Decentralized Finance

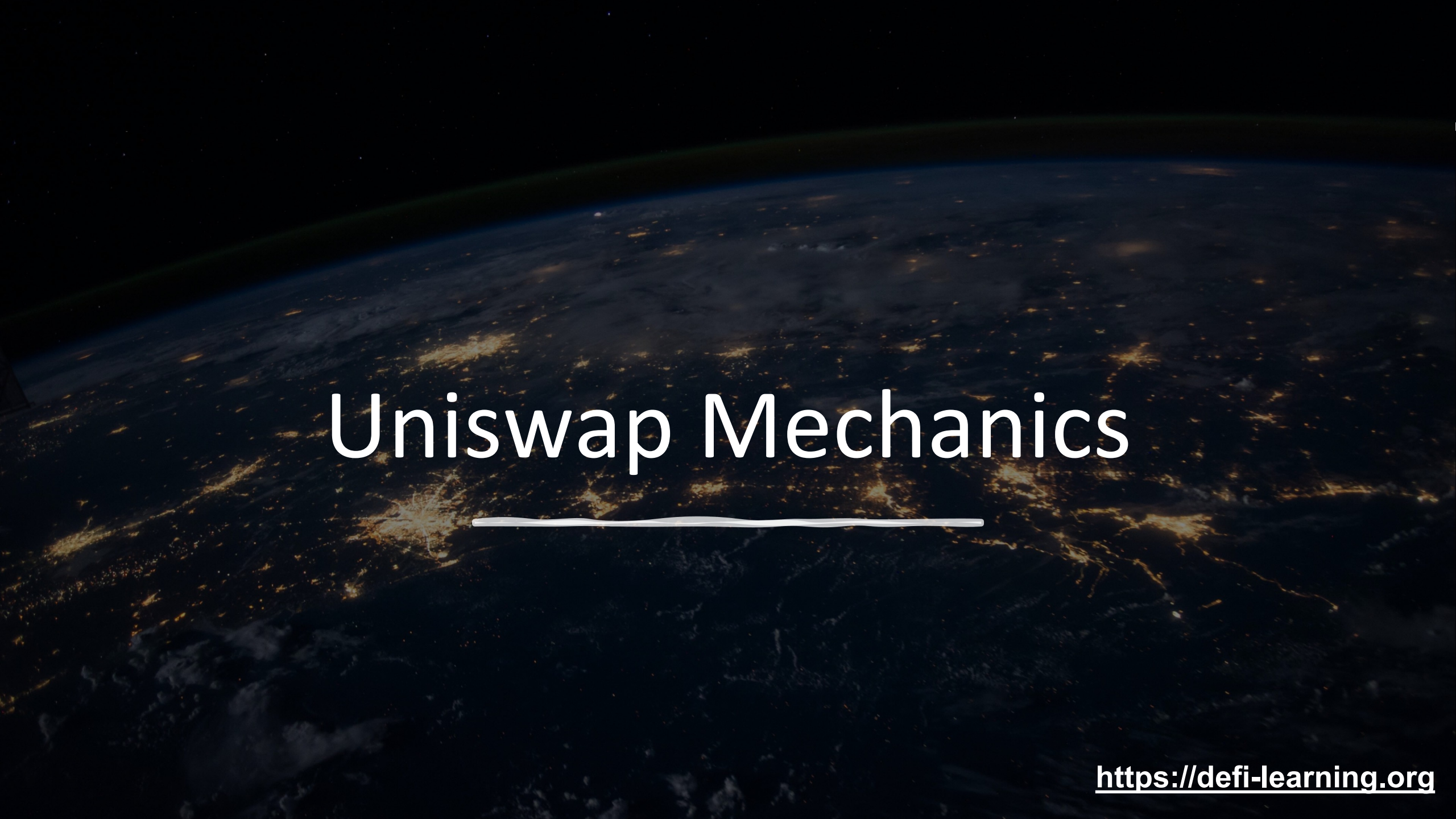
Case Study: Uniswap

Guest Lecture: **Dan Robinson** (Paradigm)

Paradigm

Uniswap

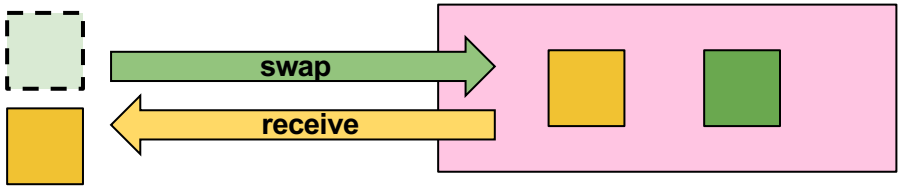
- Decentralized exchange on Ethereum
  - >$10 billion volume per week, >$6 billion of tokens used as liquidity
- Permissionless
  - Anyone can create a trading pair for any two ERC-20 tokens
- Non-custodial
  - Nobody can shut it down or steal funds (unless the blockchain is compromised or the smart contracts have a bug)
- Censorship-resistant
  - Anyone who can send transactions on Ethereum can use it



https://defi-learning.org

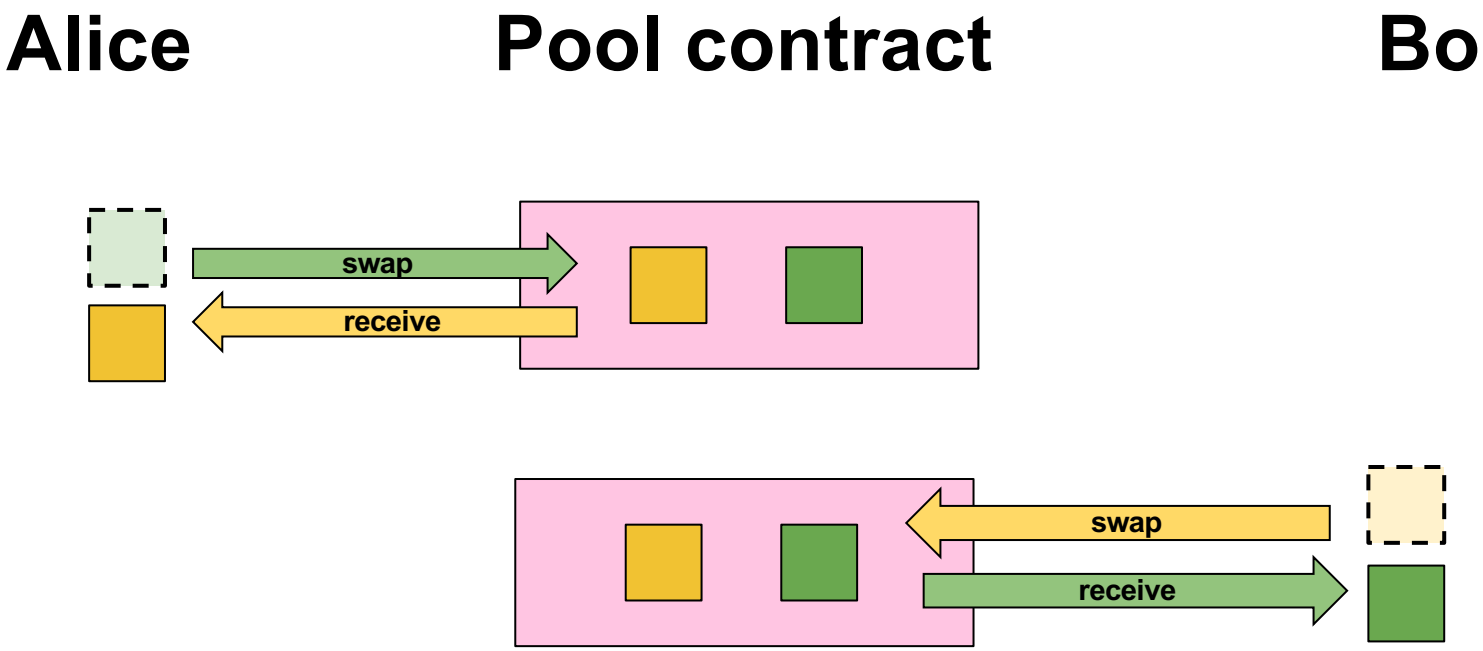
Uniswap Mechanics: Trading

Alice **Pool contract**



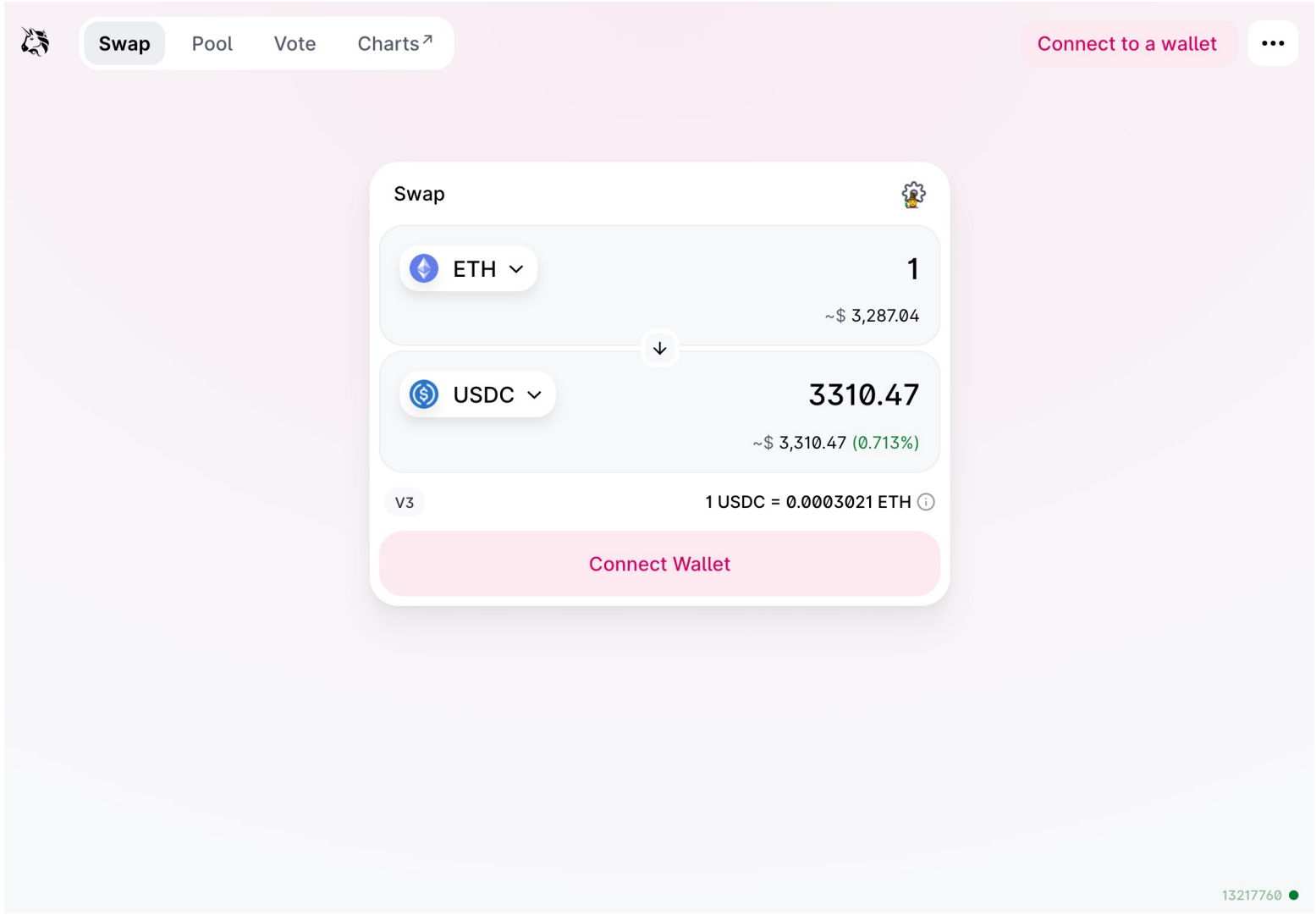

```
function swap(uint amount0Out, uint amount1Out, address to, bytes calldata data) external;
```

