Dan Robinson

Head of Research, Paradigm

# Decentralized Exchanges

October 26, 2022

CS 251, Stanford

# Decentralized Exchange (DEX)

- Type of decentralized application, built with smart contracts
- Allows users to trade ERC-20 tokens or NFTs directly with counterparties
- **Advantages**
  - **Non-custodial**: no trusted third party who can shut it down or steal funds
  - **Censorship-resistant**: anyone who can send transactions on base layer can use it
  - **Permissionless**: can support any asset
  - **Convenient**: don't have to deposit your on-chain assets into an exchange
  - **Programmable**: liquidity can be viewed and by other smart contracts
  - **Atomic**: orders can be filled atomically with other on-chain actions

# Types of Decentralized Exchange

## On-chain orderbook

- Market makers place orders on chain
- Users fill them on chain
- **Examples**: OasisDEX, EtherDelta
- **Problem**: gas-inefficient
  - Orders cost gas when placed, when cancelled, when filled, and when replaced

# Types of Decentralized Exchange

## Off-chain orderbook

- Market makers sign orders off chain
- User signs order and submits it on chain
- **Example**: 0x Protocol, OpenSea
- **Problem**: sacrifices programmability
  - Liquidity is not visible or accessible to smart contracts

# Types of Decentralized Exchange

## Dutch auctions

- User places order on-chain, price slowly adjusts to make it more attractive to fill
- Market maker fills it once they like the price
- **Examples**: MakerDAO liquidation auctions
- **Problem:** slow
- I could give a whole talk on Dutch auctions, but it's not this one

# Types of Decentralized Exchange

## Automated market maker

- Market makers deposit assets into a pool
- Users trade with the pool at an algorithmically determined price
- **Examples**: Uniswap, Balancer, Bancor
- **Advantages**:
  - Gas-efficient
  - Makes it easy to make markets
  - Programmability makes incentivization easy
- Over 90% of DEX volume on Ethereum

# Automated Market Makers

## How they work

- Consider an AMM between a risky asset X (think: ETH) and a numéraire Y (think: USD)
  - AMMs can also support N > 2 assets, but our brains can't
- The AMM's *reserves* contain **x** units of asset X, and **y** units of asset Y
- The AMM offers to either buy or sell asset X at some marginal price, **p**
  - If there is no arbitrage, then **p** must also be the true price of the asset
- **p** at any point should be a function of the reserves **x** and **y** (and maybe some other state)

# Automated Market Makers

## How to make your own

- Let's say we want an AMM that maintains a 50/50 portfolio of assets X and Y
- Since **p** is the price of asset X in terms of numéraire Y, this is equivalent to saying:

$$p \cdot x = y$$

$$p = \frac{y}{x}$$

# Automated Market Makers

## How to make your own

- Imagine someone sells an infinitesimal amount of ETH (asset X) for USD (asset Y)
- **x** (the contract's reserves of ETH) goes up and **y** (the contract's reserves of USD) goes down
- "Marginal price" is just another way of saying the amount that **y** decreases per infinitesimal increase in **x**
- So we can rewrite our formula as this differential equation:

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

# Automated Market Makers

## How to make your own

- The unique solution to that differential equation is:

$$y = \frac{k}{x}$$

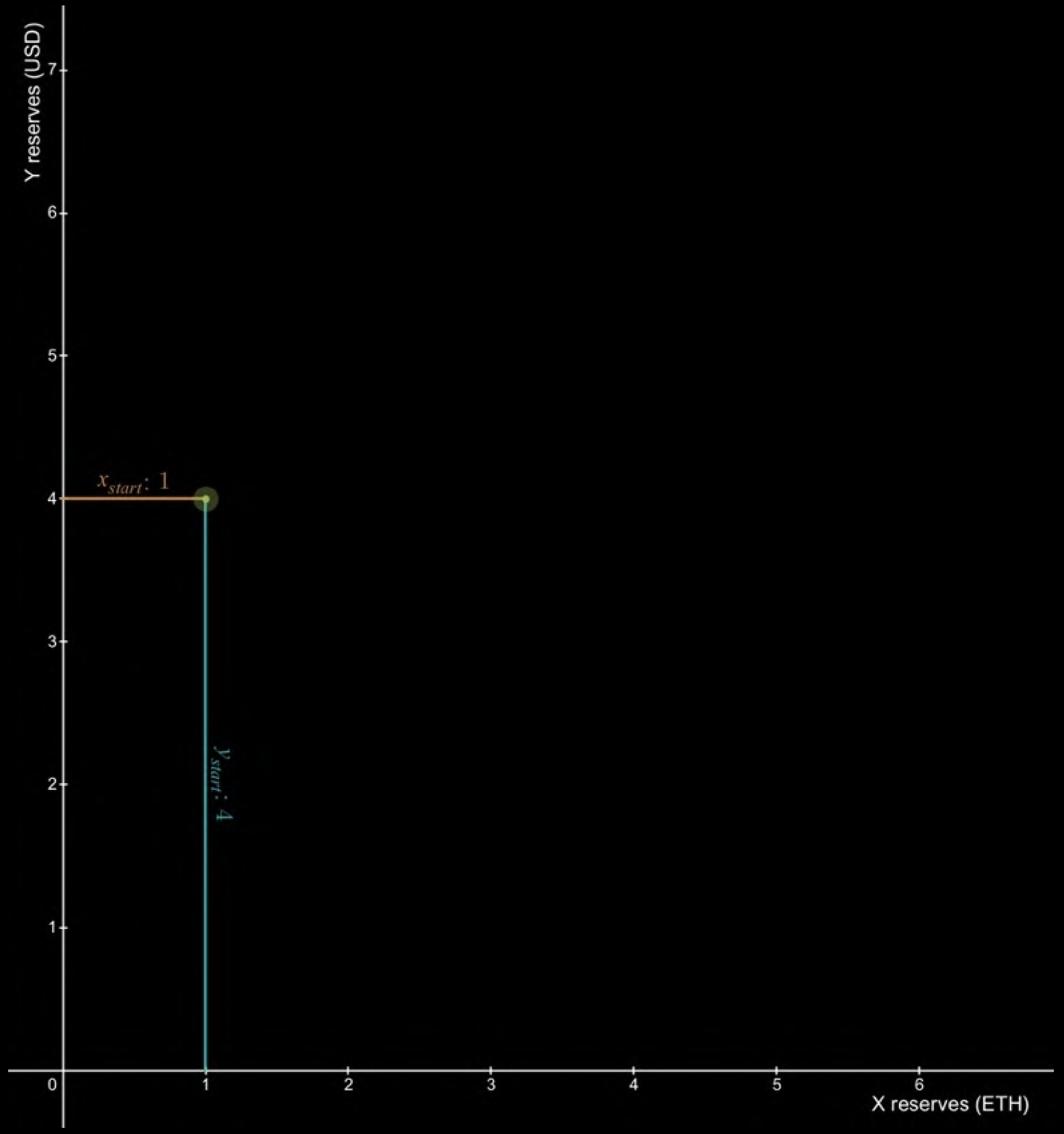
- Or, as it is better known:

