

Lesson 21: DeFi Fundamentals

Module 2: Blockchain Fundamentals

Digital Finance

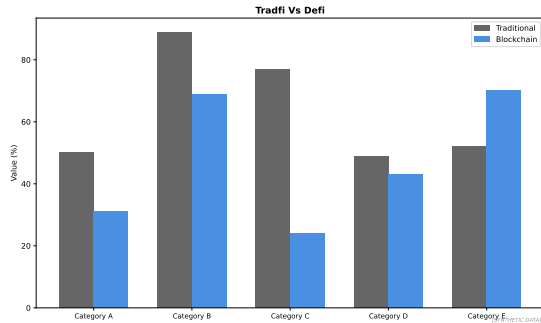
DeFi: Decentralized Finance Revolution

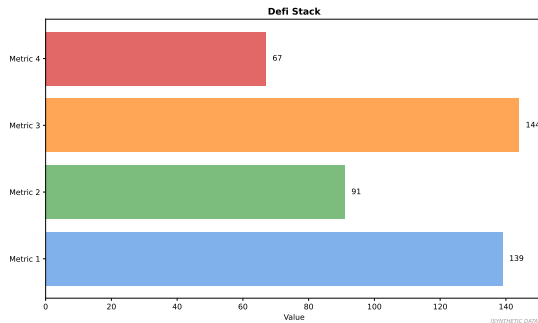
Traditional Finance (TradFi):

- Banks, brokers, exchanges
- Intermediaries control access
- Centralized custody
- Limited hours, geographic restrictions
- KYC/AML required

DeFi:

- Smart contracts replace intermediaries
- Permissionless access (anyone with wallet)
- Self-custody
- 24/7 global access
- Pseudonymous (no KYC)





Core Building Blocks:

- **Asset Layer:** Tokens (ERC-20, stablecoins)
- **Protocol Layer:** Lending, DEXs, derivatives
- **Application Layer:** Aggregators, wallets, dashboards
- **Composability:** “Money Legos” – protocols interact seamlessly

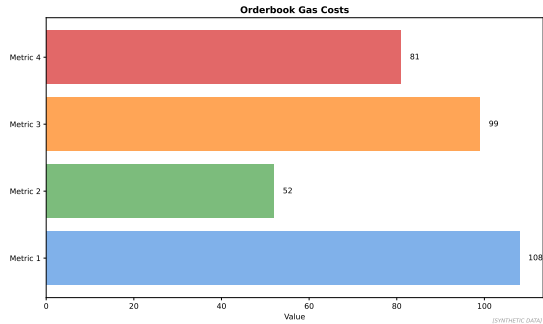
Decentralized Exchanges (DEXs): The Problem

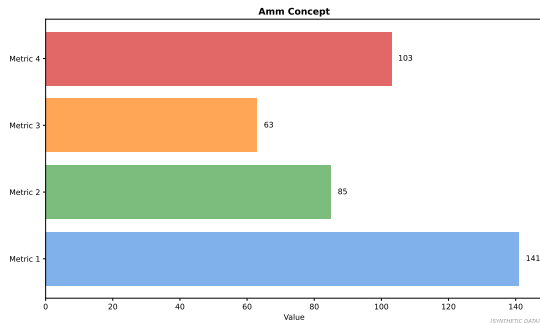
Centralized Exchanges (CEXs):

- Order book model
- Custodial (exchange holds funds)
- Counterparty risk (FTX collapse)
- KYC requirements
- Single point of failure

Challenges for DEX:

- On-chain order book too expensive
- Liquidity fragmentation
- Constant price updates





Key Idea:

- Liquidity pools replace order books
- Algorithmic pricing via bonding curve
- Anyone can provide liquidity (LP)
- Passive market making