Uniswap Mechanics: Trading




```
function swap(uint amount0Out, uint amount1Out, address to, bytes calldata data) external;
```

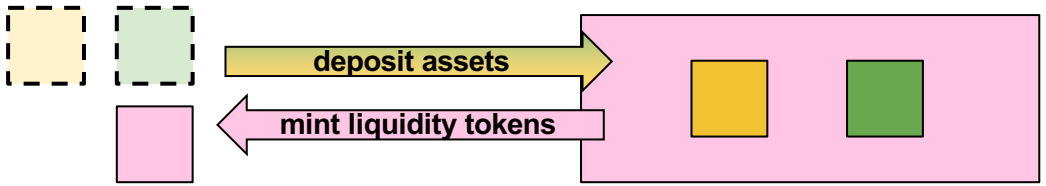
Uniswap Mechanics: Trading



Uniswap Mechanics: Adding Liquidity

Liquidity provider

Pool contract

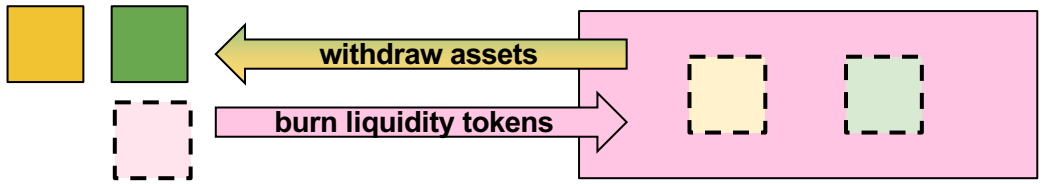



```
function mint(address to) external returns (uint liquidity);
```

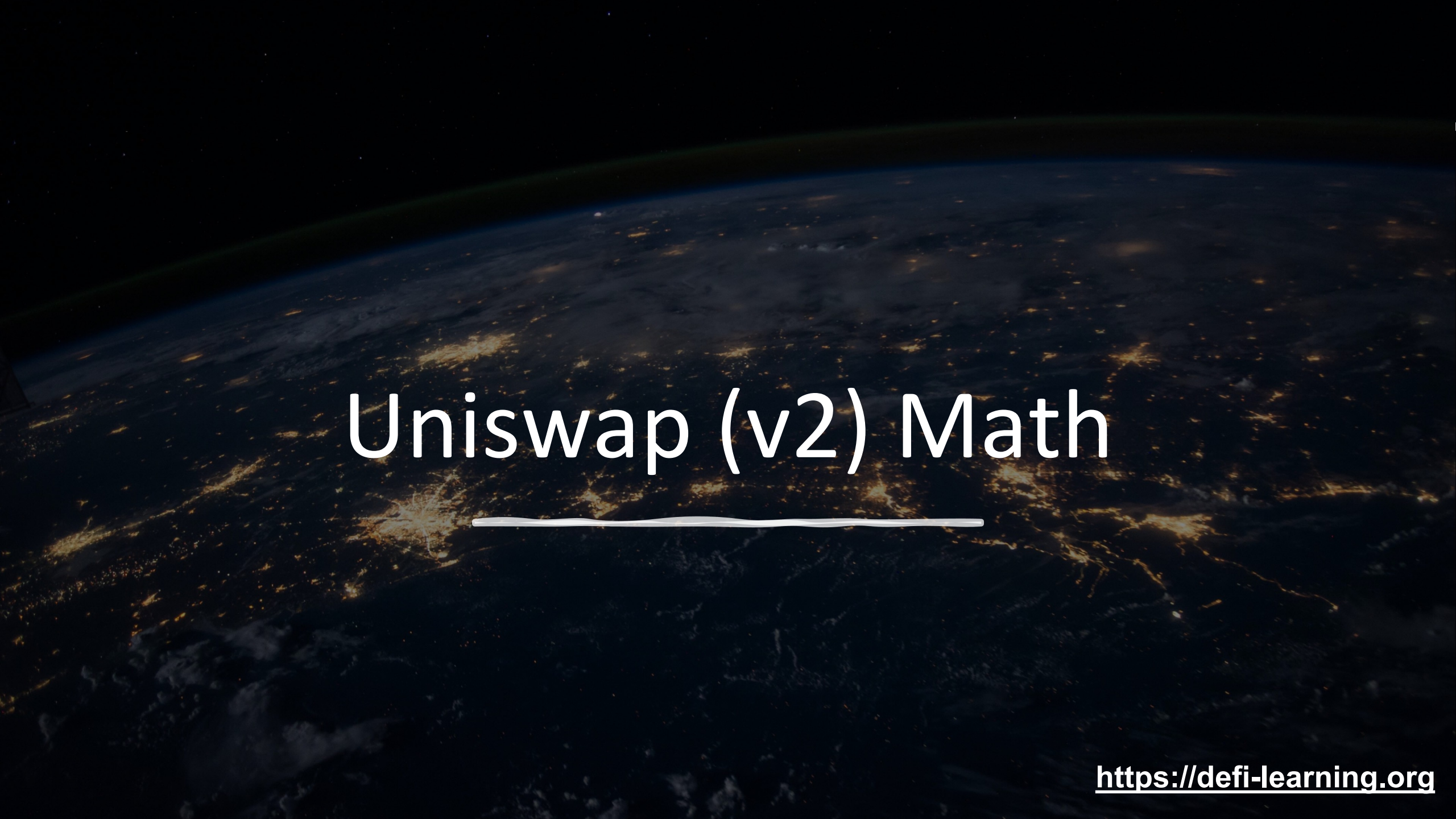
Uniswap Mechanics: Removing Liquidity

Liquidity provider

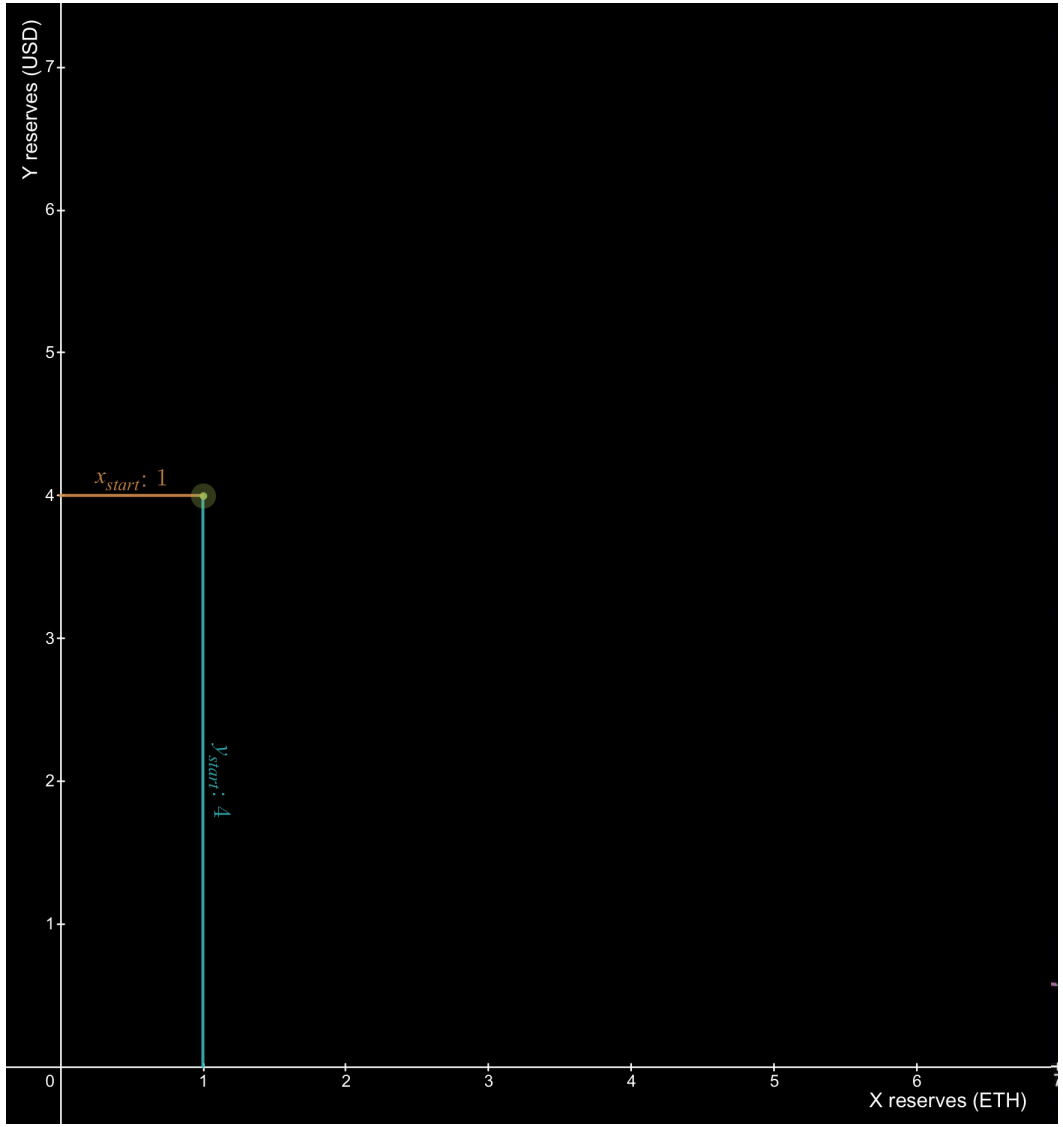
Pool contract




```
function burn(address to) external returns (uint amount0, uint amount1);
```

