Part II:

DeFi Primitives

3. Swaps and Loans

(i) Swaps

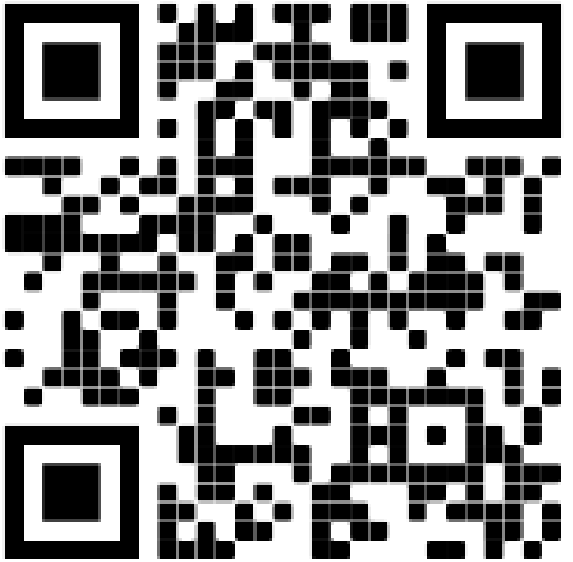
(a) Centralized Exchange

Swap

What is a swap?

- A swap is simply the exchange of one type of token to another.
- There are a number of ways to do this
- Most use a centralized exchange like Coinbase or Coinbase Pro

https://pro.coinbase.com/trade/BTC-USD



coinbase

Trade

- Home
- Portfolio
- Trade
- For You
- Learn and earn
- Notifications

Search all assets

24h | Tradable assets

Name	Price	Change	Market cap		Watch
Bitcoin BTC	$29,771.42	-3.08%	$558.6B	Buy	★
Ethereum ETH	$1,789.04	-2.12%	$209.1B	Buy	★
Tether USDT	$1.00	+0.03%	$62.0B	Buy	☆
Cardano ADA	$1.07	-5.50%	$34.2B	Buy	☆
USD Coin USDC	$1.00		$26.8B	Buy	★
Dogecoin DOGE	$0.17	-1.15%	$22.4B	Buy	☆

#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC Buy	$37,570.35	0.78%	7.87%	$711,743,713,590	$14,770,355,927 393,139 BTC	18,944,293 BTC	
2	Ethereum ETH Buy	$2,563.72	1.06%	7.37%	$306,048,631,223	$9,382,634,207 3,659,767 ETH	119,376,569 ETH	
3	Tether USDT Buy	$1.00	0.01%	0.01%	$78,143,159,428	$34,820,914,385 34,809,448,348 USDT	78,117,427,986 USDT	
4	BNB BNB Buy	$374.47	3.06%	2.59%	$61,831,029,807	$1,265,548,796 3,379,587 BNB	165,116,761 BNB	
5	USD Coin USDC	$0.9998	0.04%	0.00%	$49,766,462,083	$2,332,164,299 2,332,660,837 USDC	49,777,057,812 USDC	
6	Cardano ADA	$1.03	2.24%	2.73%	$34,643,215,262	$732,421,476 709,653,932 ADA	33,566,320,380 ADA	


Order Book
Price Charts
Trade History
Market Size
Price (USD)
My Size
5m
Candle
Overlay
O: 37,849.99 H: 37,850.00 L: 37,774.20 C: 37,790.48 V: 41
Trade Size
Price (USD)
Time
BTC-USD
$38,047.62
$38,000
$37,950
$37,900
$37,850
$37,800
$37,750
$37,700
$37,650
$37,600
$37,568.1
$37,550
$37,500
10:00
10:30
11:00
11:30
12:00
12:30
13:00
13:30
14:00
14:30
15:0
1/30/22, 11:30 EST
37,568.215
Mid Market Price
600
500
400
300
200
100
0
$37,000.00
$37,200.00
$37,400.00
$37,600.00
$37,800.00
$38,000.00
$38,200.00
USD Spread
0.23
Open Orders
Open
Fills
Side
Size
Filled (BTC)
Price (USD)
Fee (USD)
Status
No orders to show

Swap

Orderly Cryptocurrency?

- **"Arbitrageable"**: Cryptocurrencies have low transaction costs, globally fungible
  - In theory, they should have tight spreads, low volume, orderly markets
- **Instead:**
  - BTC prices differ by hundreds of dollars across exchanges
  - BTC daily volume of $25bn, 15% of entire market cap
    - Annual volume is 55x the market cap
    - Annual volume of Apple is only 1.7x market cap
  - How can this be?

#	Source	Pair	Volume (24h)	Price
1	Coinsbit	BTC/USDT	$878,944,892	$9,394.74
2	Bilaxy	BTC/USDT	$813,087,459	$9,401.63
3	BHEX	BTC/USDT	$739,387,382	$9,397.50
4	CoinBene	BTC/USDT	$724,065,563	$9,398.71
5	Folgory	BTC/USDT	$637,148,703	$9,390.86
6	EXX	BTC/USDT	$601,369,387	$9,398.71
7	BitForex	BTC/USDT	$573,580,912	$9,398.63
8	Hotbit	BTC/USDT	$526,715,554	$9,397.91
9	Coineal	BTC/USDT	$513,734,235	$9,398.71
10	ChainX	BTC/KRW	$506,932,884	$9,042.87

Source: CoinMarketCap.com

Fake Exchanges

Why would exchanges exaggerate volume

- **Initial Coin and Exchange Offerings (ICOs/IEOs)**: Showing up at the top of these lists can attract coins to list on your exchange
- **"Fake it till you make it"**: Crypto traders may be attracted to trade on your exchange, thereby increasing the "true" volume
- **Over 90% of trading volume is fake!**
  - Fake transactions can either occur off-chain (within addresses internally) or on-chain (pay transaction and show up on blockchain)
  - How can we identify a fake exchange?

What a Normal Exchange Looks Like

Source: Coinbase.com

What a Normal Exchange Looks Like

Key Elements

- **Order Book**: List of trades (size and prices) that have been submitted but not yet filled
  - Orders in red are to sell; in green are to buy
  - Spread is given by difference between minimum sell price and maximum buy price
  - Trades occur when someone is willing to sell at a price at which someone wants to buy
  - Example: 5.601 BTC being offered for sale at $10,336.30 per BTC. Buyer wants to purchase 0.4045 BTC at $10,335.05. The spread between the cheapest sale price and highest purchase price is $1.19.
- **Low spread**: The spread of BTC is $1.19 (only 0.01% of the price)
  - Spread of Apple is $0.15 (0.05% of price)
- **Round numbers**: Many orders are for round numbers of BTC, evidence of a normal exchange

Source: Coinbase.com

What a Normal Exchange Looks Like

Key Elements

- **Trade History**: Each row represents a trade that was fulfilled. Trade size, price, and time are listed.
  - Rows in green lifted the price (i.e., the trade occurred at a price higher than the price at the time of trade), while those in red reduced the price
- **Streaky**: There are often several price raises in a row, reflecting more buying then selling activity at this point in time (upward price pressure)
- **Round numbers**: Again, we see many transactions occurring at round decimals (0.03, 0.05, etc.). This is evidence of a normal exchange

