DeFi Fundamentals: A Quantitative Deep Dive

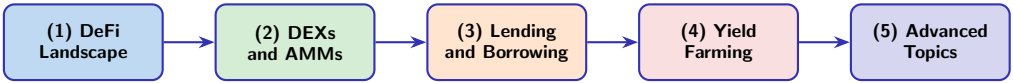
Standalone Technical Lecture

Prof. Dr. Joerg Osterrieder

University Lecture Series

March 5, 2026

Lecture Roadmap



Learning Objectives

- Understand the DeFi ecosystem and its architecture
- Analyse Automated Market Maker (AMM) mathematics
- Model lending protocols and interest rate curves
- Quantify yield farming returns and impermanent loss
- Evaluate risks: smart contract, oracle, economic

Prerequisites

- Lessons 1–4: Blockchain, Ethereum, ERC-20, smart contracts
- Basic calculus and algebra
- Familiarity with Solidity interfaces
- Understanding of token standards and gas

Durat

90 minutes — 5 sections — ˜55 frames — Prerequisite: Lessons 1–4

Table of Contents

Navig

through 5 sections covering DeFi landscape to advanced topics

Learning Objectives

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

1. **Explain** the DeFi stack and how composability enables "money legos"
2. **Calculate** AMM prices, slippage, and impermanent loss using the constant product formula
3. **Analyze** lending protocol mechanics (collateralization ratios, liquidation, health factors)
4. **Compare** yield farming strategies and distinguish real yield from token emissions
5. **Evaluate** DeFi security risks including flash loan attacks and MEV extraction

Bloom

taxonomy levels: Remember → Understand → Apply → Analyze → Evaluate → Create

Section 1: DeFi Landscape

Defining DeFi, its ecosystem, metrics, and risks

What you will learn

- Definition and properties of DeFi
- CeFi vs. DeFi architecture comparison
- Major protocol categories and their roles
- Key metrics: TVL, APY, utilisation rate

Frames in this section

- Frame 5 – What is DeFi?
- Frame 6 – CeFi vs. DeFi comparison
- Frame 7 – DeFi ecosystem map
- Frames 8–14 – Metrics, growth, risks

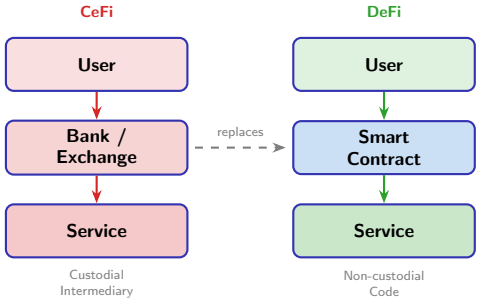
What is Decentralized Finance?

Definition

DeFi (Decentralized Finance) refers to financial services and applications built on public blockchains — primarily Ethereum — that operate without centralised intermediaries such as banks, brokers, or exchanges.

Core Properties

- **Permissionless** – anyone with a wallet can participate
- **Trustless** – rules enforced by code, not institutions
- **Transparent** – all logic and state on-chain, auditable
- **Non-custodial** – users retain control of private keys
- **Composable** – protocols interoperate like "money legos"



DeFi

operates on public blockchains using smart contracts to replace traditional financial intermediaries

CeFi vs. DeFi: A Structural Comparison

Centralised Finance (CeFi)

- × **Custody risk** – exchange holds your assets
- × **KYC/AML required** – identity verification mandatory
- × **Business hours** – limited to operating times
- × **Geographic restrictions** – jurisdictional barriers
- × **Opaque** – internal risk not publicly visible
- × **Censorship** – accounts can be frozen
- × **Single point of failure** – operational risk

Decentralised Finance (DeFi)