Constant Product Formula: $x \times y = k$

Uniswap V2 Model:

$$x \times y = k$$

where x = reserve of token A, y = reserve of token B, k = constant

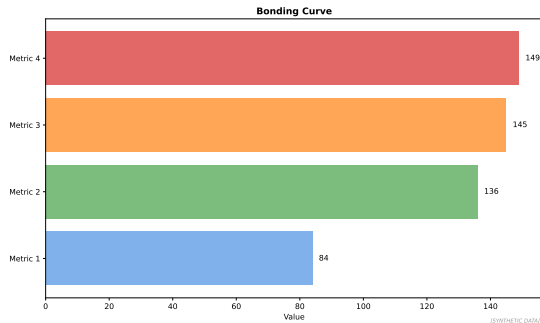
Example: ETH/USDC pool with 100 ETH and 200,000 USDC

$$k = 100 \times 200,000 = 20,000,000$$

Trade: Buy 10 ETH

- New ETH reserve: $x' = 100 - 10 = 90$
- New USDC reserve: $y' = k/x' = 20,000,000/90 = 222,222$
- USDC paid: $222,222 - 200,000 = 22,222$ (effective price $\sim \$2,222/\text{ETH}$)

AMM Bonding Curve Visualization



Properties:

- Price = slope of curve at current point: $P = y/x$
- Larger trades move price more (slippage)
- Infinite liquidity (asymptotic, but expensive for large trades)
- No order book needed

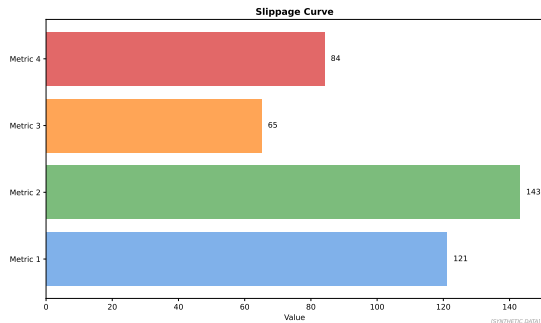
Price Impact and Slippage

Price Impact:

- How much your trade moves the price
- Larger trade → worse price
- Function of trade size relative to pool depth

Slippage:

- Difference between expected and executed price
- Set slippage tolerance (e.g., 0.5%)
- Trade reverts if exceeded



Formula: Price impact $\approx \Delta x / (x + \Delta x)$

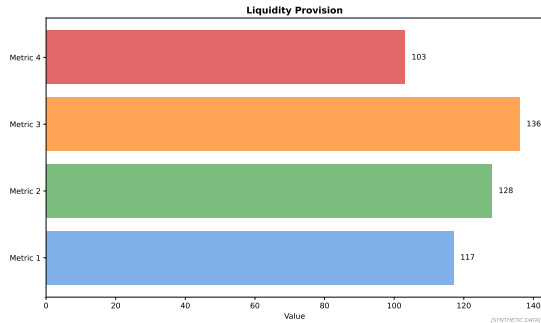
Liquidity Providers: Earning Fees

How it Works:

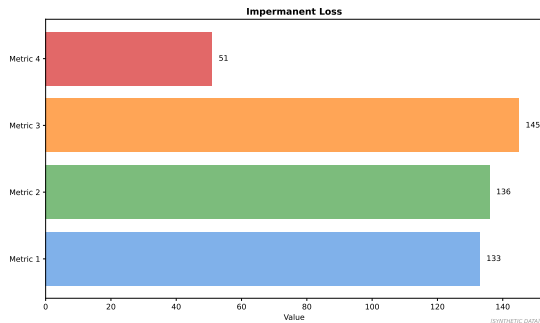
- 1 Deposit equal value of both tokens
- 2 Receive LP tokens (claim on pool share)
- 3 Earn 0.3% of all trades (Uniswap V2)
- 4 Withdraw anytime (burn LP tokens)

Example:

- Pool: 1,000 ETH + 2M USDC
- You deposit: 10 ETH + 20K USDC (1%)
- Daily volume: 500K USDC
- Your daily fees: $500,000 \times 0.003 \times 0.01 = \15



Impermanent Loss: The Hidden Cost



Definition: Loss compared to holding tokens vs providing liquidity

Example:

