Topic 4.2: DeFi Primitives

Lending, AMMs, and Financial Legos

Joerg Osterrieder

Digital Finance

2025

Learning Objectives

By the end of this topic, you will be able to:

1. **Explain** how Automated Market Makers (AMMs) price assets using the constant product formula $x \cdot y = k$ (think of a see-saw: when one side goes down, the other must go up to stay balanced)
2. **Calculate** price impact and slippage for trades of different sizes
3. **Understand** algorithmic interest rate mechanisms in DeFi lending protocols
4. **Compute** impermanent loss for various price change scenarios

   Impermanent Loss = temporary loss from prices changing while you're providing liquidity—like selling low and buying high automatically
5. **Analyze** the composability of DeFi protocols ("money legos")
6. **Evaluate** flash loans as both innovation and attack vector

Key Skills: AMM mathematics, LP token mechanics (LP = Liquidity Provider), risk assessment

---

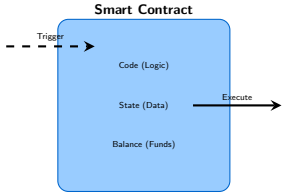
Prerequisite: Understanding of smart contracts from T4.1

Prerequisites: Smart Contract Foundations

From Topic 4.1 – Key Concepts:

Quick Check: Do You Remember?

- What is a smart contract?
- Why can't you change code after deployment?



- Smart contracts are self-executing programs on blockchain
- **Deterministic**: Same input → same output
- **Immutable**: Code cannot be changed after deployment
- **Transparent**: Anyone can verify the logic
- **Composable**: Contracts can call other contracts

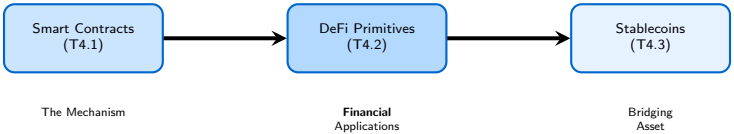
Key Insight

DeFi replaces financial intermediaries with auditable code.

Why This Matters for DeFi:

- DeFi protocols are smart contracts
- Trust in code, not institutions
- Permissionless innovation

From Smart Contracts to DeFi



The Building Block Progression:

1. **T4.1**: Smart contracts provide the *mechanism* for trustless execution
2. **T4.2**: DeFi primitives build *financial applications* on that mechanism
3. **T4.3**: Stablecoins provide the *stable value unit* for DeFi to function

Today's Focus

How do we build trading, lending, and yield generation using only smart contracts?

What is DeFi?

Definition

Decentralized Finance (DeFi) refers to financial services built on public blockchains that operate without traditional intermediaries.

Concrete Example: Imagine borrowing money directly from strangers worldwide with no bank in the middle. The smart contract automatically manages collateral, interest rates, and repayment.

Core Principles:

- **Permissionless**: Anyone can participate
- **Non-custodial**: Users control their assets
- **Transparent**: All code and transactions public
- **Composable**: Protocols can be combined

DeFi Ecosystem (2024):

- Total Value Locked (TVL = Total Value Locked = money deposited in DeFi protocols): $50B+

  That's more than the GDP of some countries!
- Daily trading volume: $2B+
- Active protocols: 500+
- Supported chains: 50+

Major Categories:

- Decentralized Exchanges
- Lending Protocols
- Derivatives
- Yield Aggregators

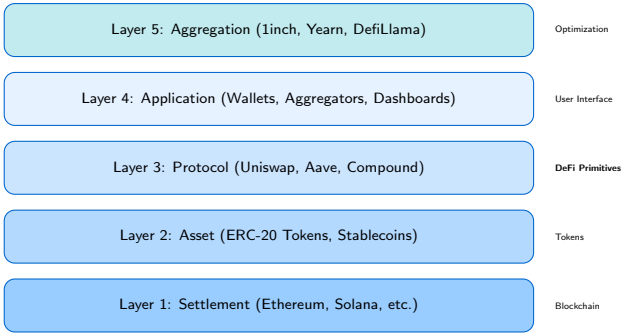
DeFi vs. Traditional Finance

Feature	Traditional Finance	DeFi
Access	KYC (Know Your Customer = proving you are who you say you are), credit checks	Wallet address only
Hours	Business hours, T+2 settlement (2 days to finalize)	24/7/365, instant
Custody	Institutions hold assets	User self-custody
Transparency	Private ledgers	Public blockchain
Innovation	Regulatory approval needed	Permissionless deployment
Risk	Counterparty, institution	Smart contract, oracle

The Composability Advantage

DeFi protocols are like "money legos"—they can be combined in ways their creators never anticipated. A flash loan can be used in an arbitrage that spans 5 different protocols in a single transaction.