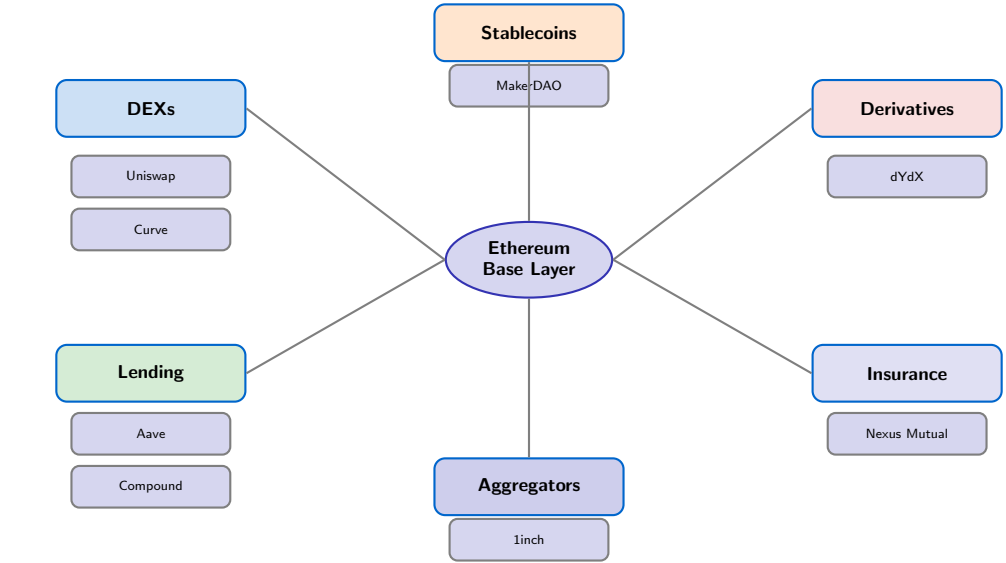
- ✓ **Self-custody** – you hold your keys
- ✓ **Permissionless** – no identity required
- ✓ **24/7 operation** – always accessible
- ✓ **Global access** – no geographic limits
- ✓ **Transparent** – all logic on-chain, auditable
- ✓ **Censorship-resistant** – no authority to freeze
- ✓ **Composable** – interoperable protocols

Analogy

CeFi is like a traditional bank vault — secure but gated. DeFi is like a vending machine — rules are mechanical, visible, and execute automatically without a cashier.

DeFi trades counterparty risk for smart contract risk; neither model is universally superior

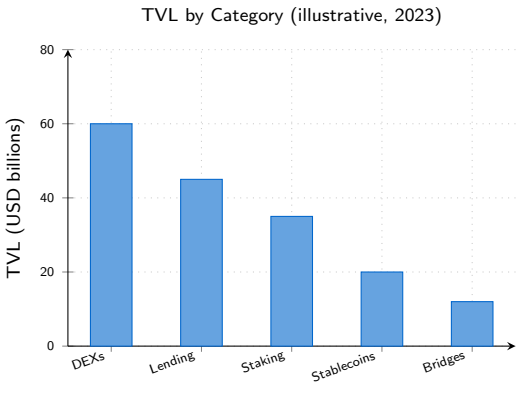
DeFi Ecosystem Map



Ether

hosts the largest DeFi ecosystem; most protocols interact via standardised token interfaces

Total Value Locked (TVL): The DeFi Thermometer



TVL Definition

$$\mathrm{TVL} = \sum_{i=1}^{N} q_i \cdot p_i$$

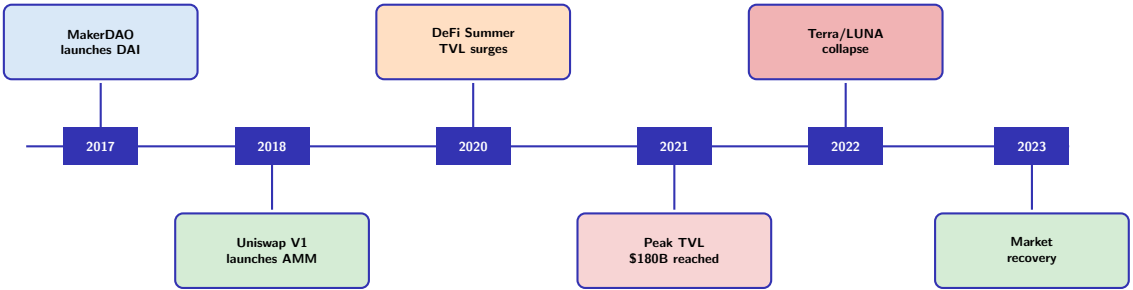
where q_i is quantity of asset i locked in protocol contracts and p_i its USD price.

Limitations of TVL

- **Double-counting**: same capital deposited in multiple layers
- **Price volatility**: TVL changes with asset prices, not just flows
- **Recursive leverage**: borrowed assets re-deposited inflate TVL
- **Not revenue**: high TVL $\neq$ high protocol earnings

TVL is the most widely cited DeFi metric but must be interpreted alongside volume, fees, and protocol revenue

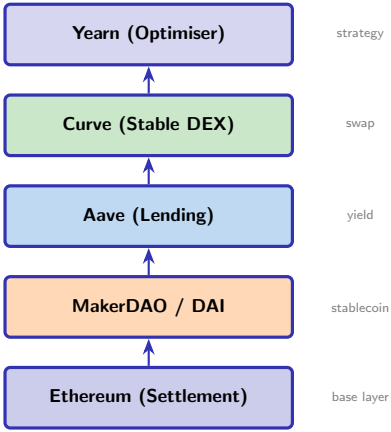
DeFi Growth Timeline



DeFi

grew from a single stablecoin protocol in 2017 to a multi-hundred-billion-dollar ecosystem by 2021

Composability: Money Legos



What is Composability?