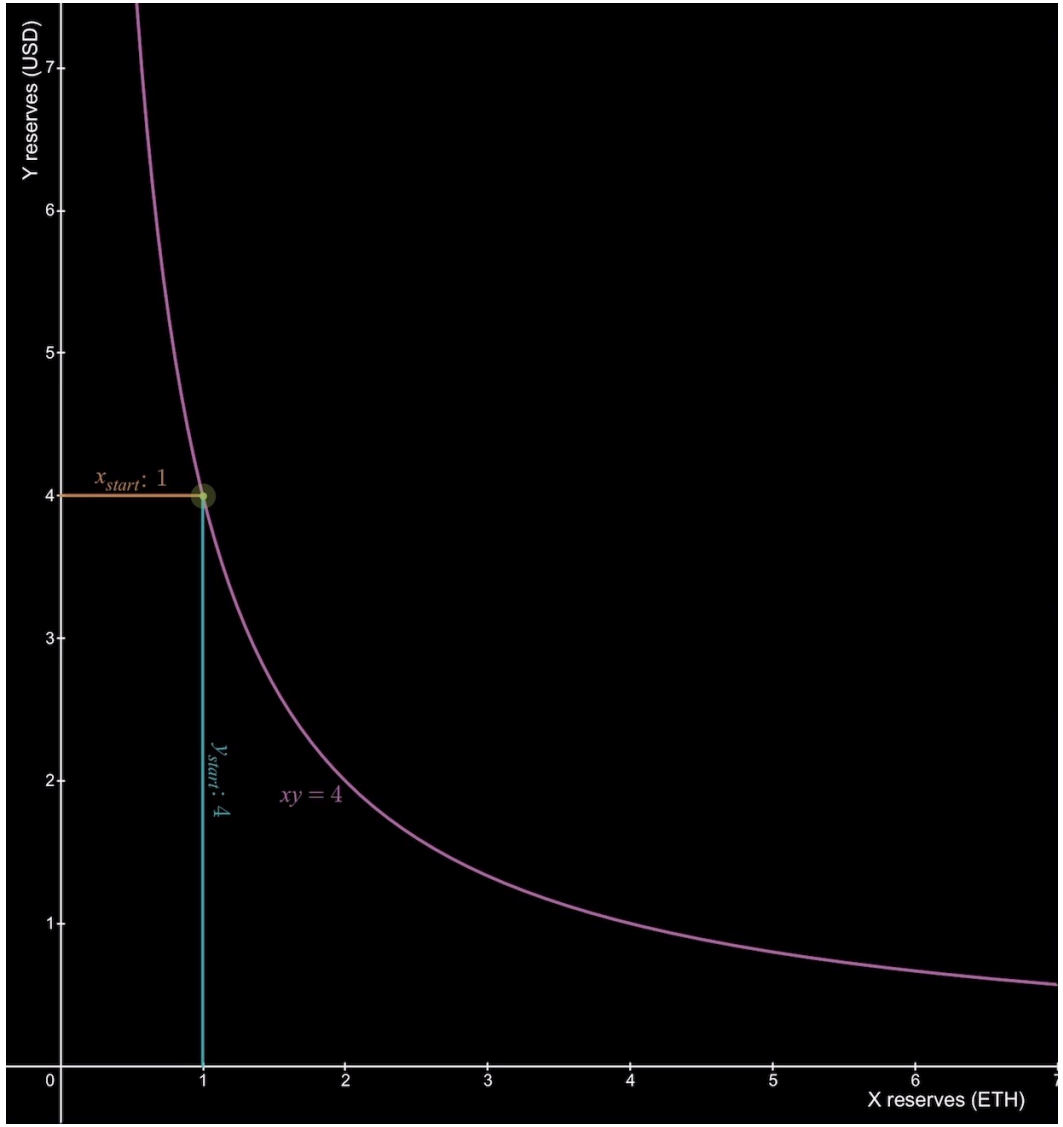

Uniswap (v2) Math
https://defi-learning.org

Uniswap (v2) Math



- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)

Uniswap (v2) Math

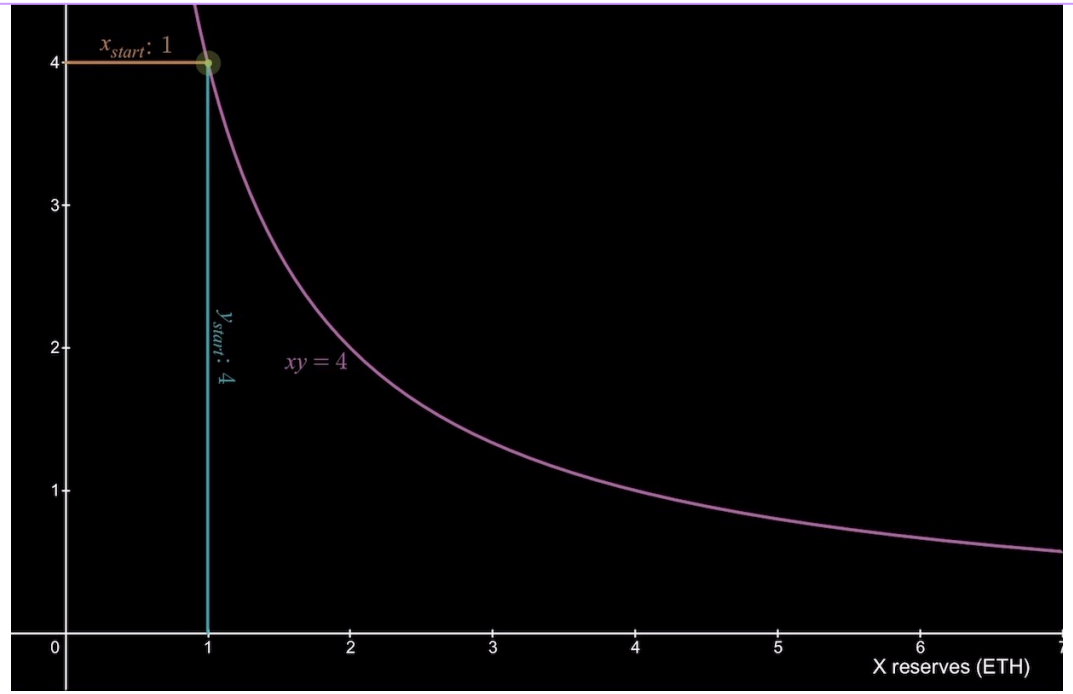


- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**

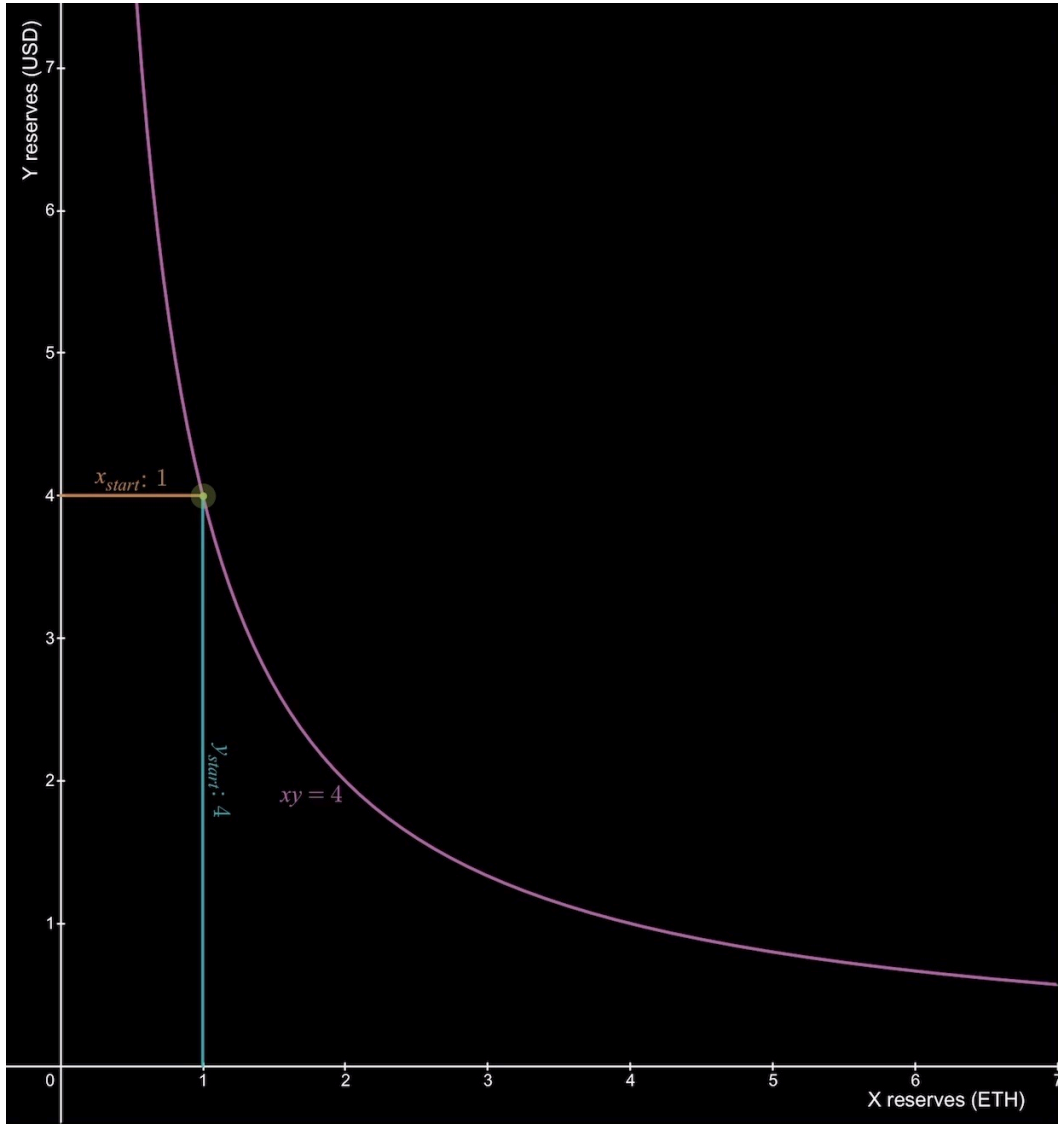
Uniswap (v2) Math

- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**

```
require(balance0Adjusted.mul(balance1Adjusted) >= uint(_reserve0).mul(_reserve1).mul(1000**2), 'UniswapV2: K');
```