The DeFi Stack

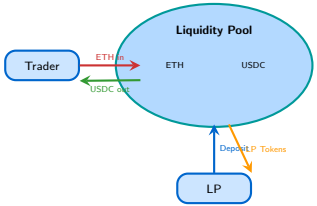


Today's Focus: Layer 3 – The core protocols that enable decentralized trading and lending

Automated Market Makers (AMMs)

Traditional Exchange:

- Order book with bids/asks (like an auction where buyers and sellers post their desired prices)
- Market makers provide liquidity
- Requires active management
- Centralized matching engine



AMM Innovation:

- No order book needed
- Liquidity pools replace market makers
- Algorithmic pricing
- Anyone can provide liquidity

Key Protocols:

- **Uniswap**: Most popular AMM, simple constant product formula
- **SushiSwap**: Uniswap fork with community governance
- **Curve**: Optimized for stablecoin swaps (low slippage)
- **Balancer**: Multi-token pools with custom weights

Follow the Money: How AMMs Work (Step-by-Step)

Scenario: You Want to Swap 1 ETH for USDC

Initial Pool State:

- Pool has: 100 ETH + 300,000 USDC
- Current price: 1 ETH = 3,000 USDC

Step 1: You deposit 1 ETH into the pool

- Pool now has: 101 ETH + 300,000 USDC

Step 2: The pool removes USDC to keep the product constant

- Before: $100 \times 300,000 = 30,000,000$
- After: $101 \times ? = 30,000,000$
- Solve: $? = 30,000,000 \div 101 = 297,030$ USDC

Step 3: You receive the difference

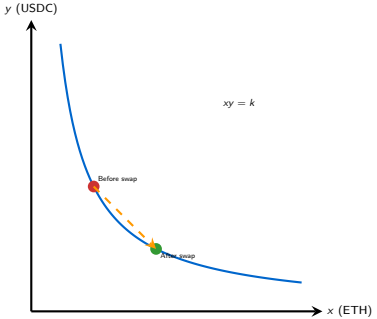
- USDC removed: $300,000 - 297,030 = 2,970 USDC$
- You get slightly less than 3,000 USDC due to price impact!

The Constant Product Formula: $x \cdot y = k$

The Core Equation

$$x \cdot y = k$$

- x = Token A reserves
- y = Token B reserves
- k = Constant (invariant)



Price Determination:

$$\text{Price of A in B} = \frac{y}{x}$$

After swap of Δx:

$$\Delta y = y - \frac{k}{x + \Delta x}$$

Price Impact

Larger trades move further along the curve, resulting in worse prices. This is called **slippage** or **price impact**.

AMM Numerical Example

Initial Pool State

- 100 ETH + 300,000 USDC
- $k = 100 \times 300,000 = 30,000,000$
- Price: 1 ETH = 3,000 USDC

Trader swaps 10 ETH for USDC:

$$\begin{aligned} \text{New ETH reserves:} \quad & x' = 100 + 10 = 110 \\ \text{New USDC reserves:} \quad & y' = \frac{30,000,000}{110} = 272,727.27 \\ \text{USDC received:} \quad & \Delta y = 300,000 - 272,727.27 = 27,272.73 \end{aligned}$$

Price Impact Analysis

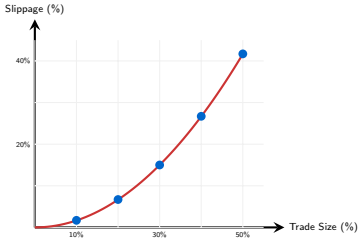
- Expected (no impact): $10 \times 3,000 = 30,000$ USDC
- Actual received: 27,272.73 USDC
- Slippage: $\frac{30,000 - 27,272.73}{30,000} = 9.09\%$
- New price: $\frac{272,727.27}{110} = 2,479.34$ USDC/ETH