DeFi protocols expose standardised interfaces (ERC-20, ERC-4626) that allow any protocol to build on top of another without permission. One transaction can:

1. Borrow DAI from Aave
2. Swap DAI for USDC on Curve
3. Deposit USDC into Yearn vault
4. Receive yield-bearing tokens

— all atomically, in a single call.

Systemic Risk

Composability also propagates failures: a bug in one protocol can cascade through all protocols that depend on it — analogous to a shared library vulnerability.

Comp

is DeFi's greatest strength and its most significant systemic risk vector

Key DeFi Metrics

Metric	Definition	Typical Range	Significance
TVL	$\sum q_i \cdot p_i$ locked in contracts	\$1M – \$50B+	Protocol size and user trust
APY	$(1 + r/n)^n - 1$, n = compound freq.	0% – 10,000%+	Return on deposited capital
Utilisation U	U = Borrowed / Supplied	0% – 100%	Drives interest rates in lending
Collateral Ratio	$CR = V_{\text{collateral}} / V_{\text{debt}}$	110% – 300%	Safety buffer before liquidation
24h Volume	Total swap notional per day	\$1M – \$5B+	Protocol activity and fee revenue

Metri

should be evaluated together; a high APY with low TVL and high utilisation may signal unsustainable incentives

DeFi Risks Overview

Technical Risks

- **Smart contract bugs** – reentrancy, overflow, access control
- **Oracle manipulation** – price feed attacks, flash loan exploits
- **Bridge vulnerabilities** – cross-chain message forgery
- **MEV / front-running** – sandwich attacks on AMM trades
- **Upgradeability risk** – admin key compromise, proxy hijacking

Economic Risks

- **Impermanent loss** – AMM LPs lose vs. holding during volatility
- **Liquidation cascades** – falling prices trigger mass liquidations
- **Stablecoin depeg** – collateral or peg mechanism failure
- **Governance attacks** – token accumulation to pass malicious proposals
- **Unsustainable yields** – token emission Ponzis, yield collapse

Warning: DeFi is Experimental Software

Over $5 billion has been lost to DeFi exploits since 2020. Users must conduct independent risk assessment before interacting with any protocol, regardless of audit status or TVL.

Risk

management in DeFi requires simultaneous assessment of technical, economic, and governance dimensions

Major DeFi Hacks: A Security Retrospective

Protocol	Year	Loss	Attack Vector	Lesson Learned
The DAO	2016	$60M	Reentrancy attack	Checks-effects-interactions
Poly Network	2021	$611M	Cross-chain auth flaw	Verify caller at all layers
Ronin Bridge	2022	$625M	Validator key compromise	Decentralise validator sets
Euler Finance	2023	$197M	Flash loan + liquidation	Audit donate() interactions

Note: Ronin Bridge funds were partially returned; Euler attacker returned most funds.

The largest hacks exploited logic flaws, not brute-force cryptography; audits reduce but do not eliminate risk

Section 1 Summary: DeFi Landscape

Key Takeaways

- **DeFi** replaces intermediaries with smart contracts, enabling permissionless, transparent, and composable financial services
- **TVL, APY, and utilisation rate** are the primary metrics — each with important caveats and limitations
- **Composability** ("money legos") unlocks novel financial primitives but introduces systemic contagion risk
- **Technical and economic risks** are both significant; over $5B lost to exploits since 2020
- **DeFi growth** from MakerDAO (2017) to $180B TVL peak (2021) demonstrated product-market fit despite volatility

Formulas to Remember

$$\text{TVL} = \sum_i q_i \cdot p_i$$

$$\text{APY} = \left(1 + \frac{r}{n}\right)^n - 1$$

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

$$CR = \frac{V_{\text{collateral}}}{V_{\text{debt}}} \geq CR_{\min}$$

Coming Up: Section 2

DEXs and Automated Market Makers — the mathematical engine behind decentralised trading.

