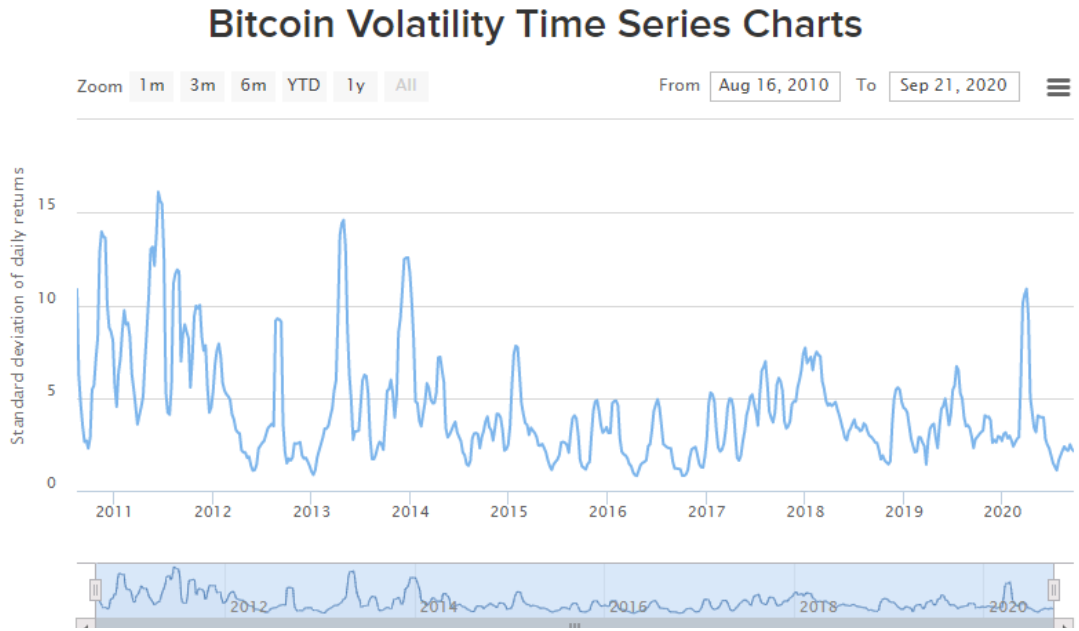
chainhaus

Issuance

- Issuance Platforms
  - tZero
  - Polymath
  - Harbor
- Manage investor, docs, compliance
- Liquidity is a problem

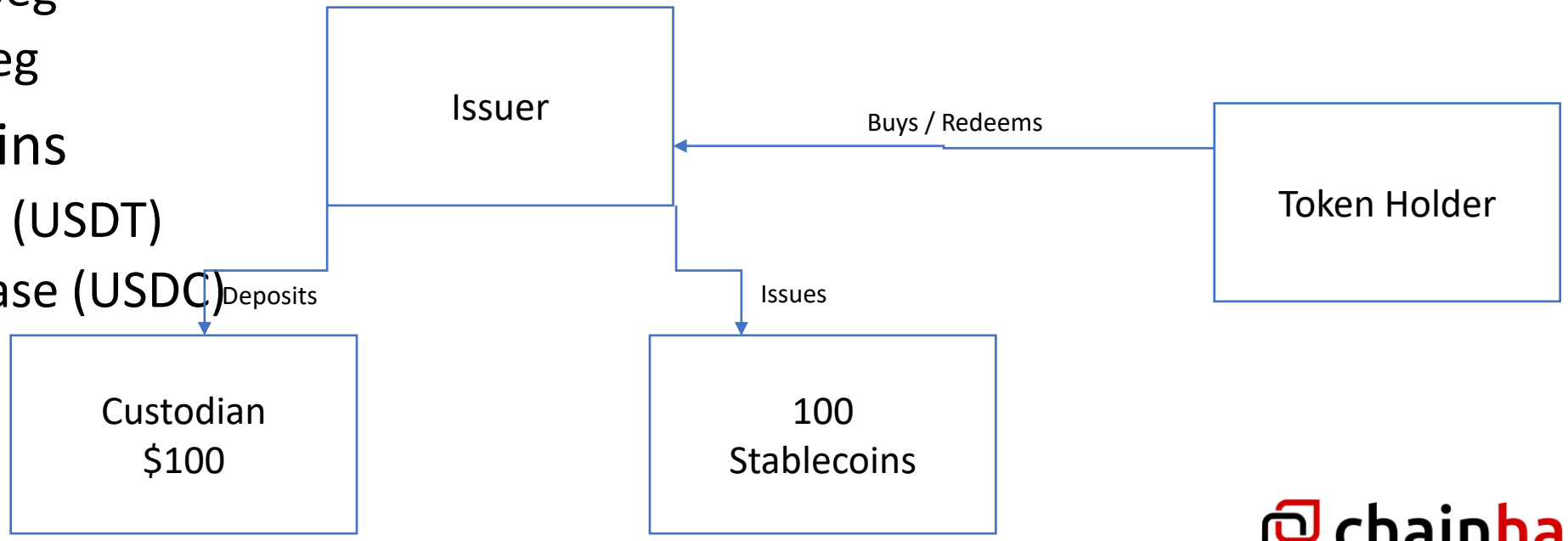
Use Case #3: Stable value

- Is it a currency?
- Currency
  - **Store of value**
  - Unit of account
  - Legal tender
  - Medium of exchange
- Psychological expectation of fixed valu
- Implies zero or close to zero volatility



Use Case #3: Stablecoins

- Token with zero to low volatility
- Pegged to an asset pool
  - Hard peg
  - Soft peg
- Stablecoins
  - Tether (USDT)
  - Coinbase (USDC)



chainhaus

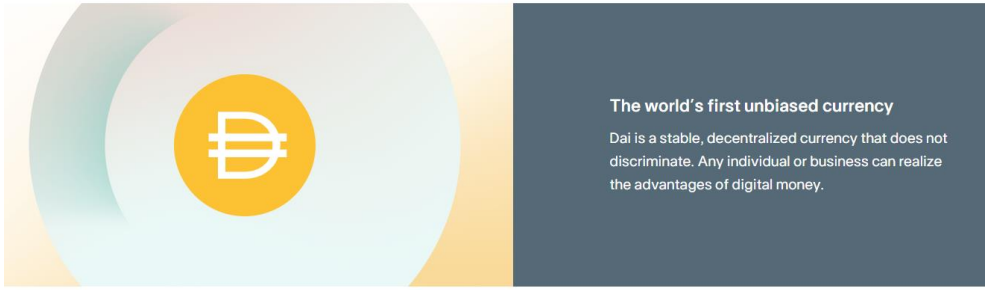
Types of stablecoins

- Fiat collateral
- Asset collateral
- Crypto collateral
- **Computational**

chainhaus

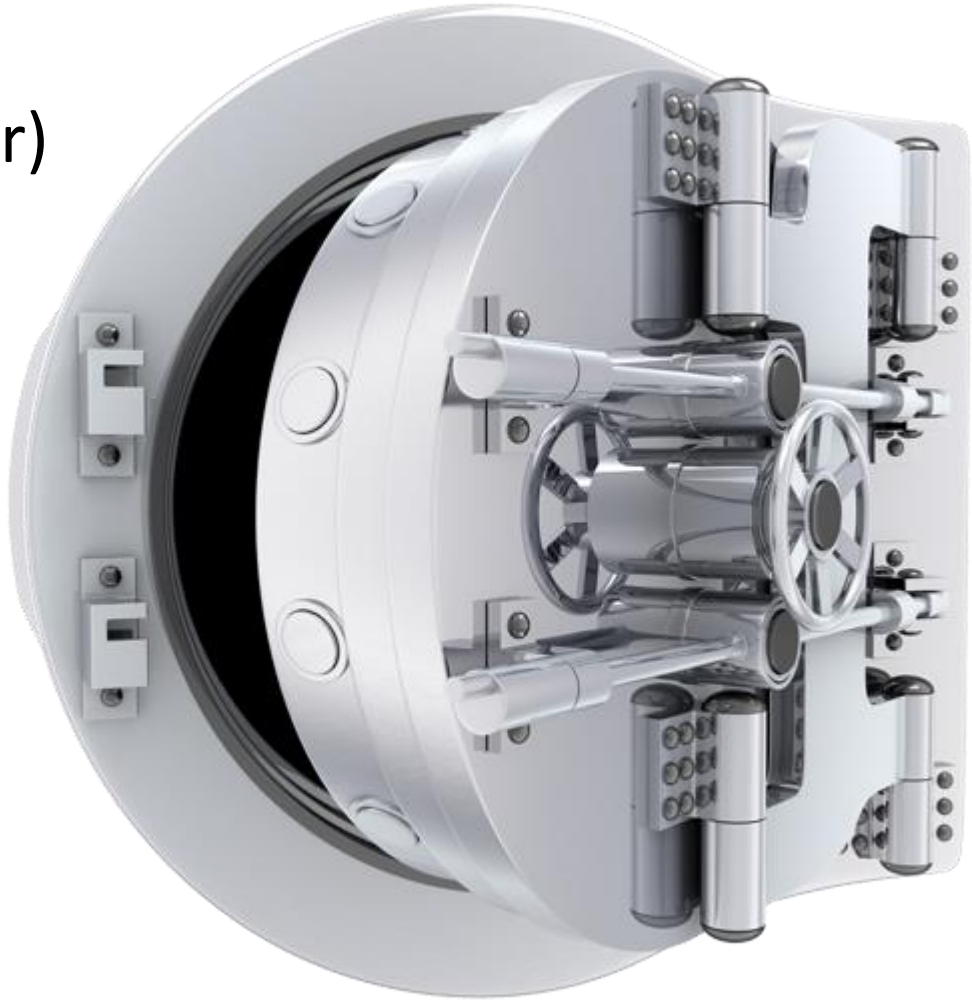
Decentralized Stablecoin

- MakerDAO
  - Founded 2015, launched 2018
- Transparent crypto as collateral
- #1 most active DeFi app on Ethereum
- Two token system
  - DAI – Stablecoin
  - MKR – Governance (vote on risk parameter changes, i.e. debt ceiling, ratios) & fees



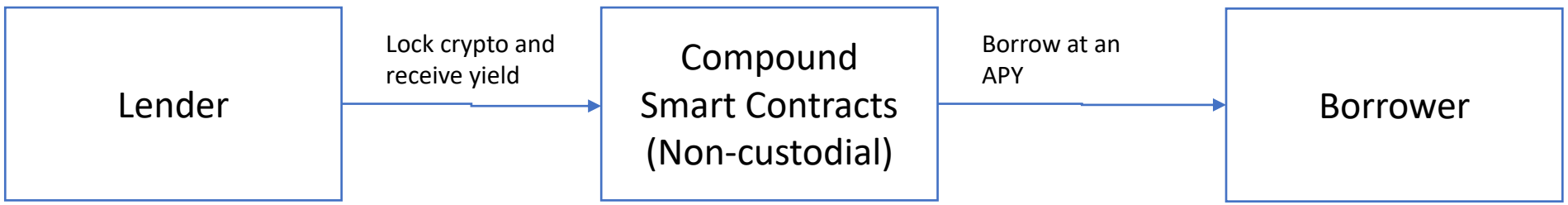
Use Case #4: Money Markets

- Cryptos can be staked (liquidity provider)
- Cryptos can be borrowed (borrower)
- APY
- Borrower must be a lender



Money Market Platforms

- **Compound** (backed by Coinbase, Bain Capital)
- Aave
- Dharma
- Celsius (Centralized)
- Many others



Return DAI + Interest fees denominated in MKR

Note: You are currently connected to the Kovan Testnet

Compound

Dashboard Vote

0.0000 0x0b...0bB7

Supply Balance
$0

Net APY
...

Borrow Balance
$0

Borrow Limit 0% $0.00

Supply Markets

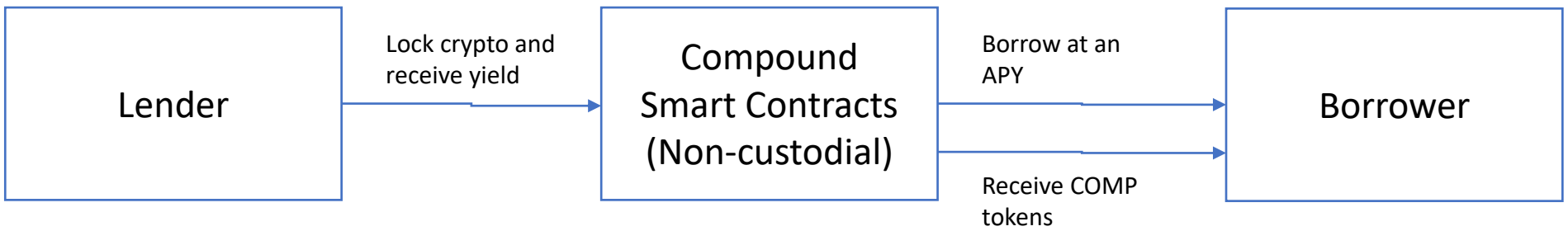
Asset	APY	Wallet	Collateral
Basic Attention ...	0.21%	0 BAT	
Dai Stablecoin	4.60%	0 DAI	
Ether	12.69%	0.9532 ETH	
USD Coin	10.58%	0 USDC	
Tether	3.26%	0 USDT	
Wrapped BTC	0%	0 WBTC	

Borrow Markets

Asset	APY	Wallet	Liquidity
Basic Attention ...	3.75%	0 BAT	$202k
Dai Stablecoin	5.70%	0 DAI	$11k
Ether	12.72%	0.9532 ETH	$7k
USD Coin	11.72%	0 USDC	$990,000,...
Tether	9.49%	0 USDT	$272k
Wrapped BTC	2.02%	0 WBTC	$509,919,0...

Compound

- COMP tokens are sweeteners to borrowers (liquidity mining)
- ..which in turn induces lending (market making)
- **Borrowers can earn a positive net APY depending on COMP price**



Return DAI + Interest fees denominated in MKR

predictions.exchange/compound/None

Predictions.Exchange Compound Balancer Metrics |

Last updated on September 1st: Matches the specifications in Compound Governance Proposal #21, where emissions have been reduced by 20%.

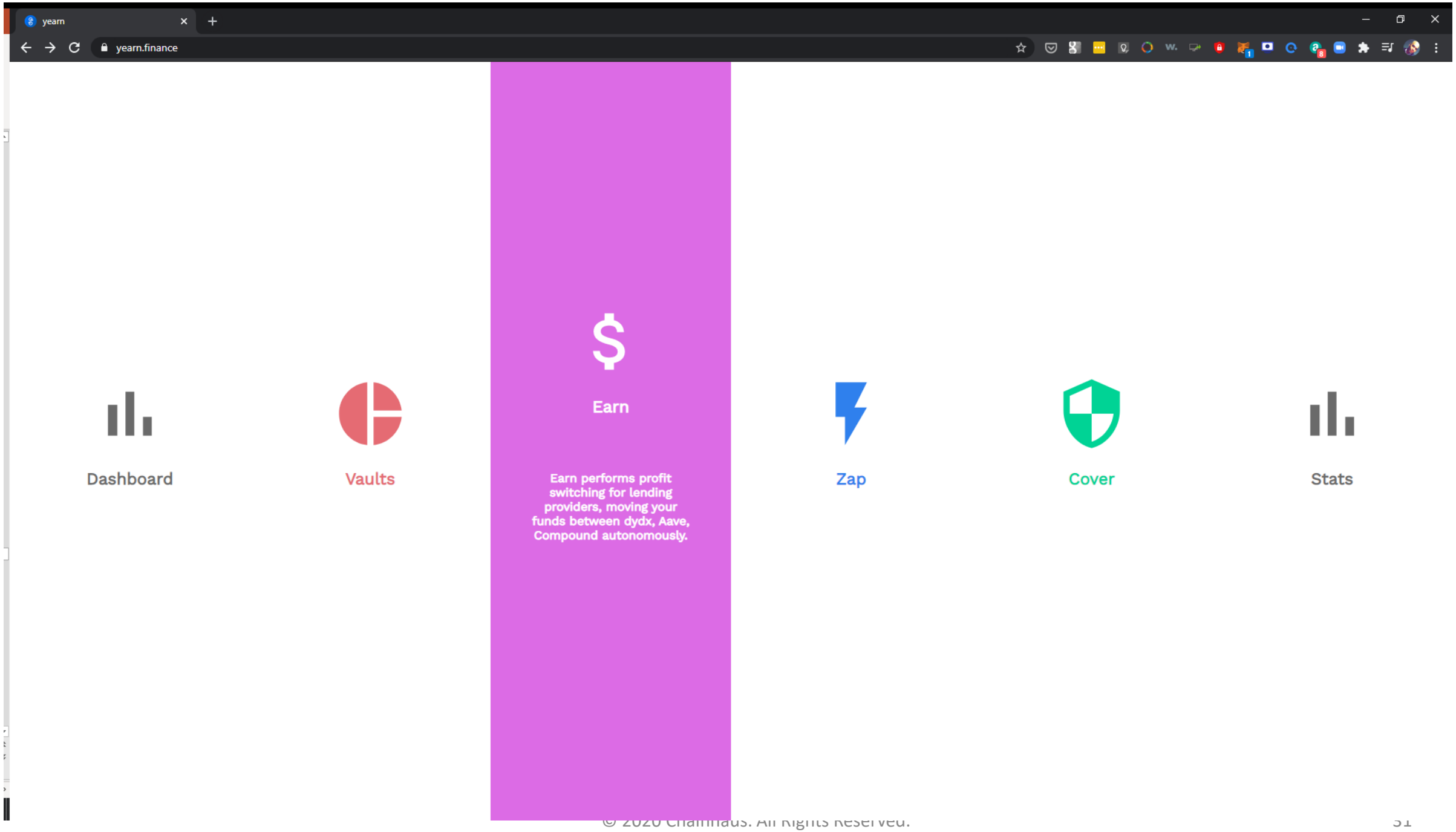
Total Supply	Annual Interest Received	Total Borrow	Annual Interest Paid	Reserve Growth	COMP Distributed / Year	Total COMP Distribution
$1,657,006,703	$33,642,253	$947,027,344	$36,597,807	$2,955,554	845,989	4.23M / 10M

Calculate My Annual COMP Distribution

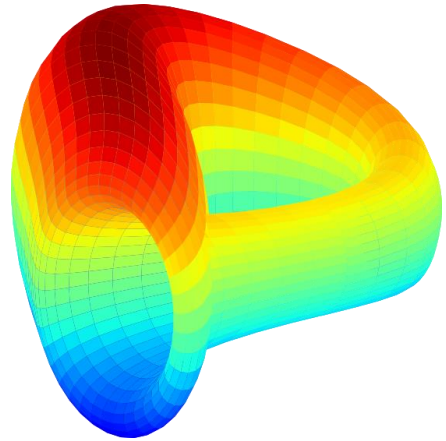
Protocol	Symbol	Price	Gross Supply	Tokens to Supply	Supply Rate	Gross Borrow	Tokens to Borrow	Borrow Rate
0x	ZRX	$0.38	$54,658,749	0	1.53%	$15,671,500	0	11.14%
Augur	REP	$13.64	$4,260,620	0	0.00%	$62,140	0	2.47%
Basic Attention Token	BAT	$0.21	$12,221,638	0	0.04%	$333,160	0	2.81%
DAI	DAI	$1.01	$1,057,237,206	0	2.88%	$818,013,564	0	3.94%
Ether	ETH	$341.42	$289,558,589	0	0.31%	$31,788,809	0	3.15%

Use Case #5: Yield Farming

- Shopping your tokens to improve APY
- Platform Example: Yearn.finance



Use Case #6: Exchanges



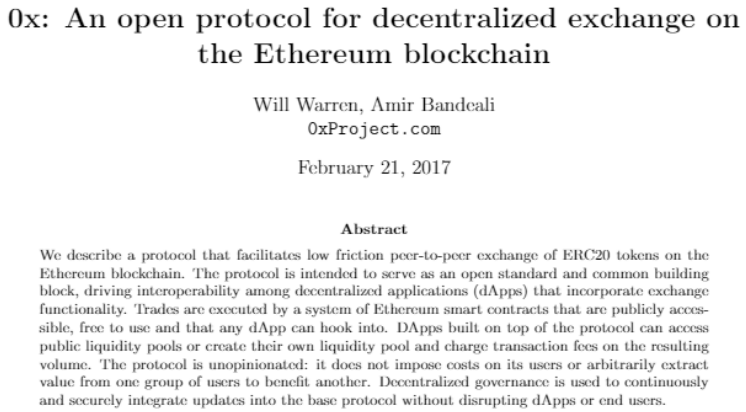
- Centralized
  - Coinbase, Gemini, Binance, etc.
- Decentralized – DEX
  - IDEX (“semi” decentralized)
  - 0x Protocol
  - **Problematic!**
- Decentralized – AMM
  - Uniswap
  - Curve
- Maximize liquidity, minimize slippage and price impact

DEX

- No single global limit order book
  - Core of a centralized exchange
  - On-chain order book? Constant Function Market Makers? (CFMM)
- Makers
- Takers
- 0x (ZRX) Protocol and 0x Relays
- Pairs are swapped or traded

0X

- Off-chain search and matching
- On-chain settlement
- Relays are pools of **makers** and **takers**
- Relays communicate with other relays
- ZRX awarded to relays



0x: An open protocol for decentralized exchange on the Ethereum blockchain

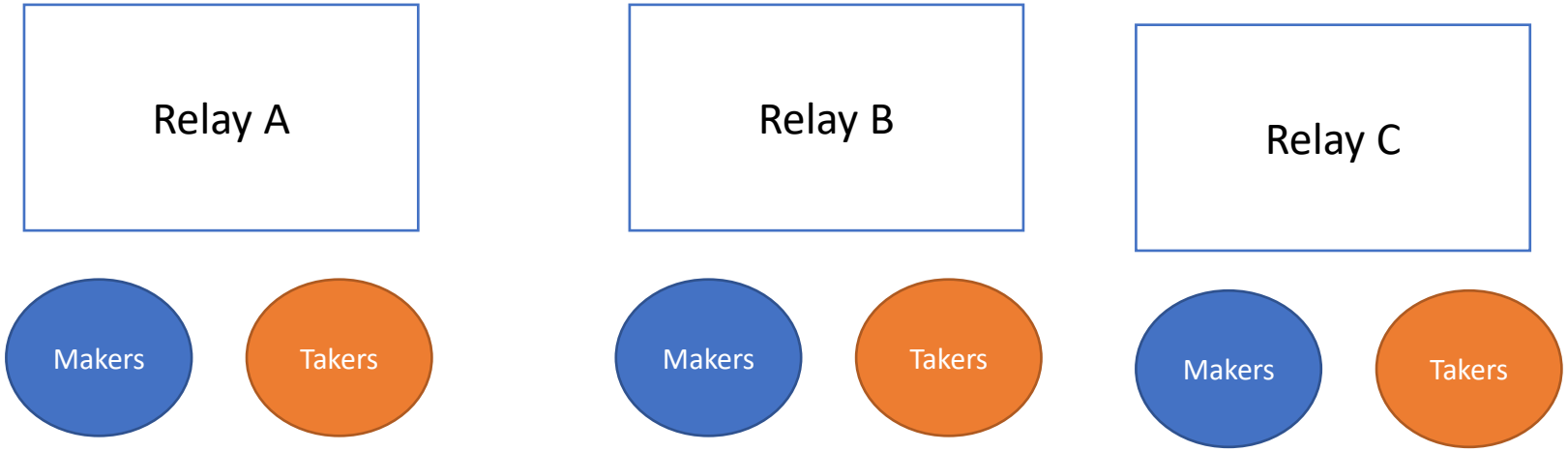
Will Warren, Amir Bandeali
0xProject.com

February 21, 2017

Abstract

We describe a protocol that facilitates low friction peer-to-peer exchange of ERC20 tokens on the Ethereum blockchain. The protocol is intended to serve as an open standard and common building block, driving interoperability among decentralized applications (dApps) that incorporate exchange functionality. Trades are executed by a system of Ethereum smart contracts that are publicly accessible, free to use and that any dApp can hook into. DApps built on top of the protocol can access public liquidity pools or create their own liquidity pool and charge transaction fees on the resulting volume. The protocol is unopinionated: it does not impose costs on its users or arbitrarily extract value from one group of users to benefit another. Decentralized governance is used to continuously and securely integrate updates into the base protocol without disrupting dApps or end users.