Why Larger Trades Have More Slippage

Trade Size vs. Slippage:

Trade	Slippage	Cost
1 ETH	0.99%	$30
5 ETH	4.76%	$714
10 ETH	9.09%	$2,727
20 ETH	16.67%	$10,000
50 ETH	33.33%	$50,000

What This Costs You: Dollar amounts lost compared to no slippage (at $3,000/ETH)

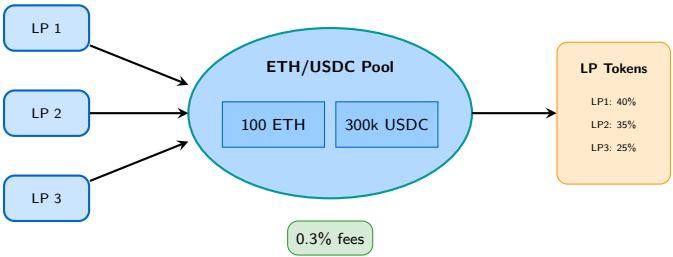


Key Insight: Slippage grows *non-linearly* because larger trades shift the reserve ratio more dramatically.

Practical Implication

Deep liquidity pools (high TVL) have less slippage for the same trade size. Always check price impact before executing large trades.

Liquidity Pool Mechanics



LP Token Mechanics:

- LP tokens represent proportional claim on pool reserves
- Fees accumulate in pool, increasing LP token value
- Withdrawal returns proportional share of *current* reserves

LP Tokens: Ownership and Fee Accrual

How LP Tokens Work:

1. Deposit both tokens in equal value
2. Receive LP tokens proportional to contribution
3. First deposit: LP $= \sqrt{x \cdot y}$
4. Later deposits: proportional to pool share

Example:

- Pool: 1,000 total LP tokens
- You hold: 100 LP tokens (10%)
- You own 10% of all reserves
- Plus 10% of accumulated fees

Fee Accrual Mechanism:

- Trading fees stay in the pool
- Reserves grow with each trade
- LP token supply unchanged
- Each LP token worth more over time

Key Point

Fees aren't distributed separately—they accumulate in the pool. You receive your share when you withdraw by burning LP tokens.

Impermanent Loss Explained

Definition

Impermanent Loss (IL) is the difference between holding assets in a liquidity pool vs. simply holding them in your wallet.

Why it happens:

1. You deposit equal value: 1 ETH ($3,000) + 3,000 USDC
2. ETH price doubles to $6,000
3. Arbitrageurs rebalance the pool
4. Your LP position: 0.707 ETH + 4,243 USDC = $8,485
5. If you had just held: 1 ETH + 3,000 USDC = $9,000
6. **Impermanent Loss: $515 (5.72%)**

Key Insight

Loss is "impermanent" because if prices return to original levels, the loss disappears. It becomes *permanent* when you withdraw at different prices.

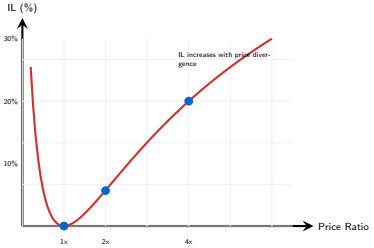
Impermanent Loss Formula and Visualization

IL Formula:

$$IL = \frac{2\sqrt{r}}{1+r} - 1$$

where $r = \frac{P_1}{P_0}$ (price ratio)

Price Change	IL
1.25x (25% up)	0.6%
1.50x (50% up)	2.0%
2x (100% up)	5.7%
3x (200% up)	13.4%
4x (300% up)	20.0%
5x (400% up)	25.5%



Mitigating IL:

- Provide liquidity to correlated pairs (stablecoin-stablecoin)
- Choose pools with high trading volume (fees offset IL)
- Use concentrated liquidity (Uniswap V3)

Impermanent Loss: Worked Example

Initial State:

- Deposit: 1 ETH + 2,000 USDC
- Initial value: $4,000
- ETH price: $2,000

Price Change:

- New ETH price: $4,000 (2x)
- Price ratio $r = 2$

If Just Holding:

- 1 ETH $\times$ $4,000 = $4,000
- 2,000 USDC = $2,000
- Total: **$6,000**

In the Pool:

- Pool rebalances via arbitrage
- New position: 0.707 ETH + 2,828 USDC
- Value: $0.707 \times 4000 + 2828$
- Total: **$5,657**

Impermanent Loss:

$$IL = \frac{2\sqrt{2}}{1+2} - 1 = -5.72\%$$

$$\text{Loss} = 6000 - 5657 = \$343$$

Break-Even

Trading fees must exceed $343 to be profitable!

