Day 2: DeFi Explained

How Uniswap and Lending Protocols Work

Prof. Jörg Osterrieder

BSc Seminar – Digital Finance

2026

BSc Seminar: Digital Finance

Recap Day 1 + Today's Roadmap

Yesterday — Crypto Pricing:

- Random walks and price models
- Fat tails: kurtosis $\gg 3$
- Volatility: BTC $\sim$65%, S&P $\sim$16%
- GARCH: volatility clusters
- Options and the volatility smile

Today — DeFi Mechanics:

1. **What is DeFi?** Finance without banks
2. **Uniswap AMM:** the $x \cdot y = k$ rule
3. **Impermanent loss:** the hidden cost of LPing
4. **DeFi lending:** Aave and overcollateralization
5. **Risks:** hacks, oracle attacks, rug pulls

Key Idea for Today

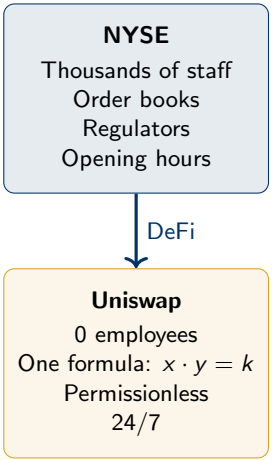
DeFi replaces banks and brokers with **mathematical formulas** encoded in smart contracts. We'll learn the math.

The $3 Billion Vending Machine

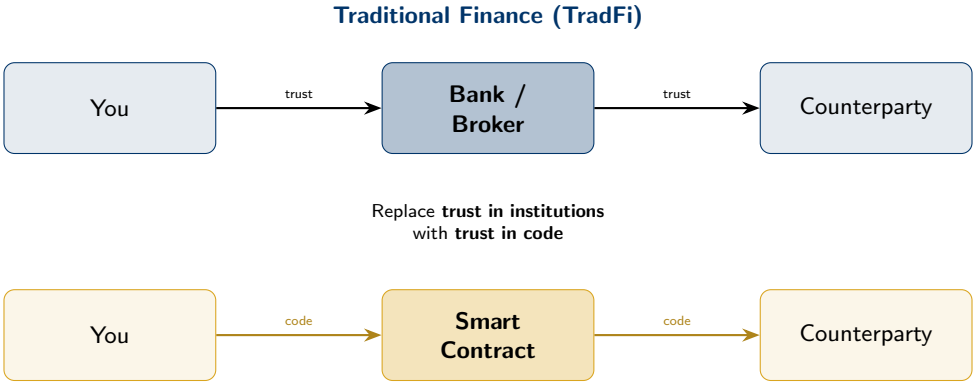
Uniswap: the world's largest decentralized exchange

- Processes $3–5 billion in trades per day
- Has **zero employees** running trades
- No CEO, no office, no order book
- Just a smart contract: ∼300 lines of code
- Anyone can trade, anyone can provide liquidity
- Runs 24/7/365 — never closes

How? A simple mathematical formula replaces the entire infrastructure of a traditional exchange.