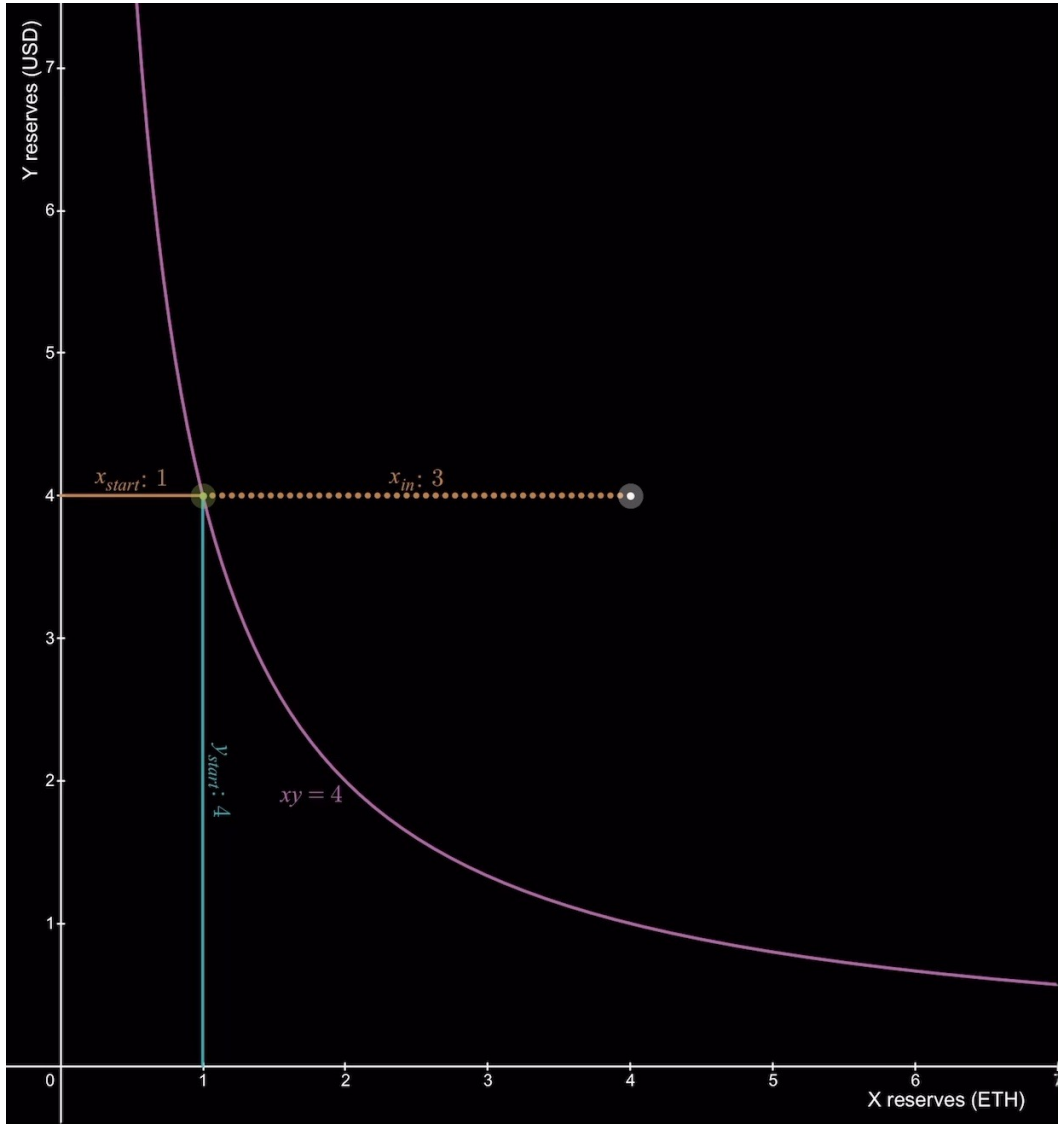


Uniswap (v2) Math



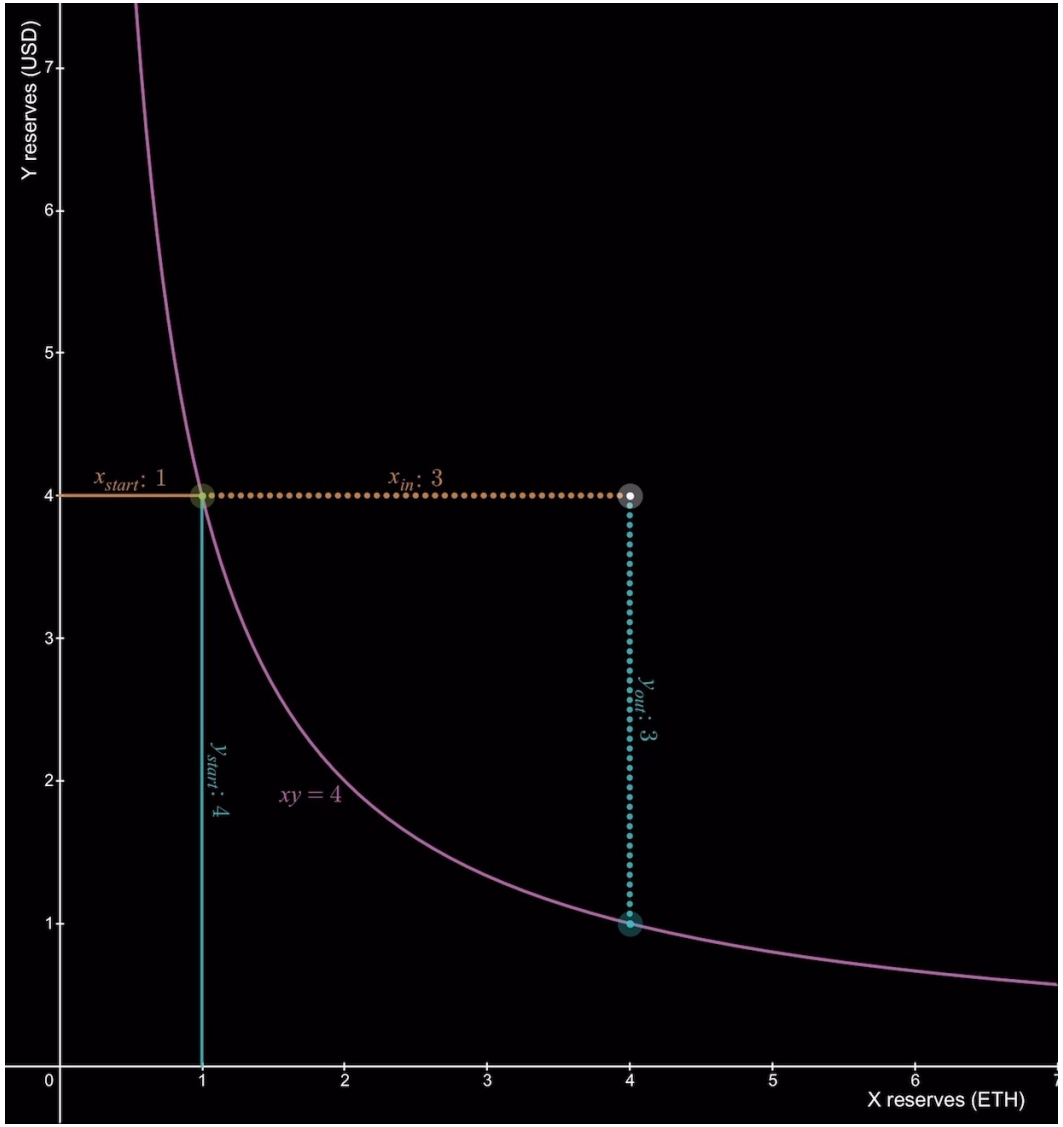
- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**

Uniswap (v2) Math



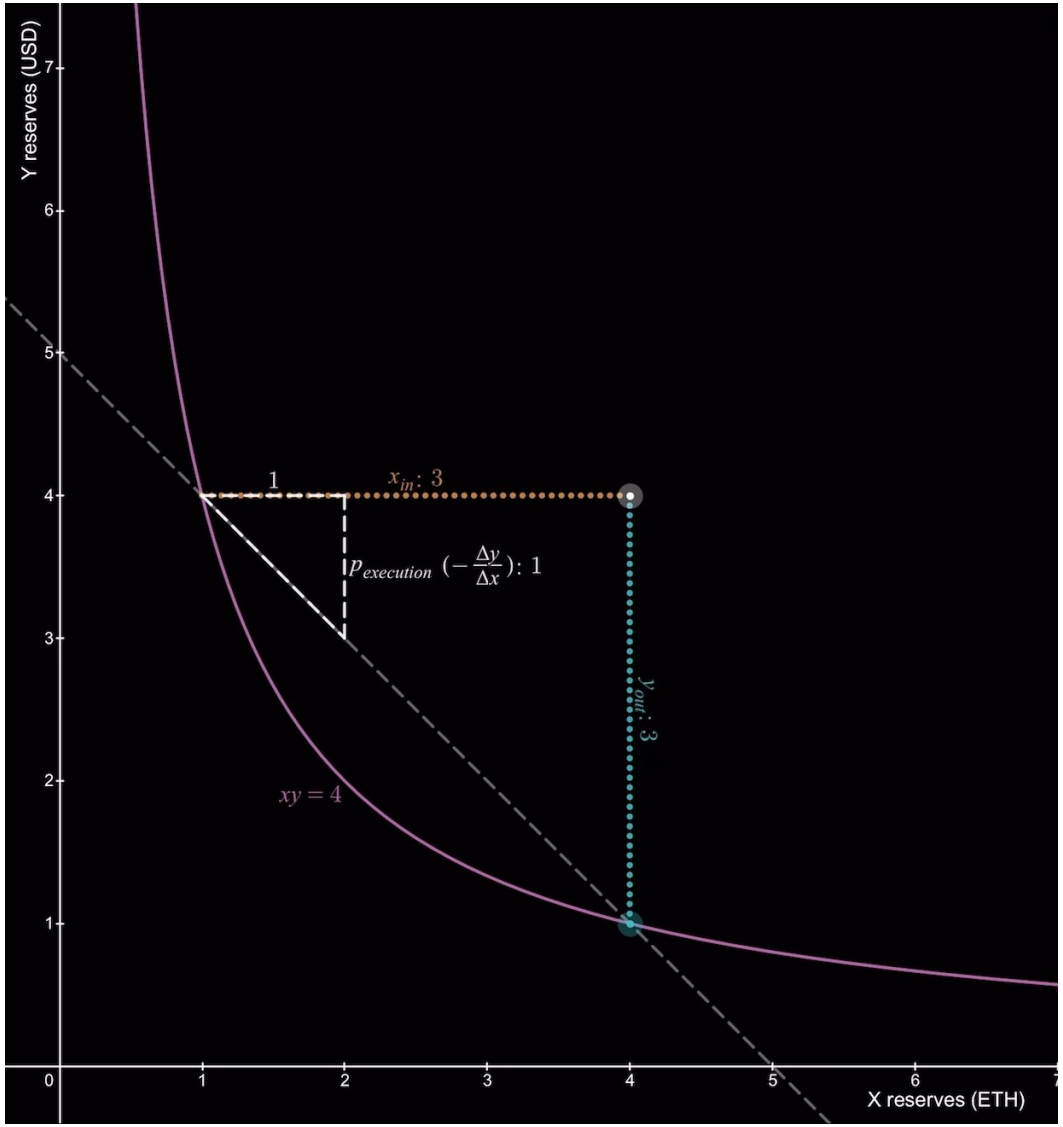
- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**
- Trader sends in some ETH