$$x \cdot y = k$$

Automated Market Makers

# The Constant Product Market Maker

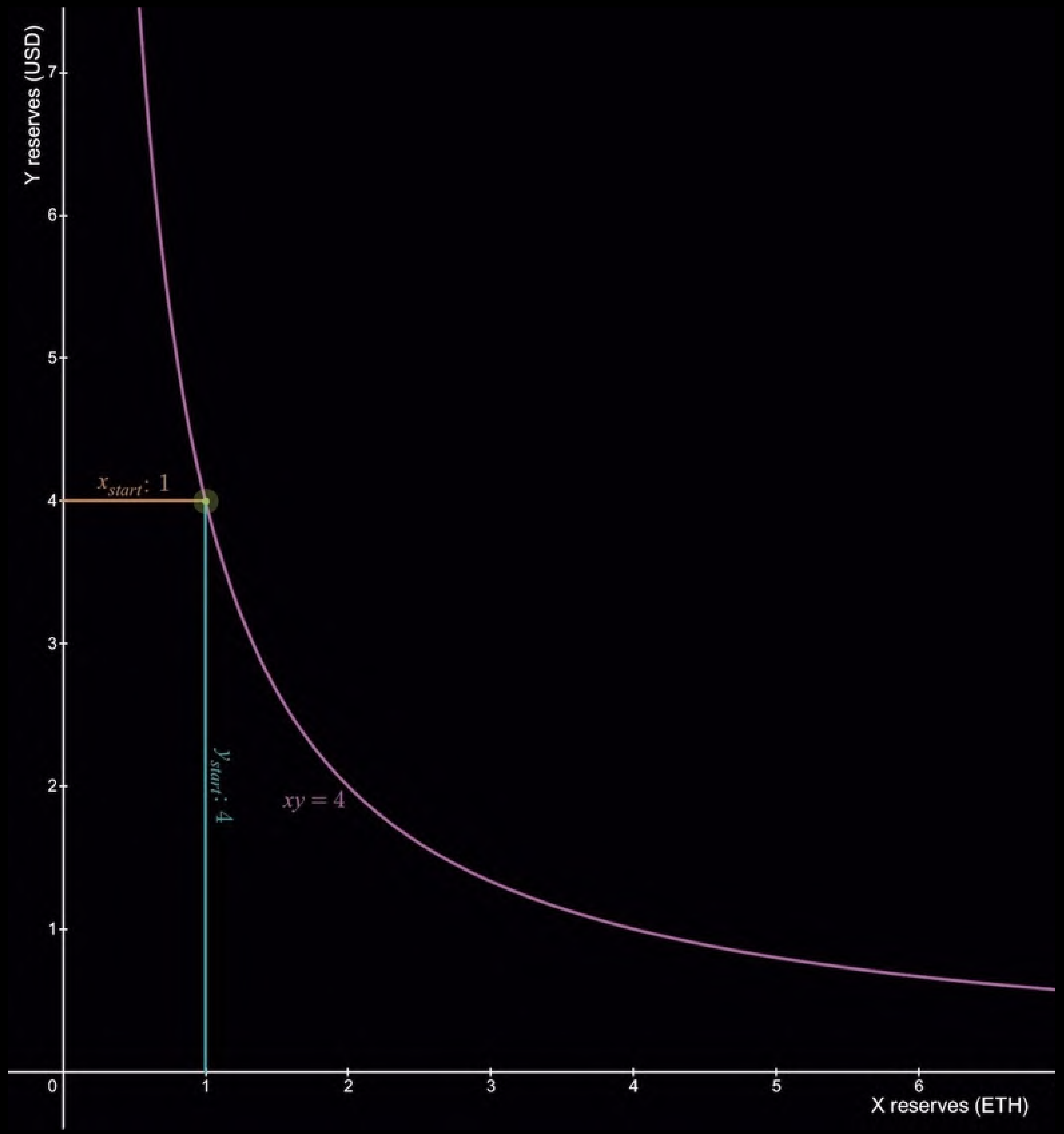
The pool holds reserves **x** of ETH, **y** of USD



Automated Market Makers

# The Constant Product Market Maker

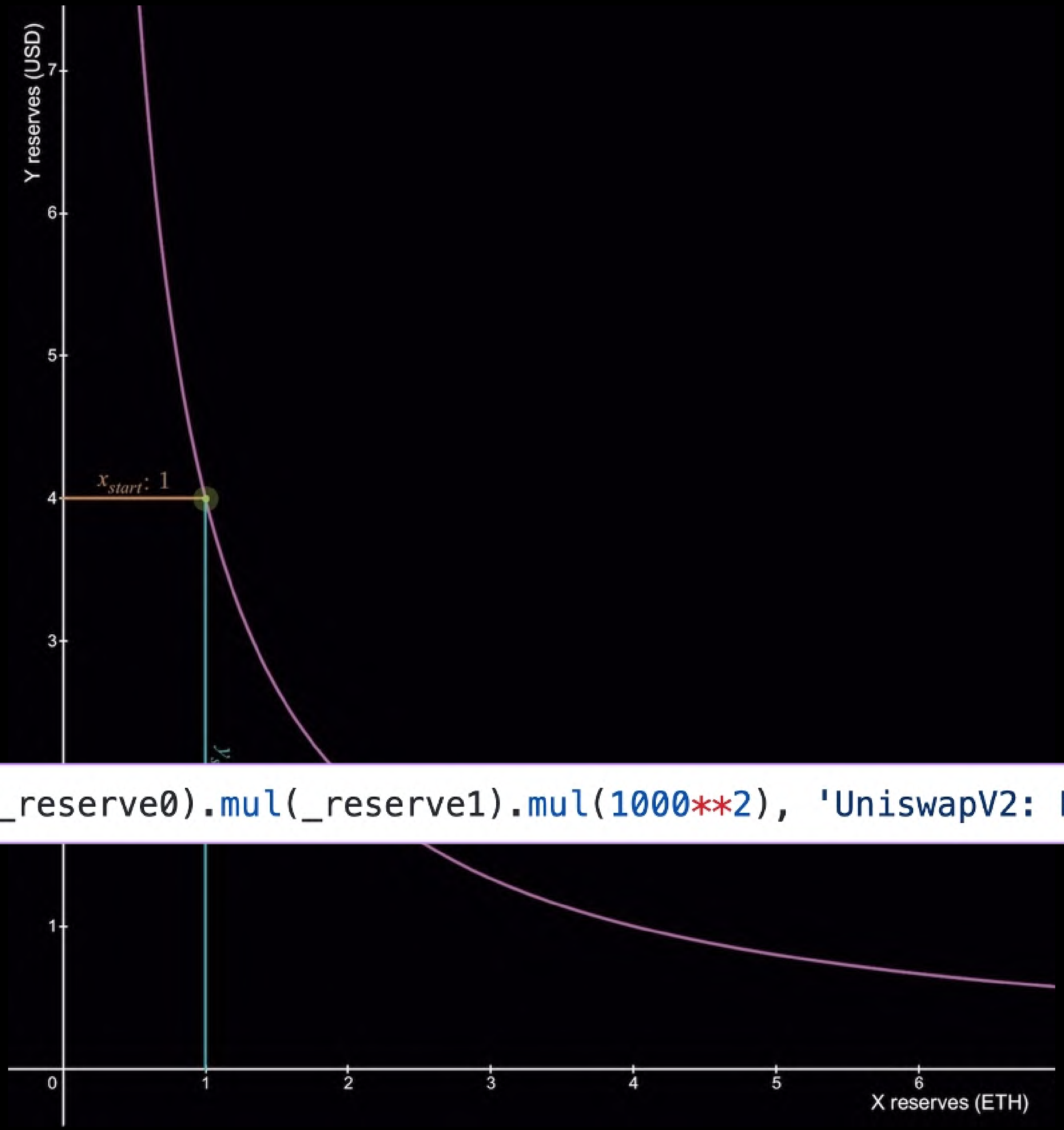
Trades preserve the invariant **xy = k**.



Automated Market Makers

# The Constant Product Market Maker

Trades preserve the invariant **xy = k**.