1



Radar Relay | Wallet to Wallet To

radarrelay.com/index.html

RELAY

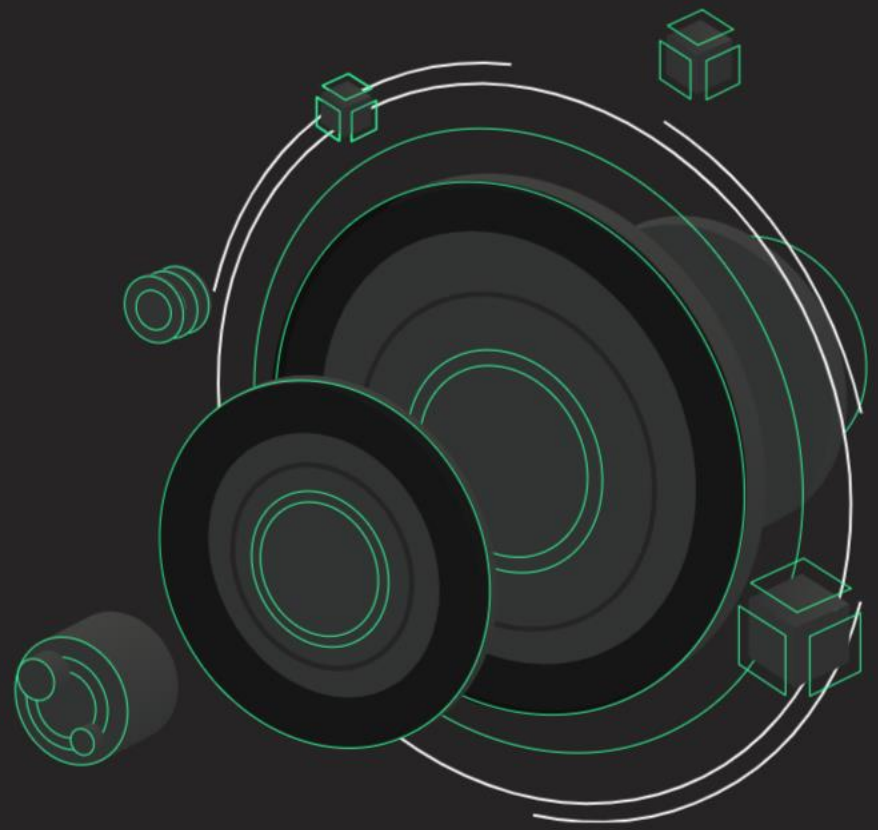
EN

OPEN APP

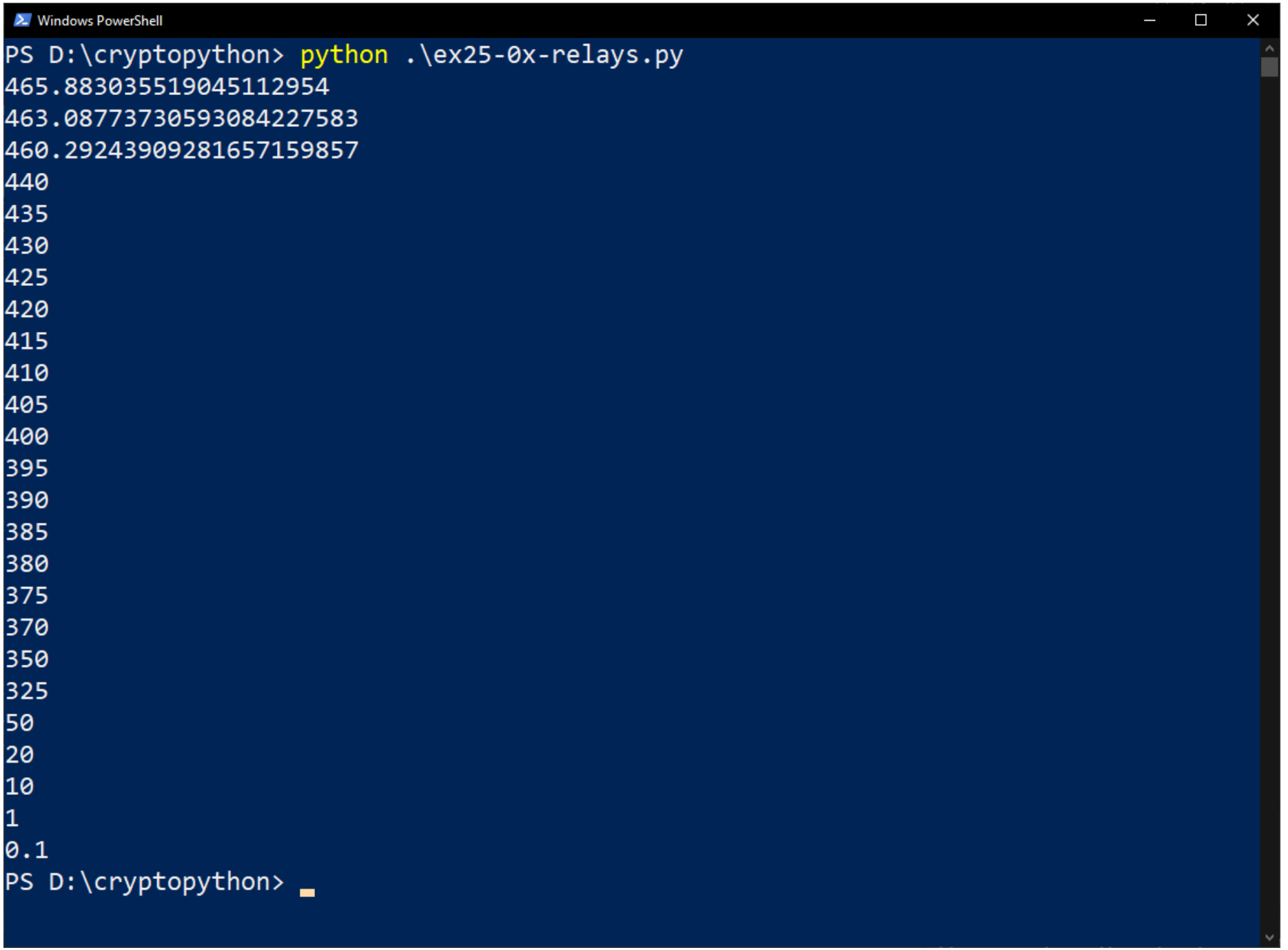
Wallet to Wallet Token Trading

The most secure way to trade ERC20 tokens directly from your Ethereum wallet.

OPEN APP



```
r = requests.get('https://api.radarrelay.com/v3/markets/WETH-DAI/book')
bat_weth_order_book = json.loads(r.text)
for bids in bat_weth_order_book['bids']:
        print(bids['price'])
```


Windows PowerShell
PS D:\cryptopython> python .\ex25-0x-relays.py
465.883035519045112954
463.08773730593084227583
460.29243909281657159857
440
435
430
425
420
415
410
405
400
395
390
385
380
375
370
350
325
50
20
10
1
0.1
PS D:\cryptopython>

Use Case #7: Prediction Markets

- Use of conditional logic
  - Will Tony Rerguson win by KO, TKO, decision against Charles Oliveira on October 12?
- Platforms
  - Augur
  - Gnosis
- Work like exchanges: Market Making
  - LMSR-AMM

The world's most accessible, no-l

bafybeidwax6qkw722zoydo643hi4fbt6xhmtsvmyz6ti765tksmyckli4y.ipfs.dweb.link/#!/markets

augur

Connect

MARKETS

Betting UI - Coming Soon!

Reporting only, trading is disabled

POPULAR CATEGORIES

- Sports
- Politics
- Entertainment
- Economics
- Crypto
- Medical

FILTERS

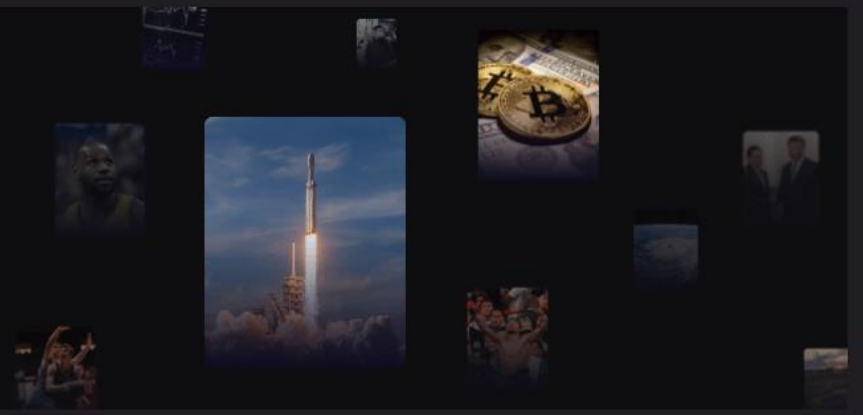
Augur

Your global, no-limit betting platform

Bet how much you want on sports, economics, world events and more.

Sign up to start trading

LEARN MORE ON AUGUR.NET



Popular Markets

Search markets

OPEN (25) IN-REPORTING RESOLVED

VIEW

SORT BY: MOST TRADED

Total Volume $98,352
Open Interest $71,201

POLITICS / US POLITICS / PRESIDENT

Event Expiration: 20 JAN 2021

Will Donald J. Trump win the 2020 U.S. Presidential election?

Yes	49.4%	No	56.9%	Invalid	0.00%

Total Volume $37,503
Open Interest $27,830

POLITICS / US POLITICS / PRESIDENT

Event Expiration: 7 JAN 2021

Will Donald Trump win the 2020 U.S. Presidential election?

Yes	45.0%	No	61.5%	Invalid	0.00%

Total Volume $10,815
Open Interest $9,700

POLITICS / US POLITICS / PRESIDENT

Event Expiration: 20 DEC 2020

Who will win the 2020 U.S. Presidential election?

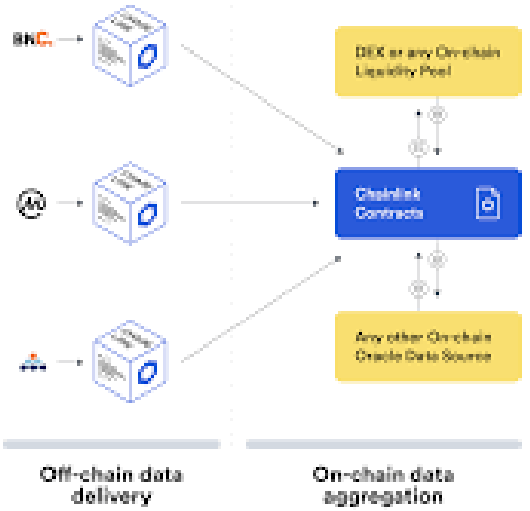
Joe Biden	50.1%	Donald Trump	46.0%	Invalid	0.00%

1 MORE OUTCOME

GLOBAL CHAT

Use Case #8: Oracles

- Need for independent external data
- Adversarial nature of blockchain and actors
- Smart contracts need to be deterministic, hence cannot access external data that is non-deterministic
- Asymmetric information



Oracles

- Centralized third-party information source (NASD, Coinbase)
- Decentralized 3rd party
- Oracle is a provider of information or market data
- Platforms
  - Chainlink
  - Provable.xyz
  - Tellor
- Uses
  - Price Feed
  - Event results (i.e. Elections)
  - Randomness (Games)

Chainlink

chain.link

Chainlink

Features Solutions Network Docs We are Hiring →

Join the Chainlink Hackathon 2020 and build the next generation of universally connected smart contracts. September 7 – 27th 2020. Register Now.

Your smart contracts connected to real world data, events and payments.

The Chainlink network provides reliable tamper-proof inputs and outputs for complex smart contracts on any blockchain.

Chainlink Reference Data →

Use Case #9: Derivatives

- Financially engineered

Uniswap

Uniswap

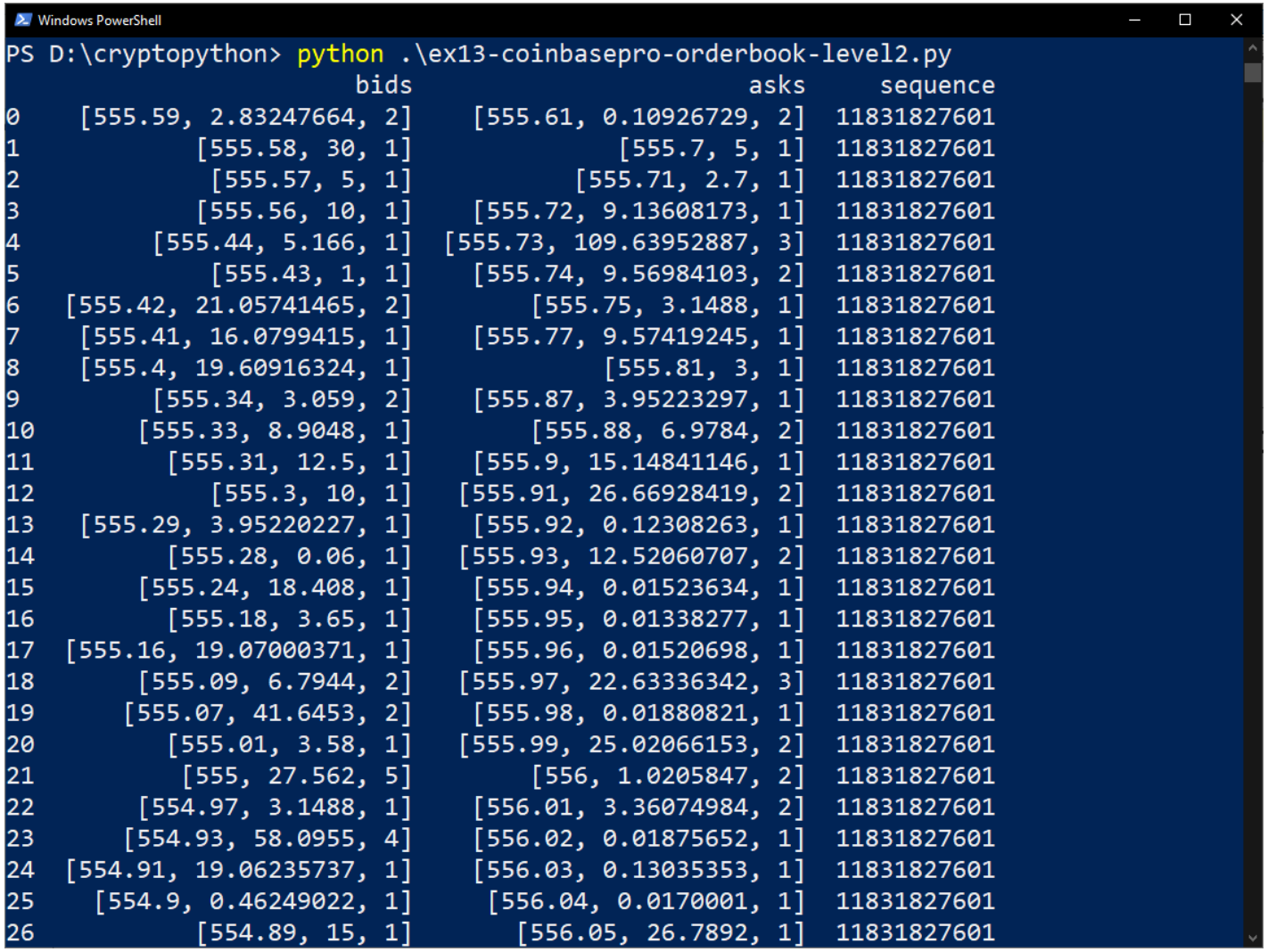
Token swapping

chainhaus

The Market Maker Problem

- Liquidity requires participants to be willing to buy and sell at certain prices
- Traditionally, this requires market makers and **limit order book**