Uniswap (v2) Math



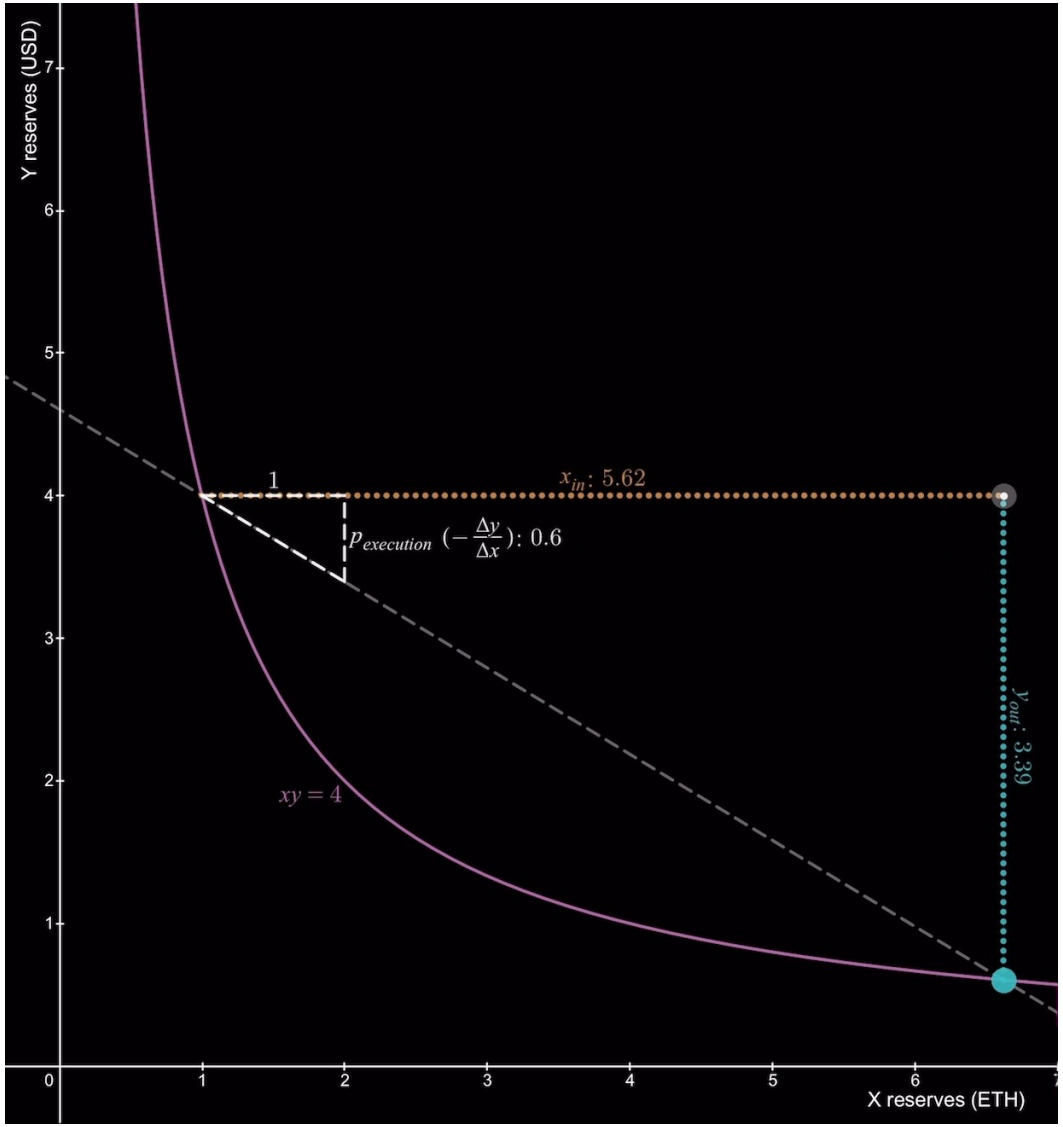
- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**
- Trader sends in some ETH
- Pool sends out as much USD as needed to return to the curve

Uniswap (v2) Math



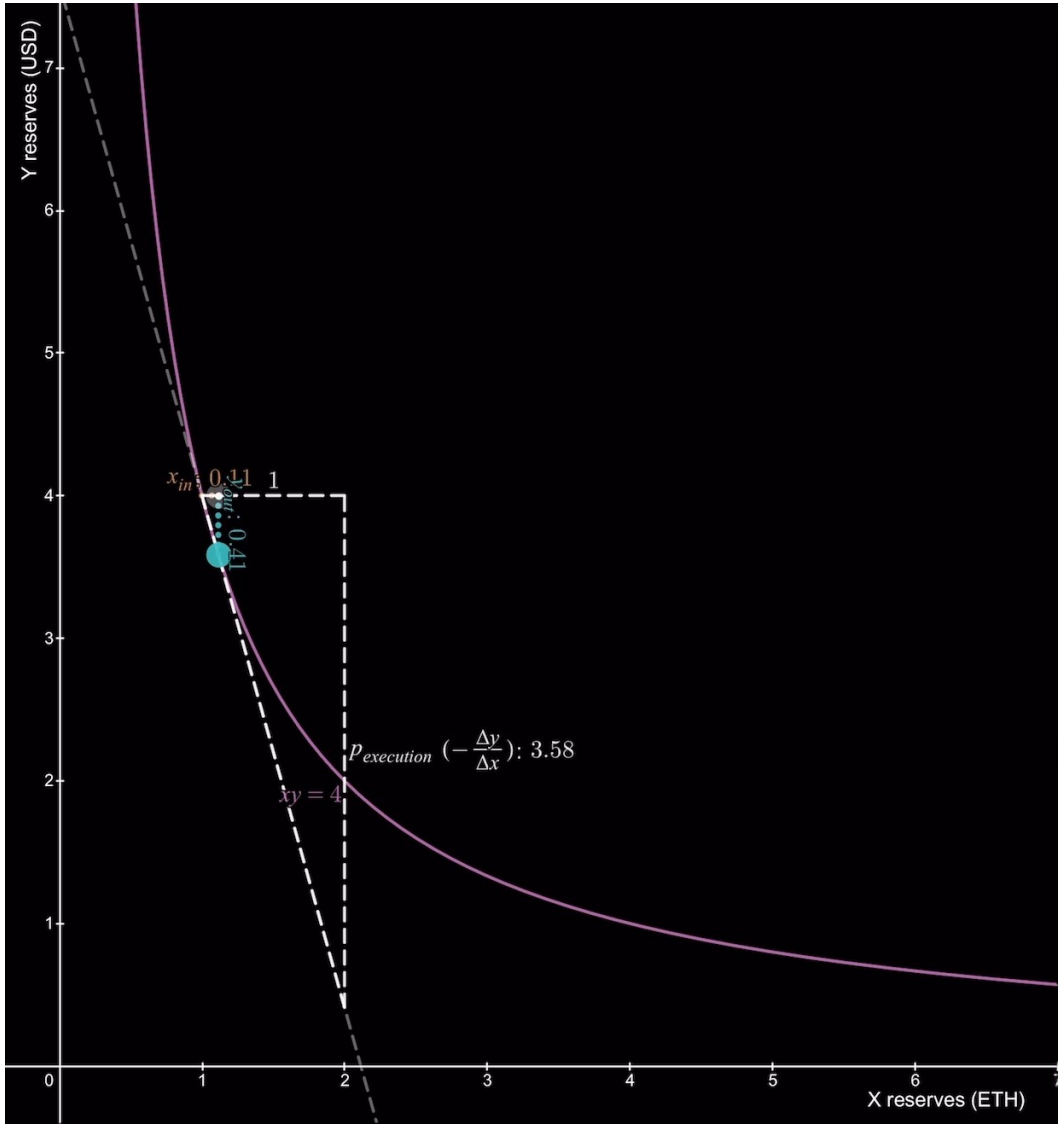
- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**
- Trader sends in some ETH
- Pool sends out as much USD as needed to return to the curve
- The slope of the line between these points is the **execution price** of the trade

Uniswap (v2) Math



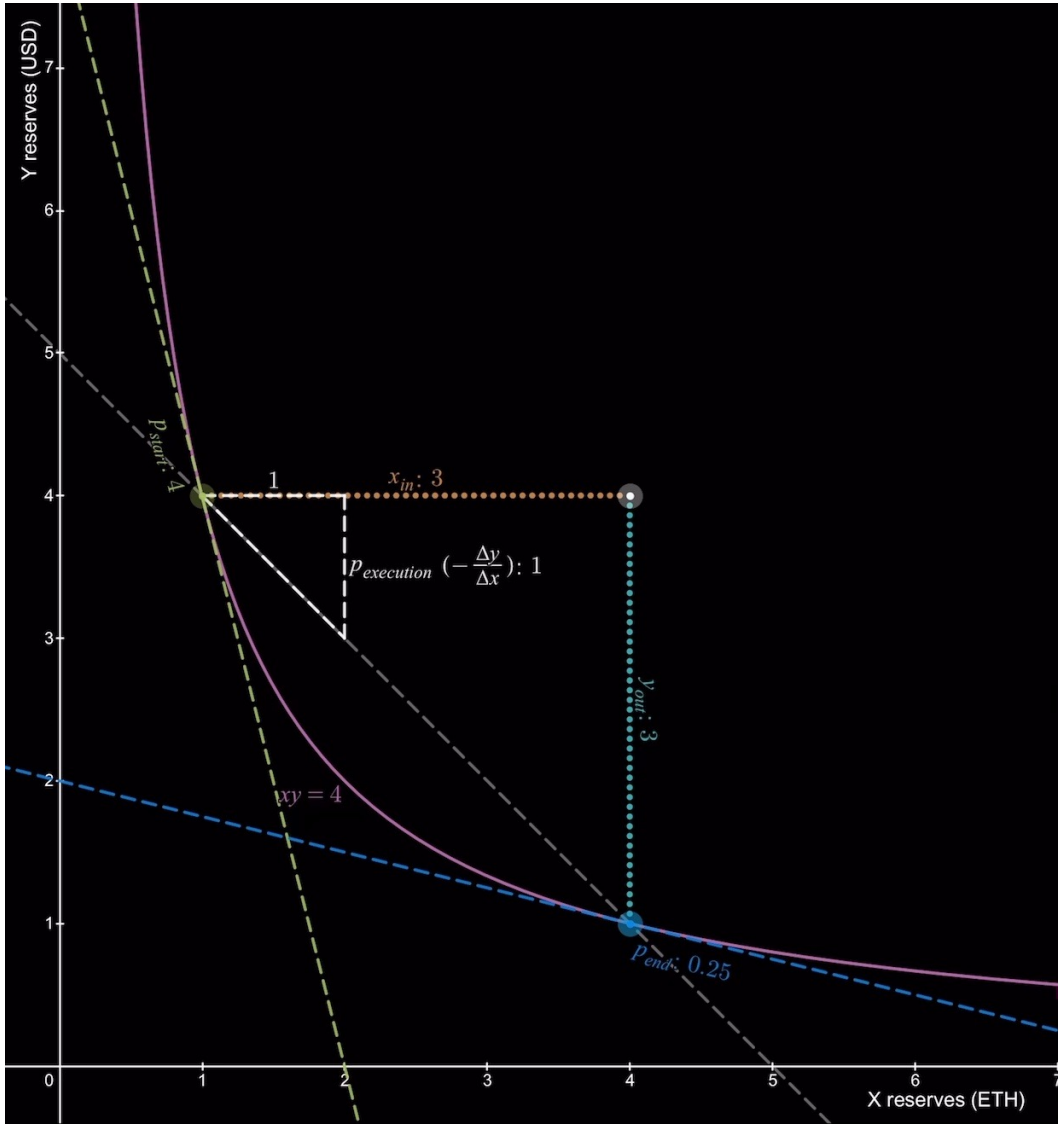
- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**
- Trader sends in some ETH
- Pool sends out as much USD as needed to return to the curve
- The slope of the line between these points is the **execution price** of the trade

Uniswap (v2) Math



- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**
- Trader sends in some ETH
- Pool sends out as much USD as needed to return to the curve
- The slope of the line between these points is the **execution price** of the trade
- The **marginal price** at a point is the slope of the tangent line