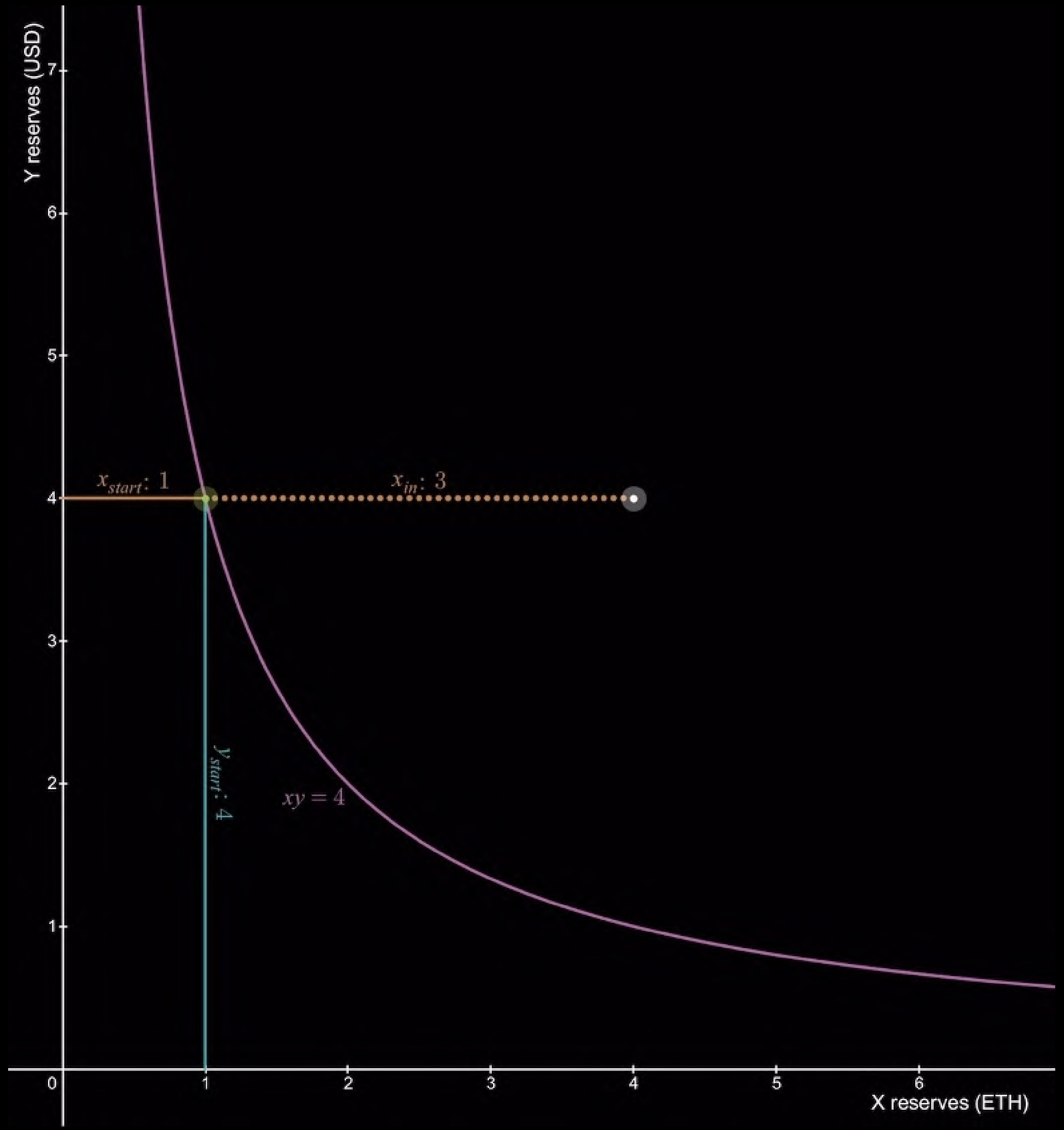


```
require(balance0Adjusted.mul(balance1Adjusted) >= uint(_reserve0).mul(_reserve1).mul(1000**2), 'UniswapV2: K');
```

Automated Market Makers

# The Constant Product Market Maker

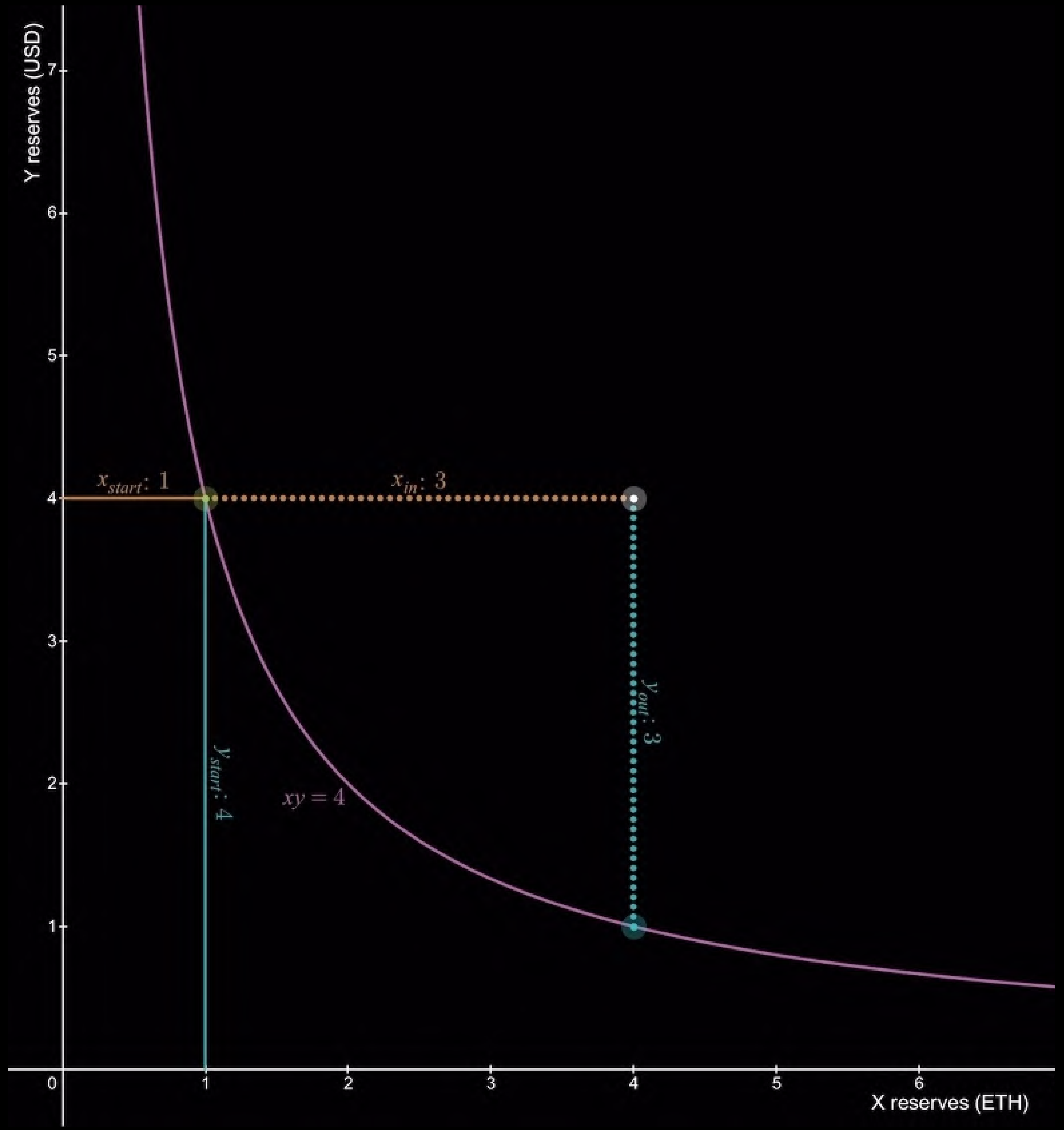
The trader sends in some ETH.



