Tutorial 5:

AMMs (Automated Market Makers)

CSCD71: Blockchains & Decentralized Applications

Nikhil Lakhwani, Nov 3 2023.

Acknowledgements

CS 251: Cryptocurrencies and Blockchain Technologies from Stanford University.

References to lecture slides:
https://cs251.stanford.edu/lectures/lecture9.pdf
https://cs251.stanford.edu/lectures/lecture10.pdf
https://cs251.stanford.edu/lectures/lecture11.pdf

What is an exchange?

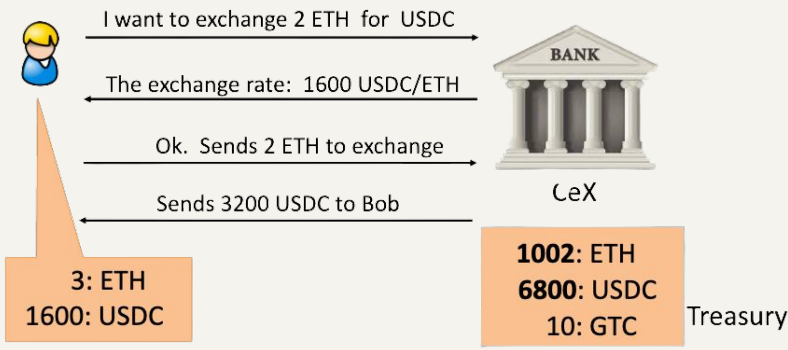
An exchange:

A platform used to convert one token to another (eg: USDC → ETH)

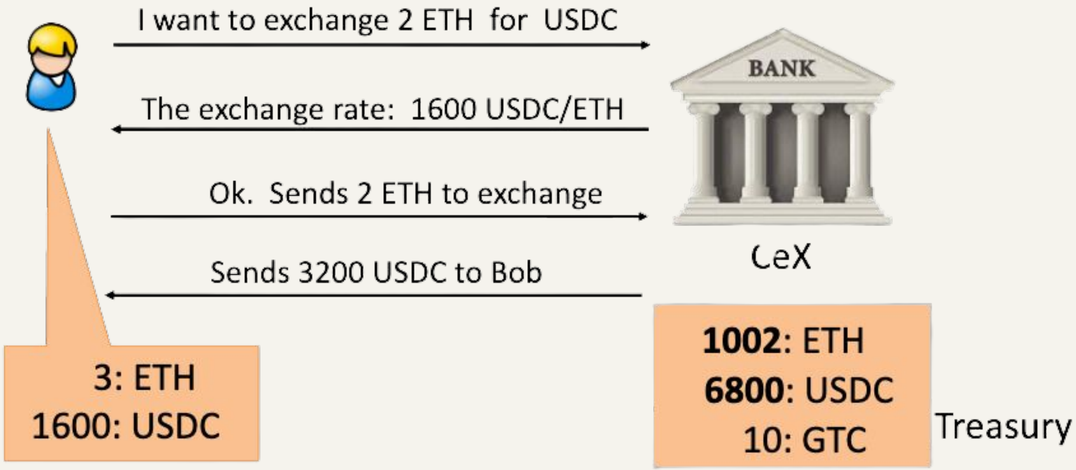
- What is the exchange rate?
- How to connect sellers and buyers?

How is the exchange rate determined?

- By supply and demand at the exchange (not transparent)
- Competition with other exchanges (bad user experience)



What is an exchange?



Considerations:
Security: What if the exchange takes Bob's 2 ETH, but never sends USDC?
Censorship: What if exchange refuses to do business with Bob?

What is a DeX?

What is a DeX (Decentralized Exchange)?
A marketplace where transactions occur directly between participants, without the need of a trusted intermediary.

Properties:
• Programmable: built on smart contracts, and be used as a service by other contracts
• Transparent: code is available for everyone to see, verify the functionality of the DeX.
• Permissionless: anyone can use them, no need for identification/verification process
• Non-Custodial: users are able to retain control of their funds

Building a DeX?

First idea: On-chain Order Book:
• Liquidity providers place buy/sell orders on-chain.
• Users fill them on-chain

Def: An order book is a list of buy and sell orders for a specific asset, organized by price level.

Problem: Gas inefficient.
• Orders cost gas: when placed, when filled, when cancelled.
• Matching buy orders to sell orders takes lots of gas (but see here).
• However, it is feasible on chains with cheap gas.