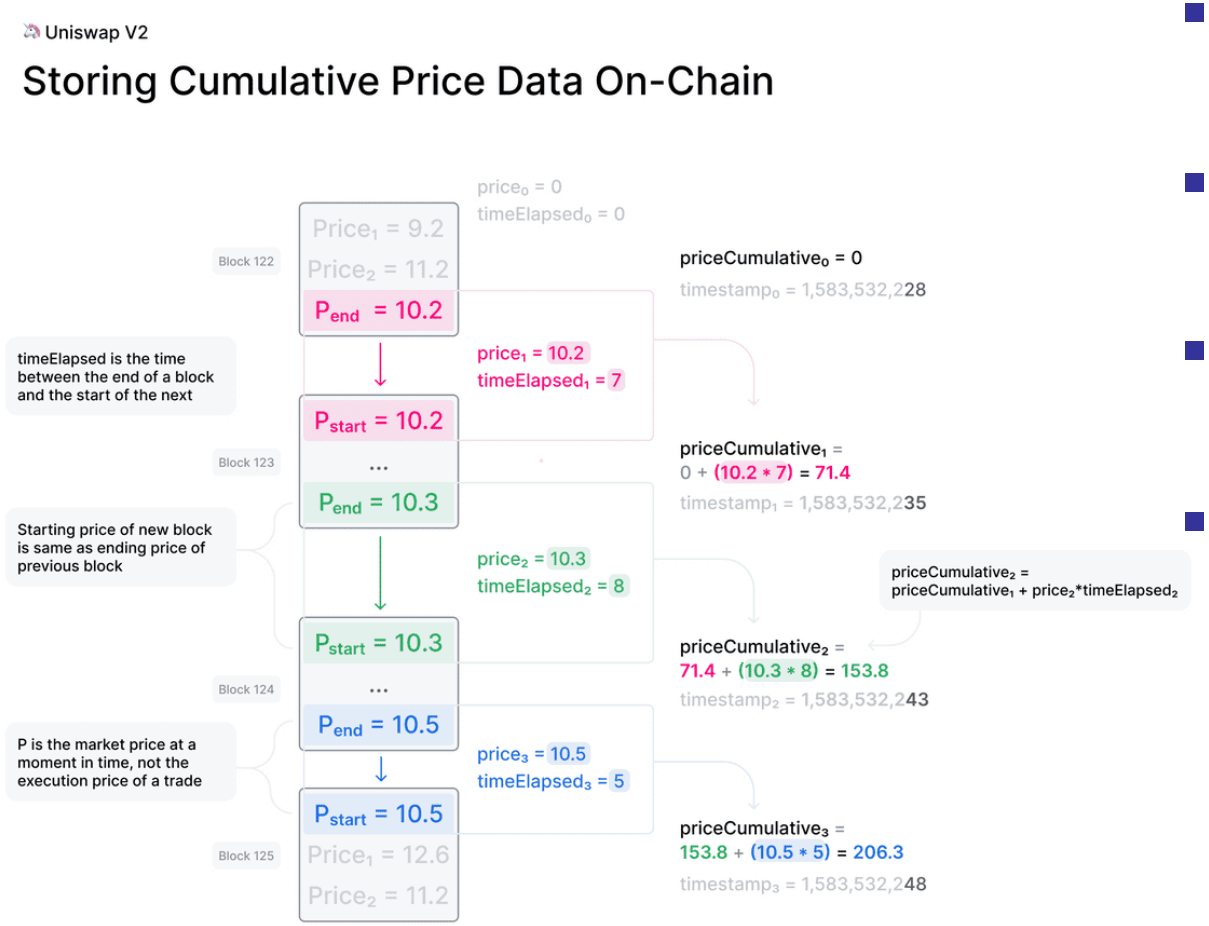
Uniswap (v2) Math



- Pool holds reserves **x** of one asset (say, ETH), **y** of another (say, USD)
- Trades preserve the invariant **xy = k**
- Trader sends in some ETH
- Pool sends out as much USD as needed to return to the curve
- The slope of the line between these points is the **execution price** of the trade
- The **marginal price** at a point is the slope of the tangent line

