Elements of DeFi

https://web3.princeton.edu/elements-of-defi/

Professor Pramod Viswanath

Princeton University

Lecture 5:
Decentralized Exchanges

Last Lecture

- Pricing smart contracts and computation on a blockchain
  - Gas fees
- Miner incentives
  - Transaction rewards
- Miner Extractable Value (MEV)
  - Basic strategies

This lecture: Decentralized Exchanges

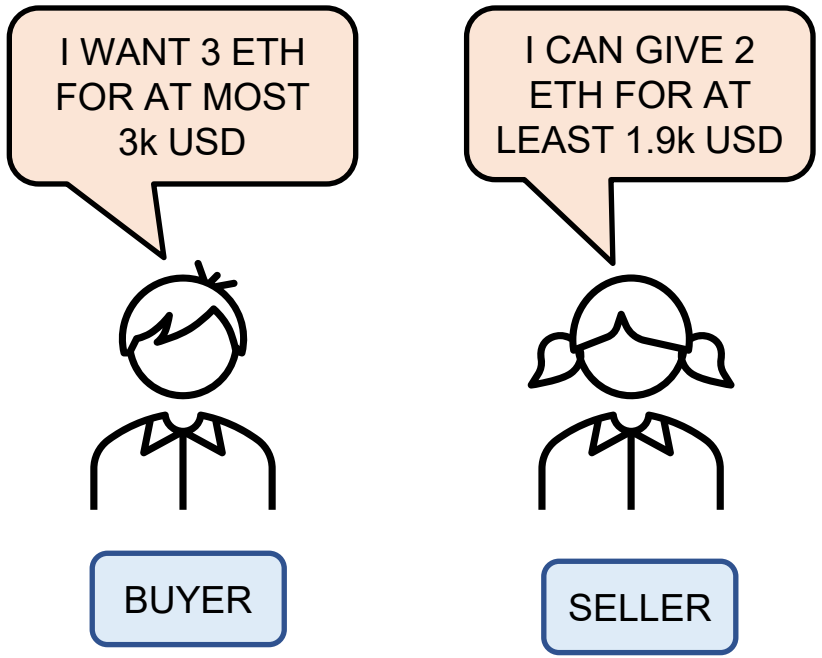
- Most basic element of finance: Market Making

- Traditional Market Makers
  - Limit Order Books
  - Peer-to-peer, centralized
  - hard to decentralize

- Automated Market Makers
  - Peer-to-pool-to-peer, can be decentralized
  - Basic example

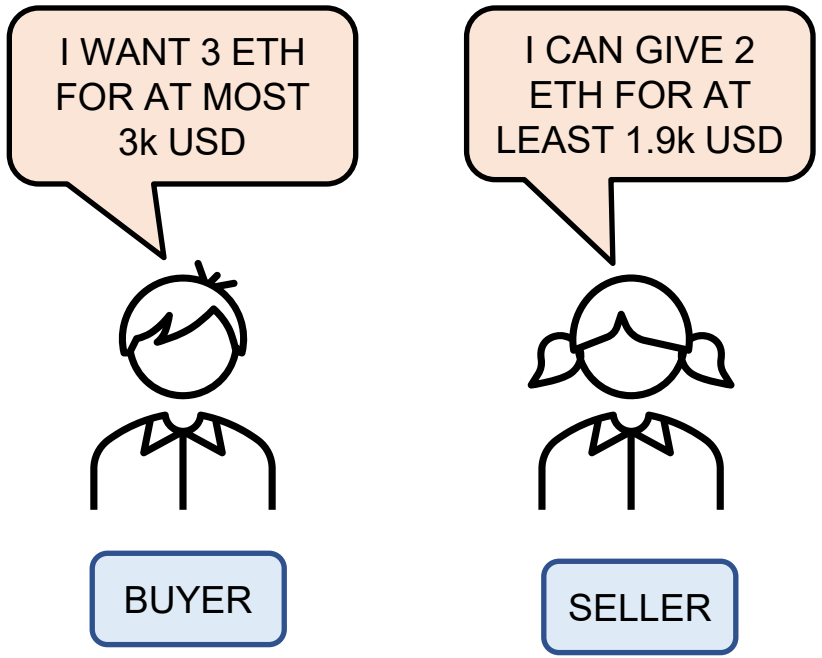
Exchanges

- As a trader: want to swap token A with token B
- Need a place which lists people willing to do the reverse
- How would you state the intention to trade ?



Limit Orders

- Intention to trade takes the form of a limit order
- What are the conditions for opposite limit orders to match?
- Can these two orders match ?
- Which order remains “on the book” after matching ?