- Deposit 1 ETH (\$2000) + 2000 USDC when ETH = \$2000
- ETH rises to \$3000
- Pool rebalances: 0.816 ETH + 2449 USDC = \$4449 total
- Holding: 1 ETH + 2000 USDC = \$5000
- Impermanent loss: \$551 (11%)

Impermanent Loss Formula

Exact Formula:

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

where r = price ratio change (final price / initial price)

Price Change	Ratio (r)	Impermanent Loss
+25%	1.25	-0.6%
+50%	1.5	-2.0%
+100% (2x)	2.0	-5.7%
+400% (5x)	5.0	-25.5%
-50%	0.5	-5.7%

Mitigation: Fees earned over time can offset IL (especially in high-volume pairs)

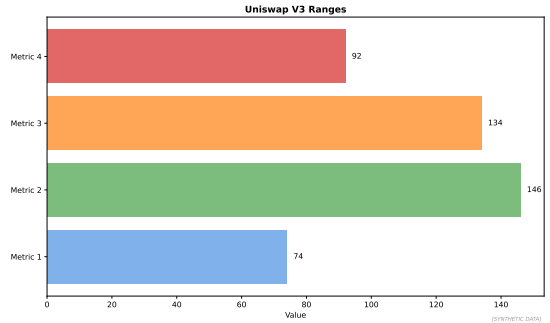
Uniswap V3: Concentrated Liquidity

V2 Limitation:

- Liquidity spread across entire price range
- Capital inefficient
- Most liquidity never used

V3 Innovation:

- Concentrated liquidity in price ranges
- LPs choose custom ranges
- Up to 4000x capital efficiency
- Active management required



Lending Protocol Architecture



[SYNTHETIC DATA]

Mechanism:

- **Lenders:** Deposit assets, earn interest (aTokens/cTokens)
- **Borrowers:** Post collateral, borrow assets, pay interest
- **Interest Rates:** Algorithmically determined by utilization
- **Liquidation:** If collateral drops below threshold, liquidators repay loan, seize collateral at discount

Over-Collateralization Requirement

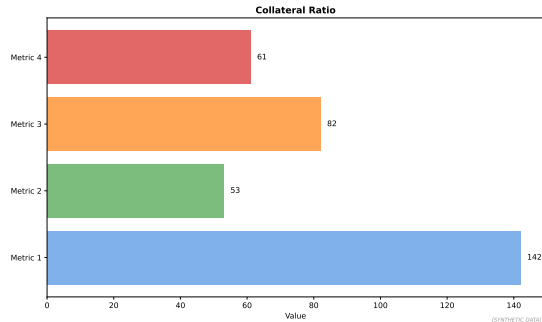
Why Over-Collateralize?

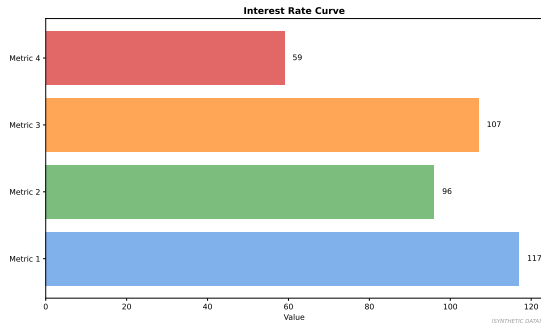
- No credit checks (permissionless)
- Price volatility protection
- Liquidation buffer

Example (Aave):

- Deposit: 10 ETH (\$20K)
- Max LTV: 80%
- Borrow: 16K USDC
- Liquidation threshold: 85%

Risk: If ETH drops >15%, position liquidated





Utilization Rate:

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

Interest Rates:

- Low utilization: Low rates (encourage borrowing)
- High utilization: High rates (incentivize deposits, discourage borrowing)
- Kinked model: Sharp increase near optimal utilization (e.g., 80%)

Flash Loans: Zero-Collateral Instant Loans

Concept:

- Borrow any amount
- No collateral required
- Must repay within same transaction
- If not repaid, entire transaction reverts

Use Cases:

- Arbitrage (exploit price differences)
- Collateral swaps
- Liquidations
- Refinancing