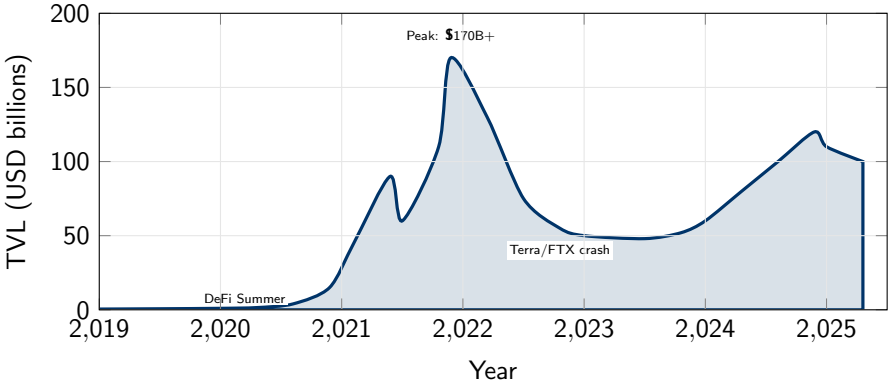


What Is DeFi? Finance Without Banks



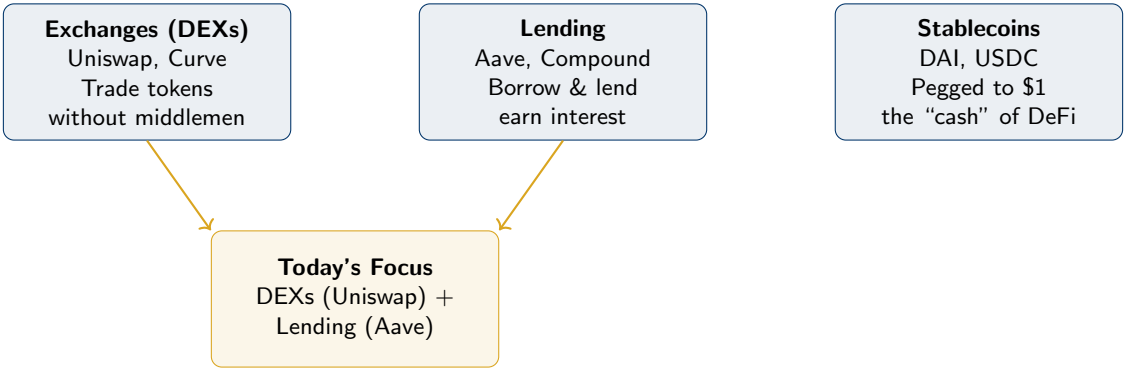
DeFi = financial services (trading, lending, borrowing, insurance) running on **smart contracts** — self-executing code on a blockchain.

DeFi Growth: Total Value Locked (TVL)



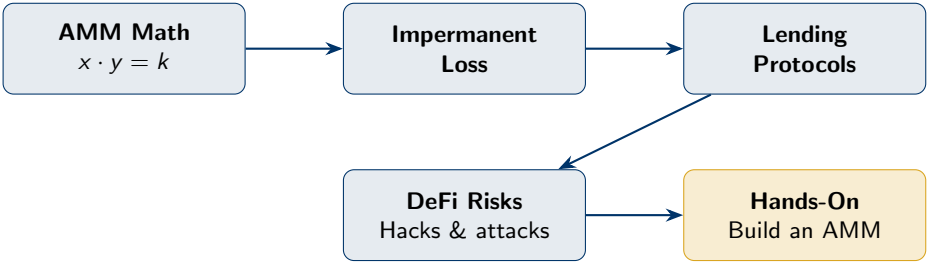
From $0 to over $100 billion in five years — all managed by code, not people.

The DeFi Ecosystem: Key Categories



Other categories: derivatives (Synthetix), insurance (Nexus Mutual), yield aggregators (Yearn), bridges, oracles, and more.

Today: The Math Behind DeFi Protocols



Learning Goals

After today you will:

- Understand the constant product formula ($x \cdot y = k$)
- Be able to calculate the price impact of a trade
- Know what impermanent loss is and when it hurts
- Understand how DeFi lending and liquidation work

Outline

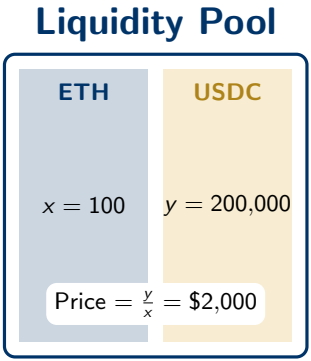
The Liquidity Pool: Two Tokens in a Pot

A Uniswap pool holds exactly two tokens:

- Example: **ETH** + **USDC**
- The pool starts with *equal value* of each
- Anyone can deposit (become a **liquidity provider**, LP)
- Anyone can trade against the pool

Variables:

- x = amount of ETH in the pool
- y = amount of USDC in the pool
- The **price** of ETH = y/x (USDC per ETH)



The Golden Rule: $x \times y = k$

Constant Product Formula [ ]

$$\boxed{x \times y = k}$$

The **product** of the two reserves must **always stay the same** (before fees).