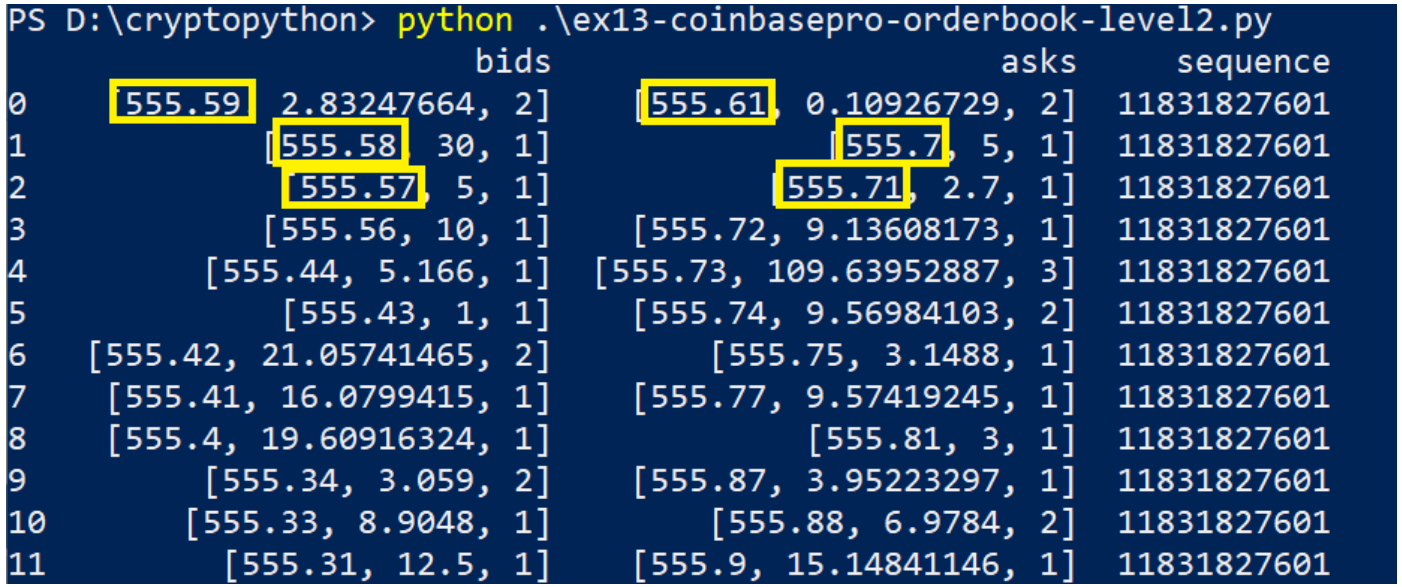
Coinbase Limit Order Book for ETHUSD



	bids	asks	sequence
0	[555.59, 2.83247664, 2]	[555.61, 0.10926729, 2]	11831827601
1	[555.58, 30, 1]	[555.7, 5, 1]	11831827601
2	[555.57, 5, 1]	[555.71, 2.7, 1]	11831827601
3	[555.56, 10, 1]	[555.72, 9.13608173, 1]	11831827601
4	[555.44, 5.166, 1]	[555.73, 109.63952887, 3]	11831827601
5	[555.43, 1, 1]	[555.74, 9.56984103, 2]	11831827601
6	[555.42, 21.05741465, 2]	[555.75, 3.1488, 1]	11831827601
7	[555.41, 16.0799415, 1]	[555.77, 9.57419245, 1]	11831827601
8	[555.4, 19.60916324, 1]	[555.81, 3, 1]	11831827601
9	[555.34, 3.059, 2]	[555.87, 3.95223297, 1]	11831827601
10	[555.33, 8.9048, 1]	[555.88, 6.9784, 2]	11831827601
11	[555.31, 12.5, 1]	[555.9, 15.14841146, 1]	11831827601
12	[555.3, 10, 1]	[555.91, 26.66928419, 2]	11831827601
13	[555.29, 3.95220227, 1]	[555.92, 0.12308263, 1]	11831827601
14	[555.28, 0.06, 1]	[555.93, 12.52060707, 2]	11831827601
15	[555.24, 18.408, 1]	[555.94, 0.01523634, 1]	11831827601
16	[555.18, 3.65, 1]	[555.95, 0.01338277, 1]	11831827601
17	[555.16, 19.07000371, 1]	[555.96, 0.01520698, 1]	11831827601
18	[555.09, 6.7944, 2]	[555.97, 22.63336342, 3]	11831827601
19	[555.07, 41.6453, 2]	[555.98, 0.01880821, 1]	11831827601
20	[555.01, 3.58, 1]	[555.99, 25.02066153, 2]	11831827601
21	[555, 27.562, 5]	[556, 1.0205847, 2]	11831827601
22	[554.97, 3.1488, 1]	[556.01, 3.36074984, 2]	11831827601
23	[554.93, 58.0955, 4]	[556.02, 0.01875652, 1]	11831827601
24	[554.91, 19.06235737, 1]	[556.03, 0.13035353, 1]	11831827601
25	[554.9, 0.46249022, 1]	[556.04, 0.0170001, 1]	11831827601
26	[554.89, 15, 1]	[556.05, 26.7892, 1]	11831827601

Eth Limit Order Book

I can sell eth at	I can buy eth at
	555.61
	555.7
555.59	**555.61**
555.58	
555.57	



Applicable to any use case

I can lend at	I can borrow at
	9%
	8%
6%	**7%**
5%	
4%	

Uniswap Protocol

- Two main functions
  - Add/remove liquidity
  - Trade (aka Swap)
- On-chain liquidity pools
- Faster matching
- Liquidity provider receives fees
- **Limit order book not required – Automated Market Making (AMM)**
- **CPMM (Constant Product Market Maker)**

Actors

- Liquidity provider
  - Puts up token pairs
  - Earns trading revenues
  - Faces **divergence** risk
- Trader
  - A swap is just a trade
  - Pays trading fees
  - You swap cash for stock when you buy equities
  - Swaps token
  - Faces **market** risk
  - i.e. Buy DAI using ETH

Exploring Constant Product Formula

- Market Prices:
  - Eth = $100
  - Dai = $1
- Example is based on
  - https://pintail.medium.com/uniswap-a-good-deal-for-liquidity-providers-104c0b6816f2

Liquidity Provider

- Initial Pool = 99 ETH, 9900 DAI
- LP provides 1 ETH, 100 DAI

Constant Product Formula

- Initial Pool = 99 ETH, 9900 DAI

$$X * Y = K$$

$$99 * 9900 = 980{,}100$$

Outcome

- Liquidity Pool is Now = 100 ETH, 1000 DAI
- LP owns 1%

	Eth Qty	Dai Qty	Mkt Value	Constant Product	Eth Liquidity	Dai Liquidity
Initial Pool	99	9900	$19,800.00	980100	99	9900
Current Pool	100	10,000	$20,000.00	1000000	100	10000

Constant Product Formula

- Liquidity Pool = 100 ETH, 10000 DAI

	Eth Qty	Dai Qty	Mkt Value	Constant Product	Eth Liquidity	Dai Liquidity
Initial Pool	99	9900	$19,800.00	980100	99	9900
Current Pool	100	10,000	$20,000.00	1000000	100	10000

$$X * Y = K$$

$$X\ (eth) * Y\ (dai)$$

$$= 100 * 10{,}000$$

$$= 1{,}000{,}000$$

Stake Valuation

- Suppose ETHDAI now = 120
- Market value of 1 eth + 100 DAI = $220
- What is LP's value?
- **1% of liquidity pool at a value such that constant product does not change**

Pool Inventory		Price							
							LP market		
Eth	Dai	Eth in terms of Dai	Dai in terms of Eth	Constant Product	Eth Liq Pool	Token Liq Pool	Eth Redemeebale	Dai Redeemable	Value
100	10000	100	0.01	1000000	100	10000	1	100	$200.00
100	10000	120	0.008333333333	1000000	91.28709292	10954.45115	0.9128709292	109.5445115	$219.09

$$X = 1{,}000{,}000 / 120$$

$$= 91.28709$$

$$1{,}000{,}000 = 91.28709 \times Y$$

$$Y = 109545.45$$

$$91.28709.. * 10954.45.. = 1{,}000{,}000$$

Pool Inventory		Price							
							LP market		
Eth	Dai	Eth in terms of Dai	Dai in terms of Eth	Constant Product	Eth Liq Pool	Token Liq Pool	Eth Redemeebale	Dai Redeemable	Value
100	10000	100	0.01	1000000	100	10000	1	100	$200.00
100	10000	120	0.008333333333	1000000	91.28709292	10954.45115	0.9128709292	109.5445115	$219.09

X * Y = K

X = sqrt(1,000,000/120) = 91.28709 * 1%

Y = sqrt(1,000,000 * 120) = 10954.45 * 1 %

91.28709.. * 10954.45.. = 1,000,000

Liquidity Provider Stake Valuation

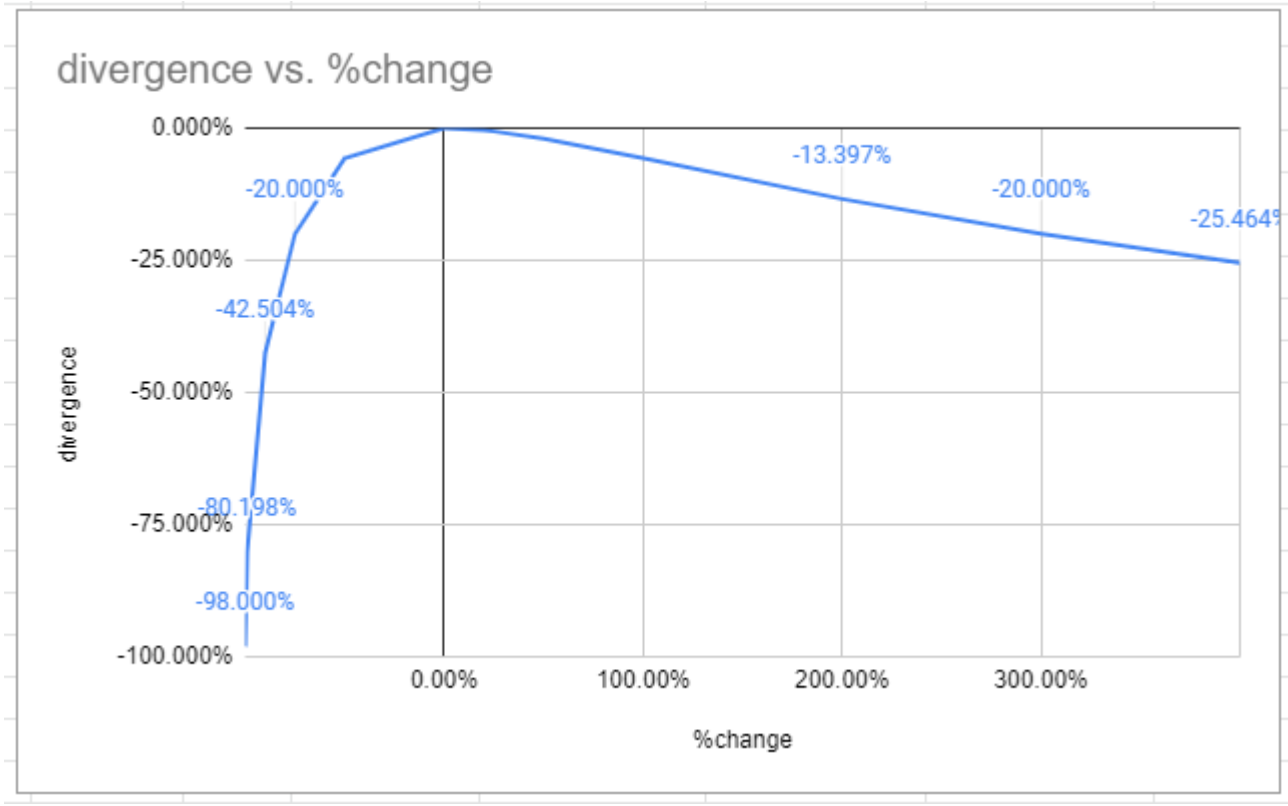
- .9128709 ETH
- 109.5445.. DAI

HODL vs. LP

- HODL = $220
- LP = $219.09
- Loss = ~ 91 cents or ~.414% loss

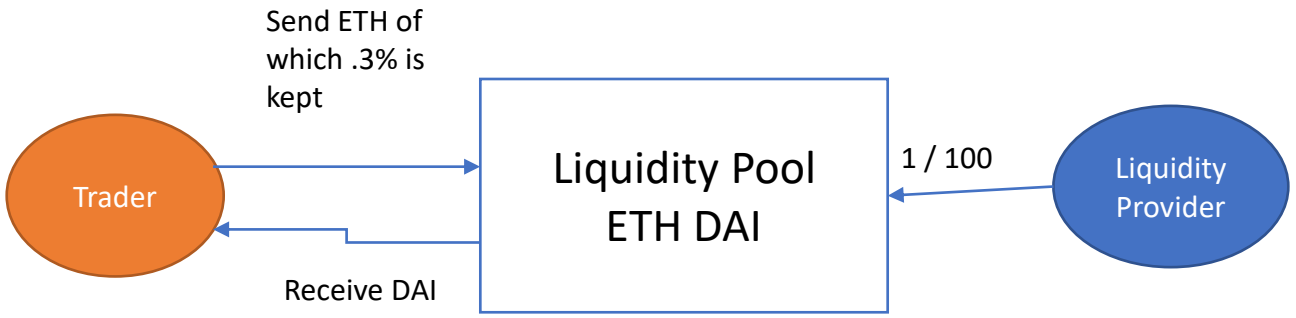
Price Swings Create Divergence Risk

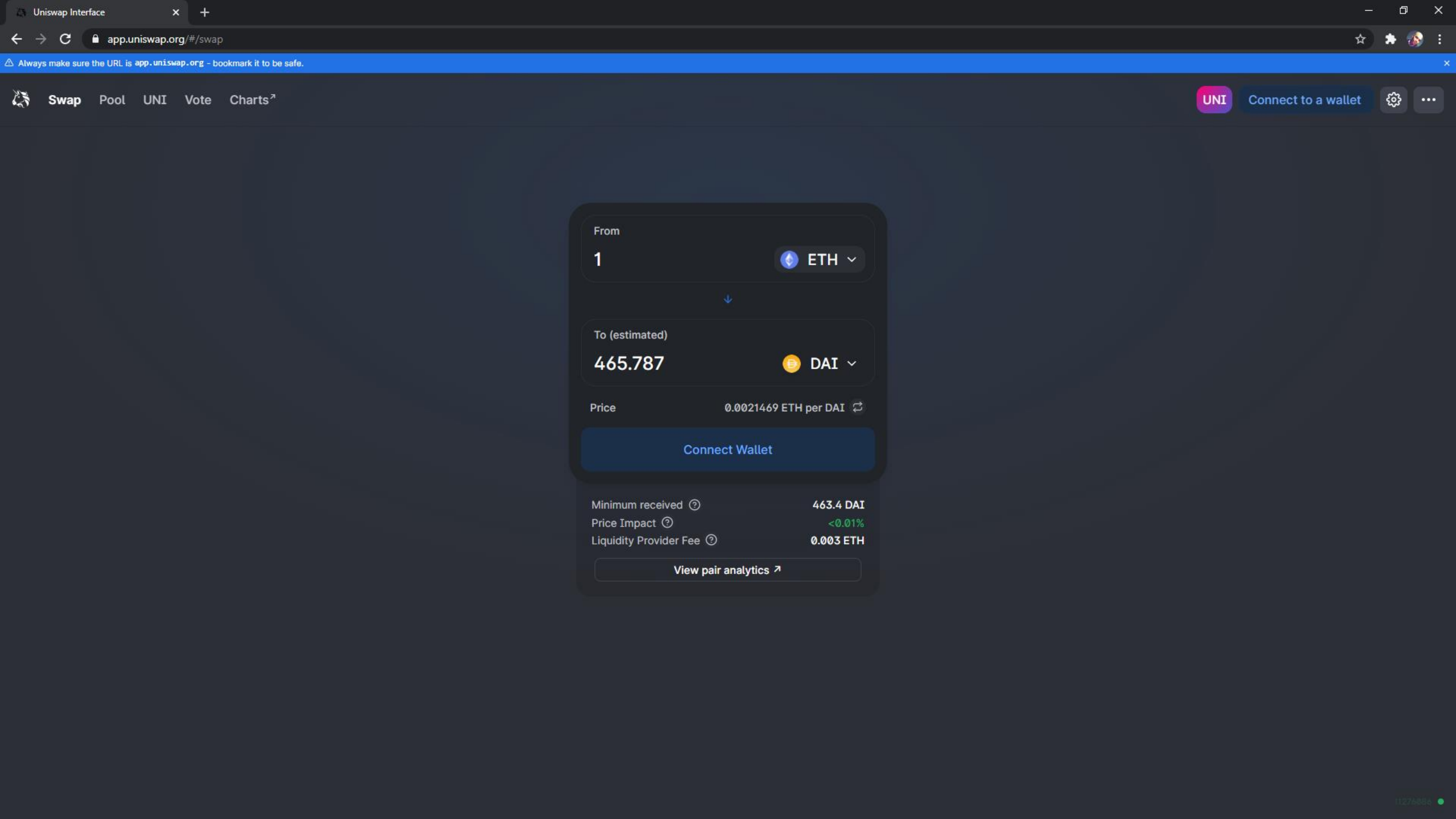
Price (p0)	Price Now	price_ratio	% Change	Divergence
100	0.01	0.00	-99.99%	-98.000%
100	1	0.01	-99.00%	-80.198%
100	10	0.10	-90.00%	-42.504%
100	25	0.25	-75.00%	-20.000%
100	50	0.50	-50.00%	-5.719%
100	100	1.00	0.00%	0.000%
100	120	1.20	20.00%	-0.414%
100	125	1.25	25.00%	-0.619%
100	150	1.50	50.00%	-2.020%
100	200	2.00	100.00%	-5.719%
100	300	3.00	200.00%	-13.397%
100	400	4.00	300.00%	-20.000%
100	500	5.00	400.00%	-25.464%

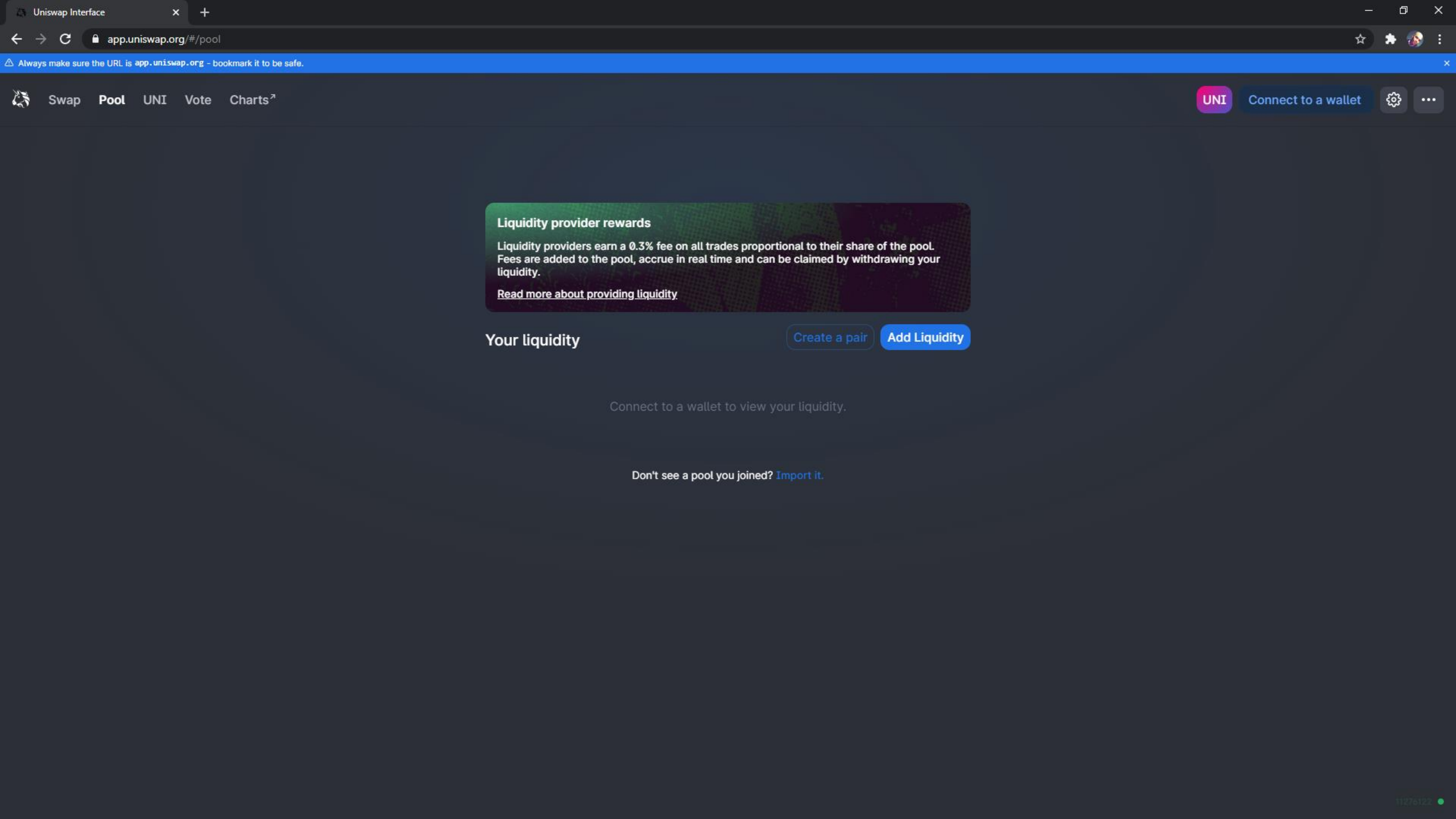


Constant Product Updates

- Updates when:
  - After liquidity added
  - After liquidity removed
  - **Trading fees added**
    - **.3% trade**




Uniswap Interface
app.uniswap.org/#/swap
Always make sure the URL is app.uniswap.org - bookmark it to be safe.
Swap
Pool
UNI
Vote
Charts
UNI
Connect to a wallet
From
1
ETH
To (estimated)
465.787
DAI
Price
0.0021469 ETH per DAI
Connect Wallet
Minimum received
463.4 DAI
Price Impact
<0.01%
Liquidity Provider Fee
0.003 ETH
View pair analytics


Uniswap Interface
app.uniswap.org/#/pool
Always make sure the URL is app.uniswap.org - bookmark it to be safe.
Swap
Pool
UNI
Vote
Charts
UNI
Connect to a wallet
Liquidity provider rewards
Liquidity providers earn a 0.3% fee on all trades proportional to their share of the pool. Fees are added to the pool, accrue in real time and can be claimed by withdrawing your liquidity.
Read more about providing liquidity
Your liquidity
Create a pair
Add Liquidity
Connect to a wallet to view your liquidity.
Don't see a pool you joined? Import it.