Source: Coinbase.com

What a Normal Exchange Looks Like

Key ingredients

- **Price History**: Red and green bars reflecting price movements every interval (typically 5-10 minutes)
  - Notice that it is again streaky
- **Trading Volume**: Gray bars at the bottom show amount of BTC traded each interval
  - Notice randomness in trading volume: some intervals have higher volume than others (i.e., slump in volume after 5:00pm)

Source: Coinbase.com

What a Fake Exchange Looks Like

Examples

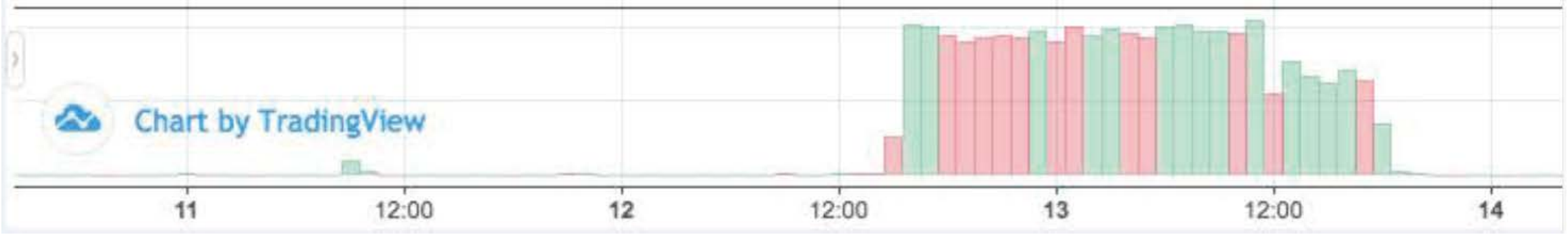
- **CoinBene**: an exchange with 6x the volume of Coinbase Pro
- **Offsetting trades**: Each second, there are two roughly offsetting trades being executed
  - None of these trades occur are for round quantities
- **Wide spreads**: The spread is $34, far greater than the spread in Coinbase

Source: Bitwise Asset Management

What a Fake Exchange Looks Like

Examples

- **RightBTC**: an exchange with 4x the volume of Coinbase Pro
- **Hours of zero trading volume**: There are large gaps (12- or even 24-hour periods) without any trading volume.

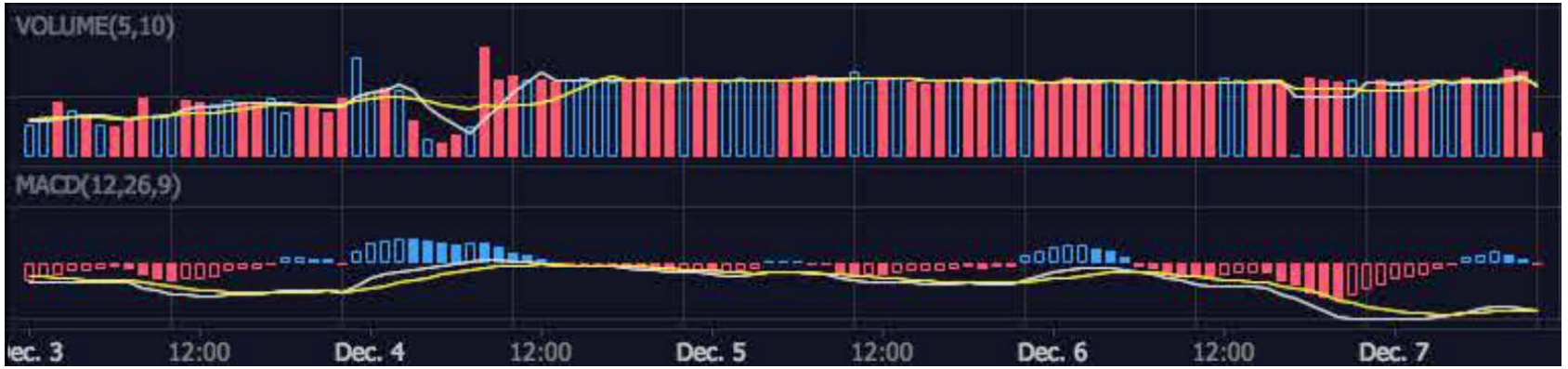


Source: Bitwise Asset Management

What a Fake Exchange Looks Like

Examples

- **CHAOEX**: an exchange with roughly the same volume as Coinbase Pro
- **Constant volume**: Note that the volume is basically constant for over 3 days in this case
  - Volume is insensitive to market hours, news, weekends, etc.