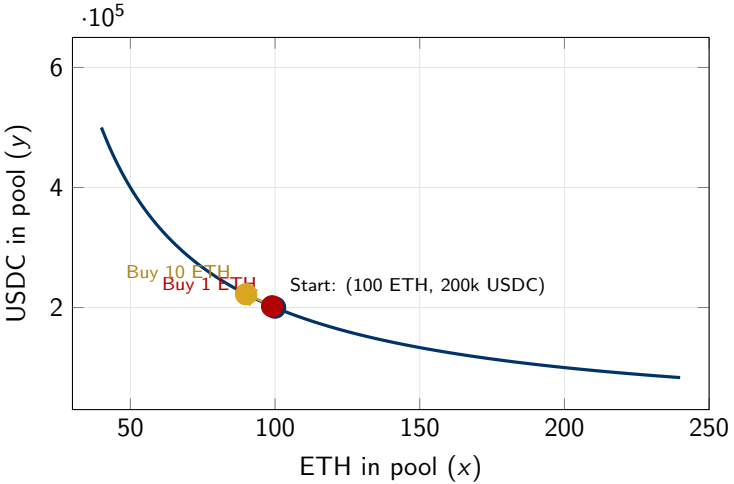
What this means:

- If someone **buys ETH** (removes ETH from pool), they must **add USDC** to keep k constant
- If someone **sells ETH** (adds ETH to pool), they receive USDC back
- The formula *automatically sets the price*
- No order book, no market maker, no human involvement!

Our Pool

$x = 100$ ETH, $y = 200{,}000$ USDC
$k = 100 \times 200{,}000 = 20{,}000{,}000$

Visualizing $x \cdot y = k$: The Hyperbola



Every trade slides along this curve. Bigger trades push further along.

Worked Example: Buying ETH from the Pool

Setup

Pool: 100 ETH + 200,000 USDC $\quad\Rightarrow\quad k = 20{,}000{,}000$
Current price: $200{,}000/100 = \$2{,}000$ per ETH

You want to buy 1 ETH. How much USDC do you pay?

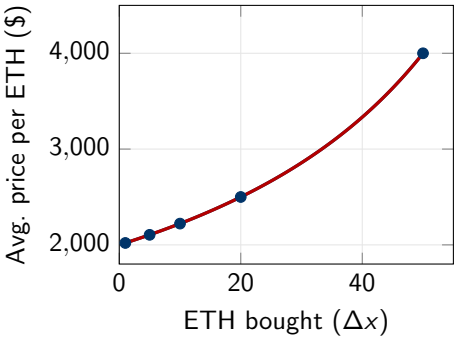
Step 1: After your trade, the pool has $x' = 100 - 1 = 99$ ETH
Step 2: Constant product: $99 \times y' = 20{,}000{,}000$
Step 3: Solve: $y' = 20{,}000{,}000/99 = 202{,}020.20$
Step 4: You pay: $y' - y = 202{,}020 - 200{,}000 = \mathbf{\$2{,}020.20}$

Price Impact

The "fair" price was \$2,000 but you paid \$2,020.
That extra \$20 is called **price impact** (or "slippage").
The formula makes you pay more to compensate the pool.

Buying More Gets More Expensive

Buy	Total Cost	Avg Price
1 ETH	\$2,020	\$2,020
5 ETH	\$10,526	\$2,105
10 ETH	\$22,222	\$2,222
20 ETH	\$50,000	\$2,500
50 ETH	\$200,000	\$4,000

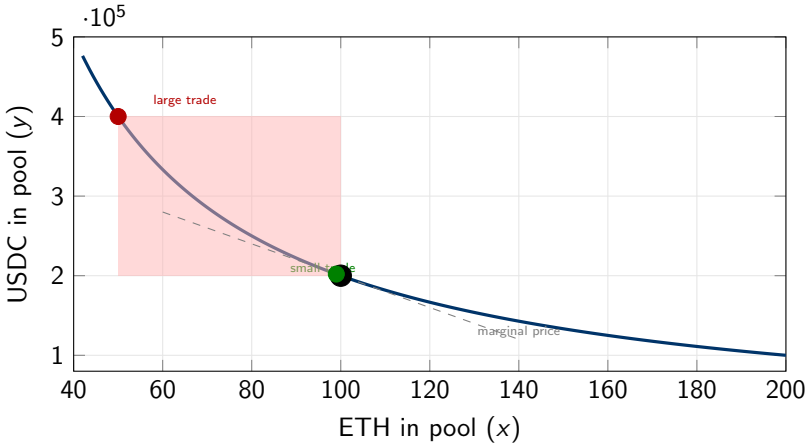


General formula:
To buy Δx ETH from a pool (x, y):

$$\text{Cost} = \frac{y \cdot \Delta x}{x - \Delta x}$$

This is by design: the curve protects the pool from being drained.