Financial Model Spreadsheet

- https://bit.ly/UniswapModel
- https://github.com/jamiels/uniswap-math

Uniswap Smart Contracts

- UniswapV2ERC20.sol
- UniswapV2Factory.sol
- UniswapV2Pair.sol

```
contract UniswapV2Pair is IUniswapV2Pair, UniswapV2ERC20 {
    using SafeMath  for uint;
    using UQ112x112 for uint224;

    uint public constant MINIMUM_LIQUIDITY = 10**3;
    bytes4 private constant SELECTOR = bytes4(keccak256(bytes('transfer(address,uint256)')));

    address public factory;
    address public token0;
    address public token1;

    uint112 private reserve0;           // uses single storage slot, accessible via getReserves
    uint112 private reserve1;           // uses single storage slot, accessible via getReserves
    uint32  private blockTimestampLast; // uses single storage slot, accessible via getReserves

    uint public price0CumulativeLast;
    uint public price1CumulativeLast;
    uint public kLast; // reserve0 * reserve1, as of immediately after the most recent liquidity event
```

Q&A

chainhaus

CONSENSYS

DeFi Topics & Technical Deep Dive

Comparing DeFi to existing infrastructure

Clemens Wan
Global Solutions Architect

Clemens Wan
Dec 12, 2020

What is “DeFi” - an intriguing and fertile field of innovation

Novel digital assets, registered on the Ethereum mainnet

Cryptocurrencies (~575 B$ market cap)

Utility tokens (~20 B$ market cap)

Digital company shares (a few B$ market cap)

Digital bonds (a few 100 M$ outstanding)

Stablecoins (~25 B$ outstanding)

Central bank digital currencies (just starting, immense potential)

see defimarketcap or coinmarketcap

Novel trading and lending models, based on immutable smart contracts

Automated issuance and servicing workflows, powered by smart contracts (several tens of B$ outstanding)

- Atomic issuance vs payment.
- Atomic delivery vs payment.
- Automated dividend calculation.
- Examples: World Bank, SocGen, Santander.

Decentralized exchanges (~ 1 B$ in daily trades)

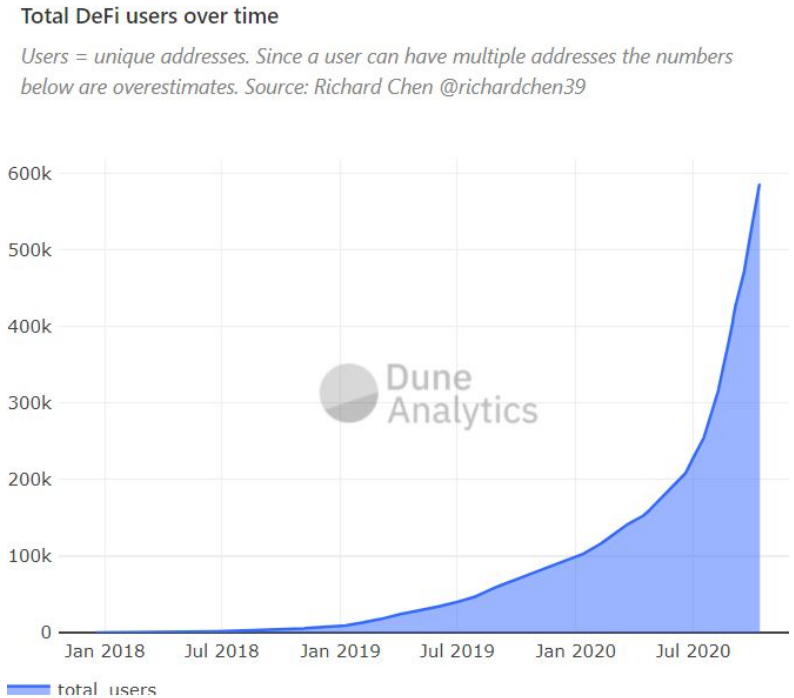
- Decentralized price formation algorithms
- Decentralized matching of buyers and sellers.
- Atomic post-trade settlement with no counterparty risk.
- Examples: ConsenSys Markets, 0x protocol, Uniswap.

Decentralized lending (~ 15 B$ outstanding)

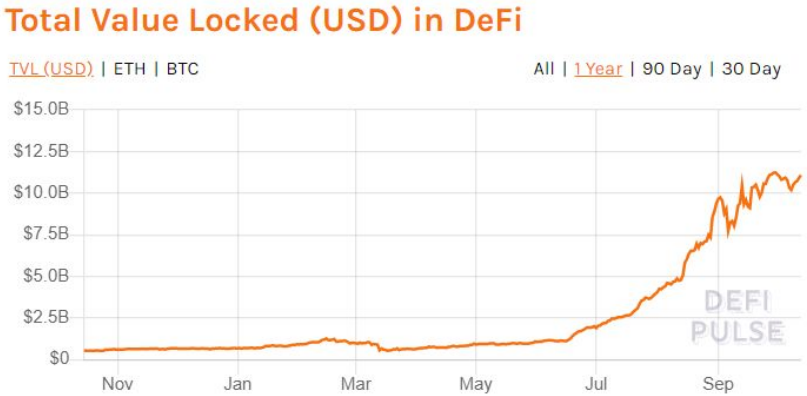
- Decentralized interest rate definition algorithms
- Decentralized matching of lenders and borrowers.
- Fully collateralized loans with no counterparty risk.
- Examples: Maker, Compound.

Almost 1MM DeFi users with $15B+ in assets

DeFi Users



Collateral Deployed



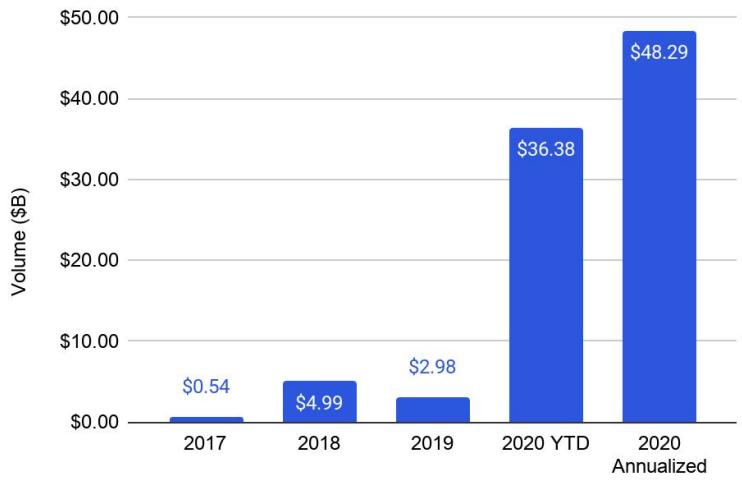
Source: Glassnode, DeFi Pulse

… and a bit of Yield Farming motivation...

- Lending (or providing liquidity) earns a yield
- Borrowing has an interest cost
- You earn 20% because someone wants to borrow it and pays 25%
- They borrow likely because they think capital appreciation will be 25%+
- Liquidity mining provides an additional incentive in the form of a protocol governance token
- This reduces the borrowing cost (25% less token reward)
- Depending on price action, borrowing cost could be negative

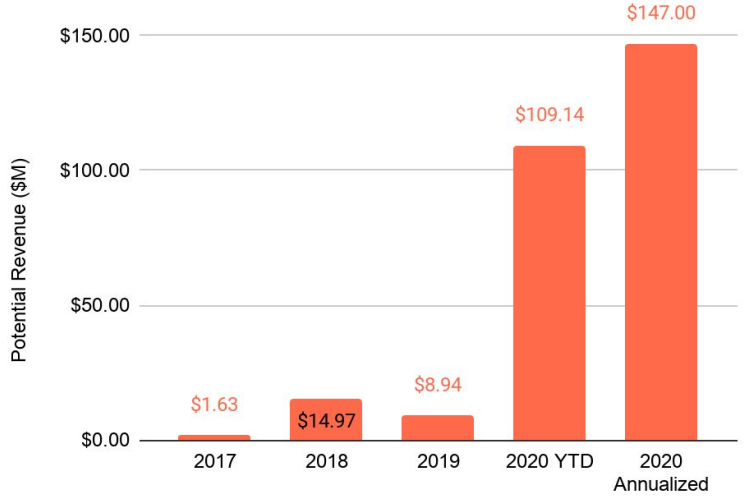
… resulting in DEX volume growing over 1,000% ….

DEX Trading Volume (USD)



YoY Growth	-	*817.3%*	*-40.3%*	*1121.1%*	*1569.3%*

DEX Potential Revenues



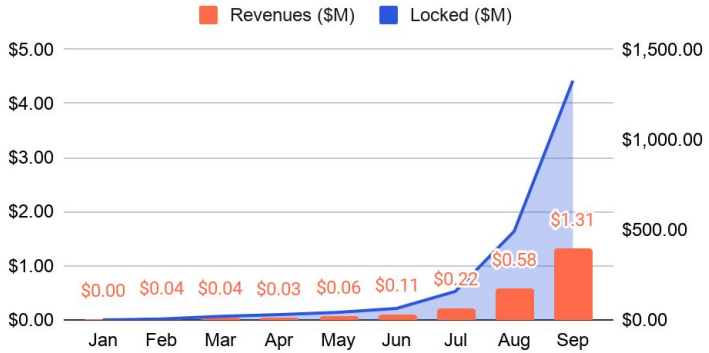
CAGR	*349.9%*

- 2020 has massive growth in DEX volume, with an annualized ~16x growth from 2019 to 2020.
- The numbers are still quite small relative to centralized exchanges. Uniswap recently overtook Coinbase in daily volume, but that is only one exchange.
- Revenue pool is split between exchanges and Liquidity Providers, with most of this revenue going to the latter.

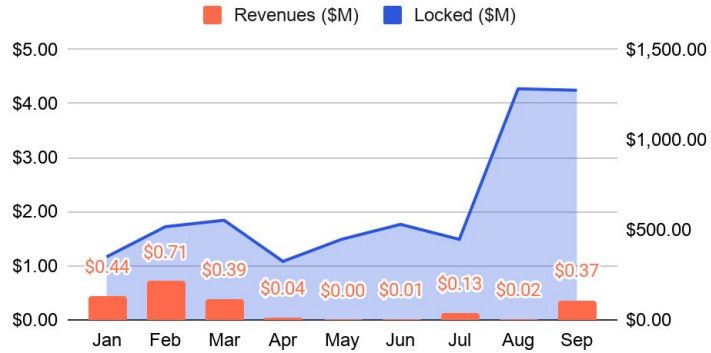
Source: Dune Analytics, various DEXes

… and Lending protocol explosive growth in Q3

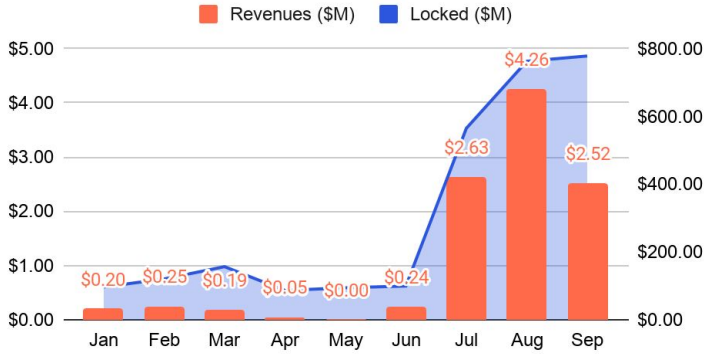
Aave



Maker



Compound

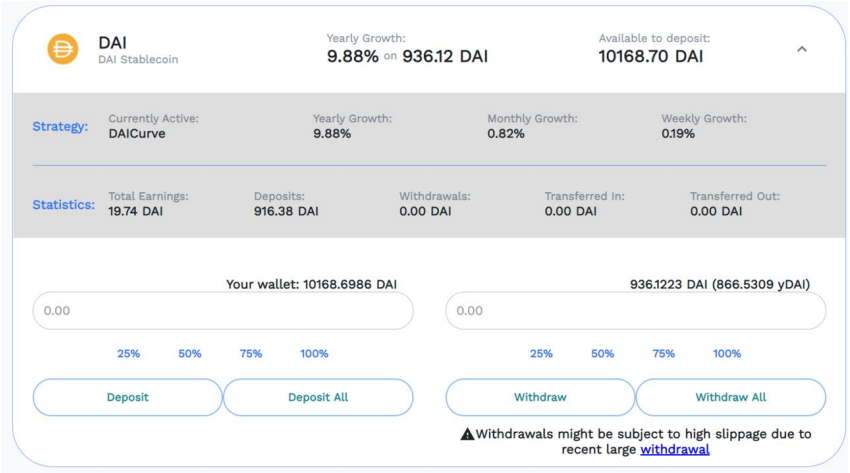


- Lending (esp. money market) protocols account for 38% of the TVL in Ethereum.
- 98% of Lending TVL is concentrated in the top 5 protocols, of which 87% is in the top 3 - Aave, Maker, Compound.
- TVL has grown ~650% since January this year.
- Total estimated revenues in 2020 (annualized) of ~$23M

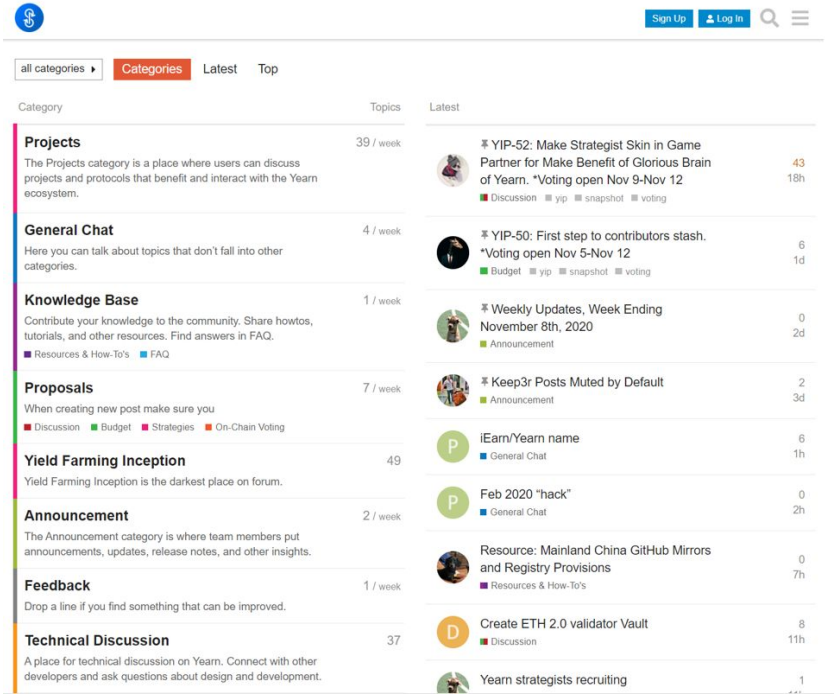
Source: Defi Pulse, Token Terminal

Packaged Financial Instruments (e.g., active fixed income funds)

Fund Interface



Governance



Important distinction between the protocol and the asset class

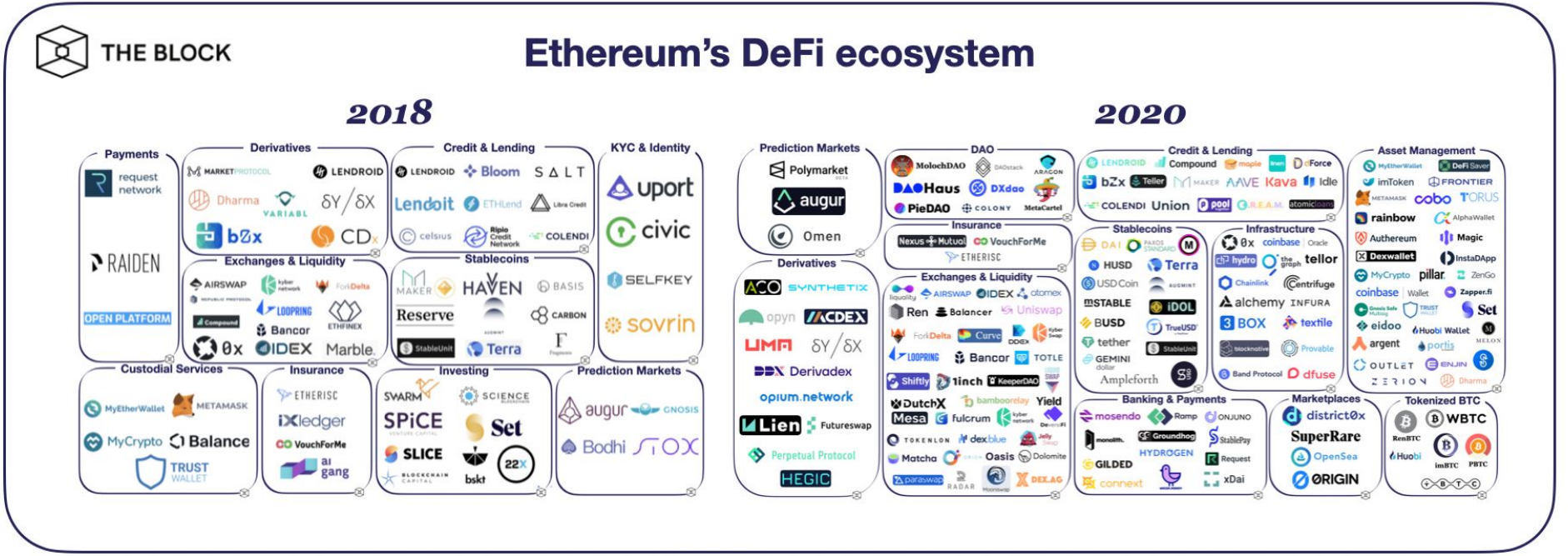
Asset

#	Name	Market Cap
1	Compound Dai Compound	$1,016,466,965
2	Dai MakerDAO	$901,705,006
3	Wrapped BTC Bitcoin	$836,099,140
4	Yearn.finance Yearn.finance • Vaults	$715,432,873
5	Curve Y Pool Curve	$627,026,100
6	EthLend Token Aave	$613,021,811
7	UMA Voting Token v1 ERC20	$556,873,183
8	Synthetix Network Token Synthetix	$530,002,960
9	Maker MakerDAO	$443,963,538
10	Compound Compound	$436,049,032
11	Uniswap WBTC/ETH Pool Uniswap V2	$418,801,032
12	Uniswap ETH/USDT Pool Uniswap V2	$397,558,769
13	Uniswap USDC/ETH Pool Uniswap V2	$358,022,379
14	Compound Ether Compound	$340,874,767
15	Uniswap Uniswap V2	$328,713,420

Protocol

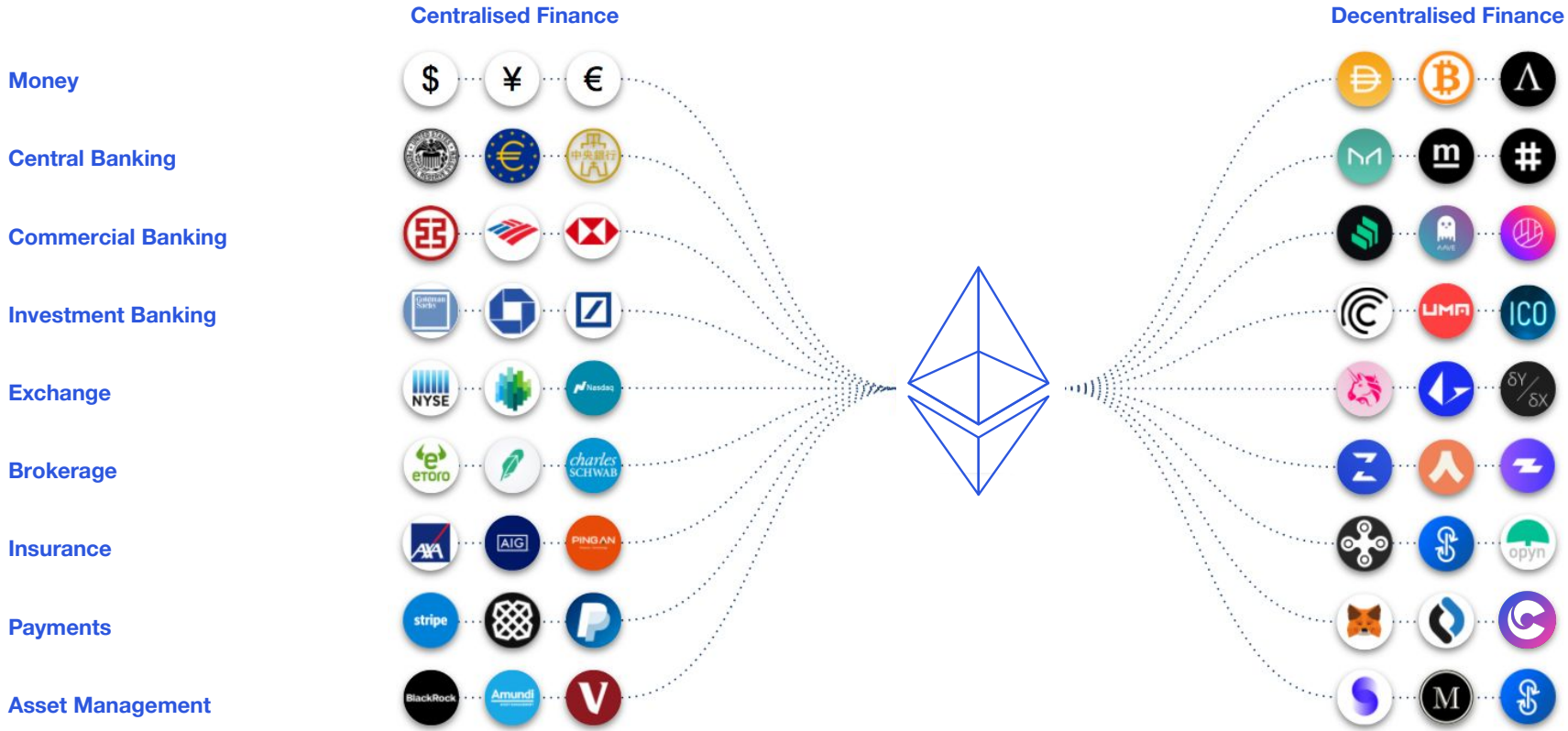
DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
1.	Maker	Ethereum	Lending	$1.89B	1.46%
2.	Uniswap	Ethereum	DEXes	$1.87B	5.55%
3.	Aave	Ethereum	Lending	$1.36B	1.97%
4.	Curve Finance	Ethereum	DEXes	$1.29B	1.35%
5.	WBTC	Ethereum	Assets	$889.8M	9.09%
6.	yearn.finance	Ethereum	Assets	$837.4M	3.31%
7.	Compound	Ethereum	Lending	$761.9M	6.68%
8.	Synthetix	Ethereum	Derivatives	$598.8M	-0.87%
9.	Balancer	Ethereum	DEXes	$435.5M	5.74%
10.	SushiSwap	Ethereum	DEXes	$434.5M	-0.85%
11.	RenVM	Ethereum	Assets	$247.7M	3.78%
12.	C.R.E.A.M. Finance	Ethereum	Lending	$215.5M	3.44%
13.	InstaDApp	Ethereum	Lending	$164.4M	0.94%
14.	Flexa	Ethereum	Payments	$149.1M	-5.61%
15.	Nexus Mutual	Ethereum	Derivatives	$68.6M	3.96%