Automated Market Makers

# The Constant Product Market Maker

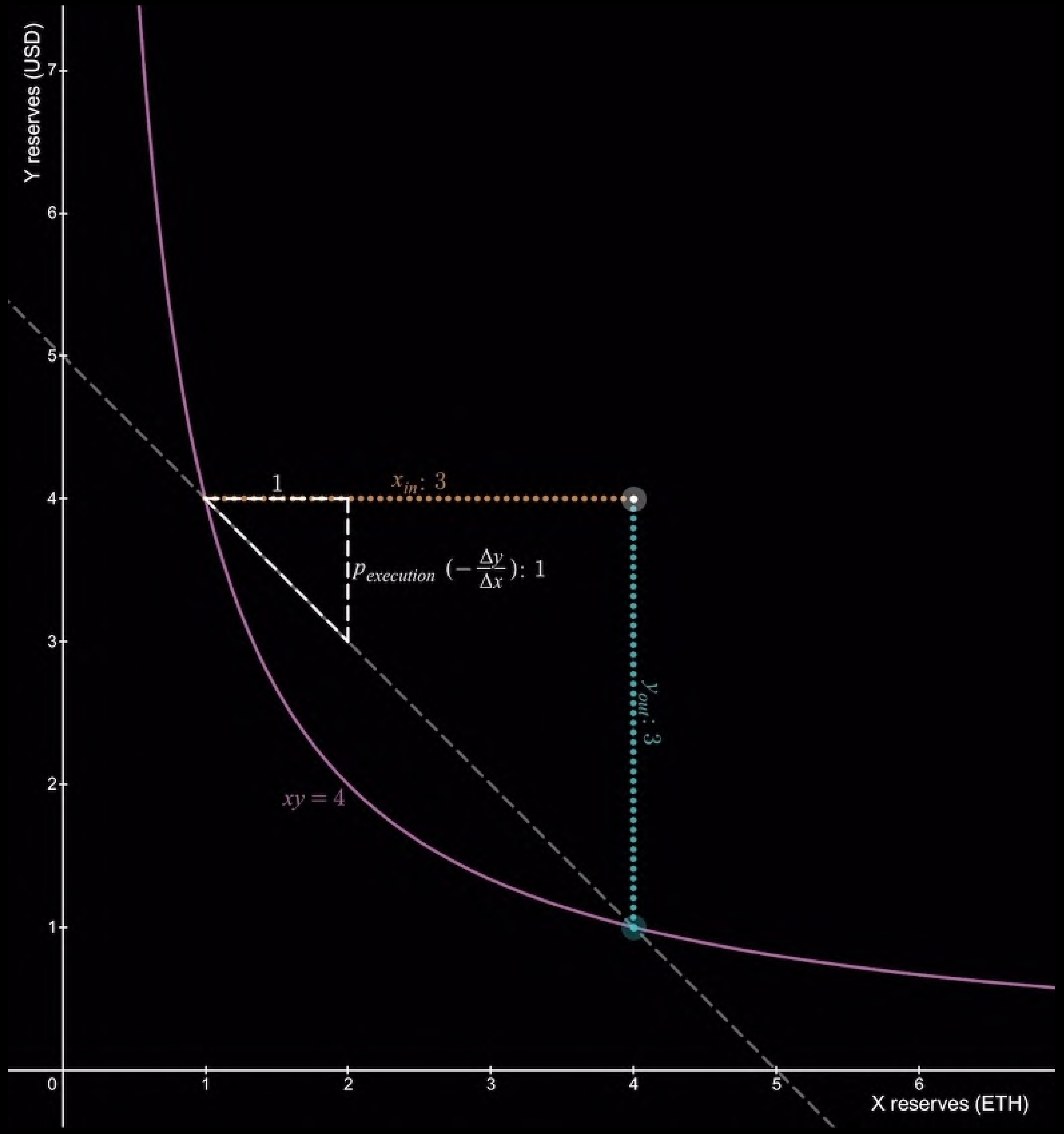
The pool sends out as much USD as needed to return to the curve.



Automated Market Makers

# The Constant Product Market Maker

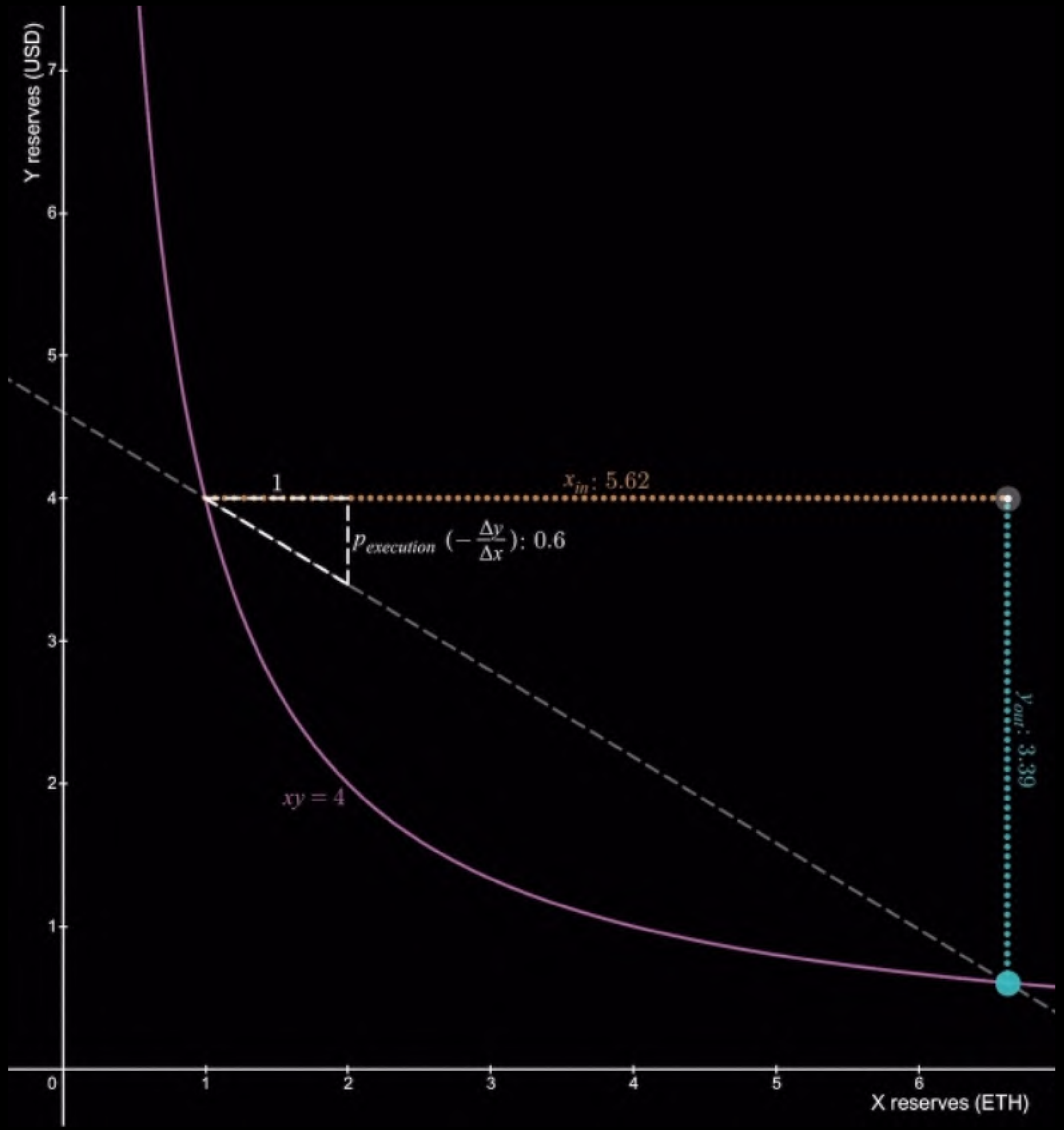
The slope of the line between these points is the **execution price** of the trade.