Visualizing Price Impact on the Curve



The curve is steep near the edges. Small trades: minimal slippage. Large trades: enormous slippage.

Swap Fees: How Liquidity Providers Earn

The Fee Mechanism

Every trade on Uniswap pays a **0.3% fee** on the input amount.
This fee goes to **liquidity providers** (LPs) proportional to their share.

Example:

- You swap 10,000 USDC for ETH
- Fee: $10{,}000 \times 0.003 = 30$ USDC goes to LPs
- You actually trade with $10{,}000 - 30 = 9{,}970$ USDC
- The 30 USDC gets added to the pool, increasing k slightly

LP Revenue

A pool doing \$10M in daily volume generates:
\$10M $\times$ 0.3% = **\$30,000 per day** in fees for LPs.

If the pool has \$50M in TVL, that's an annualized yield of:
$\frac{30{,}000 \times 365}{50{,}000{,}000} \approx 22\%$ APY (if volume stays constant)

AMMs vs. Traditional Order Books

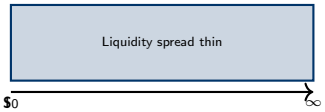
	Order Book (NYSE, Binance)	**AMM (Uniswap)** (Uniswap, Curve)
Price setting	Buyers & sellers match	Formula: $x \cdot y = k$
Liquidity from	Market makers	Anyone (LPs)
Minimum order	Depends	Any amount
Token listing	Exchange approval	Permissionless
Speed	Milliseconds	$\sim$12 seconds (Ethereum)
Slippage	Low for liquid pairs	Depends on pool size
Custody	Exchange holds funds	Your wallet

AMM advantages: permissionless, always-on, self-custody.
AMM disadvantages: higher slippage, slower, impermanent loss.

Uniswap V2 vs. V3: Concentrated Liquidity

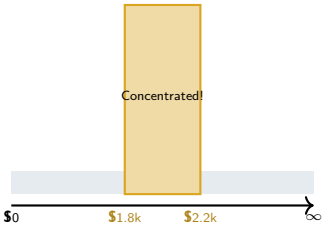
V2: Liquidity Spread Everywhere

- Your liquidity covers ALL prices from \$0 to ∞
- Most of it sits idle (who trades ETH at \$50?)
- Capital inefficient



V3: Liquidity Concentrated in a Range

- LPs choose a price range (e.g., \$1,800–\$2,200)
- All liquidity focused where trades happen
- Up to 4,000$\times$ more capital efficient!



V3 is more capital-efficient but introduces new risks: if the price leaves your range, you earn **zero fees**.

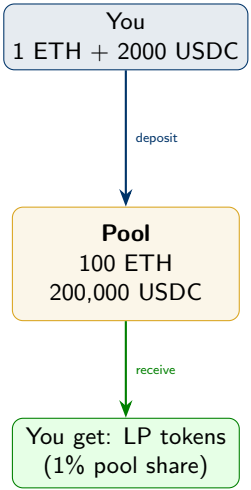
Outline

What Is Providing Liquidity?

To become a Liquidity Provider (LP):

1. Deposit **equal value** of two tokens into a pool
   Example: 1 ETH + 2,000 USDC (total: $4,000)
2. Receive **LP tokens** representing your share of the pool
3. Earn **swap fees** proportional to your share
4. Withdraw anytime by burning your LP tokens

Sounds great! Passive income from trading fees.
But there's a catch...



The Catch: Impermanent Loss (IL)

The Problem

When the price of one token changes relative to the other, an LP ends up with **less value** than if they had just held the tokens. This is called **impermanent loss**.

Simple example:

- You deposit: 1 ETH ($2,000) + 2,000 USDC = **$4,000 total**
- ETH price doubles to $4,000
- **If you had just held:** 1 ETH ($4,000) + 2,000 USDC = **$6,000**
- **As an LP:** the pool rebalances — you now have
  $\sim$0.707 ETH ($2,828) + $\sim$2,828 USDC = **$5,657**
- **IL** = $5,657 − $6,000 = −$343 (5.7% loss vs. holding!)