Flash Loan Flow



[SYNTHETIC DATA]

Scenario: Exploit Price Oracle Manipulation (2020, bZx attack)

- 1 Flash loan 10,000 ETH from dYdX
- 2 Swap 5,000 ETH for WBTC on Uniswap (moves price)
- 3 Use manipulated WBTC price to borrow over-collateralized assets on bZx
- 4 Repay flash loan, keep profit
- 5 Exploit: \$350K profit

Defense:

- Time-weighted average price (TWAP) oracles
- Multiple oracle sources (Chainlink)
- Borrow caps

Note: Flash loans are not inherently bad, but enable rapid exploitation of vulnerabilities

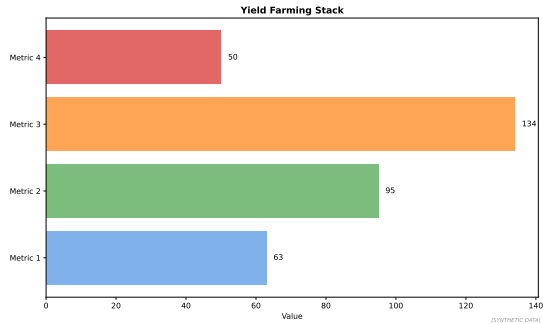
Yield Farming: Chasing Returns

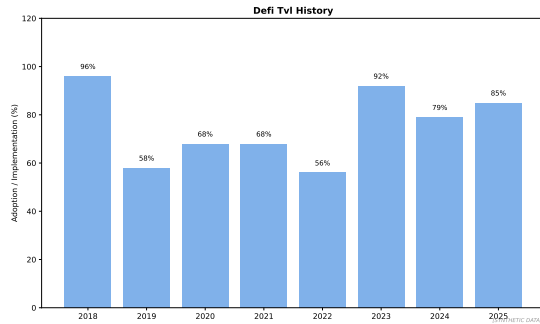
Strategy:

- Provide liquidity or lend assets
- Earn fees + protocol token rewards
- Compound yields (reinvest)
- Move capital to highest APY

Yield Sources:

- Trading fees (0.3% on Uniswap)
- Borrow interest (Aave, Compound)
- Token incentives (governance tokens)
- Staking rewards





Catalyst: Compound launches COMP token distribution (June 2020)

Result:

- Total Value Locked (TVL): \$1B → \$100B+ (2021 peak)
- APYs: 100–1000%+ (unsustainable, token inflation)
- Copycat protocols, “DeFi Degen” culture

- **Smart Contract Risk:** Bugs, exploits (e.g., The DAO, bZx)
- **Impermanent Loss:** Price divergence reduces LP returns
- **Oracle Manipulation:** Flash loan attacks on price feeds
- **Liquidation Risk:** Volatile collateral leads to forced sales
- **Rug Pulls:** Developers drain liquidity (unaudited projects)
- **Regulatory Risk:** Securities classification, AML/KYC future requirements
- **Composability Risk:** Cascading failures (one protocol exploited affects others)

Mitigation: Use audited protocols, diversify, understand risks, start small

Aspect	DeFi	CeFi
Custody	Self-custody (your keys)	Custodial (exchange holds)
Access	Permissionless (anyone)	KYC/AML required
Transparency	Open-source, on-chain	Opaque (trust exchange)
Execution	Slower (block time), higher fees	Instant, low fees
Risk	Smart contract risk	Counterparty risk (FTX)
Liquidity	Fragmented across DEXs	Concentrated on CEX

- **DeFi:** Permissionless financial services via smart contracts
- **AMMs:** Constant product formula ($x \times y = k$), liquidity pools replace order books
- **Impermanent Loss:** LPs lose vs holding when prices diverge
- **Lending:** Over-collateralized loans, algorithmic interest rates, liquidations
- **Flash Loans:** Uncollateralized loans repaid in same transaction
- **Risks:** Smart contract bugs, IL, oracle manipulation, liquidations

Next Lesson: Stablecoins and Terra/Luna collapse case study