Automated Market Makers

# The Constant Product Market Maker

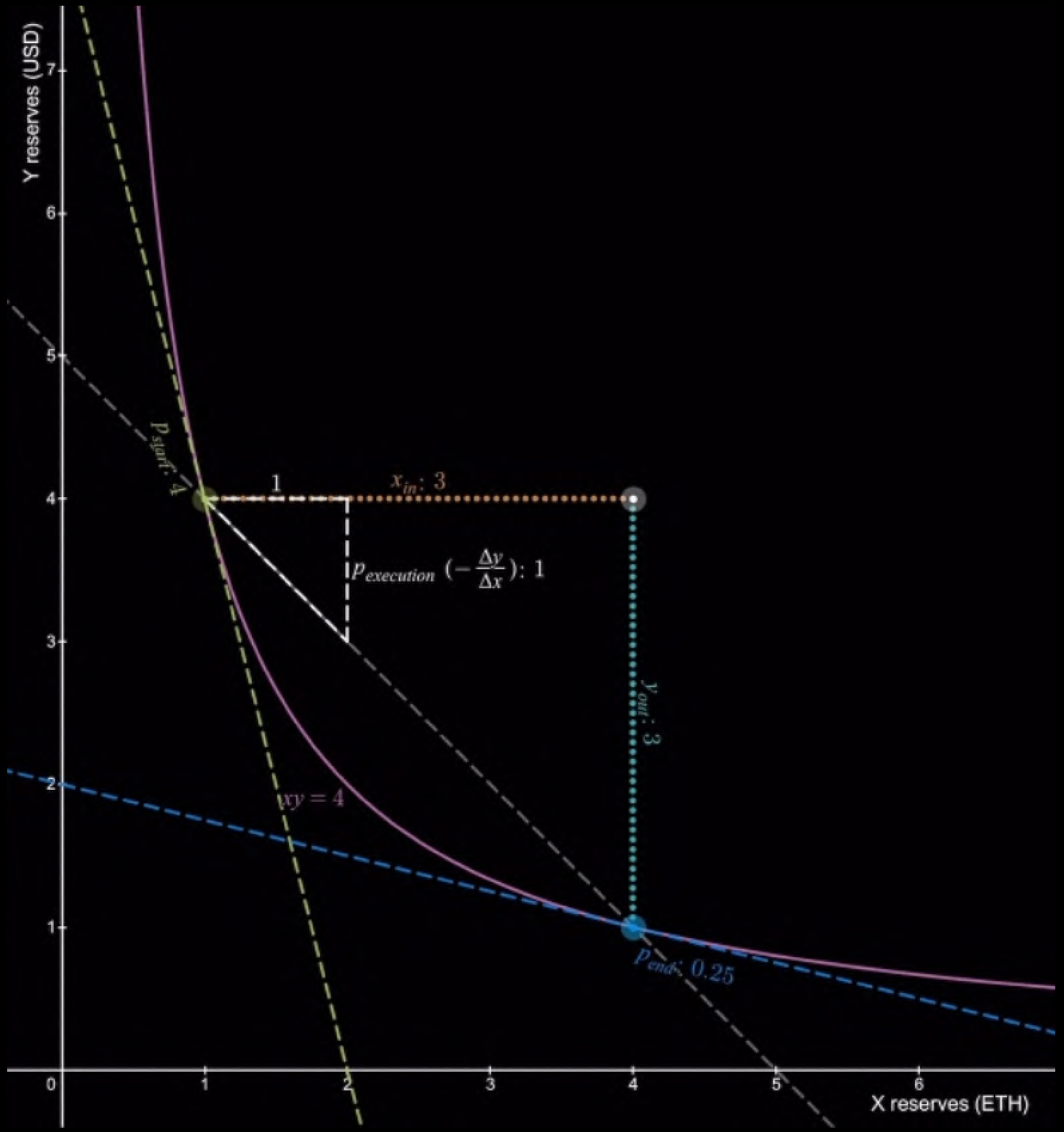
The slope of the line between these points is the **execution price** of the trade.



Automated Market Makers

# The Constant Product Market Maker

The slope of the line between these points is the **execution price** of the trade.



# The Many Faces of the Constant Product Market Maker

The state of the AMM can be described in terms of current reserves, but there are equivalent (sometimes more convenient) ways to describe it:

**Liquidity is the geometric mean of the reserves:**

$$l = \sqrt{xy}$$

**The square root of the current price is the square root of the ratio of reserves:**

$$\sqrt{p} = \sqrt{\frac{y}{x}}$$

**We can easily reconstruct x** and **y** from these ingredients:

$$x = \frac{l}{\sqrt{p}} \qquad y = l\sqrt{p}$$

# The Many Faces of the Constant Product Market Maker

As with most AMMs, there are many equivalent ways to express the logic of the constant product invariant:

## Price as a function of reserves

$$p = \frac{y}{x}$$

## Portfolio value as a function of price and liquidity

$$v = 2 \cdot l \cdot \sqrt{p}$$

## Change in reserves as a function of liquidity and change in price:

$$\Delta y = l \cdot \Delta\sqrt{p} \qquad \Delta x = l \cdot \Delta\sqrt{\frac{1}{p}}$$

# Automated Market Makers

## Other formulas

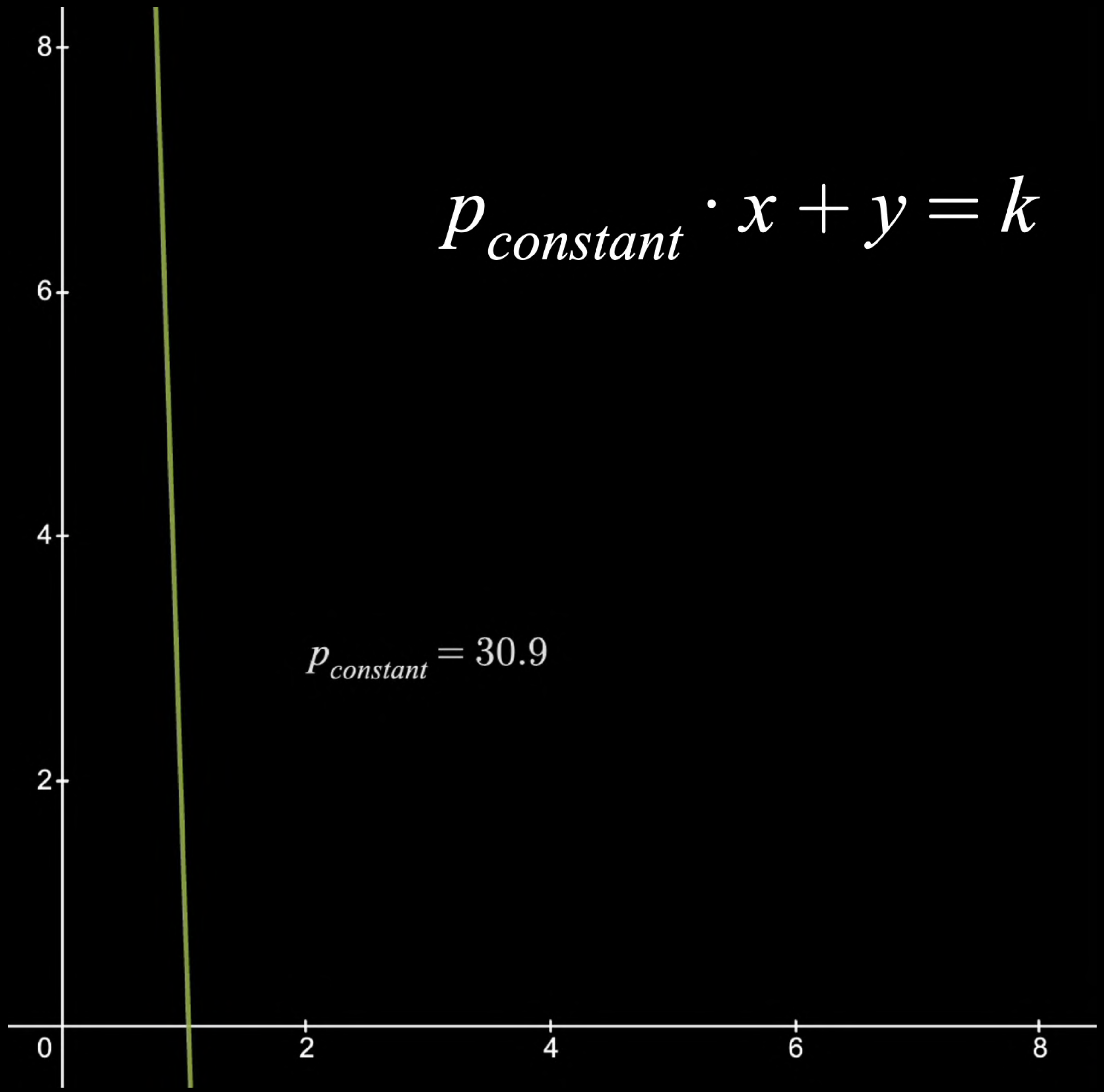
- There are as many possible AMM formulas as there are mathematical formulas
- We can discover ones that satisfy other interesting processes with the same methodology
  - (But note that it's not always possible to find a closed form solution)