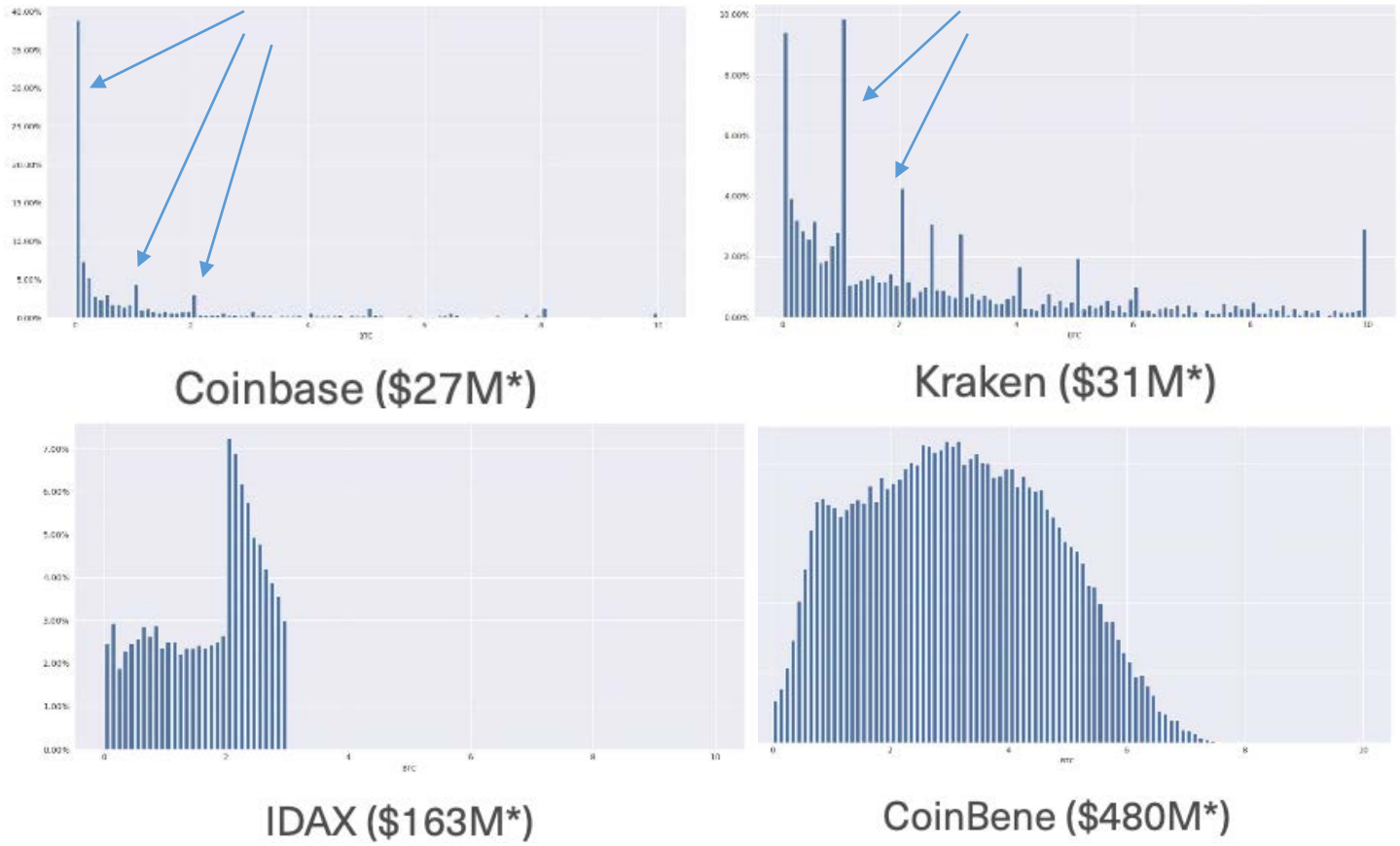


Source: Bitwise Asset Management

Trade Size of Real vs. Fake Exchanges

Huge Differences!

- Real exchanges have very few large trades, cluster around integer values
- Fake exchanges have very strange distributions
  - Random spikes, very dispersed volume, etc.

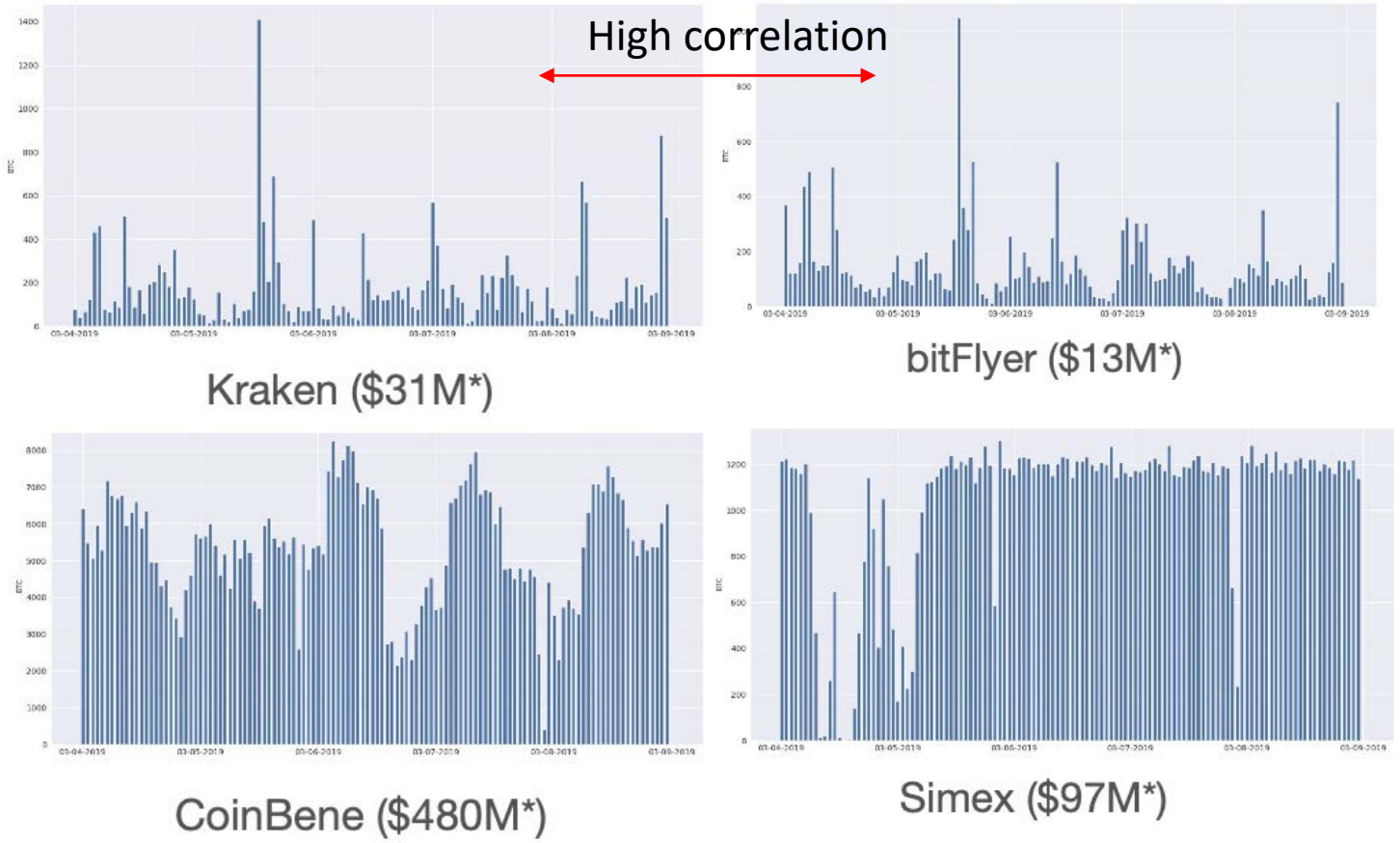


Source: Bitwise Asset Management

Trade Volume of Real vs. Fake Exchanges

Huge Differences!

- Real exchanges have similar spikes in volume at the same time, rise and fall daily
- Fake exchanges have volume that is extremely high almost constantly