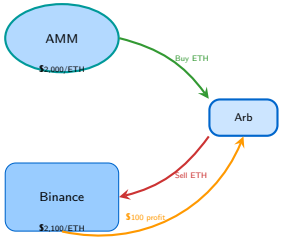
The Role of Arbitrage in AMMs

How Price Discovery Works:

1. External price changes (e.g., on Binance)
2. AMM price diverges from market
3. Arbitrageurs profit by trading the difference
4. AMM price converges to market price

Example:

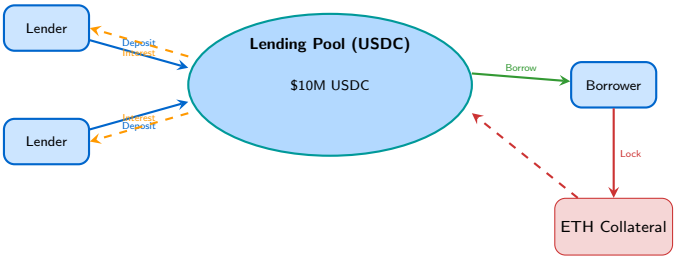
- AMM price: 1 ETH = \$2,000
- Binance price: 1 ETH = \$2,100
- Arbitrageur buys cheap on AMM
- Sells expensive on Binance
- AMM price increases toward \$2,100



Key Insight

Arbitrage is the mechanism that keeps AMM prices aligned with external markets—without oracles!

DeFi Lending: How It Works



Key Mechanics:

- **Over-collateralization**: Borrow $1,000 requires $1,500+ collateral
- **Algorithmic rates**: Interest adjusts with utilization
- **Liquidation**: If collateral falls below threshold, anyone can liquidate

Algorithmic Interest Rates

Utilization Rate:

$$U = \frac{\text{Borrowed}}{\text{Supplied}}$$

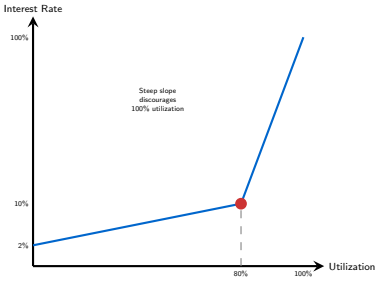
Borrow Rate (kinked model):

$$R_{\text{borrow}} = \begin{cases} R_0 + U \cdot R_{\text{slope1}} & U < U_{\text{opt}} \\ R_0 + U_{\text{opt}} \cdot R_1 + & \\ \quad (U - U_{\text{opt}}) \cdot R_2 & U \geq U_{\text{opt}} \end{cases}$$

Supply Rate:

$$R_{\text{supply}} = R_{\text{borrow}} \times U \times (1 - \text{fee})$$

Key Protocols: Aave, Compound, MakerDAO



DeFi Lending: Worked Example

Scenario:

- You have 10 ETH worth $30,000
- Need $15,000 USDC liquidity
- Don't want to sell your ETH

DeFi Solution (Aave):

1. Deposit 10 ETH as collateral
2. Borrow up to 75% LTV = $22,500
3. You borrow $15,000 USDC
4. Pay 5% APR interest

Position Metrics:

- Collateral: $30,000 (10 ETH)
- Debt: $15,000 (USDC)
- Health Factor: $\frac{30000 \times 0.825}{15000} = 1.65$
- Liquidation at: HF < 1.0

Liquidation Risk

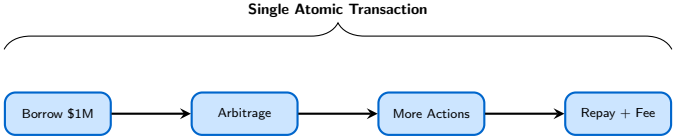
If ETH drops 40% to $1,800:

- New collateral: $18,000
- Health Factor: $\frac{18000 \times 0.825}{15000} = 0.99$
- Position liquidated!