Limit Order Books

- Collection of such limit orders
- Orders coming in are of two types
  - Market orders (get satisfied)
  - Limit orders (stay on the book)
- Buy order with largest price = bid
- Sell order with least price = ask
- Ask > Bid always

Limit Order Books

- Volume of limit orders = **liquidity**
- High liquidity markets have a very small **spread** (ask-bid), and vice-versa
- How would LOB look during a crash?
- Why would a trader want a more liquid market? - **slippage**

Properties of LOB

- Centralized
- Negligible fees
- Fast matching
- No loss due to price fluctuation – infact they are very profitable in periods of volatility
- Incentivizes market makers to provide liquidity

Centralized exchanges

- Traditional exchanges - NYSE, NASDAQ, Shenzen, ICE
  - Each handles $1-3 trillion in volume
  - Need to be heavily regulated to avoid insider trading
  - Drives down profit margin

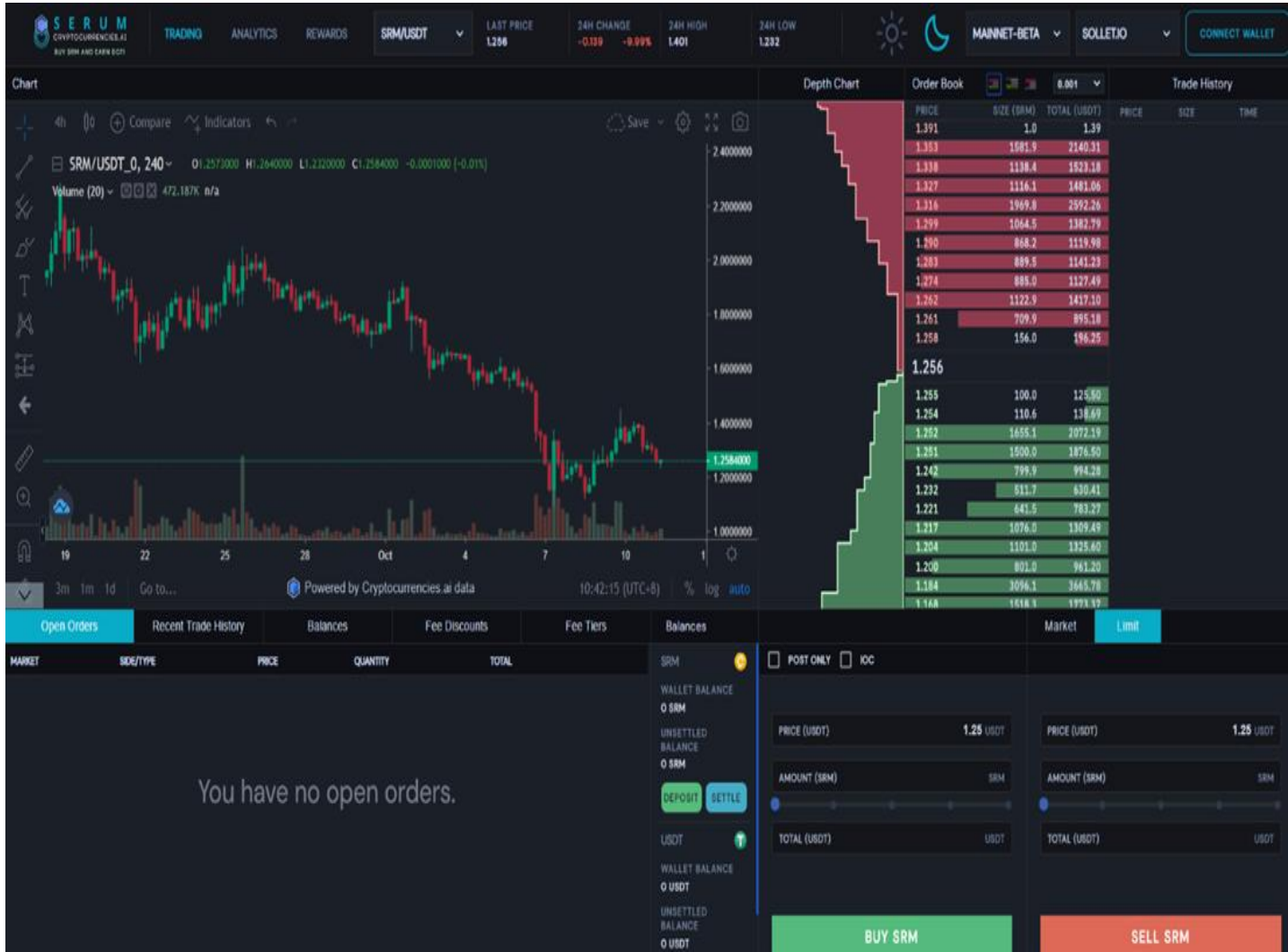
- Blockchain exchanges – Binance, Coinbase, FTX
  - Frequent regulatory issues leading to bans – Binance
  - Safety of customer funds not guaranteed – FTX
  - Need solutions like proof-of-reserves
  - Transfer custodianship of tokens – defeats the point of blockchains

Decentralize?