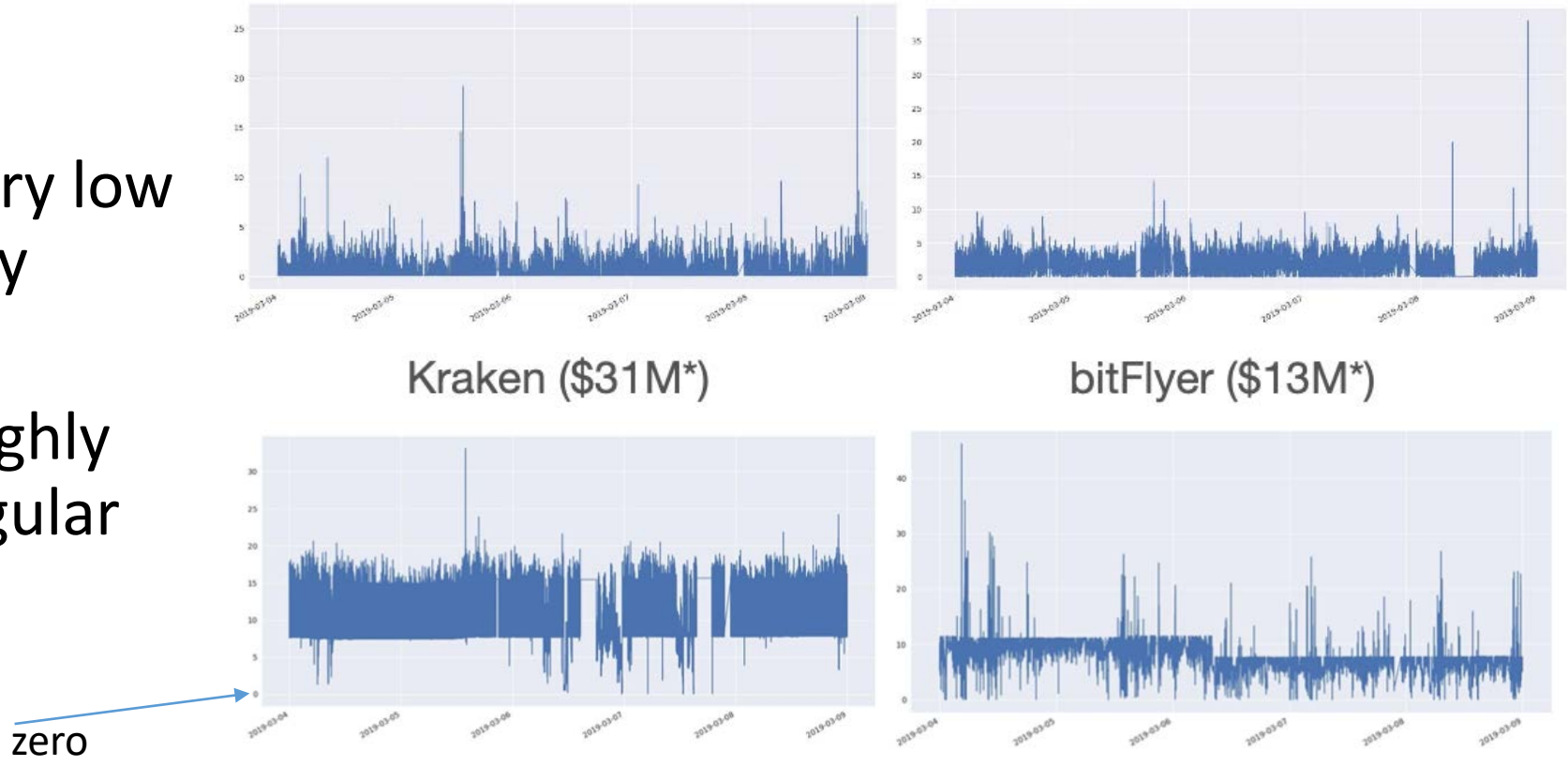


Source: Bitwise Asset Management

Spreads of Real vs. Fake Exchanges

Huge Differences!

- Real exchanges have very low spreads that do not vary much and rarely peak
- Fake exchanges have highly volatile spreads and regular peaks



Source: Bitwise Asset Management

How Much Volume is Fake

- **Only 4.5% of Total Volume is Real**: This reduces BTC daily volume from $25bn “fake” volume to just over $1bn actual volume
  - Annual “real” volume is 1.7x market cap
  - Same as Apple’s turnover
- Cryptocurrency markets look much more orderly when correcting for fake volume
- Being able to distinguish fake volume crucial to understanding centralized exchange

Part II:

DeFi Primitives

3. Swaps and Loans

(i) Swaps

(b) Decentralized Exchange

Swap

What is a swap?

- A swap is simply the exchange of one type of token to another.
- The key benefit of swapping in DeFi is that it is atomic and noncustodial.
- Funds can be custodied in a smart contract with withdrawal rights that can be exercised at any time before the swap is completed.
- If the swap does not complete, all parties involved retain their custodied funds.

Swap

What is a swap?

- The swap only executes when the exchange conditions are agreed to and met by all parties, and are enforced by the smart contract.
- If any condition is not met, the entire transaction is cancelled. A platform that facilitates token swapping on Ethereum in a noncustodial fashion is a *decentralized exchange* (DEX).
- There are two primary mechanisms for DEX liquidity: one is an order-matching approach and the other is an *Automated Market Maker.*