AMMs (Automated Market Makers)

Traditional exchanges rely on order books to match buyers and sellers. Automated Market Makers (AMMs): AMMs, on the other hand, use a different mechanism called liquidity pools.

In a **liquidity pool**, users deposit two assets, and these assets are traded against each other. The price of the assets is determined by a mathematical formula based on the ratio of the two assets in the pool.

This allows for **instant trades**, as the price is automatically calculated and doesn't rely on finding a matching buyer or seller. This mechanism enables trading even if the order book depth (i.e., the number of buy and sell orders) is low.

Examples: Uniswap, SushiSwap, PancakeSwap, Balancer.

AMMs (Automated Market Makers)

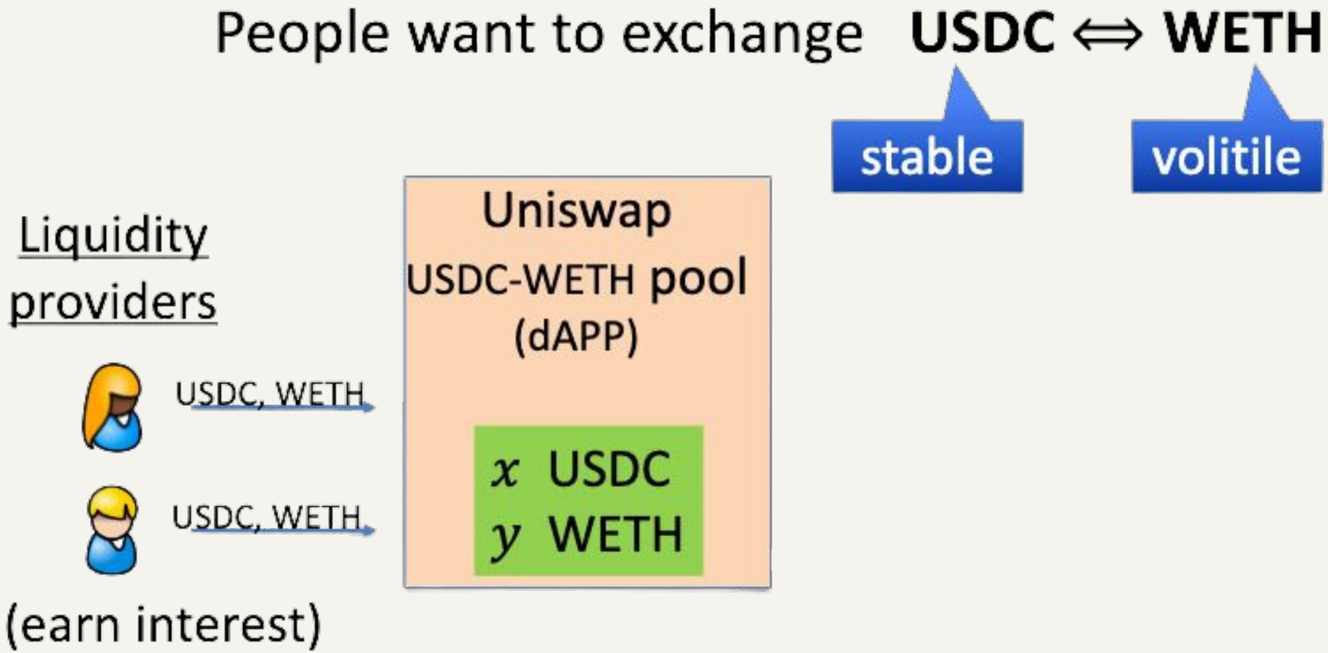
Benefits:

<u>Gas-Efficient:</u> AMMs are designed to be gas-efficient.

<u>Accessible to Contracts:</u> Because AMMs are built on smart contracts, they can be easily integrated with other smart contracts on the same blockchain.

<u>Easy to Bootstrap:</u> AMMs can be easily bootstrapped (i.e., started from scratch) because they don't require a large number of buyers and sellers to start operating. As long as there are liquidity providers willing to deposit tokens, a new AMM can start facilitating trades.