Flash Loans: Innovation or Attack Vector?

Definition

A **flash loan** is an uncollateralized loan that must be borrowed and repaid within a single transaction.



Legitimate Uses: Arbitrage, collateral swaps, self-liquidation
Attack Uses: Oracle manipulation, governance attacks, protocol exploits

The Double-Edged Sword

Flash loans democratize access to capital but have enabled over $500M in DeFi exploits.

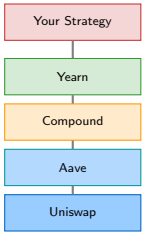
Composability: The "Money Legos" Concept

What is Composability?

- Protocols can call other protocols
- Build complex strategies from simple parts
- No permission needed to integrate
- Innovation without coordination

Example Stack:

1. Deposit ETH into Aave
2. Receive aETH (interest-bearing)
3. Deposit aETH into Uniswap
4. Earn trading fees + lending interest



Risk Compounds Too

Composability creates *systemic risk*—a bug in one protocol can cascade through the stack.

Understanding DeFi Metrics

Total Value Locked (TVL):

- Total assets deposited in protocol
- Indicator of protocol usage
- ETH/USDC Pool with 1,000 ETH ($2M) + 2M USDC = $4M TVL

Other Key Metrics:

- **Volume**: Daily trading volume
- **Fees**: Revenue generated
- **APY**: Annual percentage yield
- **Health Factor**: Lending safety

Top DeFi Protocols (2024):

Protocol	TVL
Lido	$20B+
Aave	$10B+
MakerDAO	$8B+
Uniswap	$5B+
Curve	$2B+

Why TVL Matters:

- Higher TVL = deeper liquidity
- Less slippage for traders
- More attractive to LPs

DeFi Risks: A Complete Picture

Smart Contract Risk:

- Bugs in code (The DAO: $60M)
- Reentrancy attacks
- Logic errors
- Governance exploits

Oracle Risk:

- Price manipulation
- Flash loan attacks
- Stale data

Economic Risk:

- Impermanent loss
- Liquidation cascades
- Bank runs on pools

Systemic Risk:

- Protocol dependencies
- Stablecoin de-pegs
- Contagion effects

Key Insight

DeFi doesn't eliminate risk—it transforms and redistributes it.

Hands-On Exercise: NB09 – AMM Simulation

Notebook NB09: AMM Simulation

What You Will Do:

1. **Create a Liquidity Pool**: Initialize with ETH and USDC reserves
2. **Execute Swaps**: Trade tokens and observe price changes
3. **Provide Liquidity**: Add liquidity and receive LP tokens
4. **Measure Impermanent Loss**: Calculate IL for various price scenarios
5. **Analyze Arbitrage**: See how arbitrage keeps prices aligned

Key Learning Outcomes:

- Practical understanding of $x \cdot y = k$
- Visualize slippage and price impact
- Experience the LP perspective

NB09 Preview: Core AMM Functions

```python
class SimpleAMM:
    def __init__(self, reserve_x, reserve_y):
        self.x = reserve_x  # ETH
        self.y = reserve_y  # USDC
        self.k = reserve_x * reserve_y

    def get_spot_price(self):
        return self.y / self.x  # Price of X in terms of Y

    def swap_x_for_y(self, amount_x):
        # Apply constant product formula
        new_x = self.x + amount_x
        new_y = self.k / new_x
        amount_y_out = self.y - new_y
        self.x, self.y = new_x, new_y
        return amount_y_out

    def calculate_impermanent_loss(self, price_ratio):
        return 2 * sqrt(price_ratio) / (1 + price_ratio) - 1
```

NB09 includes interactive visualizations of the bonding curve and IL

Discussion: DeFi in Practice

Case Study: The 2020 DeFi Summer

- TVL grew from $1B to $15B in 6 months
- Yield farming introduced liquidity mining
- Composability enabled rapid innovation
- Also: exploits, rug pulls, gas wars

Discussion Questions:

1. Why did DeFi grow so rapidly in 2020?
2. What are the barriers to mainstream DeFi adoption?
3. How do DeFi risks compare to traditional finance risks?
4. Can DeFi truly be "decentralized" if most users access it through centralized frontends?