Why "impermanent"? If the price returns to $2,000, the loss disappears. But if you withdraw at the new price, it's *very* permanent.

Impermanent Loss: The Formula

IL as a Function of Price Ratio

Let $r = P_{\text{new}}/P_{\text{old}}$ be the price ratio. Then:

$$\boxed{\text{IL}(r) = \frac{2\sqrt{r}}{1+r} - 1}$$

Derivation sketch (optional, for the curious):

1. Pool reserves adjust: if price goes up by factor r, then $x_{\text{new}} = x_{\text{old}}/\sqrt{r}$ and $y_{\text{new}} = y_{\text{old}} \cdot \sqrt{r}$
2. LP value $= x_{\text{new}} \cdot P_{\text{new}} + y_{\text{new}} = 2y_{\text{old}}\sqrt{r}$
3. HODL value $= x_{\text{old}} \cdot P_{\text{new}} + y_{\text{old}} = y_{\text{old}}(1+r)$
4. $\text{IL} = \dfrac{\text{LP value}}{\text{HODL value}} - 1 = \dfrac{2\sqrt{r}}{1+r} - 1$

Note: IL is **always** ≤ 0 — the LP always does worse than holding (ignoring fees).

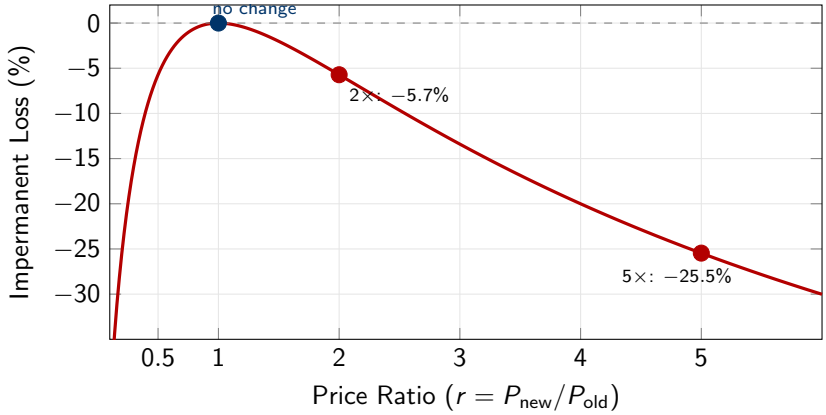
Impermanent Loss by Price Change

Price Ratio (r)	Price Change	Impermanent Loss
1.00	$\pm$0%	0.00%
1.25	+25%	−0.60%
1.50	+50%	−2.02%
2.00	+100% **(2×)**	**−5.72%**
3.00	+200% (3×)	−13.40%
5.00	+400% **(5×)**	**−25.46%**
0.50	−50%	−5.72%
0.20	−80%	−25.46%

Key observations:

- IL is **symmetric**: 2× up and 2× down give the same IL
- A 2× price move costs ∼6% — that's a LOT for passive income
- A 5× move costs ∼25% — catastrophic
- For crypto (where 5× moves happen), IL is a serious risk

Impermanent Loss Curve



The curve drops steeply for large price moves in either direction. This is the "hidden cost" of being a liquidity provider.

Why Does IL Happen? Intuition

The AMM Rebalances Against You

The constant product formula **automatically** sells your winning token and buys your losing token. It's like *rebalancing gone wrong*.

When ETH price rises:

- Arbitrageurs buy cheap ETH from the pool
- Pool sells ETH, receives USDC
- You end up with *less ETH, more USDC*
- You sold your winner too early!

When ETH price falls:

- Arbitrageurs sell ETH to the pool for USDC
- Pool buys ETH, gives up USDC
- You end up with *more ETH, less USDC*
- You bought the loser on the way down!

Either way, the AMM makes the wrong trade for you.
You always end up with more of the less-valuable token.