Automated Market Makers

# Constant Sum

The constant sum market maker offers to trade between assets at a constant price.

$$p = p_{constant}$$

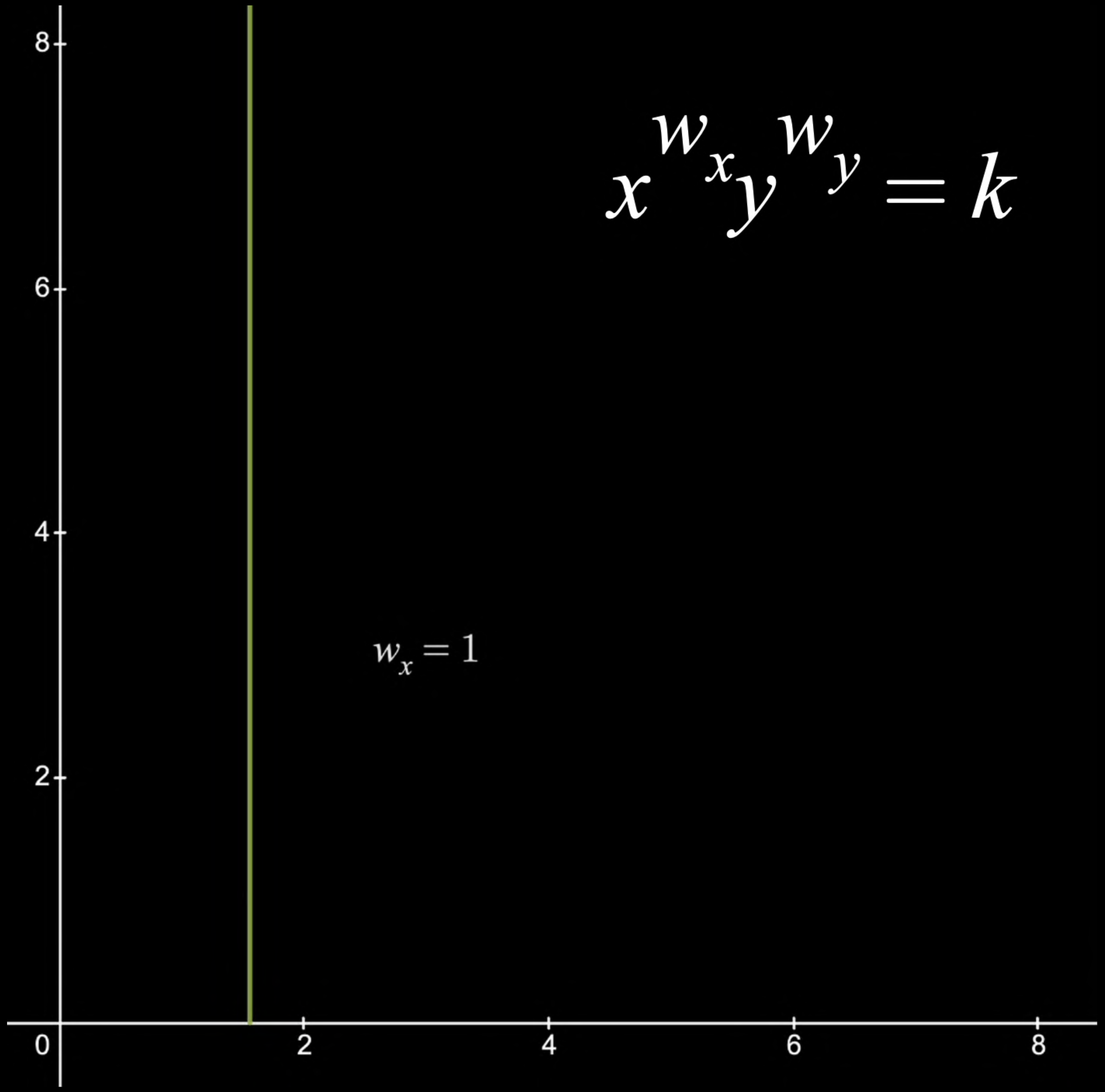


Automated Market Makers

# Constant Weighted Geometric Mean

The constant weighted geometric mean market maker maintains an *imbalanced* portfolio.