Swap

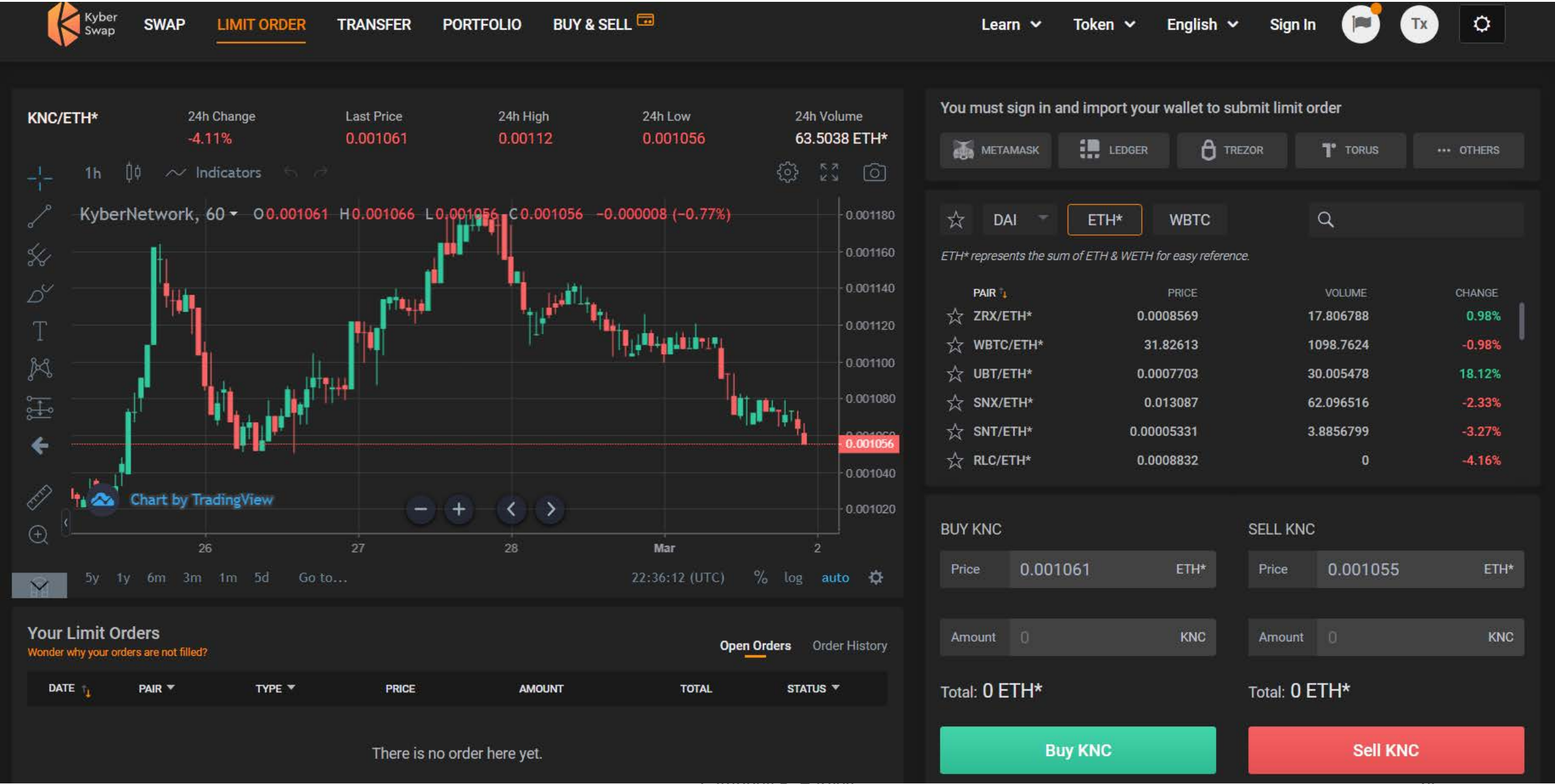
Order book matching

- *Order-book matching* is a system in which all parties must agree on the swap exchange rate.
- Market makers can post bids and asks to a DEX and allow takers to fill the quotes at the pre-agreed-upon price.
- Until the offer is taken, the market maker retains the right to remove the offer or update the exchange rate as market conditions change.

Swap

Order book matching

- A leading example of a fully on-chain order book is Kyber.
- "KyberSwap is a non custodial platform. It means you are in total control of your funds. In a typical centralized exchange - Before placing any trade, you are first required to deposit your funds to exchange. In KyberSwap you do not need to deposit any funds. Just connect your Ethereum wallet and place a trade directly from your wallet."


Kyber Swap
SWAP
LIMIT ORDER
TRANSFER
PORTFOLIO
BUY & SELL
Learn
Token
English
Sign In
Tx
KNC/ETH*
24h Change
-4.11%
Last Price
0.001061
24h High
0.00112
24h Low
0.001056
24h Volume
63.5038 ETH*
1h
Indicators
KyberNetwork, 60
O0.001061 H0.001066 L0.001056 C0.001056 −0.000008 (−0.77%)
0.001180
0.001160
0.001140
0.001120
0.001100
0.001080
0.001056
0.001040
0.001020
Chart by TradingView
26
27
28
Mar
2
5y 1y 6m 3m 1m 5d Go to...
22:36:12 (UTC)
% log auto
You must sign in and import your wallet to submit limit order
METAMASK
LEDGER
TREZOR
TORUS
OTHERS
DAI
ETH*
WBTC
ETH* represents the sum of ETH & WETH for easy reference.
PAIR
PRICE
VOLUME
CHANGE
ZRX/ETH* 0.0008569 17.806788 0.98%
WBTC/ETH* 31.82613 1098.7624 -0.98%
UBT/ETH* 0.0007703 30.005478 18.12%
SNX/ETH* 0.013087 62.096516 -2.33%
SNT/ETH* 0.00005331 3.8856799 -3.27%
RLC/ETH* 0.0008832 0 -4.16%
BUY KNC
Price 0.001061 ETH*
Amount 0 KNC
Total: 0 ETH*
Buy KNC
SELL KNC
Price 0.001055 ETH*
Amount 0 KNC
Total: 0 ETH*
Sell KNC
Your Limit Orders
Wonder why your orders are not filled?
Open Orders
Order History
DATE
PAIR
TYPE
PRICE
AMOUNT
TOTAL
STATUS
There is no order here yet.

Swap

Order book matching issues

- The order-matching approach is expensive and inefficient because each update requires an on-chain transaction.
- An insurmountable inefficiency with an order-book matching is that both counterparties must be willing and able to exchange at the agreed-upon rate for the trade to execute.
- This requirement creates limitations for many smart contract applications in which demand for exchange liquidity cannot be dependent on a counterparty's availability.

Part II:

DeFi Primitives

3. Swaps and Loans

(i) Swaps

(c) Automated Market Makers

Swap

Automated Market Makers (AMMs)

- An Automated Market Maker (AMM) is a smart contract that holds assets on both sides of a trading pair and continuously quotes a price for buying and for selling.
- Based on executed purchases and sales, the contract updates the asset size behind the bid and the ask and uses this ratio to define its pricing function.
- The contract can also take into account more complex data than relative bid/ask size when determining price.
- From the contract's perspective, the price should be risk-neutral where it is indifferent to buying or selling.

Swap

Naïve AMM

- A naive AMM might set a fixed price ratio between two assets.
- With a fixed price ratio, when the market price shifts between the assets, the more valuable asset would be drained from the AMM and arbitraged on another exchange where trading is occurring at the market price.
- The AMM should have a pricing function that can converge on the market price of an asset so that it becomes more expensive to purchase an asset from the trading pair as the ratio of that asset to the others in the contract decreases.

Swap

Advantages of AMM

- Main benefit is the constant availability 24/7 and that a traditional counterparty is not necessary to execute a trade.
- These provisions are very important for smart contracts and DeFi development because of the guarantee that a user can exchange assets at any moment if necessary.
- A user maintains custody of her funds until she completes the trade, hence, counterparty risk is zero.

Swap

Composable liquidity of AMM

- An additional benefit is *composable liquidity*, which means any exchange contract can plug into the liquidity and exchange rates of any other exchange contract.
- AMMs make this particularly easy because of their guaranteed availability and their allowing one-sided trading against the contract.
- Composable liquidity fits with concept of DeFi Legos.