- Convenient and transparent for swapping blockchain tokens
- The exchange knows about your order before the rest of the market – frontrunning
- Exchange has the power to censor txns
- e.g. Decentralized Exchanges – **Uniswap, Curve, Balancer**

Decentralized LOB

- Examples : Serum, Demex
- Order matching verified by everyone on chain
- Permissionless
- A liquidity provider can cancel and rearrange orders

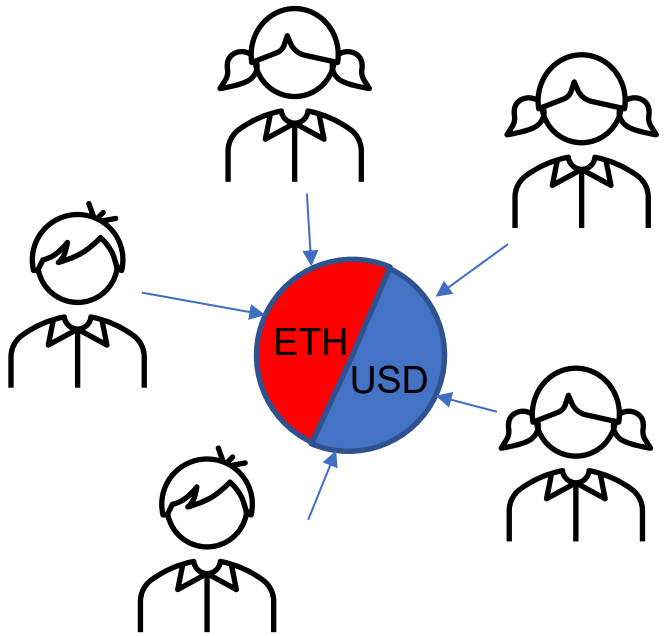


Shortcomings of Decentralized LOB

- Need high volume markets to work well – otherwise takes long time to satisfy an order
- Need to satisfy orders when traders arrive at non-overlapping times
- Fees to cancel and shift limit orders
- Higher fees than in centralized LOB

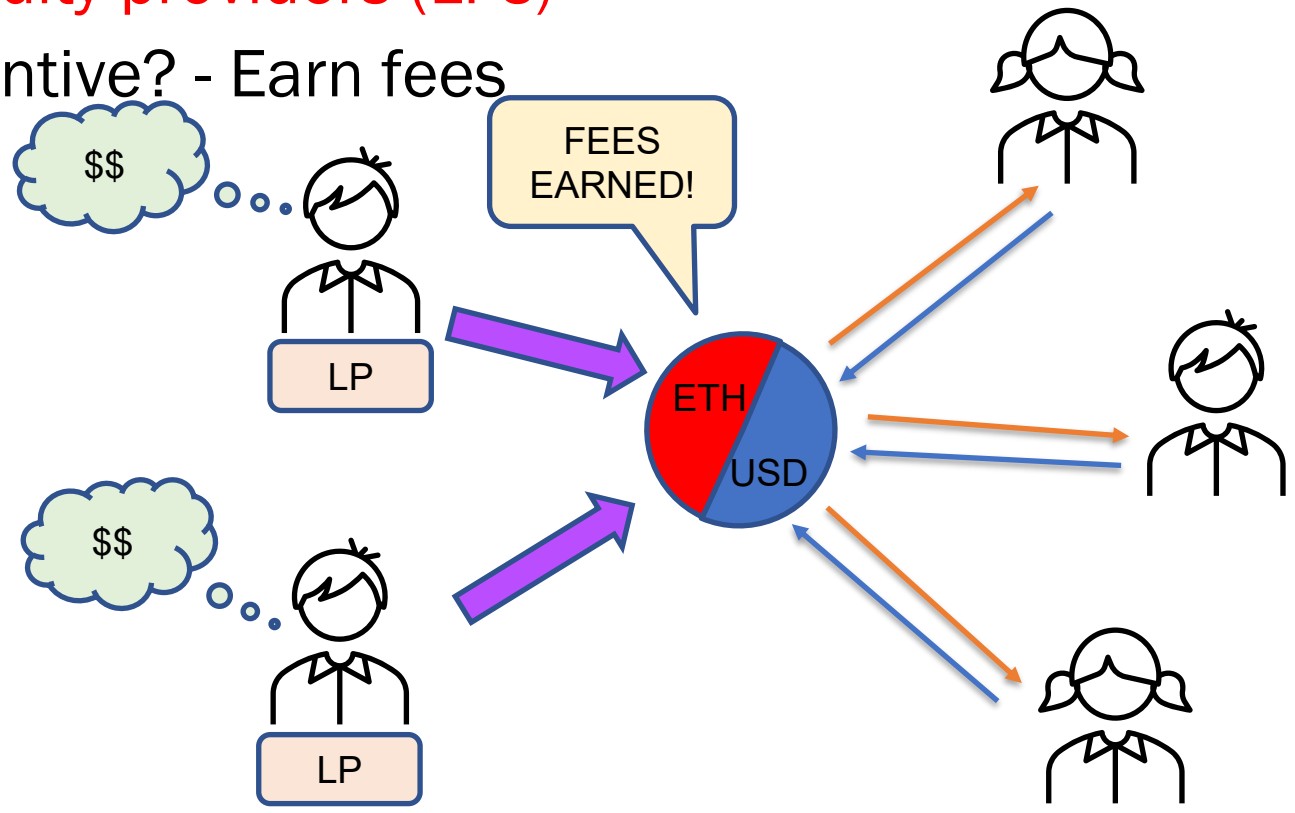
Automated Market Makers

- Need to guarantee instant exchange when volume is lacking
- Idea : Peer-Pool-Peer instead of Peer-Peer matching