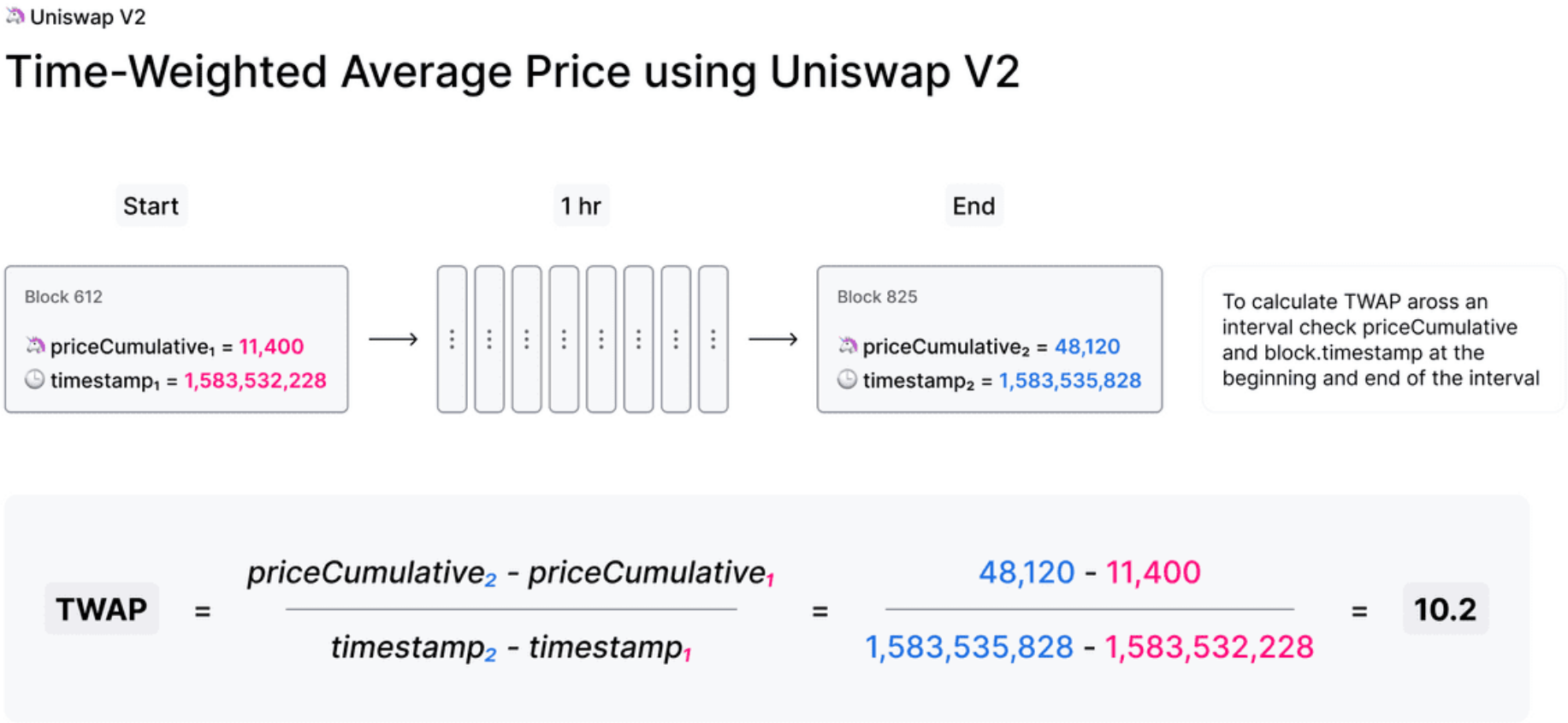
https://defi-learning.org

Uniswap Mechanics: Price Oracle

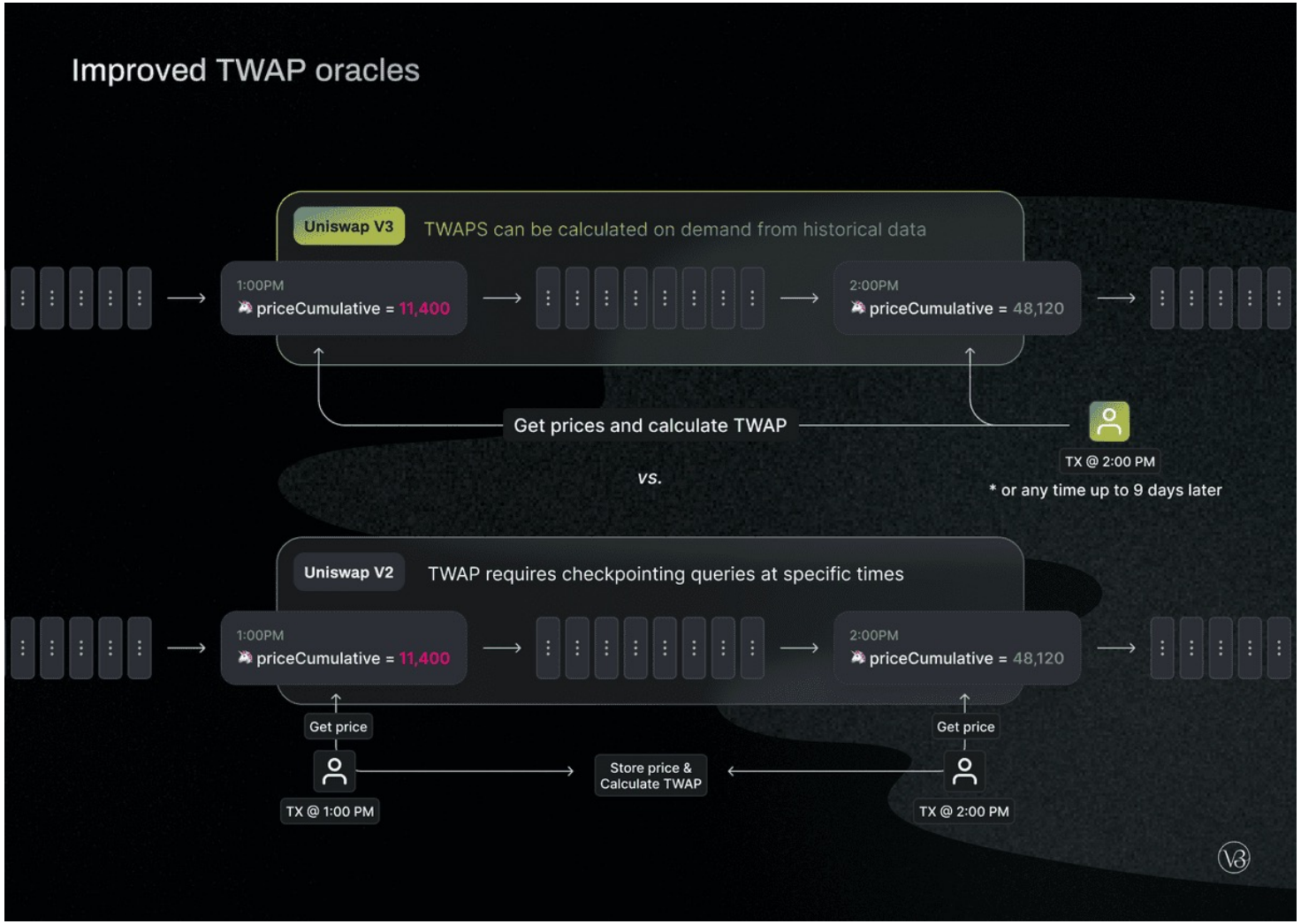


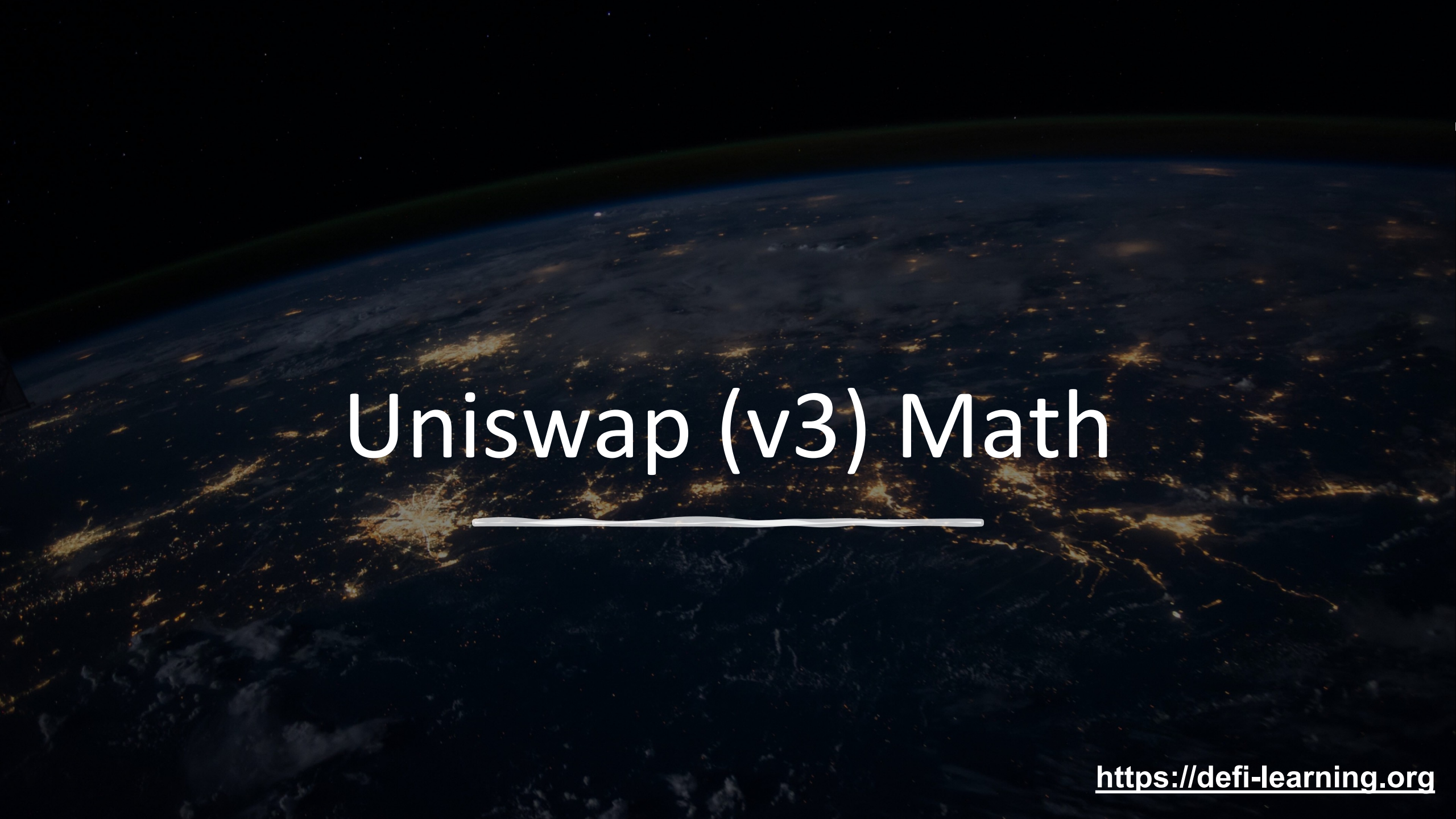
- Many DeFi applications (like synthetics and lending protocols) depend on **price oracles**
- Uniswap can be used as this price oracle for ERC-20 tokens
- But just using the current price is vulnerable to a **sandwich attack**
- To mitigate this, Uniswap v2 and v3 track an accumulator that allows computation of a **time-weighted average price** (TWAP) over many blocks

Uniswap Mechanics: Price Oracle (v2)

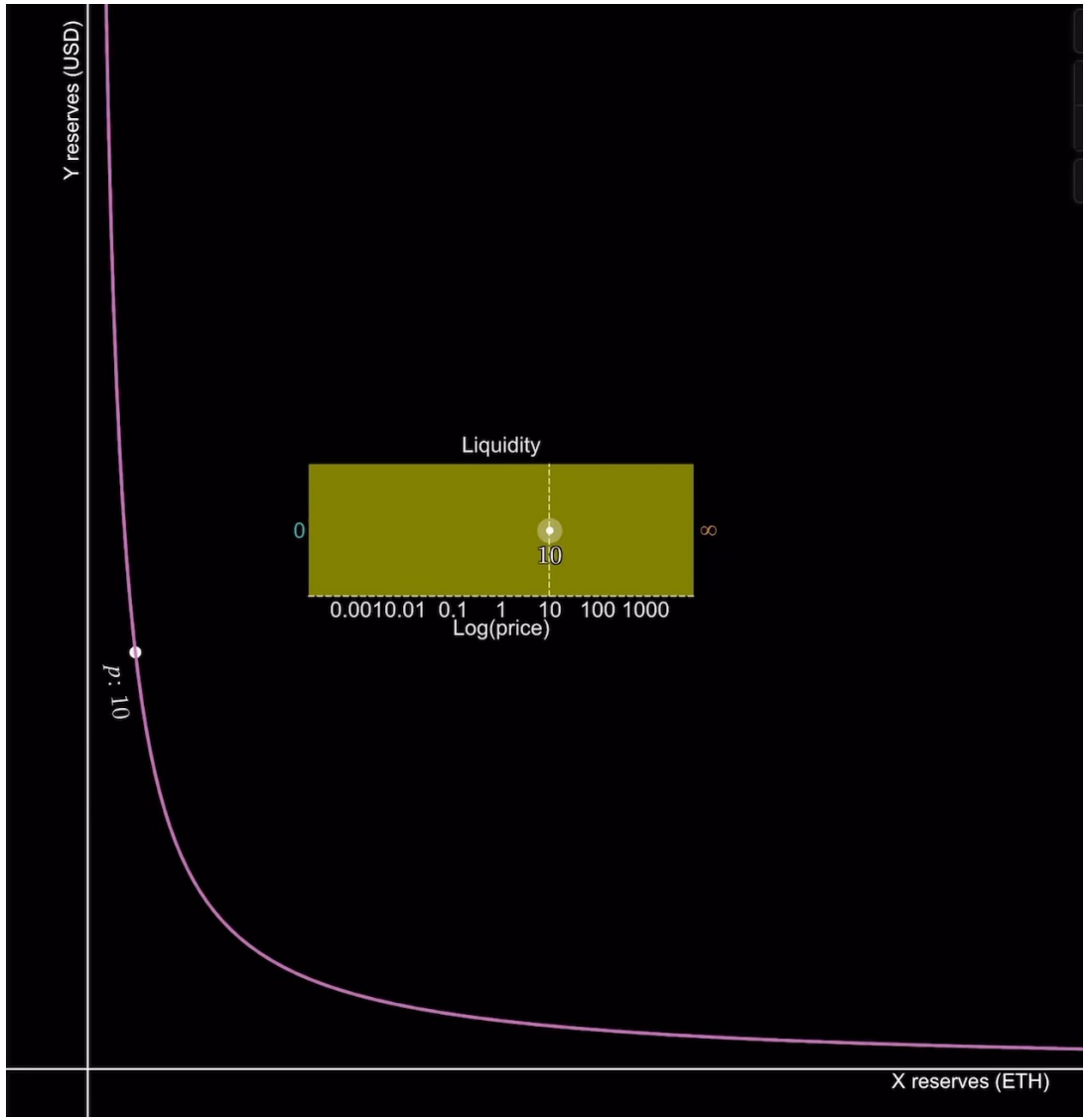


Uniswap Mechanics: Price Oracle (v3)