Swap

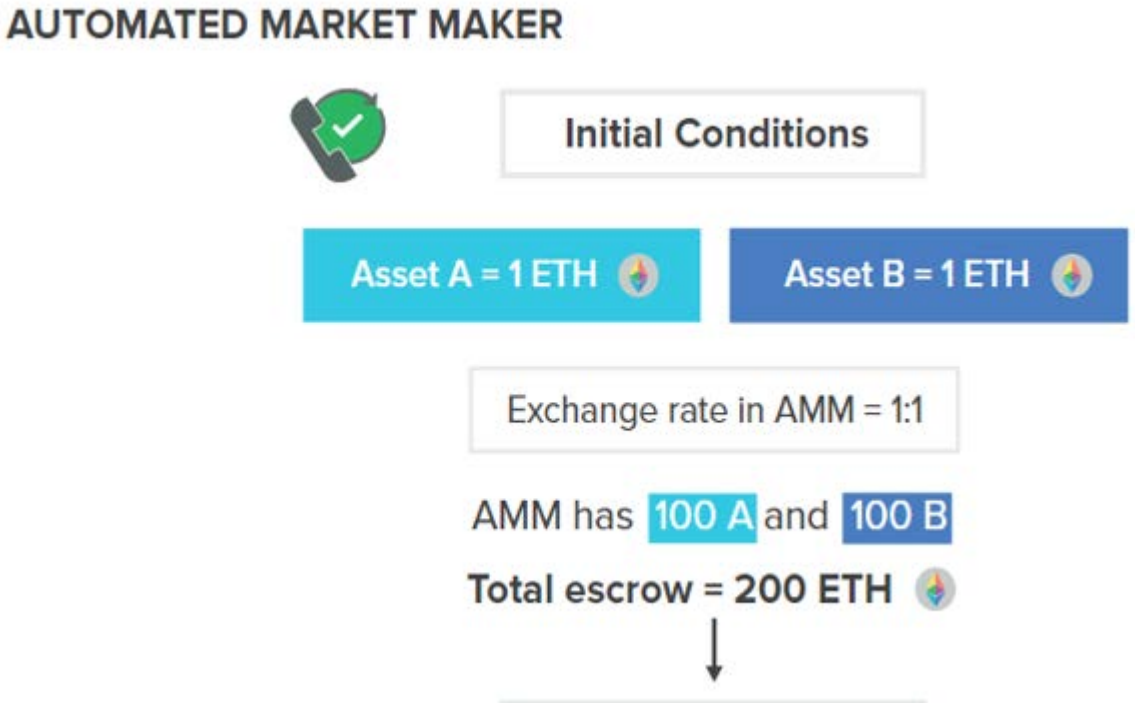
Impermanent loss of AMM

- One drawback to an AMM is the concept of *impermanent loss*, the opportunity-cost dynamic between offering assets for exchange and holding the underlying assets to potentially profit from the price movement.
- The loss is impermanent because it can be recovered if the price reverts to its original level.

Swap

Impermanent loss example

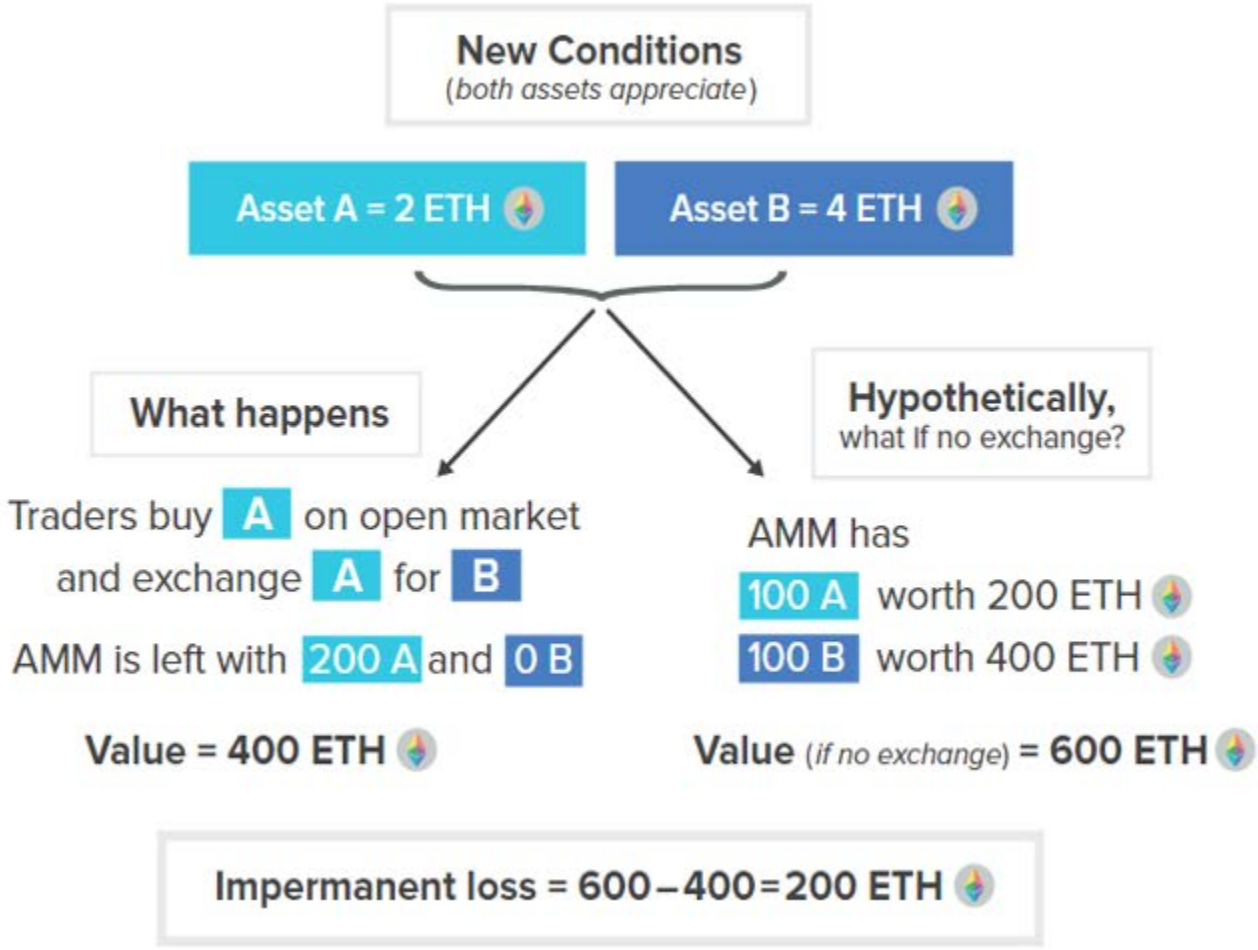
- Initial conditions in market:
  - Token A = 1 ETH and
  - Token B = 1 ETH
- AMM has an exchange rate of 1:1
- Contract has 100 A and 100 B. So the total value of escrow is 200 ETH