DeFi replicates financial services on trustless infrastructure

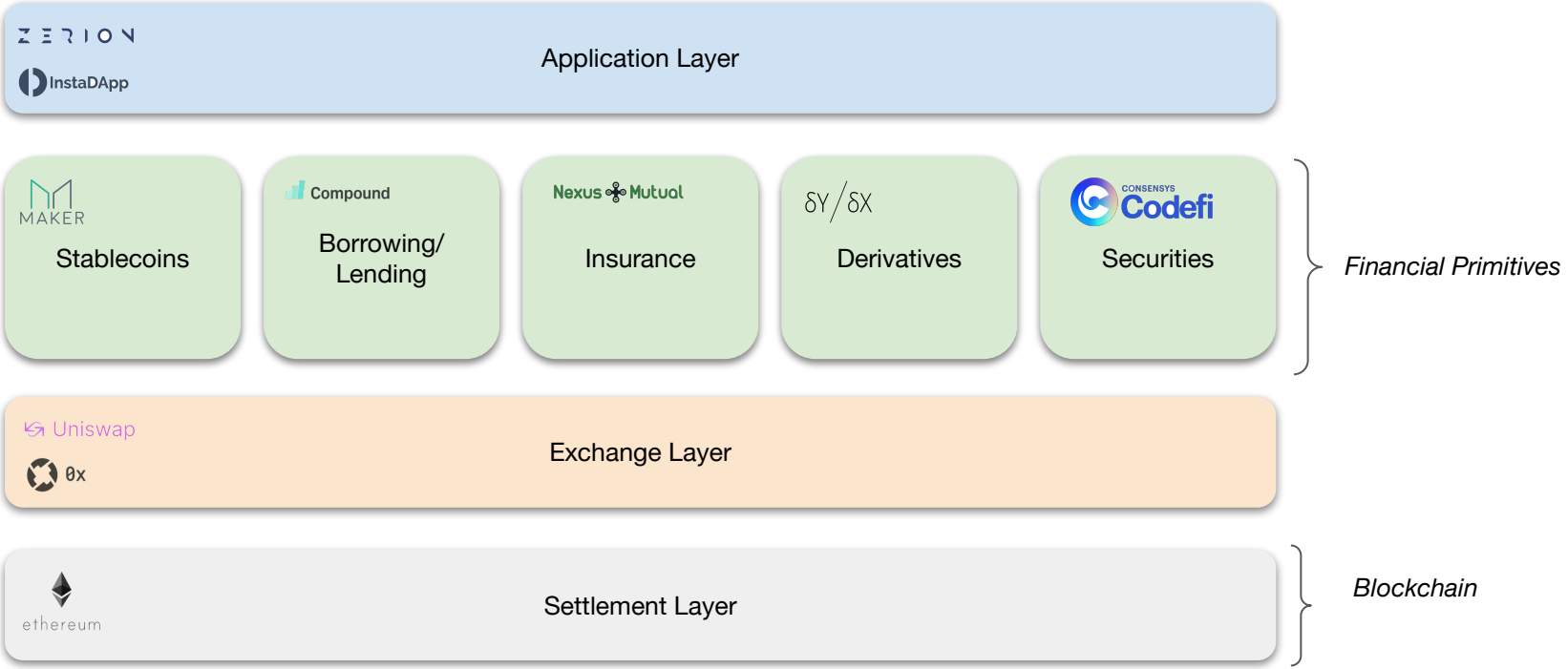


Source: The Block

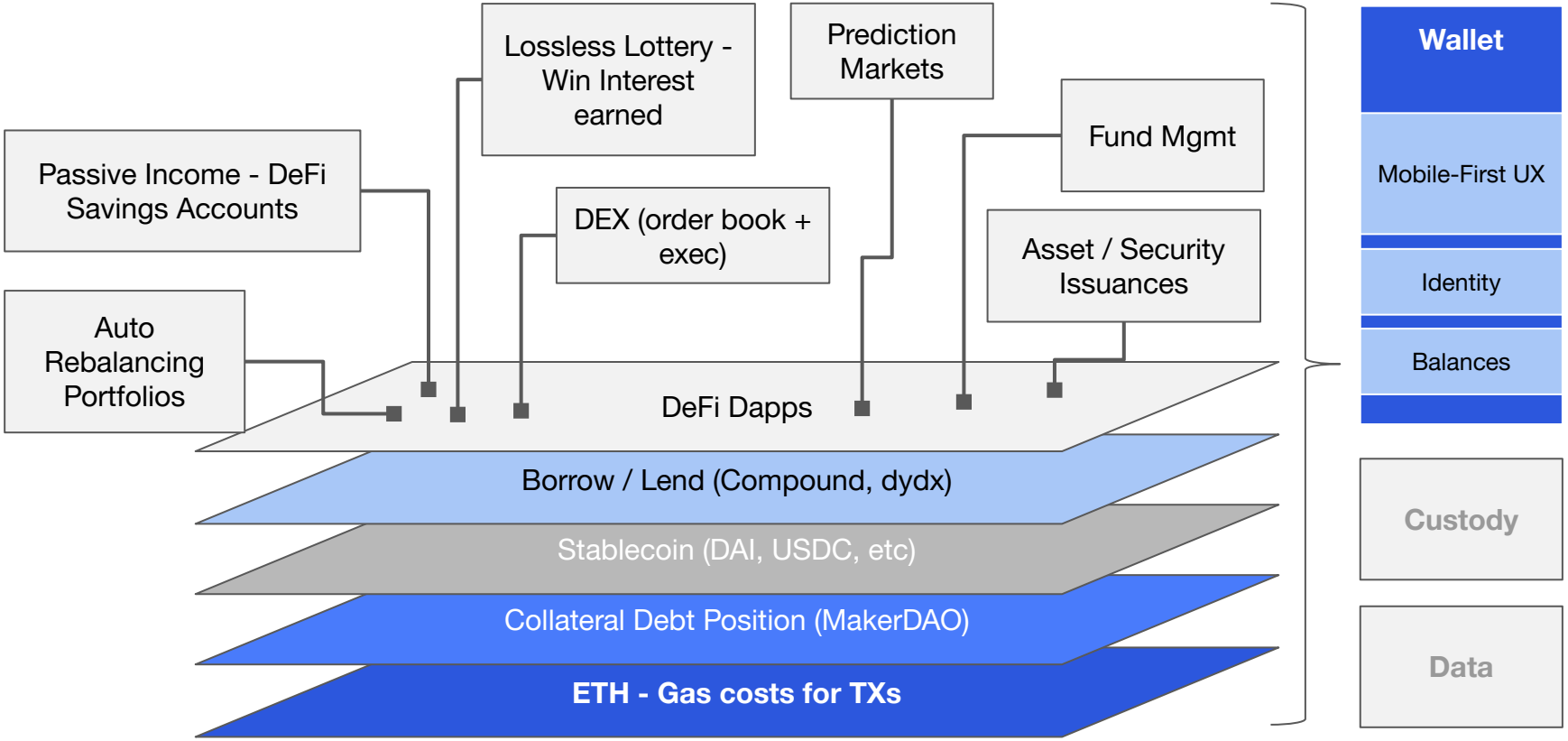
Protocols for every financial instrument and function