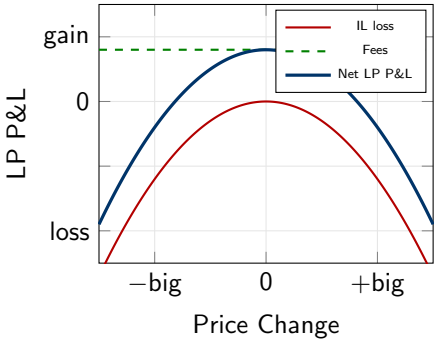
LP Payoff $\approx$ Short Straddle (Options Analogy)

From Day 1, recall options payoffs.
An LP position is economically similar to a **short straddle**:

- **Positive theta (fees):** You earn fees steadily over time, like collecting option premiums
- **Negative gamma (IL):** You lose money when prices move a lot in either direction

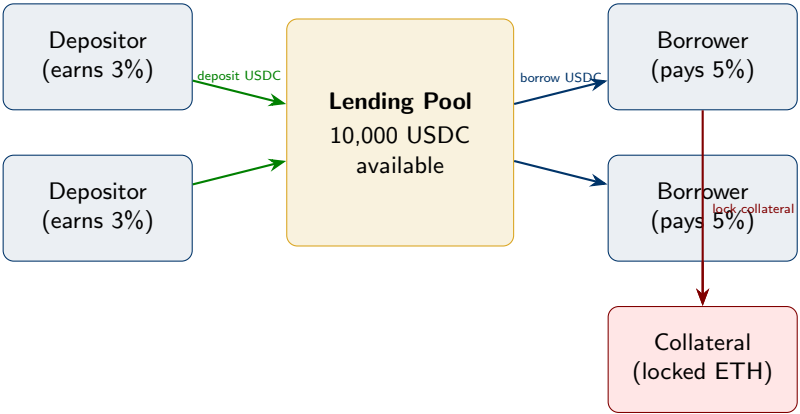
Key insight:

- LPs profit in **low-volatility, high-volume** conditions
- LPs lose in **high-volatility, low-volume** conditions
- Sound familiar? That's exactly a short straddle!



Outline

DeFi Lending: How Aave Works



No bank needed. Smart contract manages deposits, loans, interest, and liquidations automatically.

Over-Collateralization: Why You Must Deposit MORE

The Rule: Collateral > Loan

In DeFi, you must deposit **more** collateral than you borrow.
Typical ratio: **150%** (deposit $1,500 of ETH to borrow $1,000 USDC).

Why? There's no credit check! The protocol doesn't know who you are.

Example:

- You deposit 1 ETH (worth $2,000)
- Max borrow at 150%: $\frac{\$2,000}{1.50} = \$1,333$
- You borrow 1,000 USDC
- Collateral ratio: $\frac{2,000}{1,000} = 200\%$ ✓

Why over-collateralize?

- No identity / credit score
- Prices can drop fast
- Buffer protects depositors
- If ratio drops below threshold ⇒ **liquidation!**

Compare to TradFi

Mortgage: 80% LTV (you put 20% down). DeFi: ∼67% LTV (you put ∼33% down). Much more conservative!

Interest Rate Model: The "Kink"

Utilization Rate

$$U = \frac{\text{Total Borrowed}}{\text{Total Deposited}} \qquad \text{(how much of the pool is being used)}$$

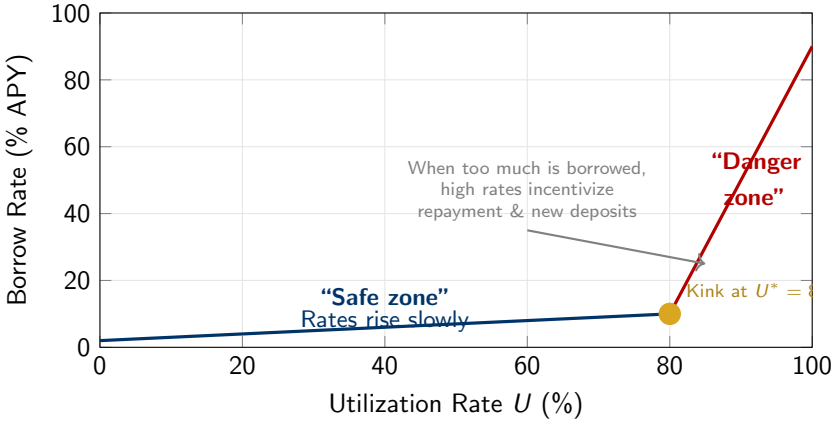
Aave's interest rate model:

$$r(U) = \begin{cases} r_0 + \dfrac{U}{U^*} \cdot r_{\text{slope1}} & \text{if } U \leq U^* \\ r_0 + r_{\text{slope1}} + \dfrac{U - U^*}{1 - U^*} \cdot r_{\text{slope2}} & \text{if } U > U^* \end{cases}$$