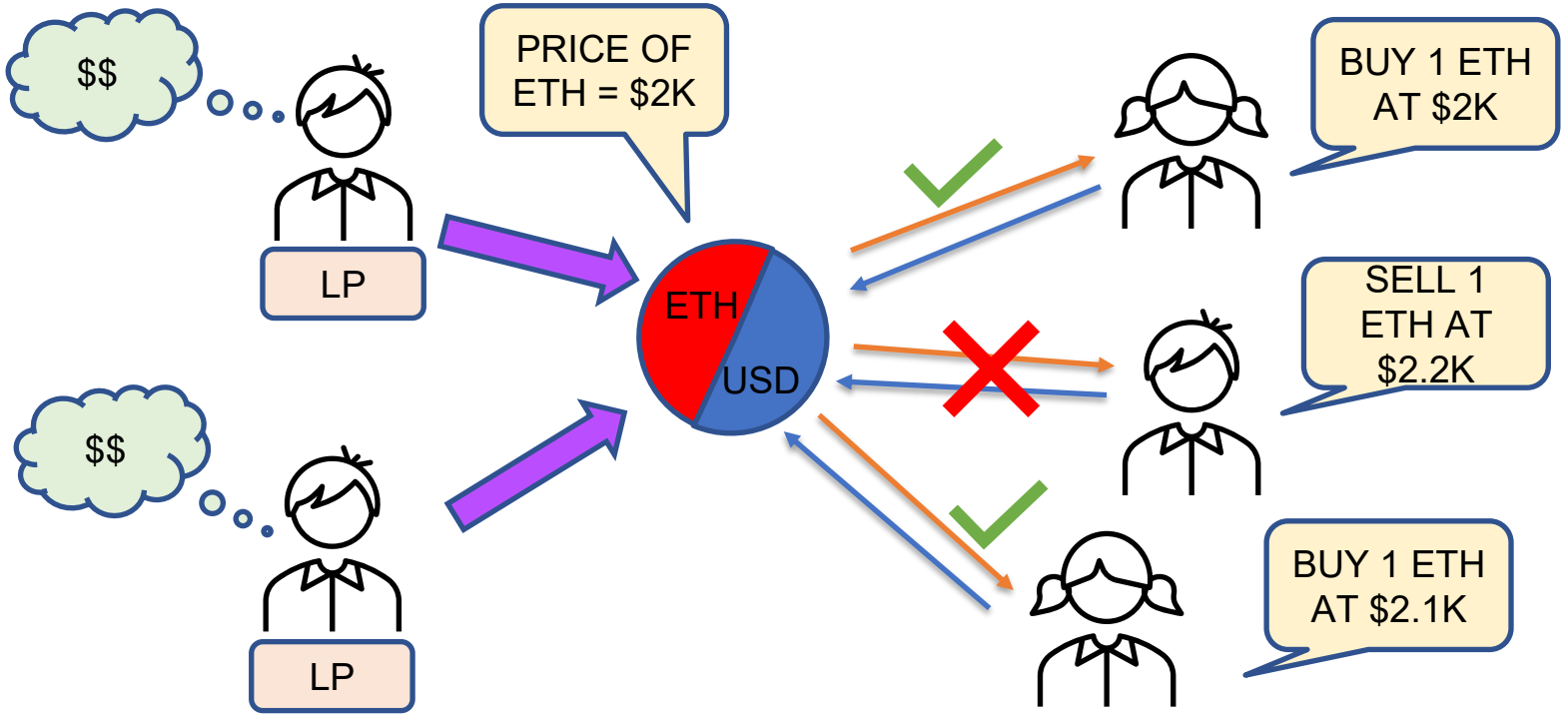
Automated Market Makers

- Keep a pool of orders that can satisfy any incoming trade
- Entities with large amount of idle liquidity pitch in to make the pool– liquidity providers (LPs)
- Incentive? - Earn fees