The DeFi Stack: a set of building blocks for the new financial age

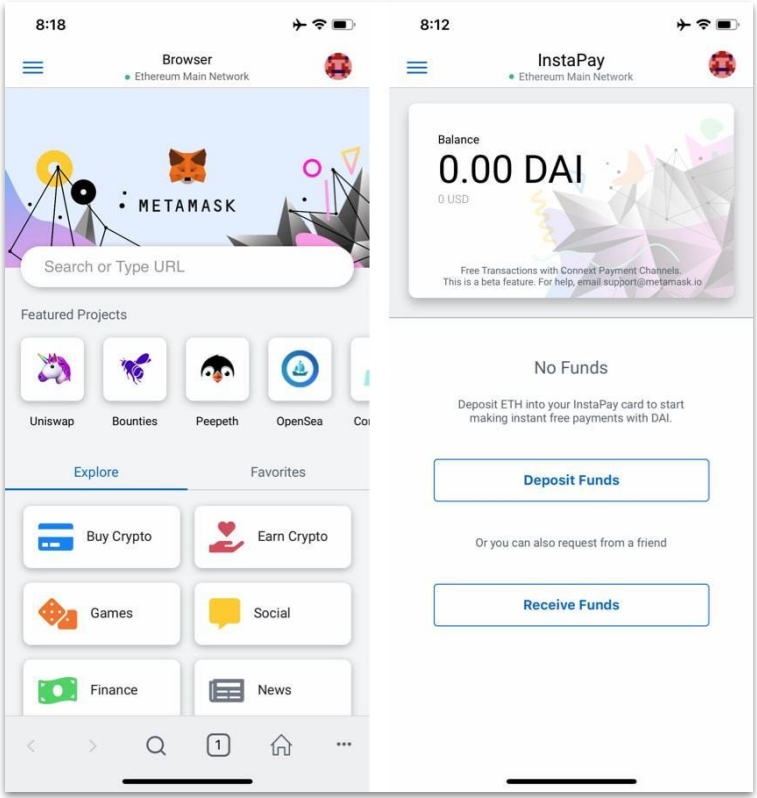


Enabled DeFi design patterns



Payments processing – tech for making a payment

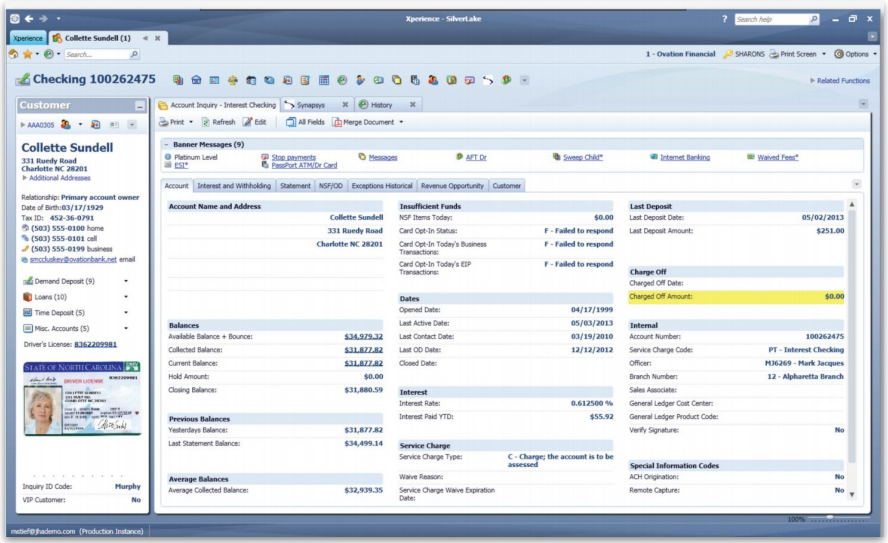
Worldpay - $35 Billion

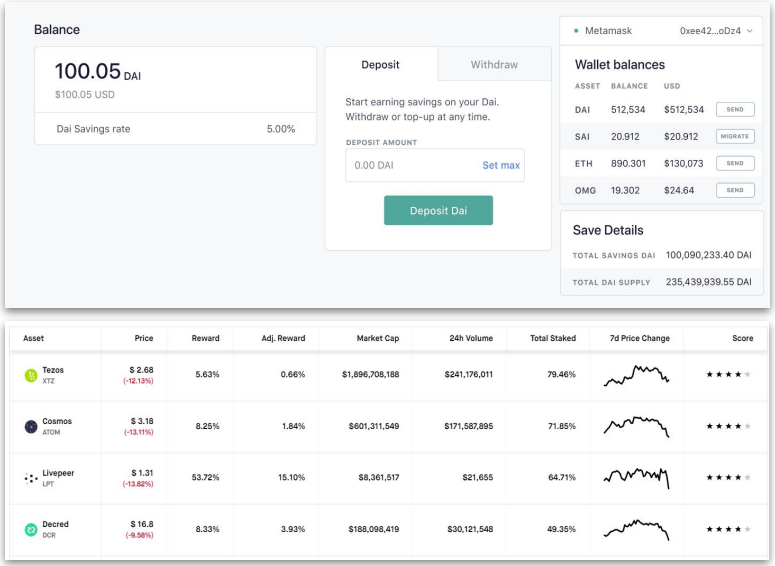


Source: Company websites

Core Banking – tech for deposits and savings

Jack Henry - $15 Billion

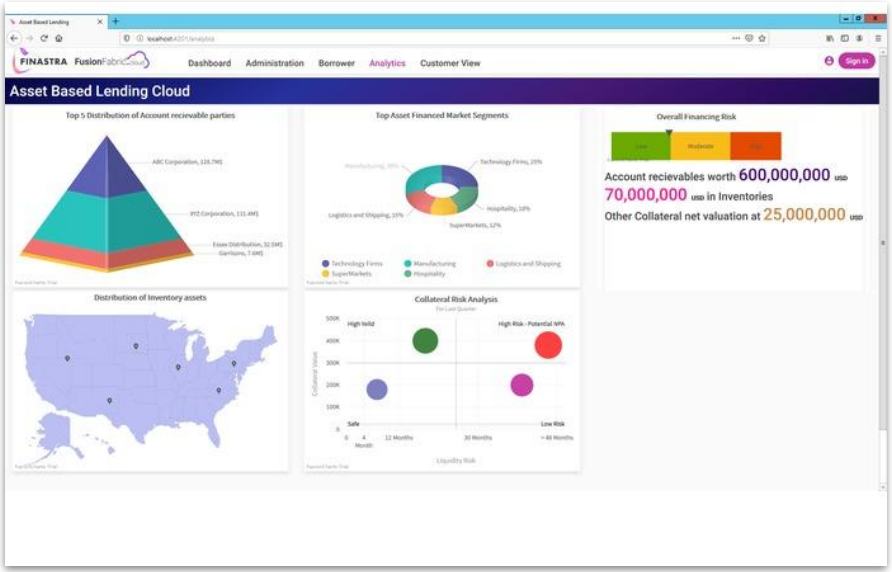


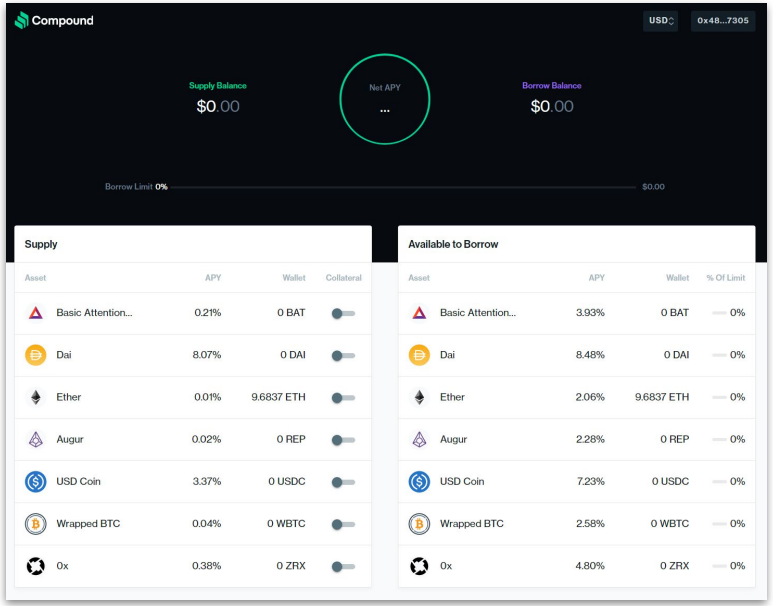


Source: Company websites, StakingRewards

Lending / underwriting – tech for managing loan books

Finastra - $5 Billion

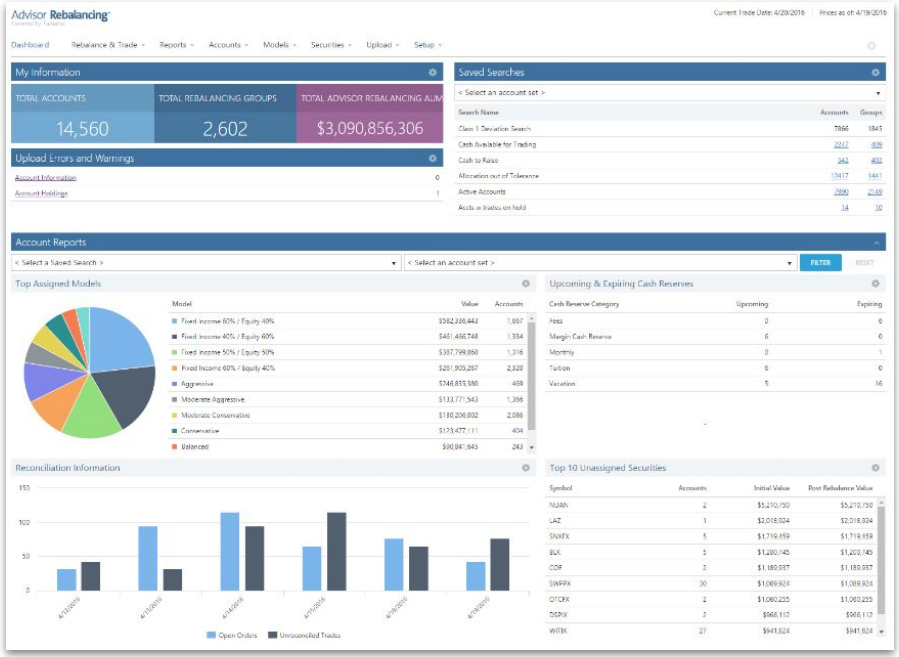


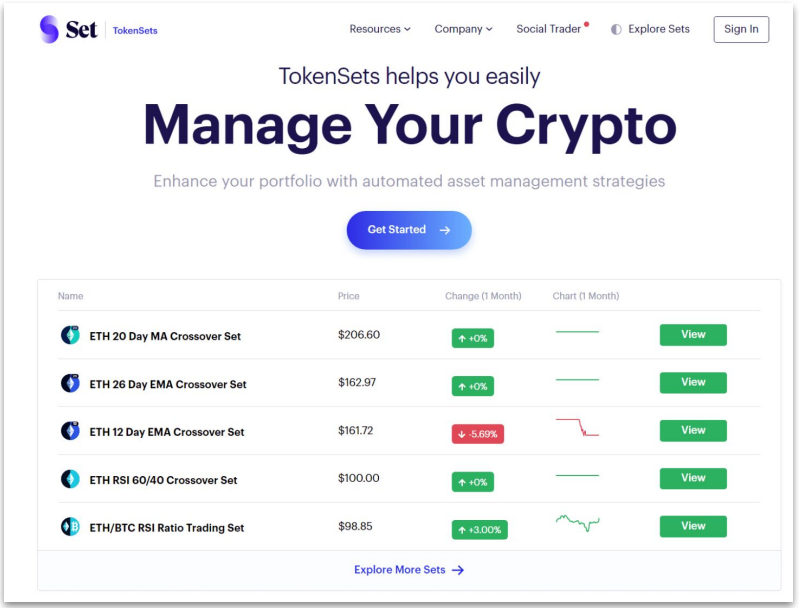


Source: Company websites, StakingRewards

Wealth Management – tech for trading and rebalancing

Envestnet – $4 billion

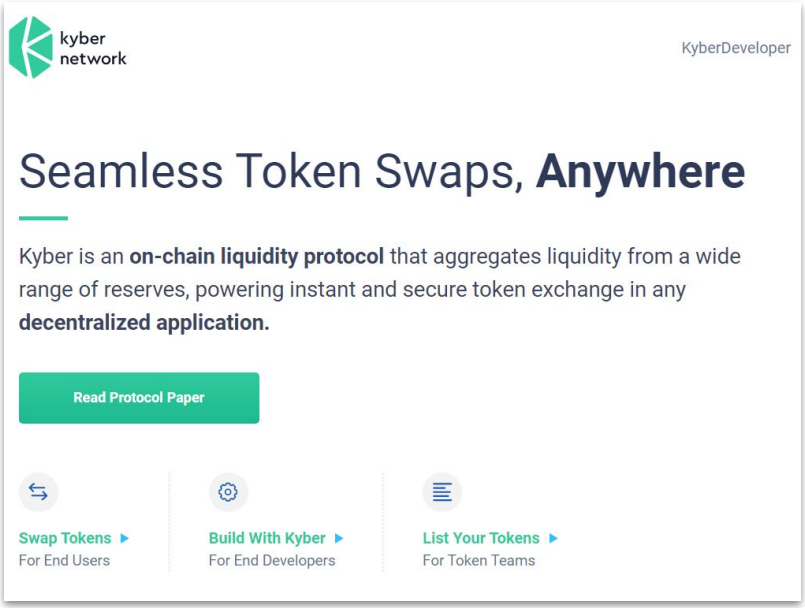




Source: Company websites,

Exchange & Clearing - tech and markets for asset exchange

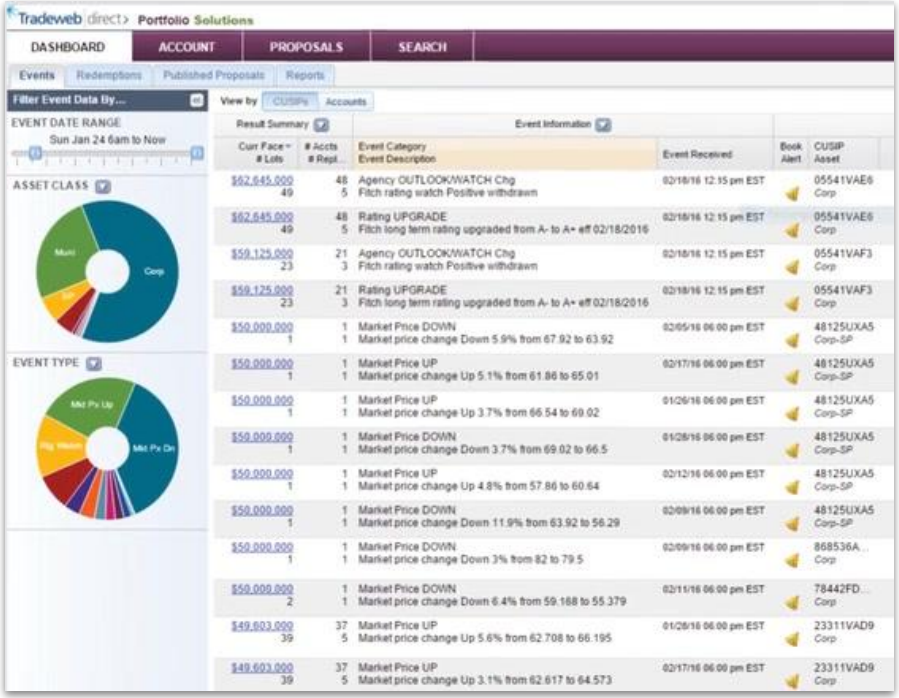
Nasdaq – $20 billion

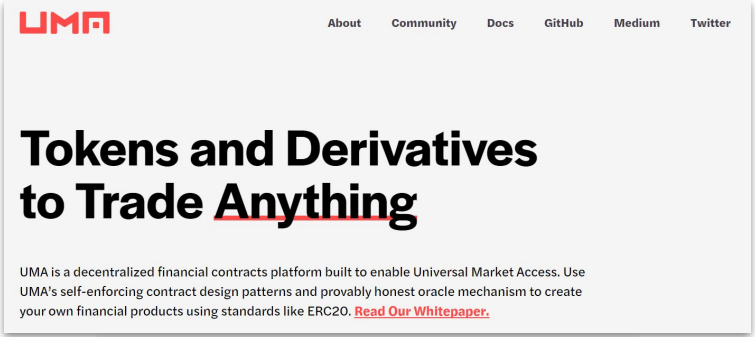


Source: Company websites,

Derivatives - tech and markets for derivative exposure

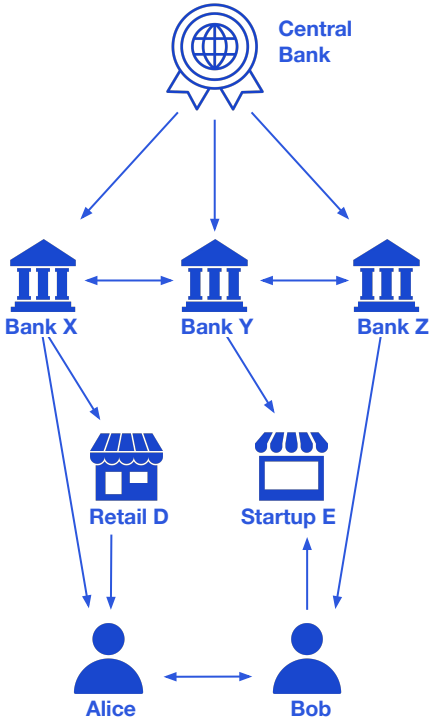
Tradeweb – $12 billion

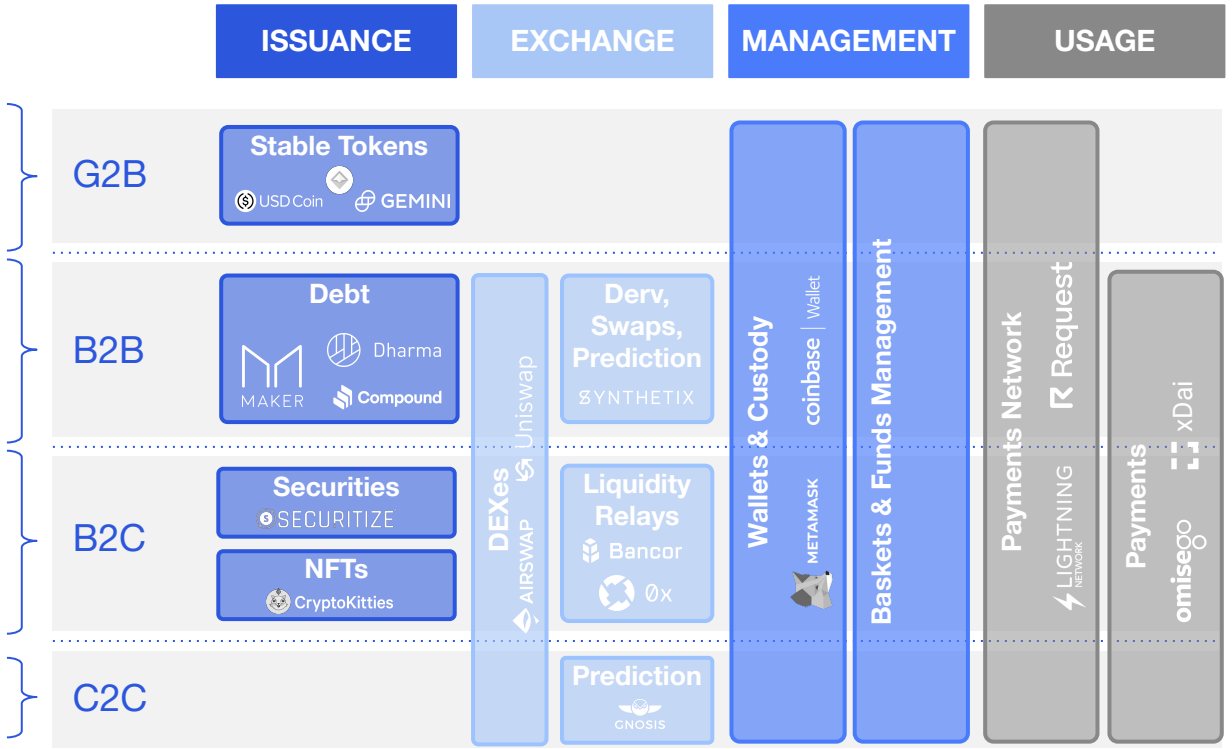




Source: Company websites, StakingRewards

Learning from DeFi: adoption is all about the ecosystem

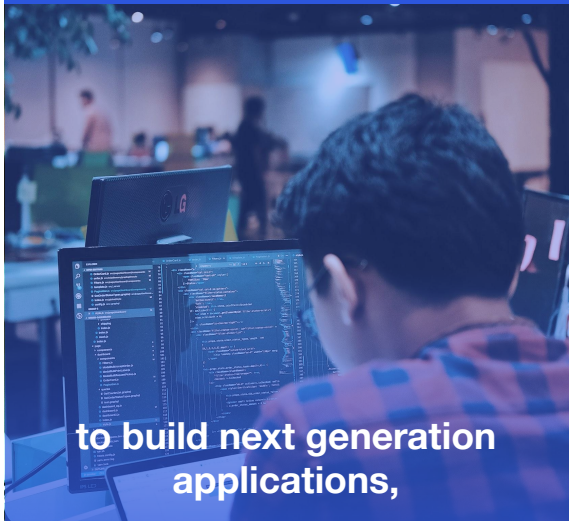




ConsenSys is the leading Ethereum software company

We enable

Developers,



Enterprises,

and people worldwide,

Using our market-leading product suite

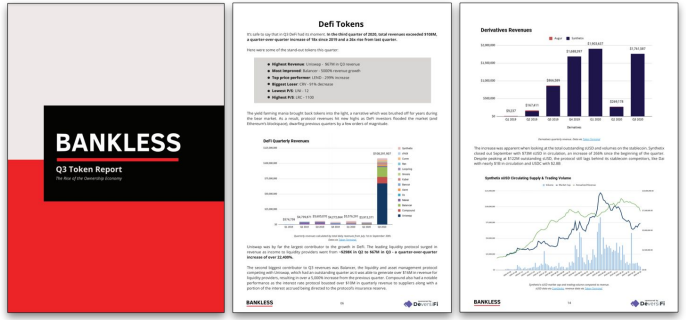
TRUFFLE | INFURA | CONSENSYS Codefi | CONSENSYS Quorum | METAMASK

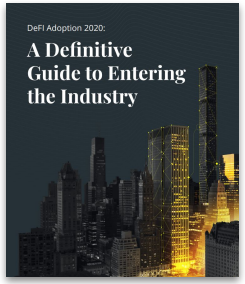
Additional Useful Resources

DeFi data points

- DeFi Total Value Locked (**Protocol level**) on defipulse
- DeFi Marketcap (**Assets level**) on defimarketcap
- Another look at token projects on Token Terminal
- DeFi lending/borrowing rates on defirate

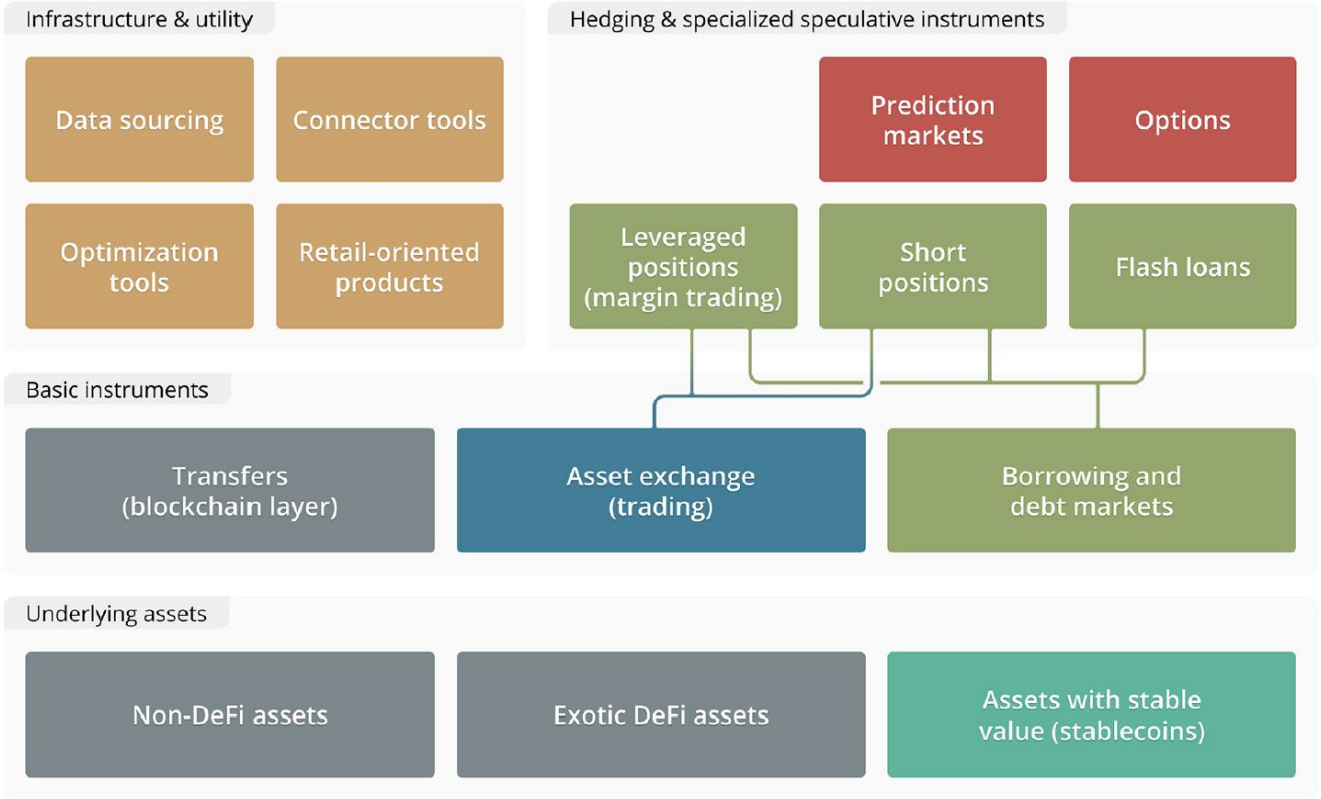
Token Reports



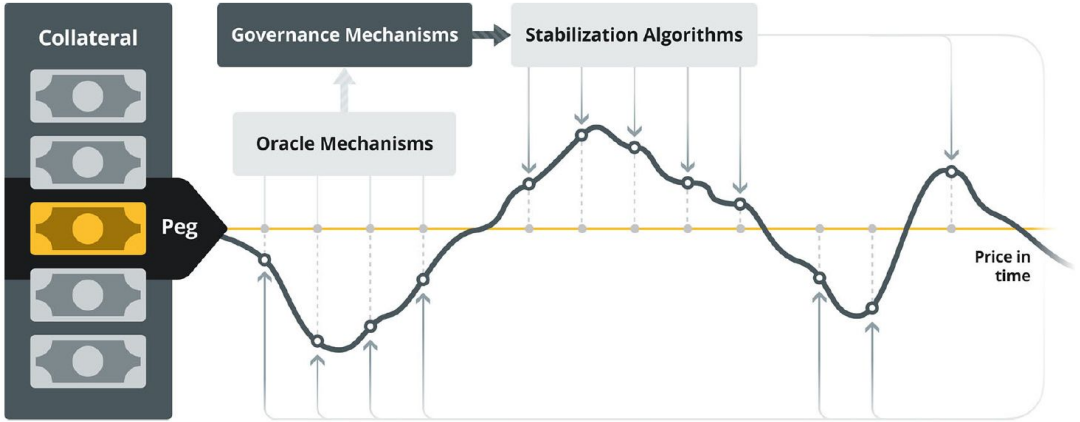


Case Study: Makerdao

DeFi Protocol Patterns



Underlying Assets: Stablecoins (CDP model)



A stablecoin is supported with three key components: oracle mechanisms that feed the market prices into the system, governance mechanisms that adjust the system's parameters in response to market events, and stabilization algorithms that adjust incentives for market participants to affect the stablecoin price and push it towards the peg.

Collateralized Debt Position (CDP) Model

MAKER

Maker.DAO uses pure form of a CDP Stablecoin.

DAI created when user locks collateral into CDP. CDP is open for anyone. Owner of CDP can borrow stablecoins from or redeem them to get their collateral back.

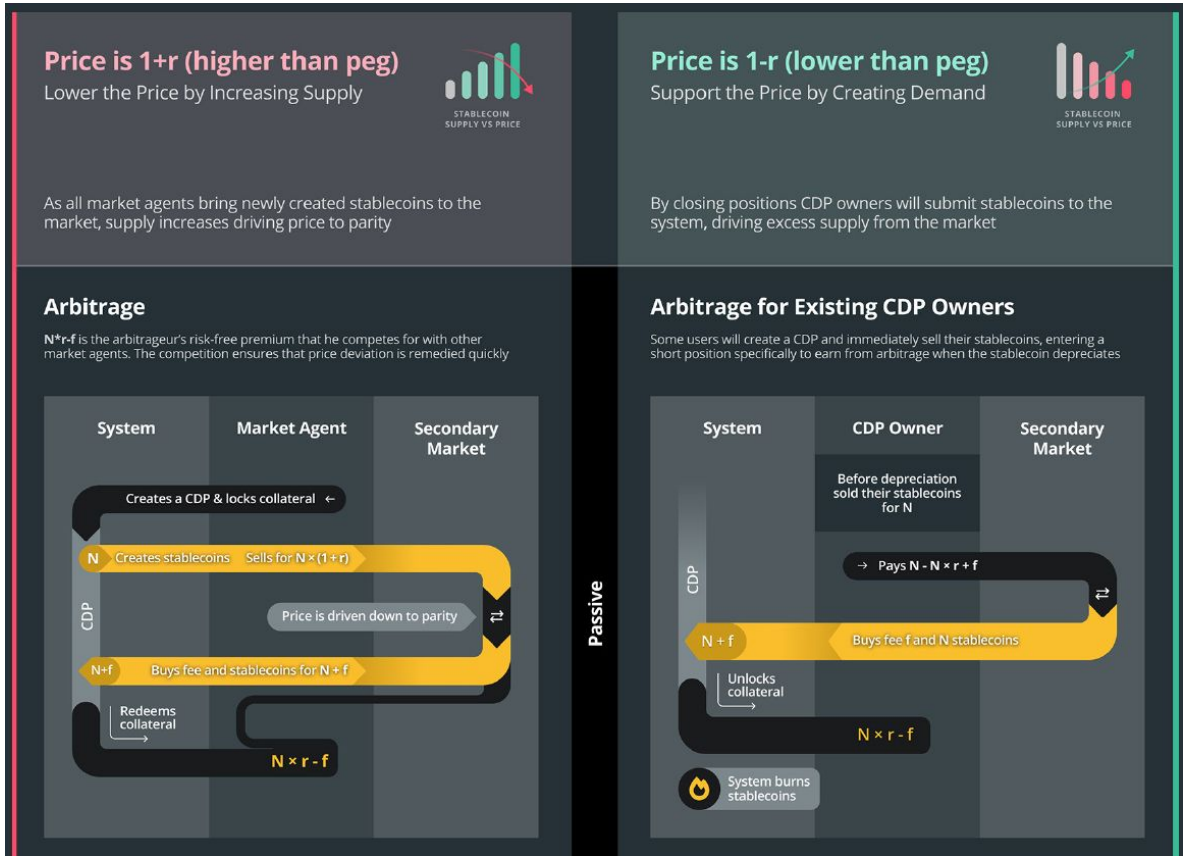
Since stablecoins are considered debt, the accrued interest rate (stability fee) is revenue distributed to platform stakeholders and insurance pools

SYNTHETIX

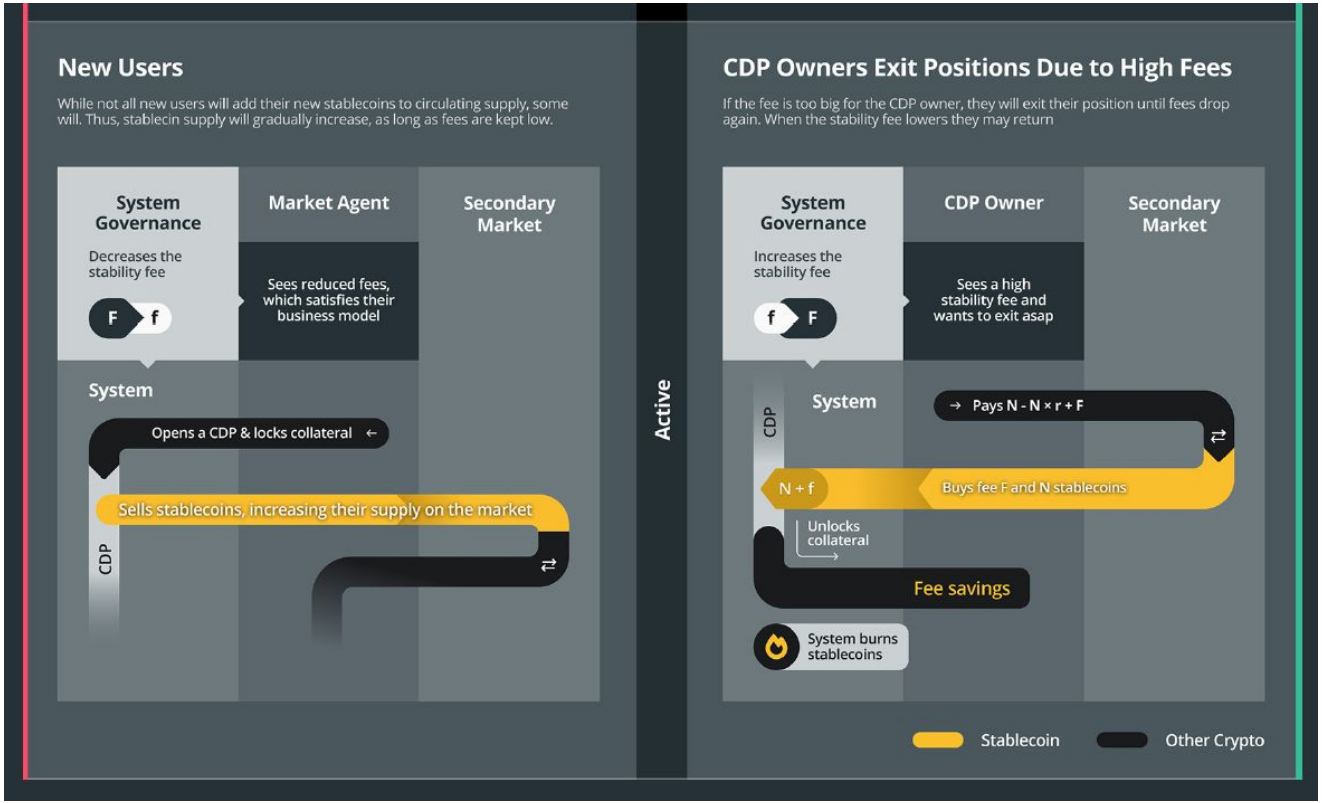
CDP owners issue multiple types of synthetic assets from the same collateralized position. Synthetics follow the price movements of assets they mirror (via oracle price feeds), but can be converted to other synthetics or burned at will with zero slippage and no need of a counterparty.