$$\frac{p \cdot x}{w_x} = \frac{y}{w_y}$$



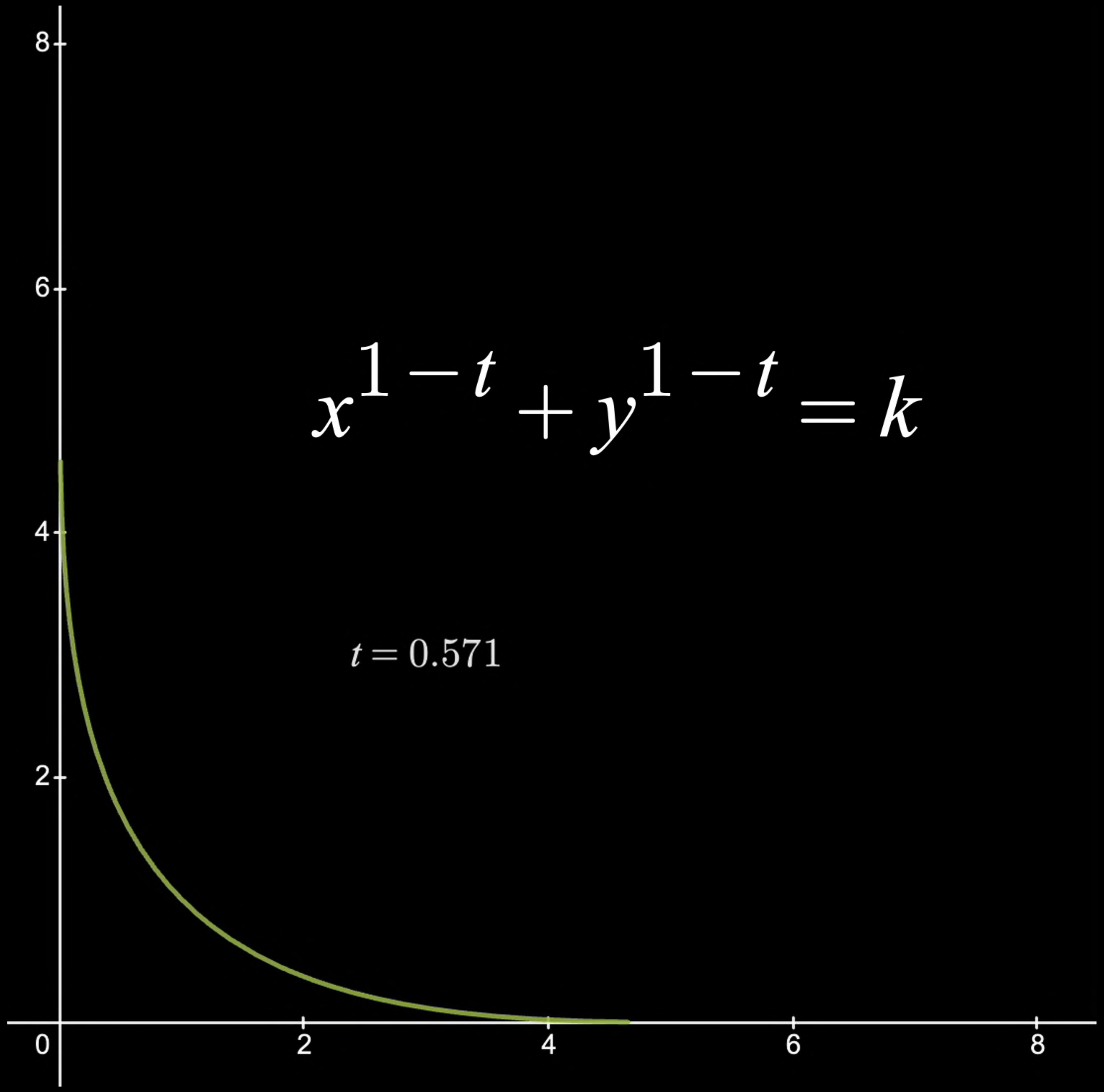
$$x^{w_x} y^{w_y} = k$$

Automated Market Makers

# Constant Power Sum

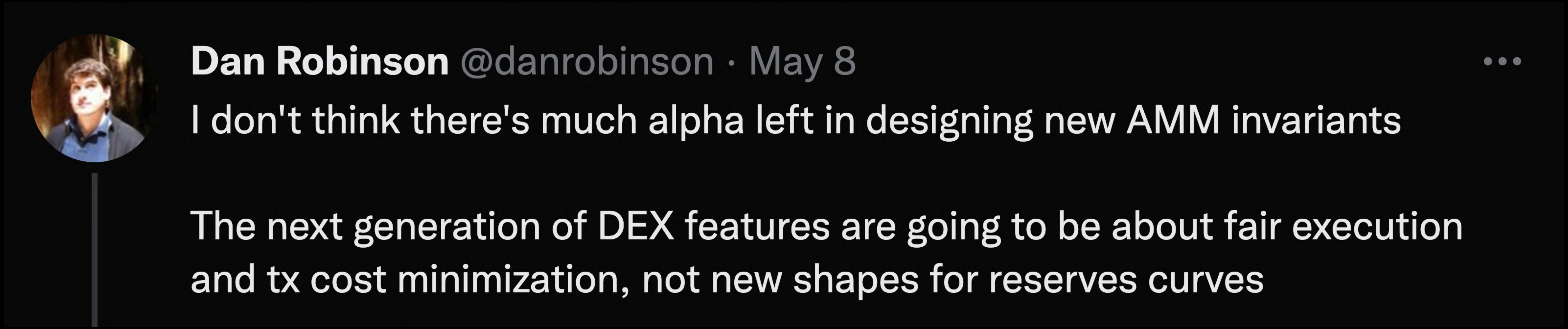
The constant power sum formula is useful for market-making assets that act like zero-coupon bonds, where **t** is time to maturity.

$$p = \left(\frac{y}{x}\right)^t$$



# Automated Market Makers

## Other areas for improvement



**Dan Robinson** @danrobinson · May 8

I don't think there's much alpha left in designing new AMM invariants

The next generation of DEX features are going to be about fair execution and tx cost minimization, not new shapes for reserves curves

# Automated Market Makers

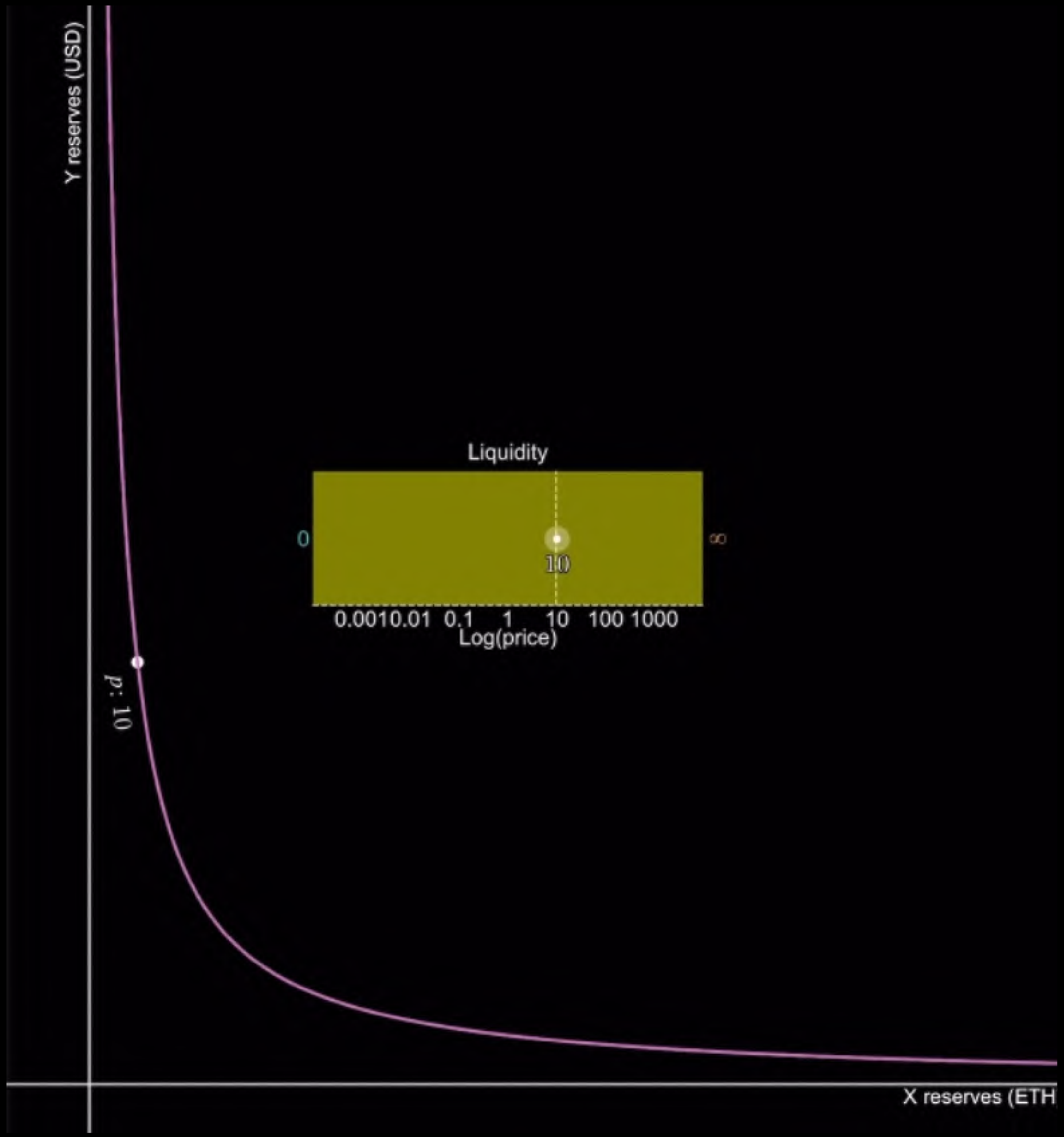
## Other areas for improvement

- Gas cost
- Slippage (price movement before the user's trade)
- Loss versus rebalancing (arbitrage at beginning of each block)
- Capital efficiency