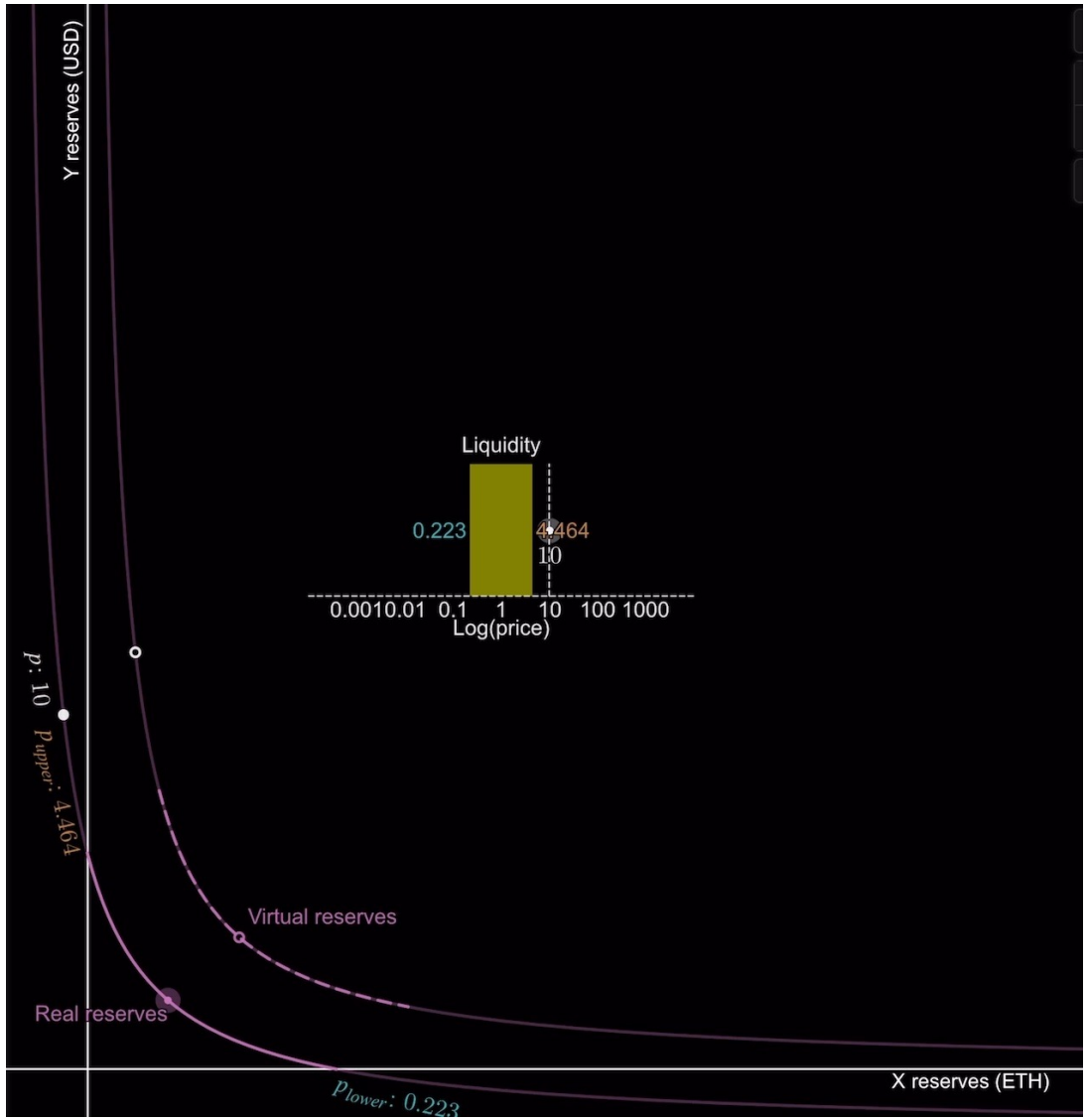

Uniswap (v3) Math
https://defi-learning.org

Uniswap (v3) Math



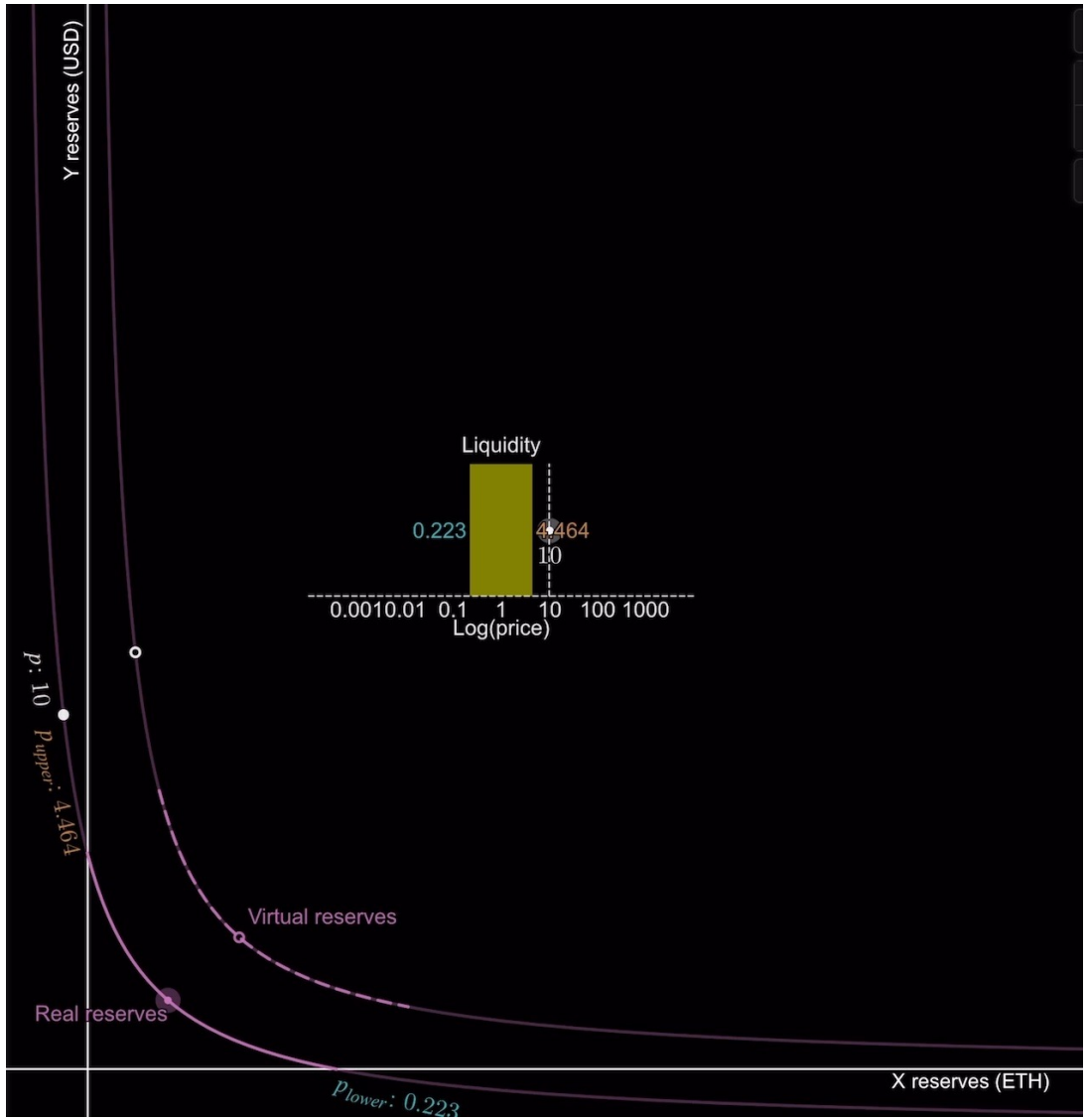
- In Uniswap v2, some reserves are saved for all possible prices, which is capital inefficient

Uniswap (v3) Math



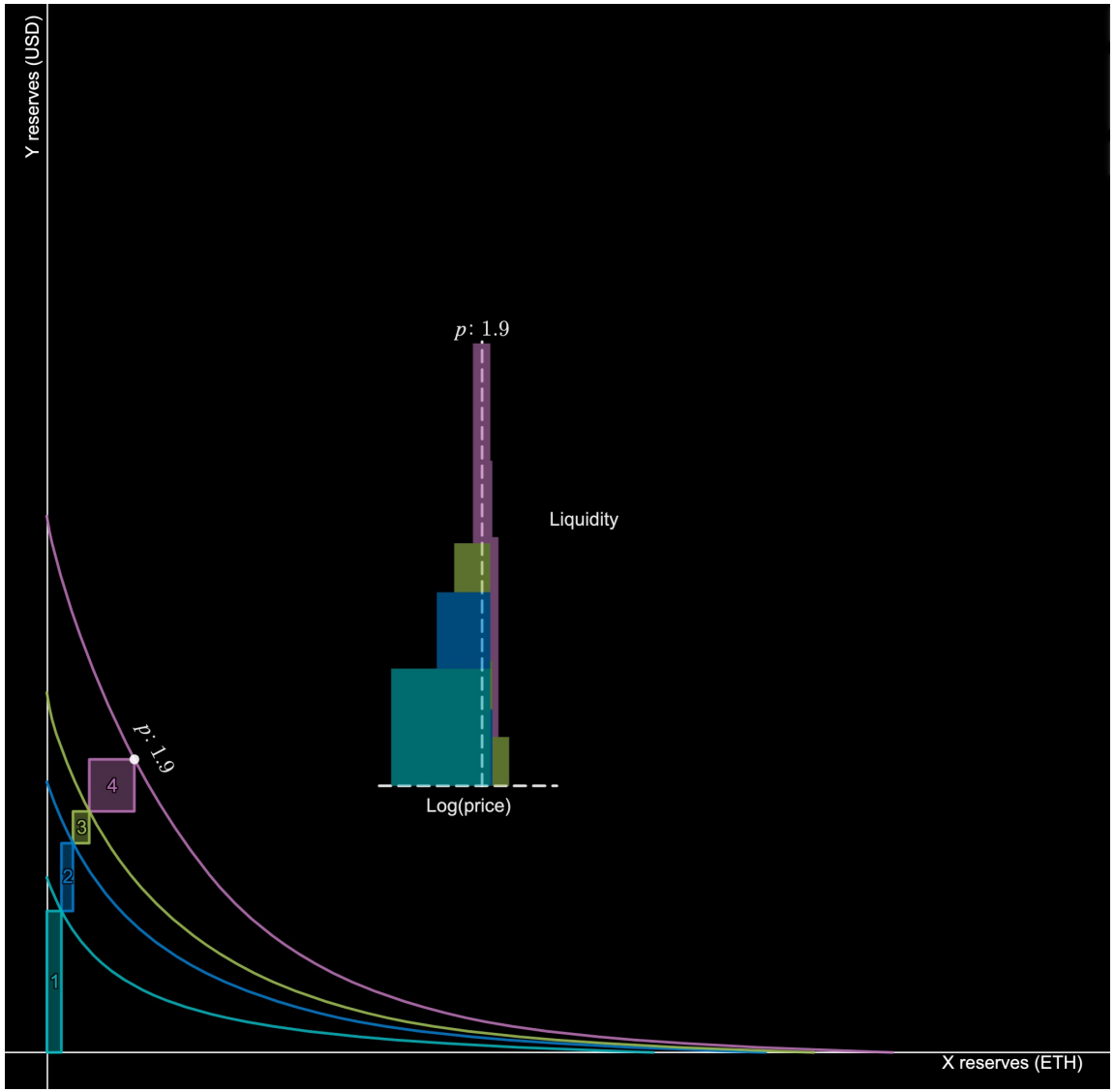
- In Uniswap v2, some reserves are saved for all possible prices, which is capital inefficient
- Uniswap v3 allows liquidity providers to add **concentrated liquidity** within a specific price range

Uniswap (v3) Math



- In Uniswap v2, some reserves are saved for all possible prices, which is capital inefficient
- Uniswap v3 allows liquidity providers to add **concentrated liquidity** within a specific price range
- This is equivalent to translating the **xy = k** curve down and to the left

Uniswap (v3) Math

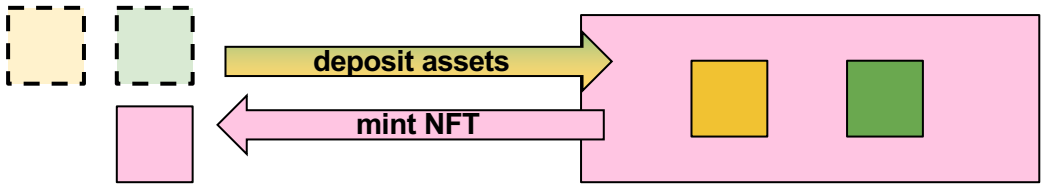


- In Uniswap v2, some reserves are saved for all possible prices, which is capital inefficient
- Uniswap v3 allows liquidity providers to add **concentrated liquidity** within a specific price range
- This is equivalent to translating the **xy = k** curve down and to the left
- Different liquidity providers can provide liquidity in custom ranges, which is all aggregated together into the same pool

Uniswap (v3) Mechanics: Adding Liquidity

Liquidity provider

Pool contract



Links

- Uniswap v2 Whitepaper
  - https://uniswap.org/whitepaper.pdf
- Uniswap v3 Whitepaper
  - https://uniswap.org/whitepaper-v3.pdf
- The graphs above are interactive visualizations on Desmos
  - https://docs.uniswap.org/protocol/concepts/advanced/resources

Disclaimer

- **This presentation (the "Presentation") is intended solely to provide general information. Any views expressed are those of the individuals presenting and are not the views of Paradigm. Any opinions expressed on this Presentation are subject to change.**
- **Nothing in this Presentation constitutes investment, accounting, tax or legal advice or is a recommendation that you purchase, sell or hold any security or other investment or that you pursue any investment style or strategy.**
- **Certain information contained herein has been obtained from third-party sources. While such information is believed to be reliable for the purposes used herein, Paradigm has not independently verified such information and Paradigm makes no representation or warranty, express or implied, as to the accuracy or completeness of the information contained herein.**