Staking is needed to obtain SNX. Then you can issue assets such as sUSD, sEUR, sETH or sBTC representing exposure to various markets. There are stable synths and volatile synths.

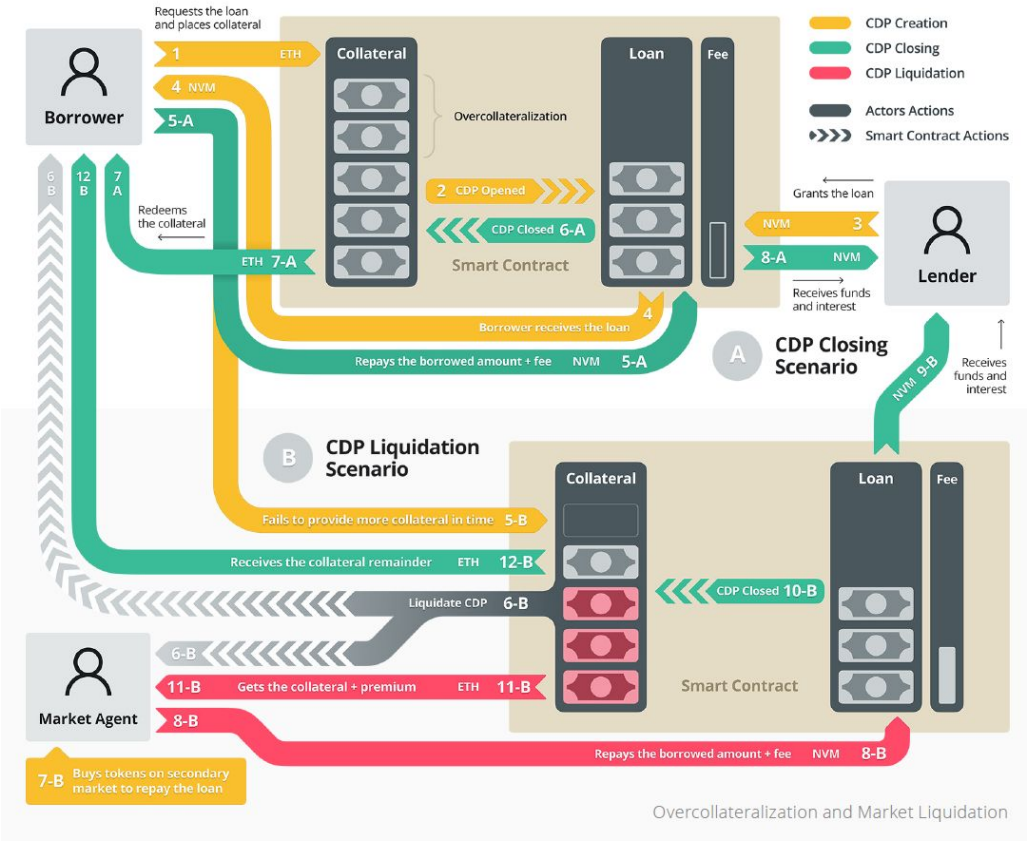
Stabilization Mechanisms: CDP (Passive & Active Incentives)



Stabilization Mechanisms: CDP (Passive & Active Incentives)



CDP Overcollateralization & market liquidation

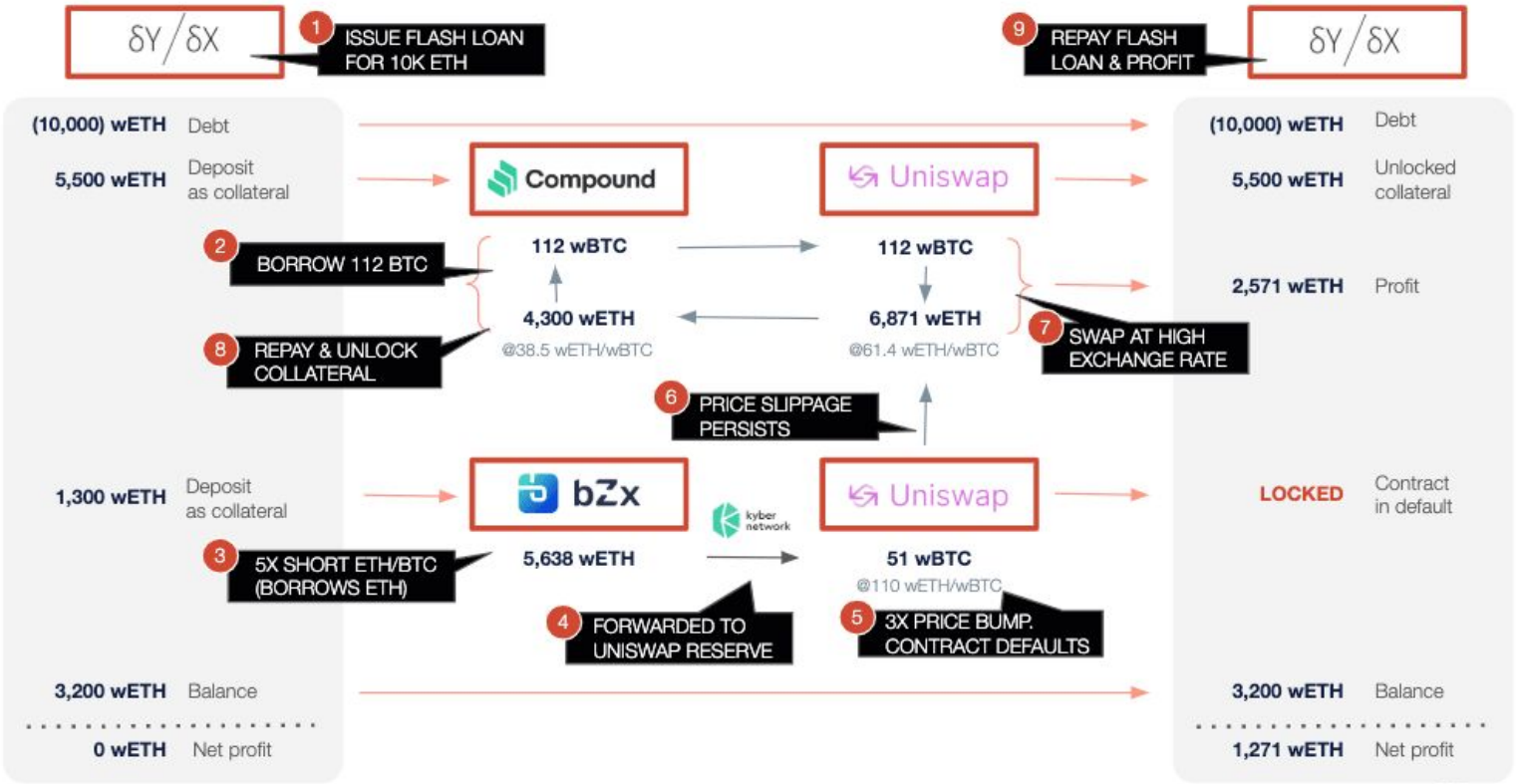


Special Topic: Exploitation of DeFi Composability

Key DeFi Composability Risk Takeaways

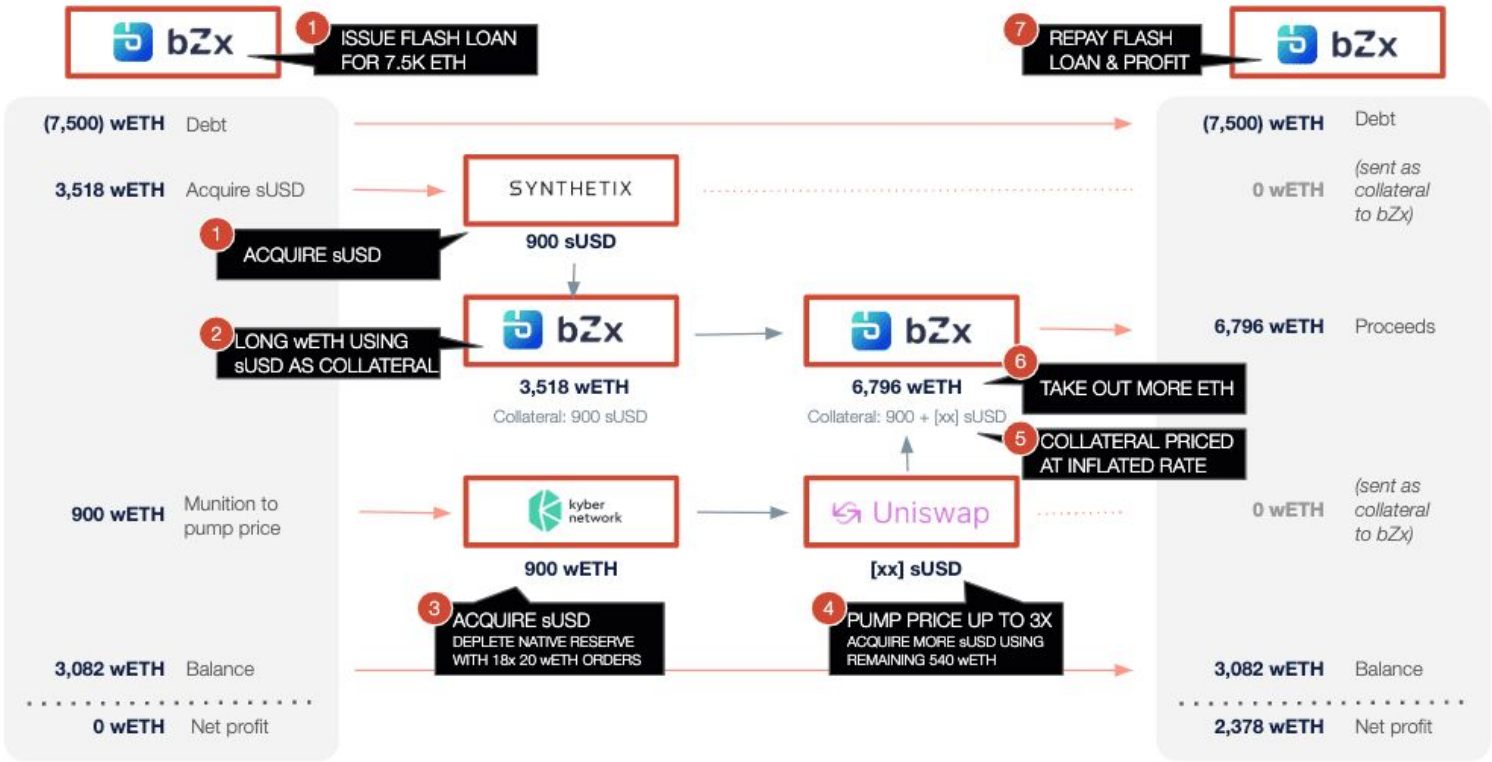
- DeFi financial primitive patterns are **growing in complexity** with each added product.
- When a new product (e.g. flash loans) was introduced, there was a path that was not traditional arbitrage across networks, but rather a **combination of financial products** that led to a direct payout.
- **Composability is the source of innovation**, but also poses a large risk to the full Ethereum ecosystem
- **Mitigations can include creation of tools** for analyzing liquidity, oracle sources, insurance, and threshold caps

#1: bZx 'Valentine's Day' Exploit 💔



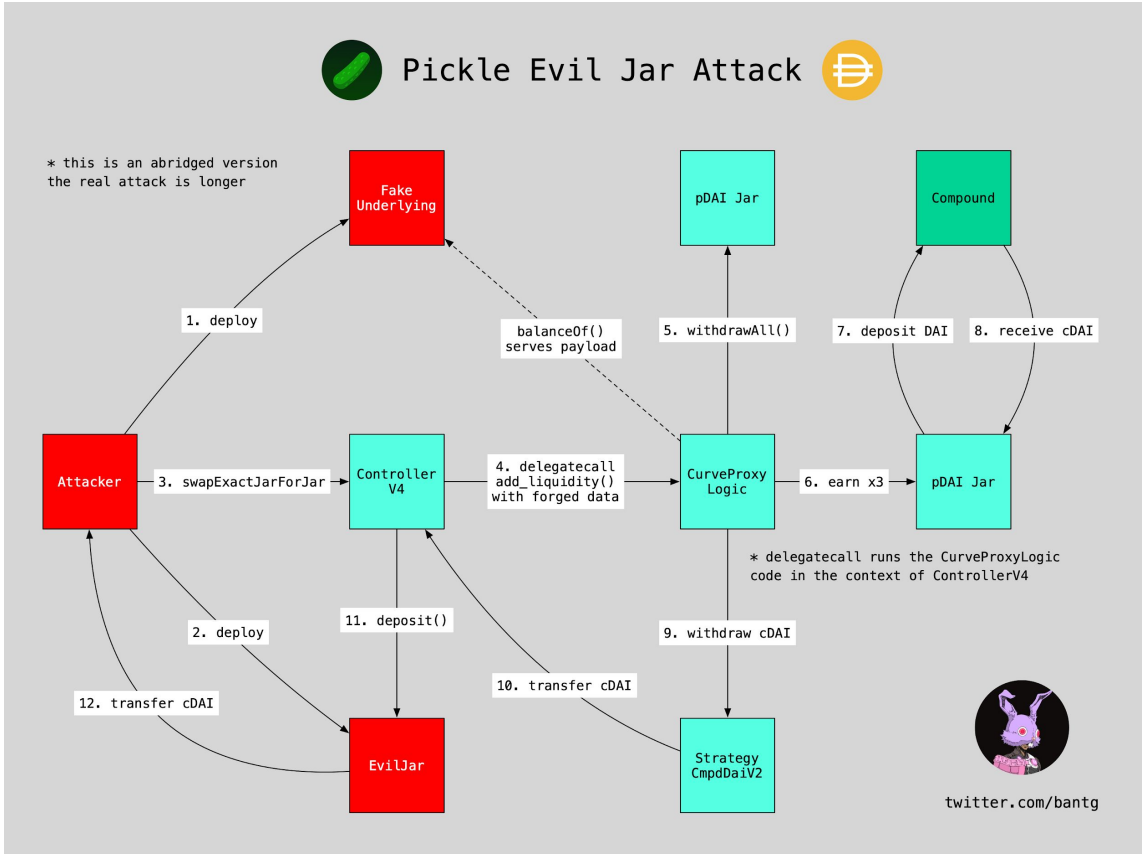
Source: Steps from Etherscan, bZx Post-Mortem, PeckShield post. wETH/wBTC ratio, profit amount from PeckShield report.

#2: bZx 'Sunday Scaries' Exploit



Source: Steps from Etherscan, @DegenSpartan, Kerman Kohli

Pickle Attack (Nov 21)



What can be done about those composability pitfalls?

Liquidity Analysis

Ongoing monitoring around the attack vector of flash loan liquidity compared to assets used by platform liquidity.

Bootstrap Insurance Liquidity

With new insurance protocols such as Nexus and Opyn, taking the other side of the insurance is a way to signal confidence that you're willing to pay out losses

Oracle Analysis

Don't just assume a large whale won't manipulate oracles, anyone can become one now.

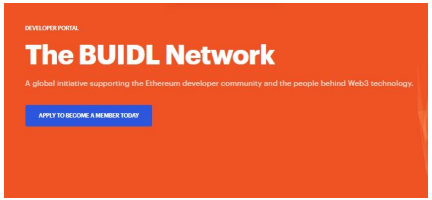
Liquidity Caps

Don’t rush the deployment process: lot of testnet time and then progressive liquidity caps to limit scale of potential losses

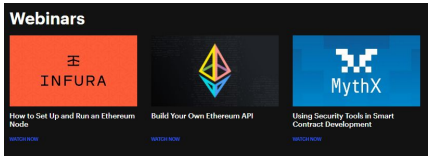
Thank You!

How Devs Get Started

Quorum Dev Quickstart - consensys.net/developers

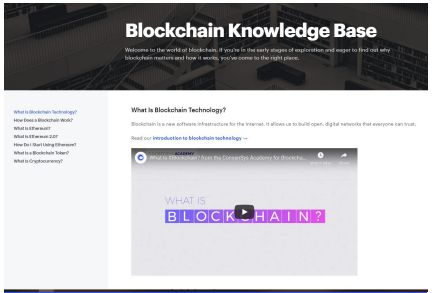


Join BUIDL Network



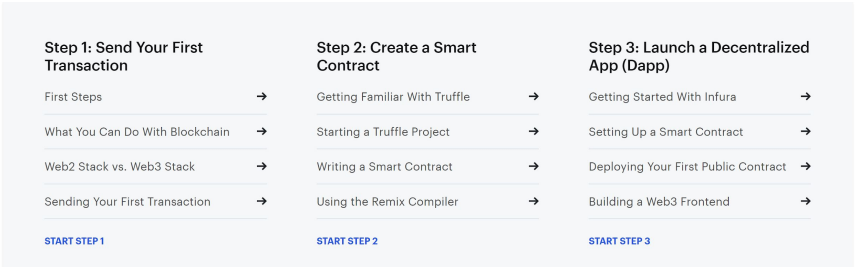
Browse Webinars

Join Discord - #Developers



Review Knowledge Base

Get Started with Ethereum



Derivatives

DISCLAIMER

Accenture holds no view regarding the merits or viability of the technologies presented.

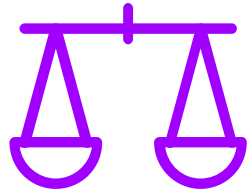
What is a derivative?

Definition

A derivative is a contract between two or more parties whose value is based on an agreed-upon underlying financial asset, index or security.

Types

Futures contracts, forward contracts, options, swaps, and warrants are commonly used derivatives.



Motivation

Derivatives can be used to either mitigate risk (hedging) or assume risk with the expectation of commensurate reward (speculation).

What is a DeFi derivative?

Blockchain-based smart contracts enable the creation of **tokenized derivatives** whose value is derived from the performance of an underlying asset and in which counterparty agreements are **hardwired in code**. DeFi derivatives can represent real-world assets such **as fiat currencies, bonds, and commodities,** as well as **cryptocurrencies.**

3 Case Studies

Case study: Synthetix (1/3)

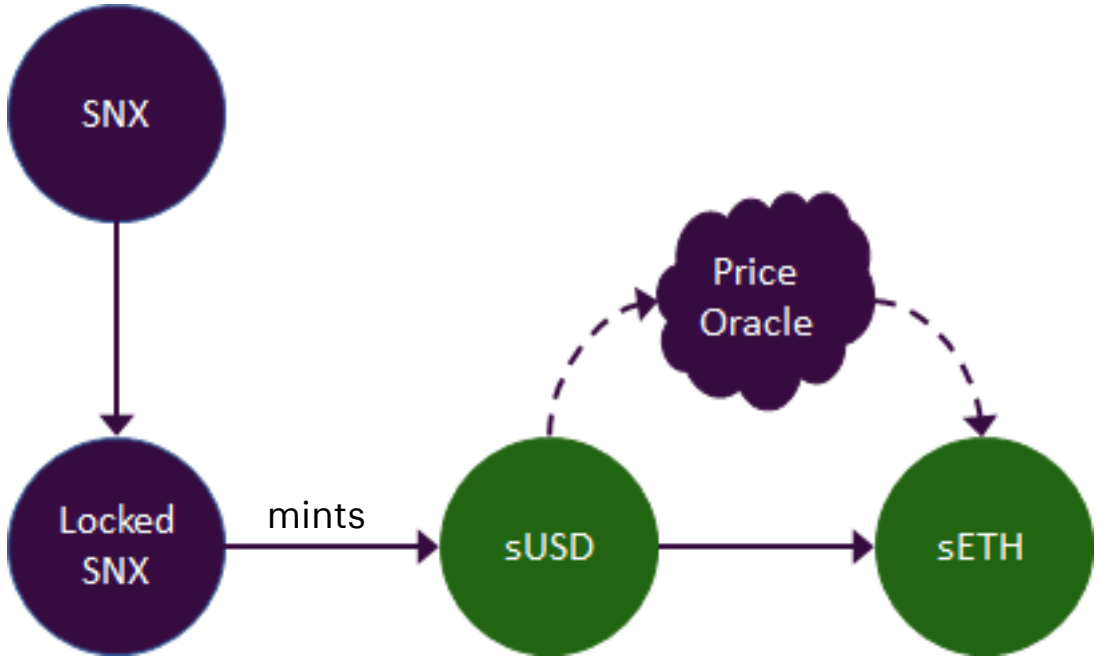
What is it?