Real-World DeFi Applications

For Individuals:

- **Trading**: Swap tokens 24/7 without KYC
- **Lending**: Earn yield on idle assets
- **Borrowing**: Access liquidity without selling
- **Yield Farming**: Optimize returns across protocols

For Institutions:

- Treasury management
- On-chain settlement
- Tokenized collateral
- Automated market making

Success Stories:

- Uniswap: $1.5T+ cumulative volume
- Aave: $10B+ in active loans
- Curve: $100B+ stablecoin swaps

Emerging Use Cases:

- Real-world asset lending
- Cross-border payments
- Institutional DeFi (permissioned pools)
- DeFi-TradFi bridges

Critical Analysis: Is DeFi Really Decentralized?

Centralization Points:

- **Frontends**: Most users access via websites
- **Oracles**: Price feeds are critical dependencies
- **Governance**: Token holders control protocols
- **Infrastructure**: RPC providers, block builders

The Ownership Question:

- Top 1% often holds majority tokens
- VC funding creates concentrated ownership
- "Decentralization theater"?

What IS Decentralized:

- Smart contract execution
- Permissionless access
- Transparent rules
- No single point of failure

Nuanced View

DeFi is more accurately "disintermediated" than "decentralized." It removes certain intermediaries while creating new dependencies and power structures.

The Future of DeFi

Technical Evolution:

- **Layer 2**: Lower fees, faster transactions
- **Cross-chain**: Unified liquidity across chains
- **Account Abstraction**: Better UX
- **Intent-based**: Express what, not how

Market Evolution:

- Institutional adoption growing
- Regulatory clarity emerging
- TradFi-DeFi convergence
- Real-world asset integration

Key Challenges:

- Scalability limitations
- User experience complexity
- Regulatory uncertainty
- Smart contract risks

The Big Question

Will DeFi remain a parallel financial system, or will it merge with traditional finance? The answer likely lies somewhere in between.

Executive Summary

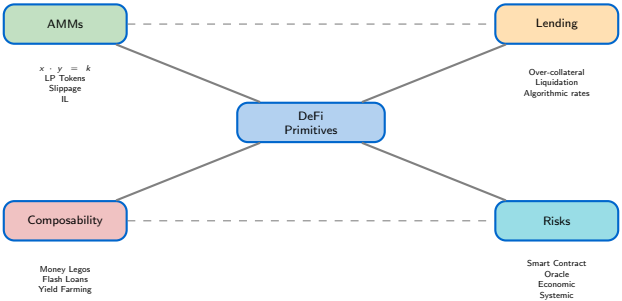
Core Concepts

- **AMMs** replace order books with liquidity pools and mathematical formulas ($x \cdot y = k$)
- **Liquidity providers** earn fees but face impermanent loss risk
- **DeFi lending** uses over-collateralization and algorithmic rates
- **Composability** enables innovation but creates systemic risk
- **Flash loans** democratize capital but enable attacks

Key Equations:

- Constant Product: $x \cdot y = k$
- Spot Price: $P = \frac{y}{x}$
- Impermanent Loss: $IL = \frac{2\sqrt{r}}{1+r} - 1$
- Utilization: $U = \frac{\text{Borrowed}}{\text{Supplied}}$

Concept Map: DeFi Primitives



Key Terms (Part 1)

AMM (Automated Market Maker):
A protocol that uses algorithms to price assets instead of order books.

Liquidity Pool:
A smart contract holding reserves of two tokens for trading.

LP Token:
Token representing ownership share in a liquidity pool.

Constant Product Formula:
$x \cdot y = k$ — the invariant that governs AMM pricing.

Slippage (Price Impact):
The difference between expected and actual execution price.

Impermanent Loss:
Opportunity cost of providing liquidity vs. holding assets.

TVL (Total Value Locked):
Total assets deposited in a DeFi protocol.

Utilization Rate:
Percentage of supplied assets currently borrowed.