Swap

Impermanent loss example

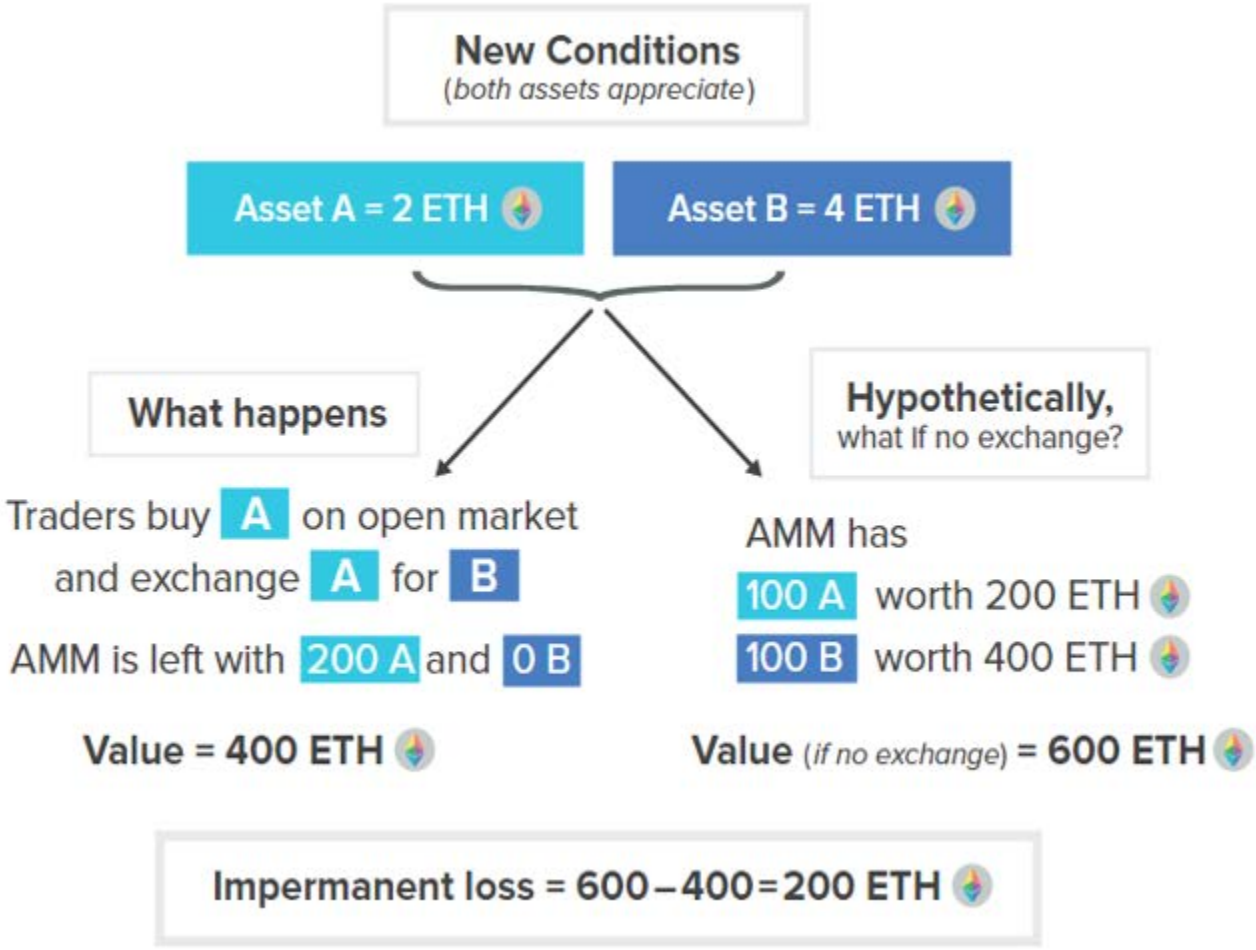
- New conditions. Both tokens appreciate in value. Now:
  - Token A = 2 ETH and
  - Token B = 4 ETH
- AMM has an exchange rate of 1:1
- Traders buy token A on open market (like Coinbase) and exchange it in the AMM for B – draining all the B.



Swap

Impermanent loss example

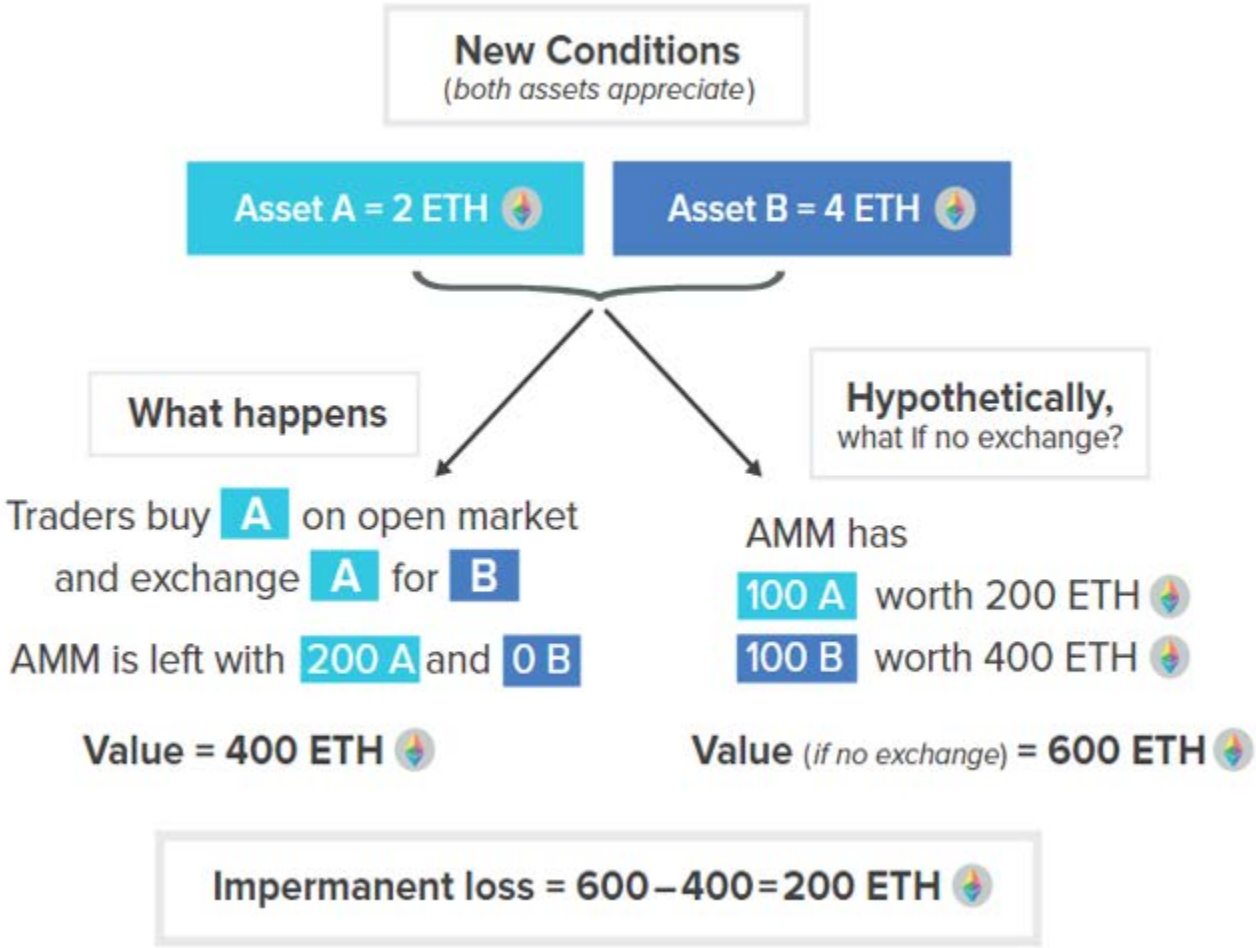
- Contract left with 200 A and zero B.
- Value = 400 ETH
- However, if there was no exchange in the AMM, the value would be 600 ETH
- Impermanent loss is the difference 600 – 400 = 200 ETH