- Decentralized synthetic asset issuance protocol built on Ethereum
- Create DeFi derivatives that track real-world assets
- crypt-native exposure to traditional markets.
  - fiat currencies, ETFs, commodities and cryptocurrencies, the platform offers

Case study: Synthetix (2/3)

How does it work?

- SNX as *collateral* to mint Synthetic assets (Synths)
- Conversions between Synths *directly* avoiding the need for counterparties.
- All Synths are backed with up *to 800% collateral*



Synthetix doc intermezzo

Case study: Synthetix (3/3)

What are the risks?

- Price shock: under-collateralization
- Centralisation risk:
  - dev team dependency
  - Chainlink
- Regulatory uncertainty

Home / News / FCA bans the sale of crypto-derivatives to retail consumers

FCA bans the sale of crypto-derivatives to retail consumers

Press Releases | First published: 06/10/2020 | Last updated: 06/10/2020

The FCA has published final rules banning the sale of derivatives and exchange traded notes (ETNs) that reference certain types of cryptoassets to retail consumers.

The FCA considers these products to be ill-suited for retail consumers due to the harm they pose. These products cannot be reliably valued by retail consumers because of the:

- inherent nature of the underlying assets, which means they have no reliable basis for valuation
- prevalence of market abuse and financial crime in the secondary market (eg cyber theft)
- extreme volatility in cryptoasset price movements
- inadequate understanding of cryptoassets by retail consumers
- lack of legitimate investment need for retail consumers to invest in these products

These features mean retail consumers might suffer harm from sudden and unexpected losses if they invest in these products.

Unregulated transferable cryptoassets are tokens that are not 'specified investments' or e-money, and can be traded, which includes well-known tokens such as Bitcoin, Ether or Ripple. Specified investments are types of investment which are specified in legislation. Firms that carry out particular types of regulated activity in relation to those investments must be authorised by the FCA.

Source: https://www.fca.org.uk/news/press-releases/fca-bans-sale-crypto-derivatives-retail-consumers

Excel Intermezzo

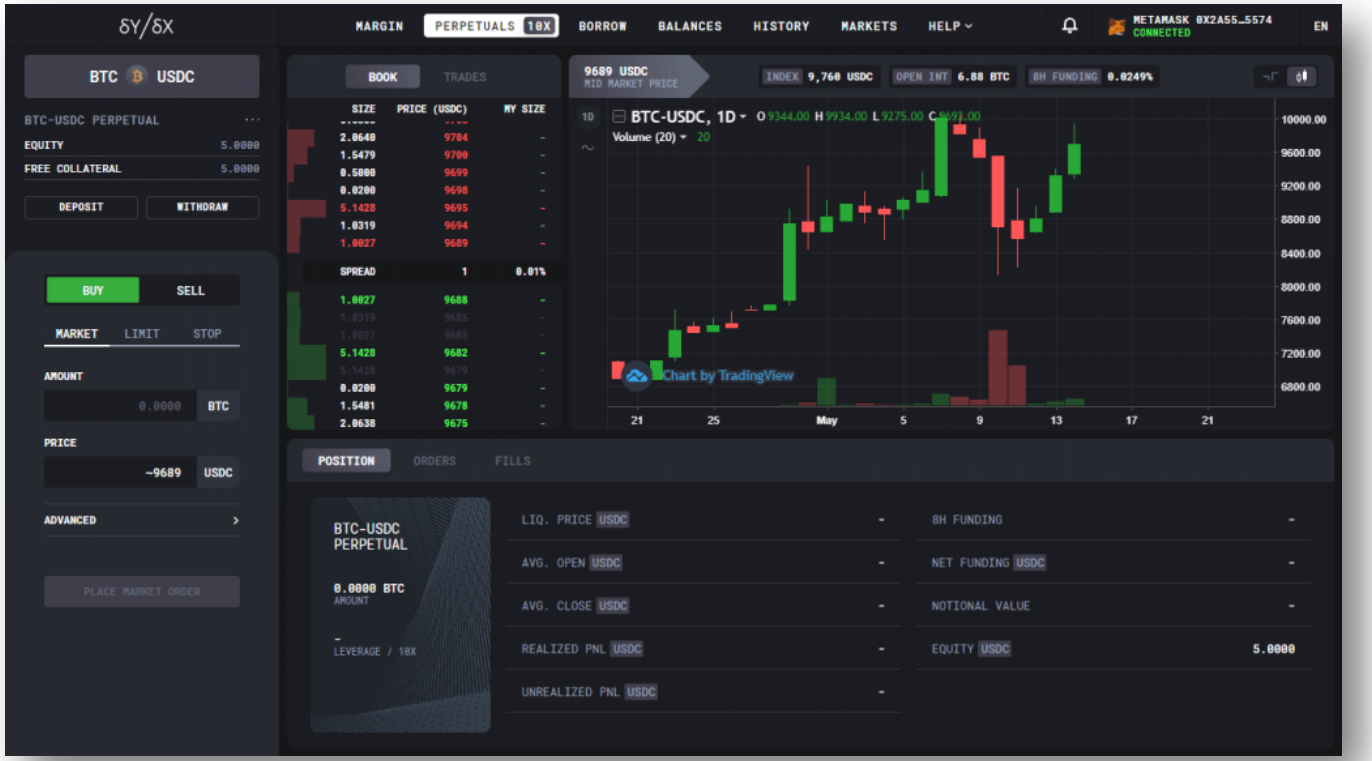
Link to Sheet

Case study: dYdX (1/3)

δY/δX

What is it?

- dYdX is a decentralized trading platform
- currently supports *margin trading, perp-futures, spot trading, lending, and borrowing*
- High volume due to blend of different features

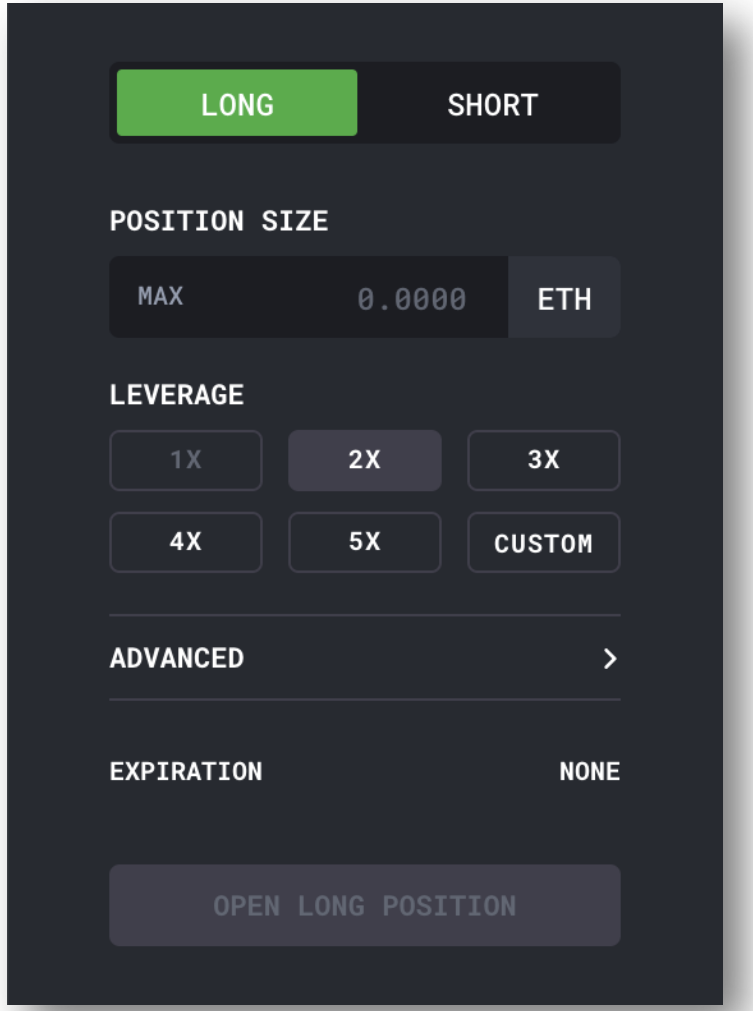


Case study: dYdX (2/3)

δY / δX

How does it work (Margin)?

- *"The longs pay the shorts and the shorts pay the longs"*
- Isolated margin
  - 'isolate' a certain amount of funds as part of a trade, at a specific leverage.
  - Leverage determines how much margin deposit is required
  - If liquidation occurs, losses are capped by the size of the isolated position.
- Cross margin
  - utilizes all assets in your dYdX account balance as collateral
  - More value at risk, higher leverage
- More here



Case study: dYdX (3/3)

δY/δX

What are the risks?

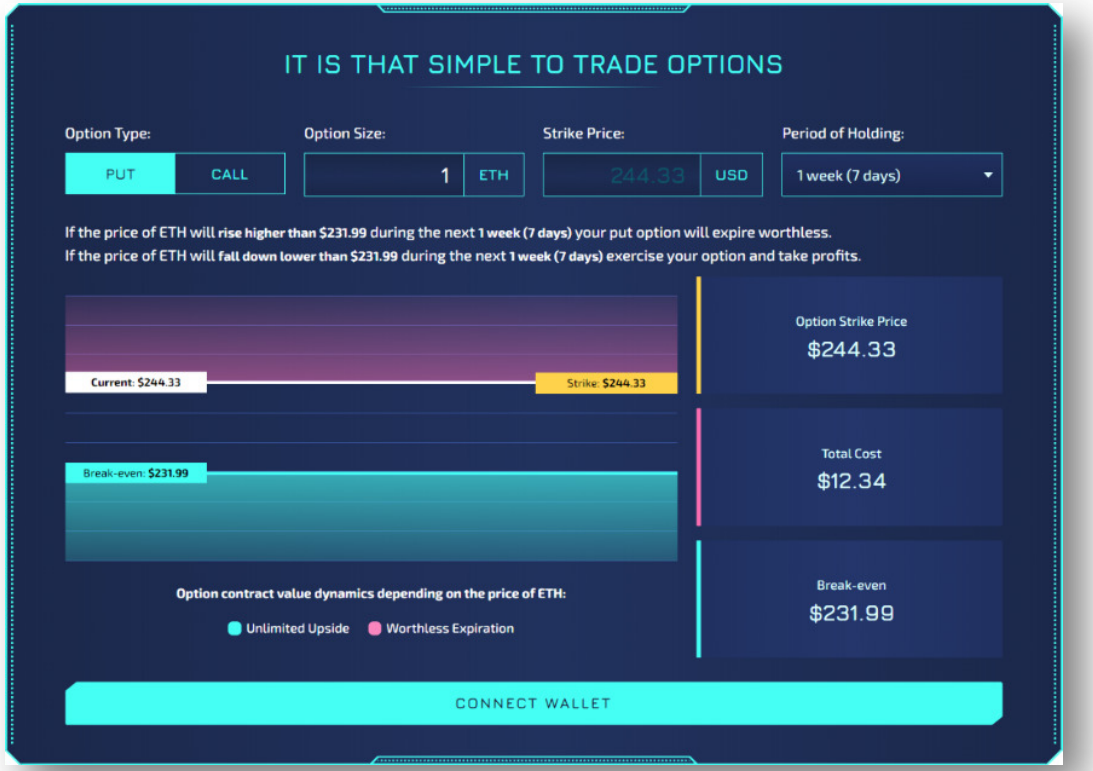
- Price volatility: margin-call
- Centralisation risk
  - dev team dependency
  - Chainlink
- Regulatory uncertainty
  - Known dev team

dYdX Exchange Intermezzo

Case study: Hegic (1/3)

What is it?

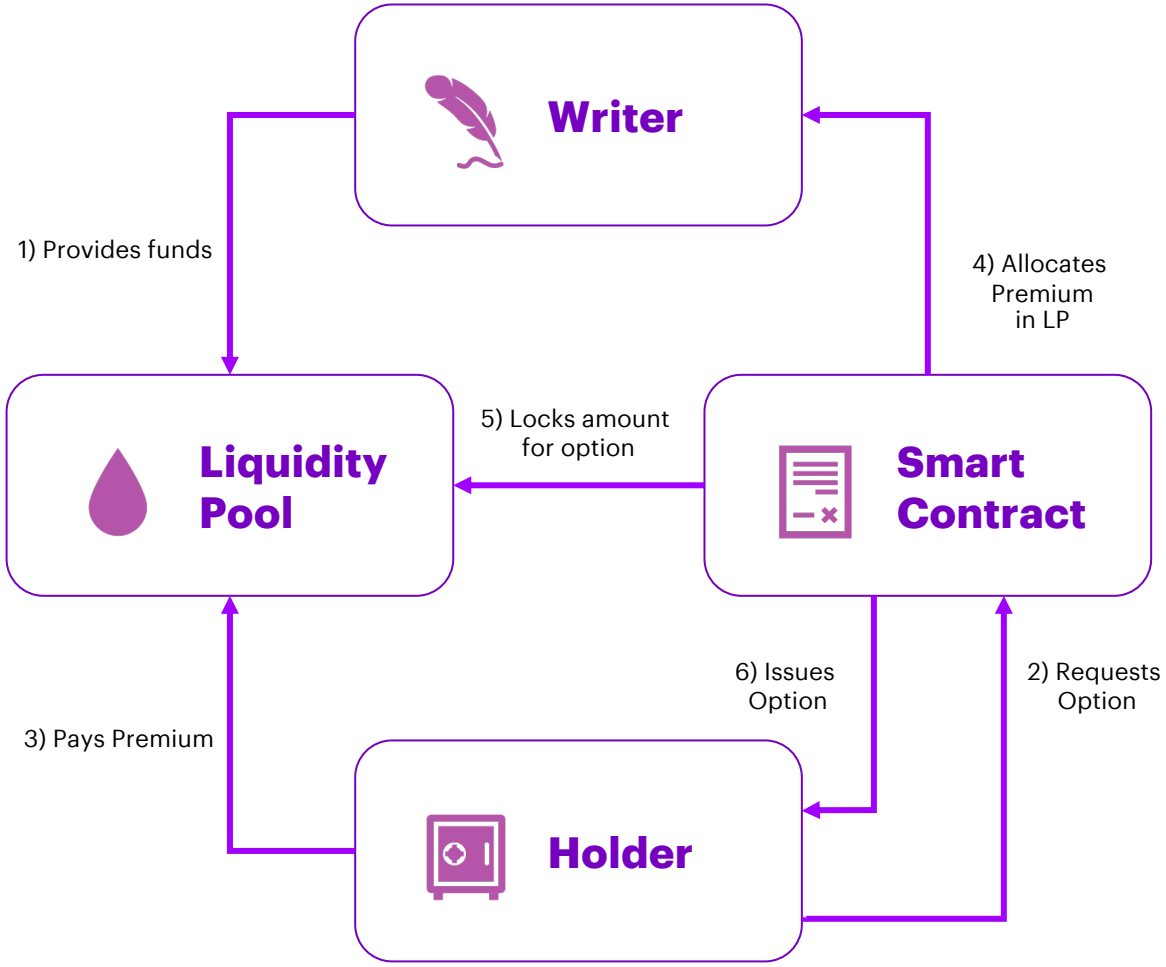
- on-chain options trading protocol on Ethereum
- Buy WBTC or ETH call and put options as a holder (buyer)
- Sell call and put options as one of the liquidity providers
- Hedge or leverage your position



Case study: Hegic (2/3)

How does it work?

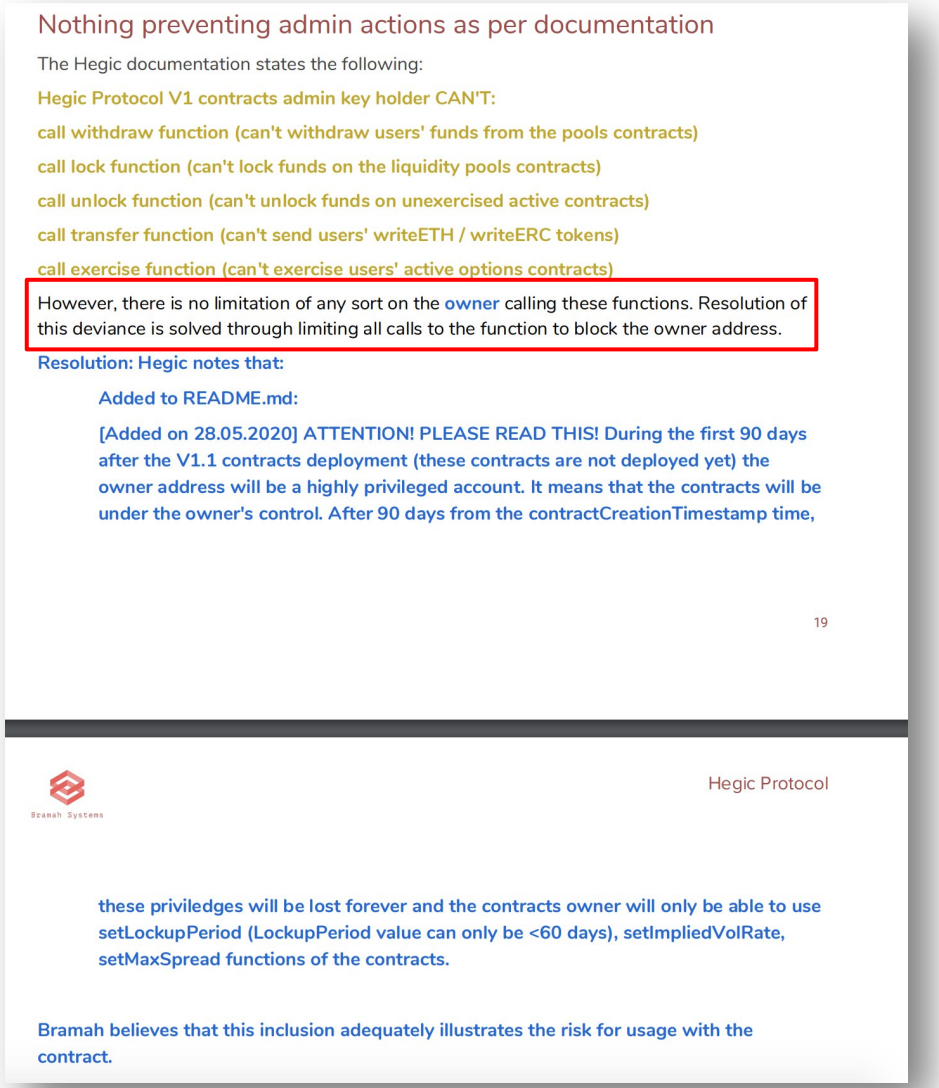
- Options Writers
  - Write call and put options.
  - Provide liquidity and start earning yield on WBTC or ETH. Auto diversification of capital allocation.
- Option Holders
  - Trade call and put options.
  - Non-custodial options with on-chain settlement. Choose any strike price, exercise at any moment.
- More here and here



Case study: Hegic (3/3)

What are the risks?

- Centralisation risk
  - dev team dependency (Admin control)
  - Chainlink
- Regulatory uncertainty
- Pseudonymous dev team
- V888 is in Beta at the time of this writing
- Value at Risk (however Risk is shared by LPs pro-rata)
- More here



Nothing preventing admin actions as per documentation

The Hegic documentation states the following:

Hegic Protocol V1 contracts admin key holder CAN'T:

call withdraw function (can't withdraw users' funds from the pools contracts)

call lock function (can't lock funds on the liquidity pools contracts)

call unlock function (can't unlock funds on unexercised active contracts)

call transfer function (can't send users' writeETH / writeERC tokens)

call exercise function (can't exercise users' active options contracts)

However, there is no limitation of any sort on the owner calling these functions. Resolution of this deviance is solved through limiting all calls to the function to block the owner address.

Resolution: Hegic notes that:

Added to README.md:

[Added on 28.05.2020] ATTENTION! PLEASE READ THIS! During the first 90 days after the V1.1 contracts deployment (these contracts are not deployed yet) the owner address will be a highly privileged account. It means that the contracts will be under the owner's control. After 90 days from the contractCreationTimestamp time,

19

Bramah Systems

Hegic Protocol

these priviledges will be lost forever and the contracts owner will only be able to use setLockupPeriod (LockupPeriod value can only be <60 days), setImpliedVolRate, setMaxSpread functions of the contracts.

Bramah believes that this inclusion adequately illustrates the risk for usage with the contract.

Source: https://bramah.systems/audits/Hegic_Audit_Bramah.pdf

Hegic Smart-Contract Intermezzo

DeFi M&A

- Hedged DeFi strategies
- Hedged yield farming
- Stabilize yield for a premium