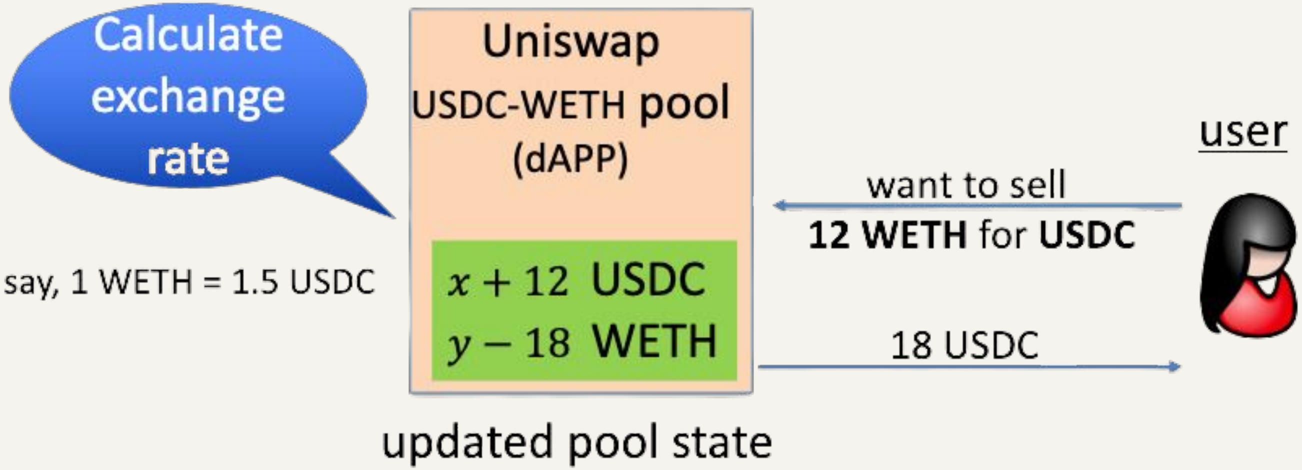
AMMs (Automated Market Makers)



Credit: Dan Boneh

AMMs (Automated Market Makers)

Goal: People want to exchange **USDC ⟺ WETH**



Credit: Dan Boneh

AMMs (Automated Market Makers)

Example:

Imagine a pool that starts with an equal number of two tokens, say 100 X tokens and 100 Y tokens. Now, if someone wants to buy X using Y, they'd have to deposit Y tokens and remove/get back X tokens.

If they decide to buy 10 X tokens, they might need to deposit, say, 12 Y tokens (due to the price increase as per the formula).

Now the pool has 90 X and 112 Y. As you can see, the quantities have changed, and so has the price for the next person who wants to trade.

AMMs (Automated Market Makers)

How to determine the exchange rate?

1. Context of the Pool:
    - The pool has two assets: X and Y. The current state of the pool is described by x units of X and y units of Y.

2. Trade Scenario:
    - Let's imagine Alice decides to trade with the pool. She sends a very small amount dx of X to the pool.
    - In return, the pool sends her an amount dy of Y.

3. Marginal Price Explanation:
    - The term "marginal" is often used in the context of a small or incremental change. Here, it's about the change in the price or rate for that tiny transaction.
    - The change in X (represented by dx) is positive because Alice is adding to the pool.
    - The change in Y (represented by dy) is negative because Alice is receiving Y from the pool. The pool's amount of Y is decreasing by dy.

AMMs (Automated Market Makers)

How to determine the exchange rate?

Pool has (x units of X) and (y units of Y)

<u>Def:</u> marginal price.

Suppose Alice sent dx (an infinitesimal) amount of X to pool; and the pool sent back dy amount of Y.

(change in X is positive, change in Y is negative)

Then the **marginal price** is defined as $p = -dy/dx$ (>0)

The price of a small amount Y in units of X

Credit: Dan Boneh

AMMs (Automated Market Makers)

How to determine the exchange rate?

$$-\frac{dy}{dx} = y/x$$

This diff. eq. has a unique solution:

$$y = \frac{k}{x}\ , \quad \text{for a constant } k \in \mathbb{R}$$

or equivalently, the pool must maintain: $\boxed{x \cdot y = k}$

The constant product formula

NOTE: The formula x * y = k ensures that the total value in the pool remains constant.

Credit: Dan Boneh

AMMs (Automated Market Makers)

How to determine the exchange rate?

$$-\frac{dy}{dx} = y/x$$

This diff. eq. has a unique solution:

$$y = \frac{k}{x}, \quad \text{for a constant } k \in \mathbb{R}$$

or equivalently, the pool must maintain: $x \cdot y = k$

The constant product formula

The derivative -dy/dx represents the rate of change of y with respect to x. In other words, it tells us how much y changes for a small change in x.

The negative sign indicates that y and x are inversely related. As x increases, y decreases, and vice versa.