Swap

Impermanent loss example

- This simplified example had an exchange rate of 1:1
- We will talk in greater detail about Uniswap but let me preview an example and calculate impermanent loss



https://academy.binance.com/en/articles/impermanent-loss-explained

Swap

Impermanent loss Uniswap v2

- Initial market prices are 1 ETH = 100 DAI
- Alicia deposits 1 ETH and 100 DAI into a liquidity pool
- Alicia will earn a fee for providing liquidity
- Notice that an equal value of DAI and ETH are deposited
- There are others like Alicia in the pool which has a total of 10 ETH and 1,000 DAI. The total liquidity is 10,000 = 10 x 1,000
- Alicia owns 10% of the pool

Swap

Impermanent loss Uniswap v2

- New market prices are 1 ETH = 400 DAI
- Arbitrageurs see the opportunity and buy DAI in open market and use DAI to withdraw ETH. The exchange price depends on the ratio of price whereas the liquidity (10,000) remains constant.
- Arbitrageurs will drain 5 ETH so the pool now has 5 ETH and 2,000 DAI. Notice liquidity is still 10,000 and the new ratio is 1:400 (reflecting market prices).

Swap

Impermanent loss Uniswap v2

Vault	x*y=k	k is constant	
ETH	**DAI**	**product**	**price of ETH in DAI**
10	1,000.00	10,000	100.00
9	1,111.11	10,000	123.46
8	1,250.00	10,000	156.25
7	1,428.57	10,000	204.08
6	1,666.67	10,000	277.78
5	2,000.00	10,000	400.00

Swap

Impermanent loss Uniswap v2

- Alicia owns 10% and withdraws all her funds from the pool. That will be 0.5 ETH and 200 DAI.
- USD value is $400 ($400 x 0.5 + $1 x 200)
- Her original investment was $200
- However, if she did not deposit into the pool, the value of the assets would have been $500 ($400 x 1 + $1 x 100)
- The impermanent loss is $100 ($500-$400)
- Note that there is a profit overall plus we are not accounting for the fees that Alicia would earn for providing liquidity

Swap

Impermanent loss features

- Impermanent loss occurs for any shift in price and liquidity, because the contract is structured to sell the appreciating asset and to buy the depreciating asset.
- An important feature of impermanent loss is *path independence*. In our example, it is irrelevant whether 1 or 100 traders consumed all the liquidity.
- The final exchange rate and contract asset ratios yield the same impermanent loss regardless of the number of trades or the direction of the trades.

Swap

Impermanent loss features

- Because of path independence, impermanent loss is minimized on trading pairs that have correlated prices (*mean-reverting pairs*).
- Thus, stablecoin trading pairs are particularly attractive for AMMs.

Part II:

DeFi Primitives

3. Swaps and Loans

(ii) Collateralized Loans

Collateralized loans

Role of debt and lending in DeFi

- Debt and lending are perhaps the most important financial mechanisms that exist in DeFi, and in traditional finance.
- Any loan of non-zero duration (e.g., foreshadowing flash loan) must be backed by an equivalent or excess amount of collateral.
- Requiring collateral contractually prevents a counterparty from defaulting.
- An uncollateralized mechanism raises the risk that a counterparty could steal funds, especially in an open and anonymous system such as Ethereum.

Collateralized loans

Foreclosure risk

- A risk of overcollateralized positions is that the collateral becomes less valuable than the debt, leading to a foreclosure without an option for recovery.
- Therefore, more-volatile types of collateral require larger collateralization ratios in order to mitigate this risk.

Collateralized loans

Liquidation

- To avoid liquidation it is imperative that debt remain overcollateralized by a margin sufficiently large that moderate price volatility does not place the collateral value in jeopardy.
- Smart contracts commonly define a minimum collateralization threshold below which the collateral can be liquidated and the position closed.
- The collateral could be auctioned or directly sold on a DEX, likely with an AMM, at the market price.

Collateralized loans

Liquidation trigger

- Positions in the Ethereum blockchain cannot be liquidated automatically, so an incentive is needed.
- The incentive often takes the form of a percentage fee allocated to an external **keeper** who is able to liquidate the position and collect the reward.
- Any remaining collateral is left to the original holder of the position.
- In some cases, the system will leave all remaining collateral to the keeper as a stronger incentive.
- Because the penalty for liquidation is high and most collateral types are volatile, platforms generally allow users to top up their collateral to maintain healthy collateralization ratios.

Collateralized loans

Collateralization can back a token

- An implication of collateralized loans and token supply adjustment is that collateralization can back the value of a synthetic token.
- The synthetic token is an asset created and funded by a debt, which is the requirement to repay the synthetic token in order to reclaim the collateral.
- The synthetic token can have a utility mechanism or represent a complex financial derivative, such as an option or bond (e.g., Synthetix Synth and Yield yToken). A stablecoin that tracks the price of an underlying asset can also be a synthetic token of this type (e.g., MakerDAO DAI).

Part II:

DeFi Primitives

3. Swaps and Loans

(iii) Flash Loans

Flash loans

Traditional finance

- A financial primitive that uniquely exists in DeFi and dramatically broadens certain types of financial access is a *flash loan.*
- In traditional finance, a lender is compensated for providing the capital and bearing the risk of default by the interest amount charged over the life of the loan.
- The interest rate is typically higher the longer the duration of the loan, because the longer time to repay exposes the lender to greater risk that the borrower may default.

Flash loans

Zero-duration loans

- Reversing the concept leads to the conclusion that shorter-term loans should be less risky and therefore require less compensation for the lender.
- A flash loan is an instantaneous loan paid back within the same transaction.
- A flash loan is similar to an overnight loan in traditional finance, but with a crucial difference—repayment is required within the transaction and enforced by the smart contract.

Flash loans

Risk of flash loans

- A thorough understanding of an Ethereum transaction is important for understanding how flash loans work.
- One clause in the transaction is vital: if the loan is not repaid with required interest by the end of the transaction, the whole process reverts to the state before any money ever left the lender's account.
- In other words, either the user successfully employs the loan for the desired use case and completely repays it in the transaction or the transaction fails and everything resets as if the user had not borrowed any money.

Flash loans

Risk of flash loans

- Flash loans essentially have zero counterparty risk or duration risk.
- They allow a user to take advantage of arbitrage opportunities or refinance loans without pledging collateral.
- This capability allows anyone in the world to have access to opportunities that typically require very large amounts of capital investment.
- This type of innovations that cannot exist in the world of traditional finance.
- However, these are not “risk free” because of smart contract risk.

I. DeFi Infrastructure

Modules

1. Mechanics
2. Supply and Ownership
3. Swaps and Loans
4. **Joining the World of DeFi**
   i. MetaMask
   ii. Blockchain Tech Big Picture