In plain English:

- Below the "kink" ($U^* \approx 80\%$): rates rise gently
- Above the kink: rates **skyrocket** to discourage over-borrowing
- This ensures depositors can always withdraw (there's always some buffer)

The Interest Rate Kink: Visual



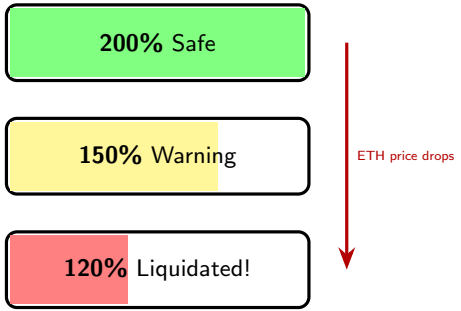
The kink design is elegant: **market-driven self-regulation** without human intervention.

Liquidation: When Collateral Drops Too Low

What happens when the collateral ratio falls below the threshold?

Example sequence:

1. You borrow 1,000 USDC against 1 ETH ($2,000)
2. Collateral ratio: 200% (safe)
3. ETH drops to $1,200
4. Collateral ratio: $1{,}200/1{,}000 = 120\%$ (below 150% threshold!)
5. **Liquidation triggered:** anyone can repay part of your debt and claim your ETH at a discount (typically 5–10%)
6. You lose a chunk of your collateral



Key Risk

In a flash crash, liquidations cascade: sell pressure → lower prices → more liquidations → lower prices...

Outline

DeFi Risk 1: Smart Contract Bugs and Hacks

"Code Is Law" — Until It Has a Bug

- **The DAO hack (2016):** $60M stolen due to a reentrancy bug
- **Wormhole (2022):** $320M — bridge vulnerability
- **Ronin (2022):** $625M — validator key compromise
- **Euler Finance (2023):** $197M — flash loan attack

Oracle Manipulation

- DeFi protocols need **price feeds** ("oracles")
- Attacker manipulates the oracle price
- Protocol thinks collateral is worth more/less
- Attacker extracts profit
- Example: Mango Markets — $114M (2022)

Total DeFi hacks since 2020: over $10 billion lost.

"Don't trust, verify" only works if you can read Solidity code.

How to Spot Red Flags in DeFi

Red Flags (RUN!)

- "Guaranteed" 1,000%+ APY
- Anonymous team, no audits
- Forked code with no changes
- Admin keys that can drain funds
- TVL from a single whale
- "Just trust us" governance

Green Flags (More Trustworthy)

- Multiple independent audits (Trail of Bits, OpenZeppelin)
- Open-source, verified contracts
- Time-locked admin functions
- High, diverse TVL over months
- Known, doxxed team
- Bug bounty program
- Governance token voting

Rule of Thumb

If the yield seems too good to be true, **you are the yield.**
(i.e., your money is what pays the "returns" for earlier depositors — a Ponzi)

Outline

Hands-On Exercise

Build Your Own AMM in Python

Exercise: Implement $x \cdot y = k$ in Python

Your AMM in 10 Lines

```
class SimpleAMM:
    def __init__(self, x, y):
        self.x = x          # token A reserves
        self.y = y          # token B reserves
        self.k = x * y      # constant product

    def swap_A_for_B(self, dx):
        new_x = self.x + dx
        new_y = self.k / new_x
        dy = self.y - new_y  # amount of B received
        self.x = new_x
        self.y = new_y
        return dy

    def price(self):
        return self.y / self.x
```

Simulate 20 Trades and Track Prices

Simulation Code

```
import random
amm = SimpleAMM(100, 200000)  # 100 ETH, 200k USDC

for i in range(20):
    # Random trade: buy or sell 0.5-3 ETH
    size = random.uniform(0.5, 3.0)
    if random.random() > 0.5:
        dy = amm.swap_A_for_B(size)
        print(f"Buy {size:.1f} ETH, pay {dy:.0f} USDC")
    else:
        dx = amm.swap_B_for_A(size * amm.price())
        print(f"Sell ~{dx:.1f} ETH worth of USDC")
    print(f"  Price: ${amm.price():.2f}")
```