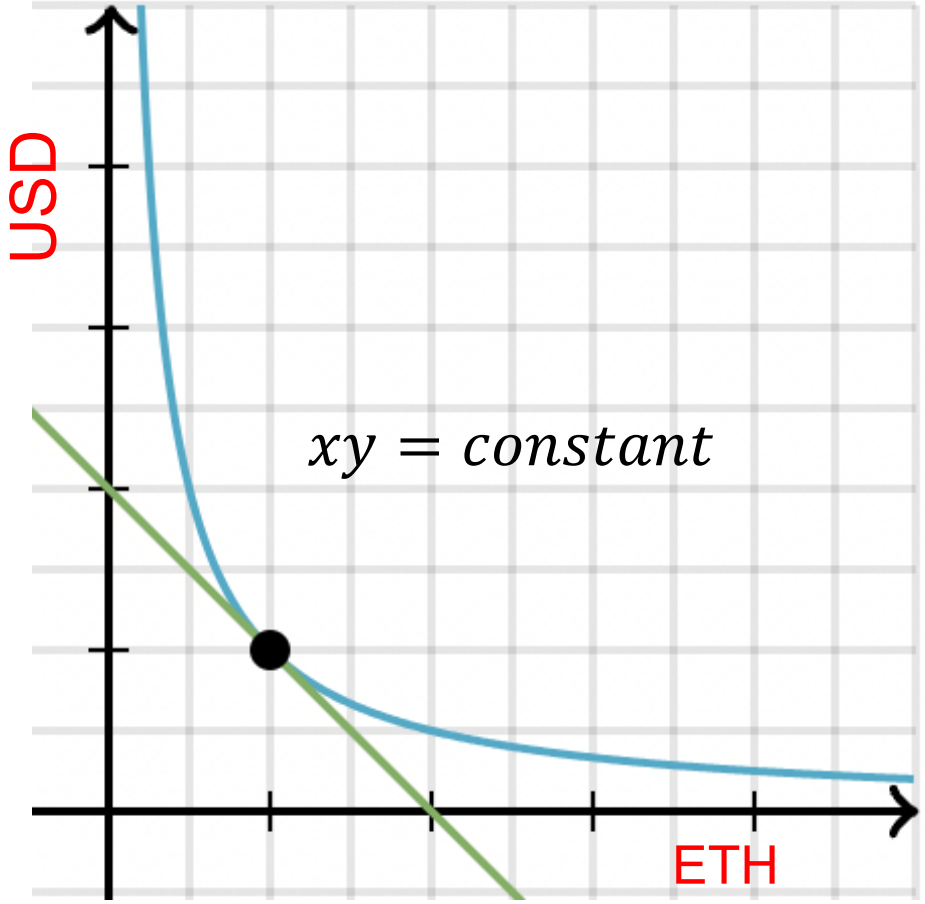
Automated Market Makers

- LPs do not constrain prices like in LOB
- How do you decide prices? Which trades are allowed?
- Make the reserves/inventory of the AMM follow specific rules



A solution: CFMMs

- CFMM: Constant Function Market Makers
- Use Bonding Curves to constrain reserves
- Intuition:
  - What happens when AMM has lots of ETH?
  - What happens when AMM has lots of USD?



CFMMs: general model

- Each CFMM pool between tokens A and B have reserves that satisfy

$$\psi(x, y) = \psi(x + \Delta_x, y - \Delta_y)$$

OR

$$\psi(x, y) = constant$$

- Here x = reserves of token A, and y = reserves of token B

- Each trade earns fees – given to liquidity providers

Top CFMMs

- Uniswap, Sushiswap:

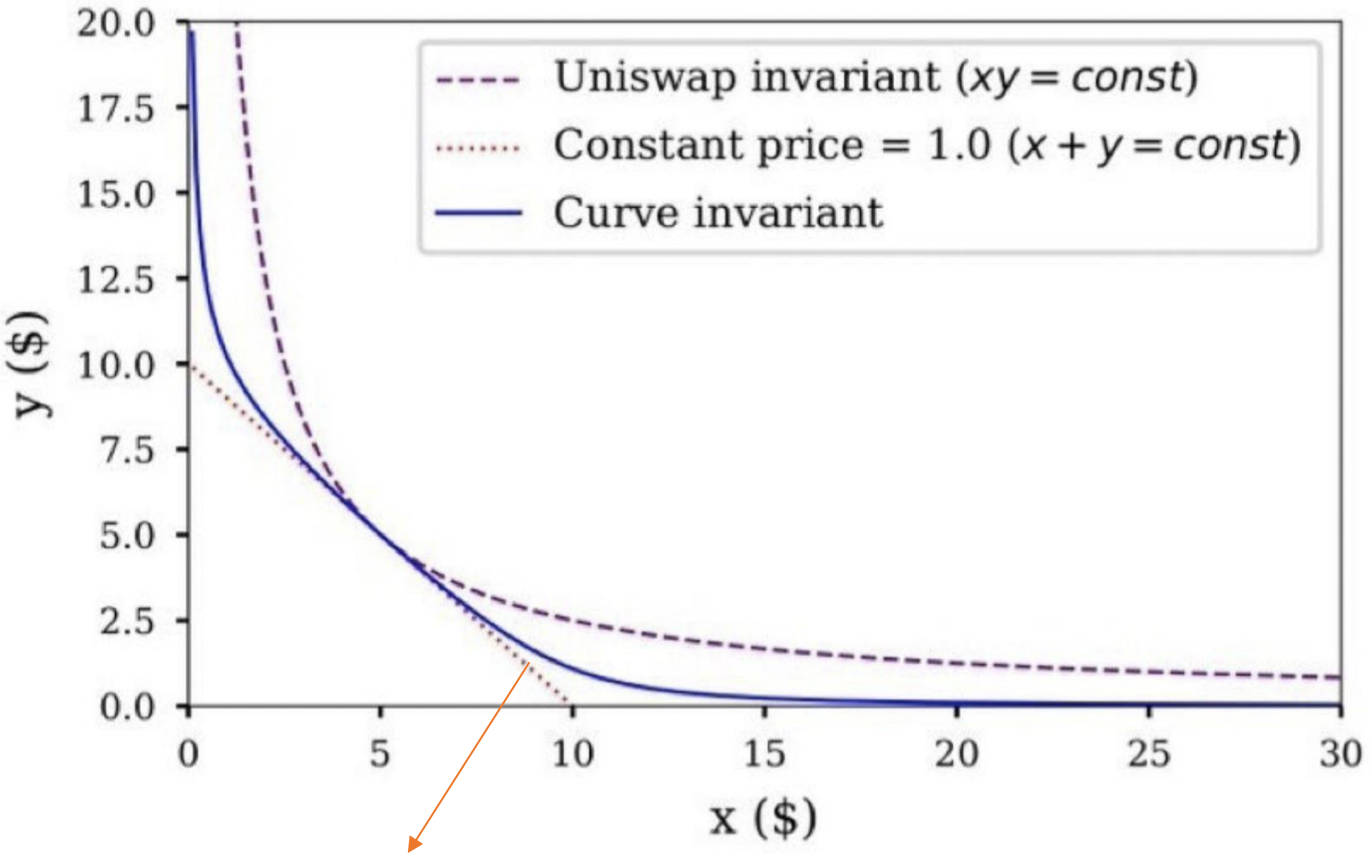
$$xy = constant$$

- Balancer:

$$x^{\theta} y^{1-\theta} = constant$$

- Curve:

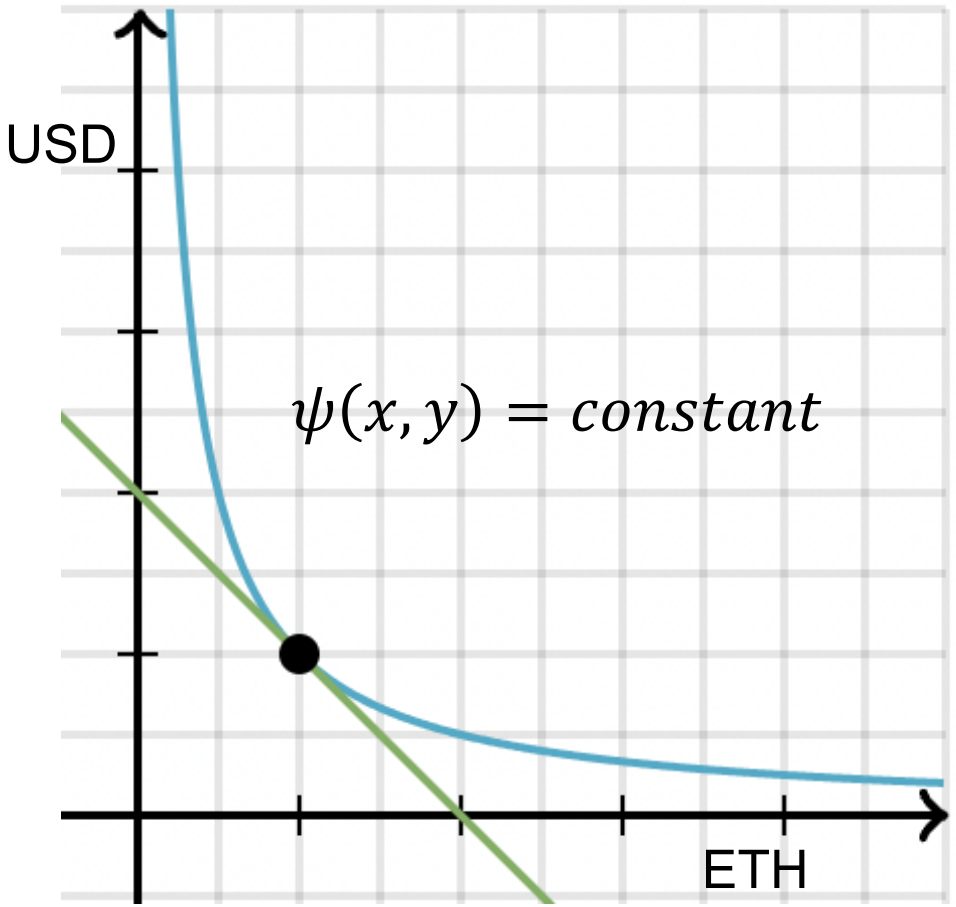
$$x + y + \frac{\alpha}{xy} = constant$$



Why is this curve called constant price?