If we rearrange the derivative equation dy/dx = y / x to dy = -y/x * dx and integrate both sides, we get the equation x * y = k, where k is the constant of integration.

NOTE: The formula x * y = k ensures that the total value in the pool remains constant.

AMMs (Automated Market Makers)

How to determine the exchange rate?

$$x * y = k$$

$$x \cdot y = 120$$

The constant product market maker:

- Say: $x = 10$ WETH, $y = 12$ USDC

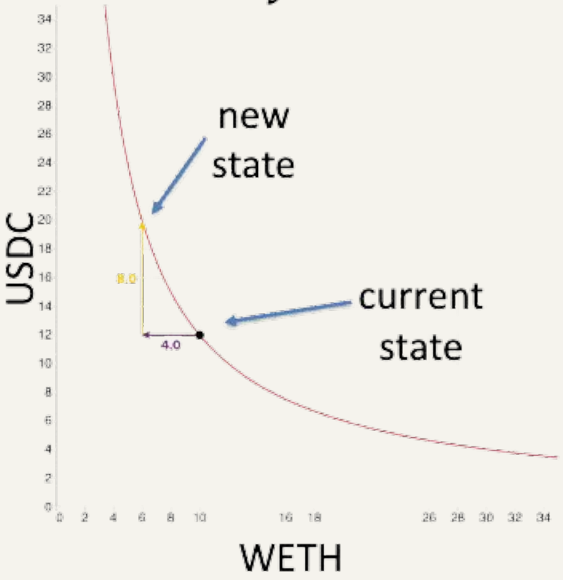
  $10 \times 12 = 120$

- Alice wants to buy 4 WETH from pool

  $x \rightarrow x - 4 = 6$

  To maintain $x * y = 120$ Alice needs to send 8 USDC to pool

  $y \rightarrow y + 8 = 20$



Credit: Dan Boneh

Uniswap v2

$x \cdot y = k$; Alice wants to buy $\Delta x \in (0, x)$ from pool.

How much Δy should she pay?

$$(x - \Delta x) \cdot (y + \Delta y) = k \quad \Rightarrow \quad \boxed{\Delta y = \frac{y \cdot \Delta x}{x - \Delta x}}$$

(solve for Δy and simplify)

But liquidity providers (LP's) take a fee $\phi \in [0,1]$ (say ϕ=0.97)

Alice pays Δy: pool gets $\phi \Delta y$, LP's get $(1 - \phi)\Delta y$

so: $(x - \Delta x) \cdot (y + \phi \Delta y) = k \quad \Rightarrow \quad \boxed{\Delta y = \frac{1}{\phi} \cdot \frac{y \cdot \Delta x}{x - \Delta x}}$

Credit: Dan Boneh

Uniswap v2

Uniswap V2 uses the constant product formula for its Automated Market Maker (AMM) system, which is given by:

$x \cdot y = k$

Here:

- x and y are the quantities of the two tokens in the liquidity pool.
- k is a constant value.

Now, Uniswap doesn't execute trades for free. Liquidity Providers (LPs) earn a fee for the liquidity they provide. This fee is taken from the traded amount.

- If ϕ represents the fee fraction (for example, $\phi = 0.03$ or 3%), then:
  - The pool receives $\phi\Delta y$ of the trade.
  - Alice will receive $(1 - \phi)\Delta y$.

The updated trade equation with the fee becomes:

$(x - \Delta x) \cdot (y + \phi\Delta y) = k$

And the amount Alice receives after accounting for the fee is:

$\Delta y = \frac{1}{\phi} \cdot \frac{y \cdot \Delta x}{x - \Delta x}$

Uniswap v2

Now, Uniswap doesn't execute trades for free. Liquidity Providers (LPs) earn a fee for the liquidity they provide. This fee is taken from the traded amount.

- If ϕ represents the fee fraction (for example, $\phi = 0.03$ or 3%), then:
  - The pool receives $\phi \Delta y$ of the trade.
  - Alice will receive $(1 - \phi)\Delta y$.