Tasks:

1. Implement swap_B_for_A (reverse direction)

Calculate Impermanent Loss for Different Scenarios

IL Calculator

```
import numpy as np

def impermanent_loss(r):
    """r = new_price / old_price"""
    return 2 * np.sqrt(r) / (1 + r) - 1

# Test different price changes
ratios = [0.5, 0.8, 1.0, 1.25, 1.5, 2.0, 3.0, 5.0]
for r in ratios:
    il = impermanent_loss(r)
    print(f"Price ratio {r:.2f}x -> IL = {il*100:.2f}%")
```

Questions to answer:

- At what price ratio does IL exceed 10%?
- How does IL compare for stablecoin pairs (small r) vs. volatile pairs?
- What happens when $r = 0$ or $r \to \infty$?

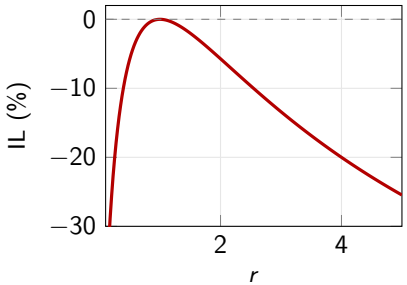
Plot the IL Curve

Code

```
import matplotlib.pyplot as plt
r = np.linspace(0.1, 5, 500)
il = impermanent_loss(r) * 100

plt.figure(figsize=(8,5))
plt.plot(r, il, 'r-', lw=2)
plt.axhline(y=0, color='gray',
            linestyle='--')
plt.xlabel('Price Ratio r')
plt.ylabel('IL (%)')
plt.title('Impermanent Loss')
plt.grid(True, alpha=0.3)
plt.show()
```

Expected output:



Extension: add a horizontal line for your estimated fee income (e.g., +10% APY) and find the "breakeven" price range.

LP Returns: When Is It Profitable?

Net LP Return = Fee Income − Impermanent Loss

$$\text{LP Return} = \underbrace{\text{Fee APY}}_{\text{positive}} + \underbrace{\text{IL}}_{\text{negative}}$$

Scenario	Fee APY	IL	Net
Stablecoin pair, stable prices	5%	−0.1%	+4.9%
ETH/USDC, moderate move (1.5×)	20%	−2.0%	+18.0%
ETH/USDC, big move (3×)	20%	−13.4%	+6.6%
ETH/USDC, huge move (5×)	20%	−25.5%	−5.5%
Meme coin, wild move (10×)	50%	−42.3%	+7.7%

Takeaway: LP-ing is profitable when fee income exceeds IL. This works best for **high-volume, low-volatility** pairs.

Discussion: Would You Provide Liquidity?

Arguments FOR LP-ing

- Earn passive income (fees)
- Contribute to a public good (liquidity)
- Permissionless: anyone can participate
- Some pairs have very high APY
- IL is manageable for stable pairs

Arguments AGAINST

- Impermanent loss can exceed fees
- Smart contract risk (hacks)
- Tax complexity (every swap is a taxable event?)
- Opportunity cost (could just HODL)
- V3 requires active management

Think About

- Which pairs would you LP? (ETH/USDC? USDC/DAI? DOGE/ETH?)
- How would you hedge impermanent loss?
- At what APY does the risk become worth it for you?

Day 2 Summary and Key Takeaways

What We Learned Today

1. **DeFi** replaces banks with smart contracts — permissionless, 24/7, global
2. **Uniswap's AMM** uses $x \cdot y = k$ to set prices automatically
3. **Price impact** increases with trade size — the curve protects the pool
4. **Impermanent loss** $= 2\sqrt{r}/(1+r) - 1$ hurts LPs when prices move
5. **DeFi lending** requires over-collateralization; the kink model controls interest rates
6. **Risks are real:** \$10B+ lost to hacks — always check audits

Day 3 Preview: Blockchain Economics

How does a blockchain actually work?
Mining vs. staking — what secures the network?
Game theory: why do validators play by the rules?

References I

[1] Alfred Lehar and Christine A. Parlour. “Decentralized Exchange: The Uniswap Automated Market Maker”. In: *Journal of Finance* 80.1 (2025), pp. 321–374.