Pricing in CFMMs

- Intuition from last slide : constant price = constant slope
- For a general curve what is the price at any point?
- Slope of the tangent
- Formula for price of ETH in terms of USD?



Pricing in CFMMs

- Formula for price of ETH in terms of USD?

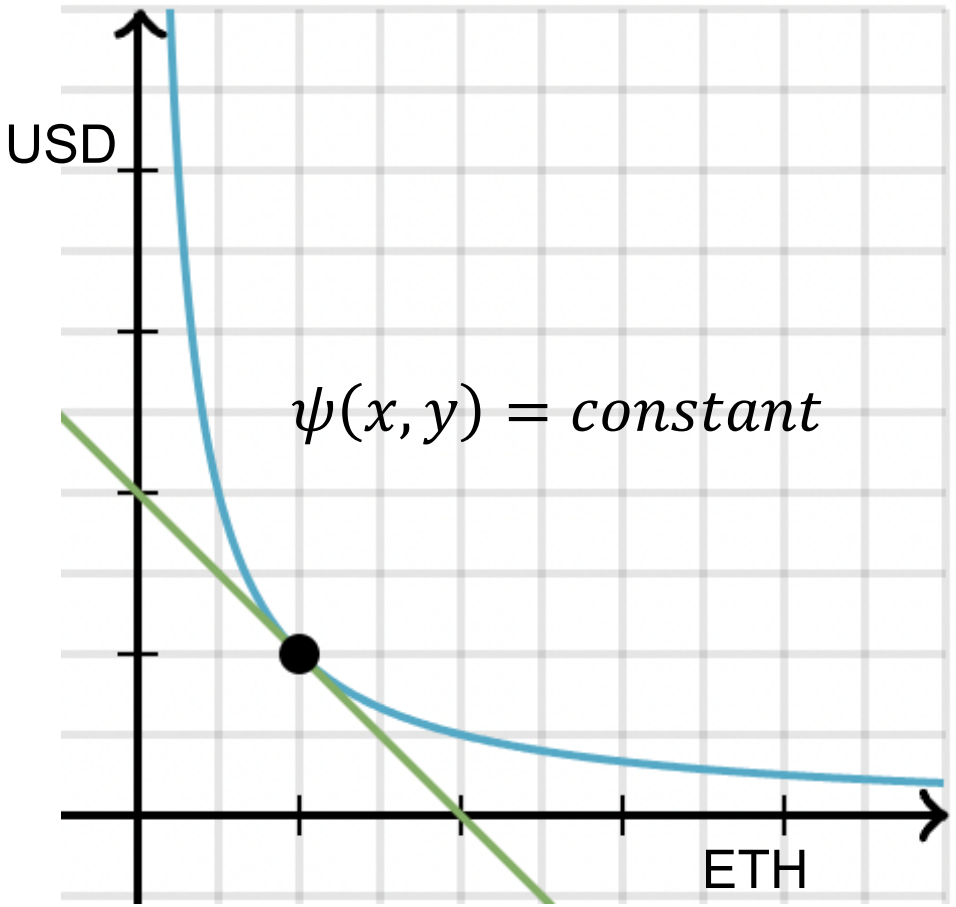
WHY?

$$Price = P_x = \frac{dy}{dx} = -\frac{\partial_x \psi}{\partial_y \psi}$$

$$d\psi(x, y) = 0$$

$$\implies \frac{\partial \psi}{\partial x} dx + \frac{\partial \psi}{\partial y} dy = 0$$

- Example :
  - $xy = constant$ – what is the price?



Popular CFMM and Pricing

- Uniswap, Sushiswap:

$$xy = constant \qquad P_x = \frac{y}{x}$$

- Balancer:

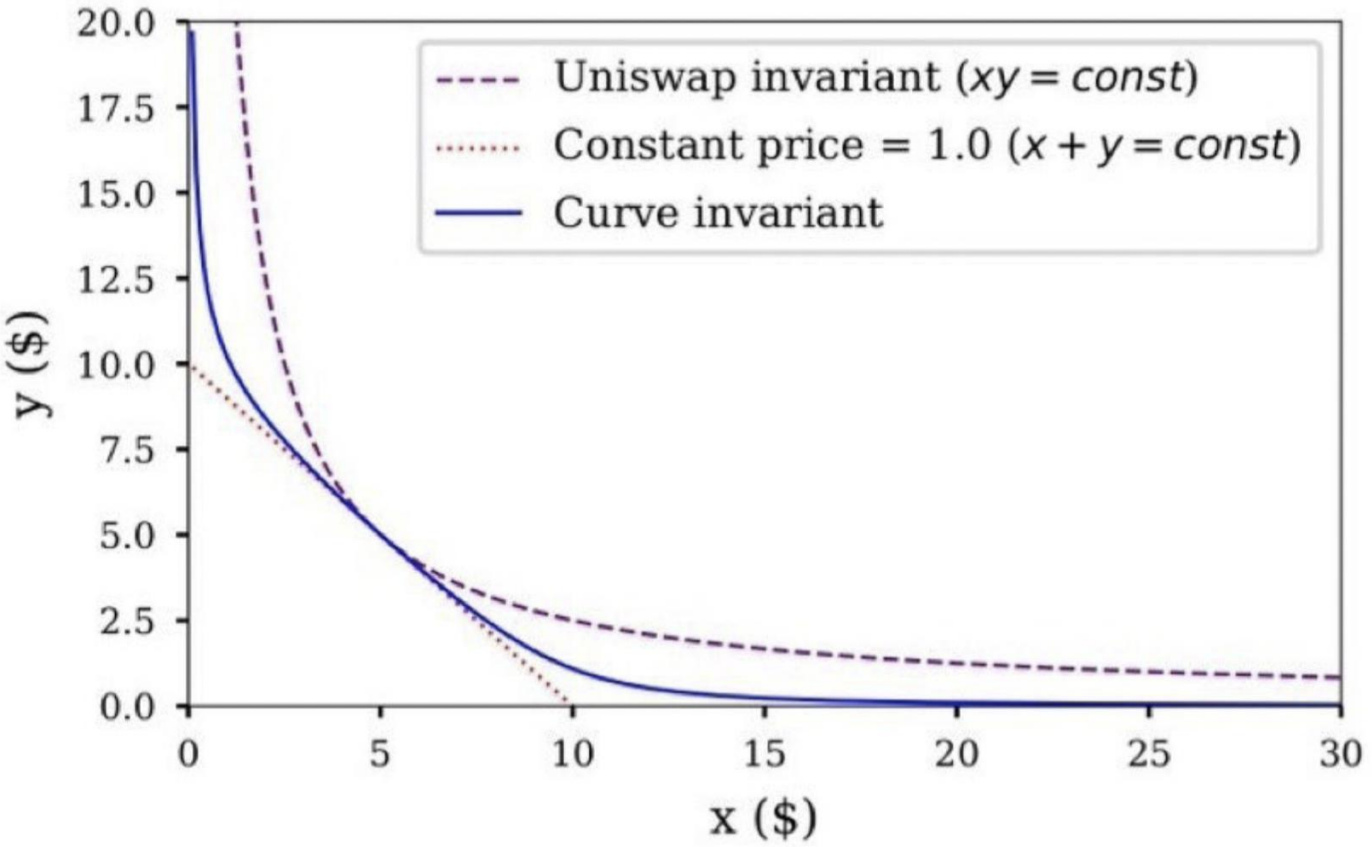
$$x^{\theta} y^{1-\theta} = constant \qquad P_x = \frac{\theta y}{(1-\theta)x}$$

- Constant Price :

$$x + y = constant \qquad P_x = 1$$

- Curve:

$$x + y + \frac{\alpha}{xy} = constant$$



Conclusion

- Ways of exchanging assets in DeFi
  - CLOB
  - AMM

- Focus on AMMs
  - Inspired from betting markets
  - CFMMs and their pricing

Next Lecture

- What curve to pick?
- Trader strategies
  - Routing
- Liquidity Provider performance
  - Arbitrage, exposure to informed traders
- Efficient CFMM:
  - Fees set such that both liquidity providers and traders are satisfied

LECTURE ENDS

CFMM origins : betting markets

- Suppose you want the forecast of an uncertain event (weather, elections, sport) from a group of experts
- Event has N outcomes, each expert gives pmf p as their prediction
- If outcome ‘i’ happens, then each expert rewarded S(p,i)
- What we want : every expert to speak the truth
- How should S be to incentivize each expert to be truthful?

$$q = argmax_p \sum_{i=1\ldots N} q_i S(p,i)$$

CFMM origins : betting markets

$$q = argmax_p \sum_{i=1\ldots N} q_i S(p,i)$$

- What happens if S(p,i) = p_i ?
- Is there a truthful scoring rule ?
- Yes – there are many!
- Examples :

$$S(p,i) = p_i - \sum_{j=1\ldots N} \frac{p_j^2}{2}$$

$$S(p,i) = \ln(p_i)$$

CFMM origins : betting markets

- So far, each bet was only interacting with one “expert”
- What if we want aggregate opinion by large group of people?
- Use the scoring rule sequentially
  - Start at t=0, with beliefs set at some q_0
  - At time t, a trader reports their belief q_t if it is different from q_(t-1)
  - At time T, check outcome and reward trader t with S(q_t,i)-S(q_(t-1),i)
- Truthful S stay the same! Why?

CFMM origins : betting markets

- Problem : Reporting pmfs is unintuitive – how can we make this more like a real market?