Key Terms (Part 2)

Over-Collateralization:
Requiring more collateral than loan value (e.g., 150%).

Liquidation:
Forced sale of collateral when health factor drops below threshold.

Health Factor:
Ratio measuring loan safety; liquidation occurs when < 1.

Flash Loan:
Uncollateralized loan borrowed and repaid in one transaction.

Composability:
Ability of protocols to interact and build upon each other.

Yield Farming:
Strategy of moving assets between protocols to maximize returns.

Arbitrage:
Profiting from price differences across markets, keeping prices aligned.

Sandwich Attack:
MEV attack that front-runs and back-runs a victim's trade.

Common Misconceptions

Misconception 1:
"LPs always make money from fees"
Reality: Impermanent loss can exceed fee income, especially in volatile pairs.

Misconception 2:
"DeFi is completely trustless"
Reality: You still trust the code, oracles, governance, and infrastructure providers.

Misconception 3:
"Flash loans are only for attacks"
Reality: Most flash loans are used for legitimate arbitrage and collateral management.

Misconception 4:
"Higher APY means better investment"
Reality: High yields often indicate higher risk (smart contract, IL, or token inflation).

Misconception 5:
"Impermanent loss only matters if you withdraw"
Reality: IL represents real opportunity cost—you would have more value if you had just held.

Misconception 6:
"Audited protocols are safe"
Reality: Audits reduce but don't eliminate risk. Many exploited protocols were audited.

Self-Assessment Questions (1/2)

Question 1: Liquidity Pools

What is a liquidity pool in the context of AMMs?

A. A database storing all pending trades waiting to be executed

B. A smart contract holding reserves of two tokens that traders can swap against using a pricing formula

C. A group of traders who manually set prices for token pairs

D. A backup storage system for blockchain data

Question 2: Impermanent Loss Formula

What is the mathematical formula for impermanent loss given price ratio r?

A. $IL = r - 1$

B. $IL = \frac{2\sqrt{r}}{1+r} - 1$

C. $IL = \frac{r^2-1}{r+1}$

D. $IL = \sqrt{r} - 1$

Self-Assessment Questions (2/2)

Question 3: Fee Accrual Mechanism

How do trading fees accrue to LP token holders?

A. Fees are distributed monthly as separate token rewards

B. Fees are automatically deposited into LP wallets after each trade

C. Fees remain in the pool, increasing the reserves, so each LP token represents a growing share of value

D. Fees must be manually claimed through a governance process

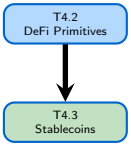
Answers:

- Question 1: **B** — A liquidity pool is a smart contract holding token reserves
- Question 2: **B** — The IL formula captures value loss from price divergence
- Question 3: **C** — Fees grow the pool; LP tokens represent larger shares

What's Next: Topic 4.3 – Stablecoins

Preview of T4.3:

- Why stablecoins matter for DeFi
- Three design approaches:
  - Fiat-backed (USDC, USDT)
  - Crypto-collateralized (DAI)
  - Algorithmic (and why they fail)
- The stablecoin trilemma
- Regulatory landscape



Connection to T4.2:

- Stablecoins are the "stable leg" in most DeFi pools
- Understanding stability mechanisms is crucial

Hands-on: NB10 – Stablecoin price stability analysis

Resources for Further Learning

Essential Reading:

- Uniswap V2 Whitepaper
- Aave Documentation
- "DeFi and the Future of Finance" (Campbell Harvey)

Interactive Tools:

- DefiLlama (TVL tracking)
- Dune Analytics (on-chain data)
- Impermanent Loss calculators

Technical Resources:

- Ethereum.org DeFi docs
- Curve Finance resources
- Chainlink education

Stay Updated:

- The Defiant newsletter
- Bankless podcast
- Week in Ethereum News

Course Materials

Notebook NB09: AMM Simulation – practice with $x \cdot y = k$, slippage, and IL calculations

Topic 4.2: DeFi Primitives

Lending, AMMs, and Financial Legos

Questions & Discussion

Next Topic: T4.3 – Stablecoins: The Bridge Between Two Worlds

Joerg Osterrieder — Digital Finance — 2025