Automated Market Makers

# Concentrated liquidity

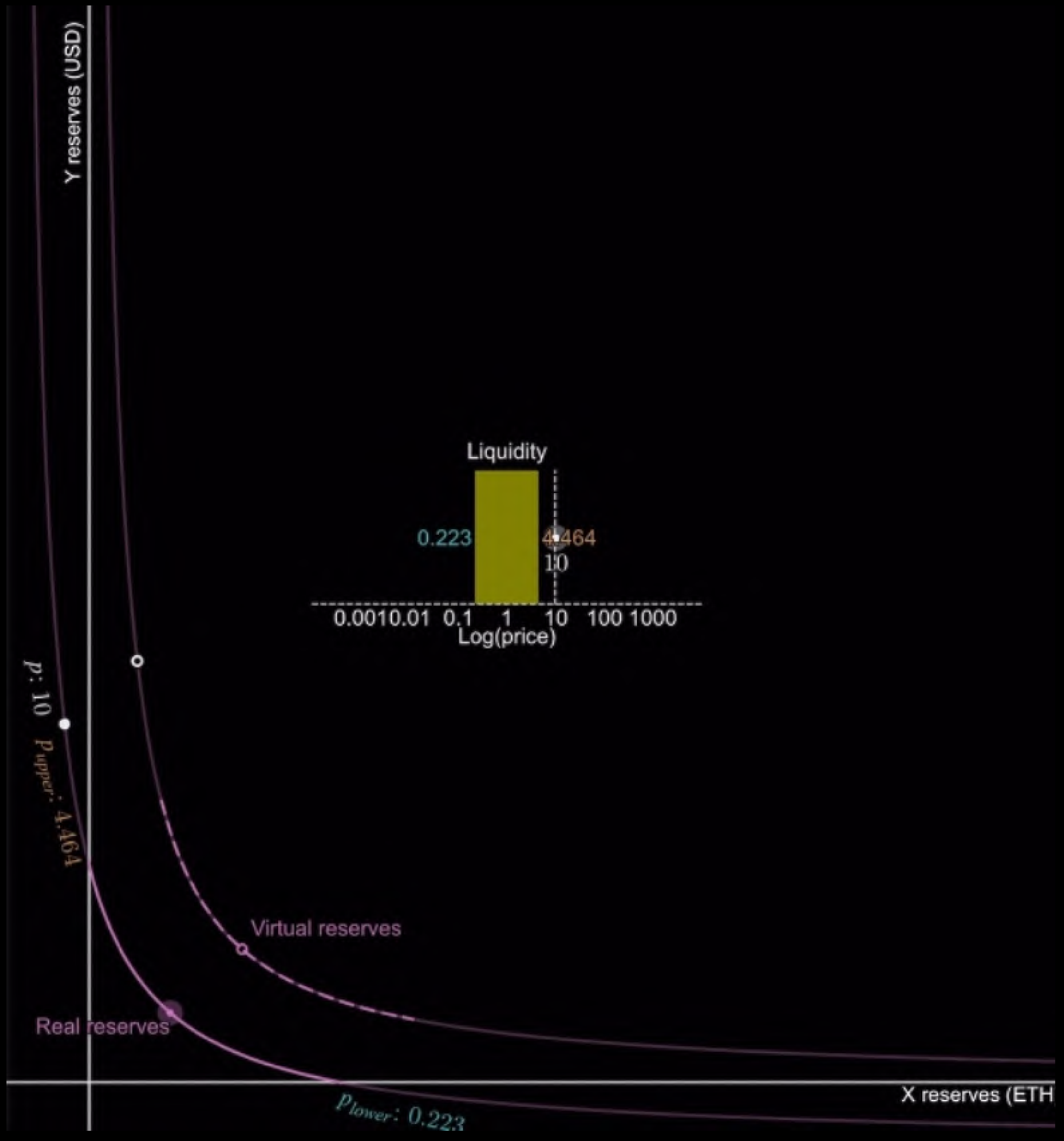
In the constant product market maker used in Uniswap v2, some reserves are saved for all possible prices, which is inefficient



Automated Market Makers

# Concentrated liquidity

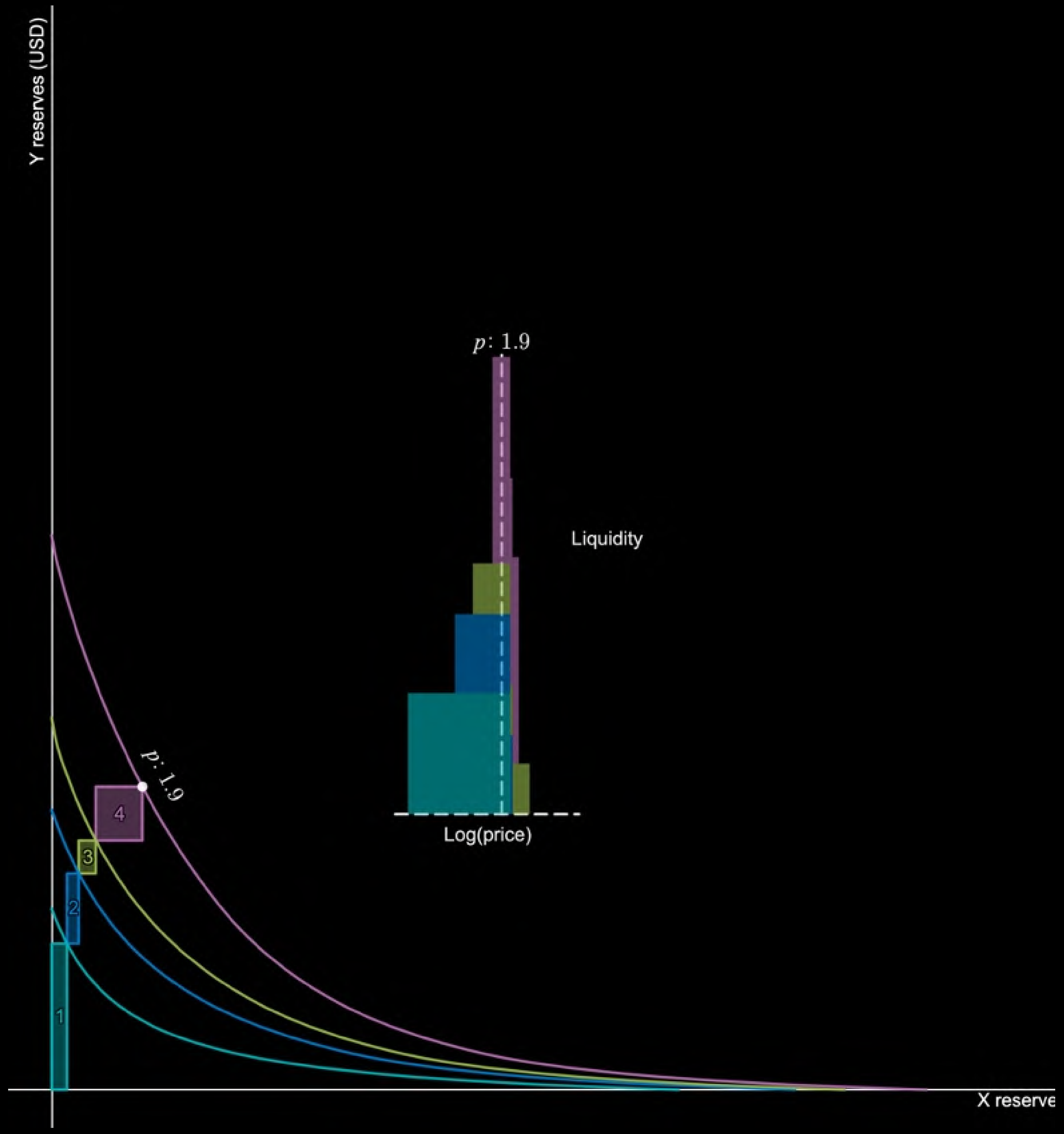
Uniswap v3 allows liquidity providers to add **concentrated liquidity** within a specific price range, which is like translating the **xy = k** curve down and to the left.



Automated Market Makers

# Concentrated liquidity

Different liquidity providers can provide liquidity in custom ranges, which is all aggregated together into the same pool.



# Questions?

# Disclosures

- 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.