The updated trade equation with the fee becomes:

$(x - \Delta x) \cdot (y + \phi \Delta y) = k$

And the amount Alice receives after accounting for the fee is:

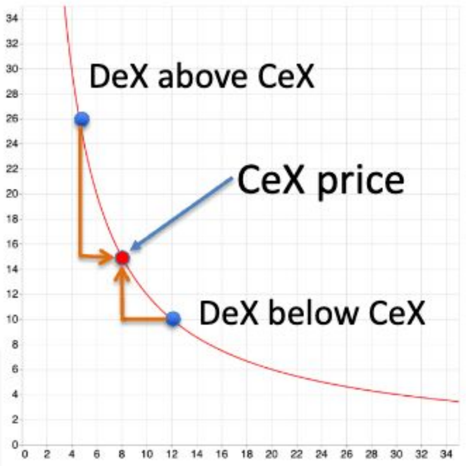
$\Delta y = \frac{1}{\phi} \cdot \frac{y \cdot \Delta x}{x - \Delta x}$

Feature: Automatic Price Discovery

Thm: the marginal price y/x converges to the market exchange rate

To summarize:

- DeX state is below CeX state
  $\Rightarrow$ arbitrageurs will move DeX up
- DeX state is above CeX state
  $\Rightarrow$ arbitrageurs will move DeX down



DeX marginal price matches market price, without ever being told the market price !!

Credit: Dan Boneh

Uniswap v3

Introducing Concentrated Liquidity

Concentrated Liquidity:

- Uniswap V3 introduced the concept of "Concentrated Liquidity."
- In V3, LPs can specify a price range where their liquidity will be utilized.
- If the price of the assets stays within this specified range, LPs can achieve much better returns because their capital is used more efficiently.
- This also results in deeper liquidity for users transacting within that price range.

Benefits of Concentrated Liquidity in V3:

- Allows LPs to provide liquidity with less capital.
- More capital efficiency can lead to better returns for LPs.
- Users get deeper liquidity in the price ranges where liquidity is concentrated.

AMMs (Automated Market Makers)

Problem 1: Slippage

Definition: Slippage occurs when the executed trade price is different from the expected price.

Causes:
In Automated Market Makers (AMMs) like Uniswap, the larger the trade, the worse the exchange rate becomes for the user.
The user ends up paying more or receiving less than what the initial price indicated.

Example:
If Alice wants to purchase the entire pool (i.e., $\Delta x = x$), the price would be infinite. This indicates that a user can never deplete an entire liquidity pool in such AMMs.
The effective price is represented by the negative slope of the tangent, which signifies the market price.
Users often end up paying more than what the market price indicates due to slippage.

Conclusion: The pool will never run out of X or Y tokens due to the mechanics of AMMs.

AMMs (Automated Market Makers)

Problem 2: Sandwich Attack

Scenario:
Alice wants to sell Δx USDC to a pool.
Under normal conditions, she'd get back $\Delta y = y\ \Delta x/(x - \Delta x)$ WETH.

Attack:
Sam sees Alice's transaction in the mempool (a pool of pending transactions).
He exploits this by making two transactions of his own:
In Tx1, Sam sells 5 USDC to the pool, receiving some amount **n** WETH (with a high transaction fee for quicker execution).
In Tx2, Sam then sells the **n** WETH he just acquired, getting back **n’** USDC (with a low transaction fee).

Impact:
Sam's first transaction (Tx1) impacts the pool's rates, so when Alice's transaction executes, she receives less WETH ($\Delta y'$) than she should have (Δy).
Sam profits from Alice, as the USDC he gets back in his second transaction (**n'**) is more than the 5 USDC he initially sold, making him a profit of (**n'** - 5) USDC at Alice's expense.

Note: Such frontrunning attacks aren't exclusive to crypto markets. They also occur in traditional financial markets.

AMMs (Automated Market Makers)

FAQs

Who sets the original price of the pool?

The initial price in an AMM like Uniswap is set by the first liquidity provider when they seed the pool with a certain quantity of two assets. The ratio at which they deposit these assets effectively sets the initial price. For example, if someone initializes a pool with 10 ETH and 2000 USDC, the initial price is effectively set at 200 USDC per ETH.

AMMs (Automated Market Makers)

FAQs

If there were no centralized exchange, how would the DeX know the price of the assets in the pool without the use of arbitrage opportunities?

If there's no centralized exchange (CeX) for reference, the DeX wouldn't "know" the price in the traditional sense. Instead, the price would be set purely by supply and demand dynamics on the DeX. Traders would come to the platform and buy/sell, and with each trade, the price would adjust based on the constant product formula. The price would simply reflect the collective valuation of that asset by the market participants on that DeX. In a way, CeXes also function similarly: their prices are determined by the supply and demand of their own users, but the presence of many external references and higher liquidity often makes their prices a reference point for other markets.

Thanks!

Do you have any questions?