Secti

1 complete — Next: Section 2 — DEXs and AMMs — Frames 15 onward

Section 2: DEXs and Automated Market Makers

Constant product formula, price impact, slippage, LP mechanics, and impermanent loss

What you will learn

- Order books vs. AMM pool architecture
- Constant product formula $x \cdot y = k$ and its geometry
- Price impact, slippage, and execution cost
- Liquidity provision mechanics and fee accrual
- Impermanent loss derivation and mitigation

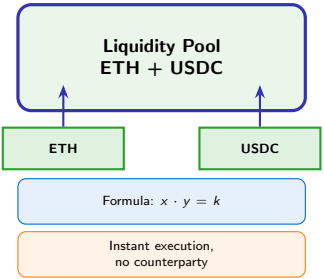
Frames in this section

- Frame 16 – Order Books vs. AMMs
- Frame 17 – The Constant Product Formula
- Frames 18–19 – Worked example, price impact
- Frames 20–21 – Slippage, LP mechanics
- Frames 22–26 – Uniswap V3, AMM models, IL, aggregators

Order Books vs. AMMs

Order Book (CeFi/CEX)

AMM Pool (DeFi/DEX)



Property	Order Book	AMM
Price discovery	Bid/ask matching	Formula-determined
Liquidity	Maker orders	Pooled reserves
Execution speed	Depends on liquidity	Instant
Counterparty	Another trader	The pool contract
Capital eff.	High (concentrated)	Low (full range)

AMM replace discrete order matching with a continuous pricing function: liquidity providers replace market makers

The Constant Product Formula

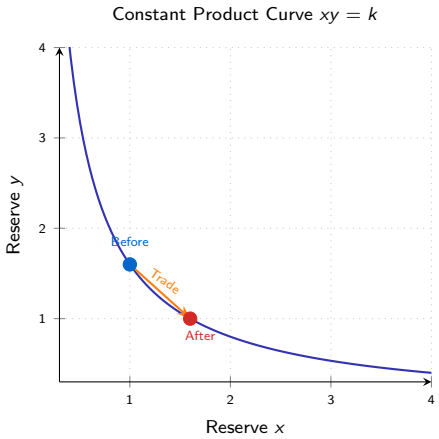
Core Invariant

$$x \cdot y = k$$

where x = reserve of token X, y = reserve of token Y, k = constant (invariant).

Step-by-Step Derivation

1. Initial state: $x_0 \cdot y_0 = k$
2. Trader sends Δx of token X to pool
3. New reserve: $x_1 = x_0 + \Delta x$
4. Invariant must hold: $x_1 \cdot y_1 = k$
5. Amount out: $\Delta y = y_0 - \dfrac{k}{x_0 + \Delta x}$
6. Marginal price: $P = \dfrac{y_0}{x_0}$ (before trade)
7. Effective price: $P_{\text{eff}} = \dfrac{\Delta y}{\Delta x}$



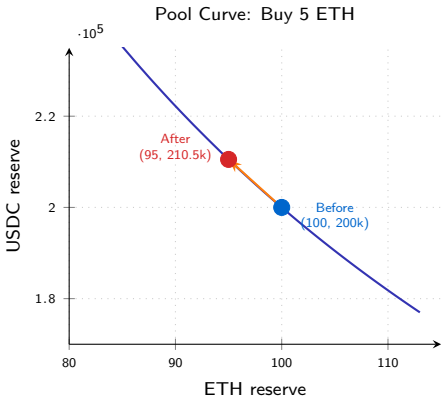
Constant Product: Worked Example

Scenario: Buy 5 ETH from Pool

1. **Initial pool**: 100 ETH + 200,000 USDC
2. **Invariant**: $k = 100 \times 200{,}000 = 20{,}000{,}000$
3. **Buy 5 ETH**: new ETH reserve $= 100 - 5 = 95$
4. **New USDC reserve**:

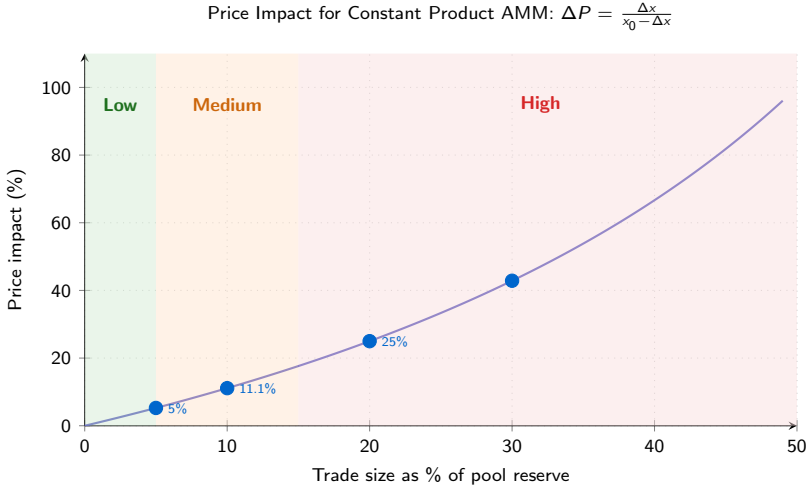
$$y_1 = \frac{k}{x_1} = \frac{20{,}000{,}000}{95} \approx 210{,}526.32$$

5. **USDC cost**: $210{,}526.32 - 200{,}000 = \mathbf{10{,}526.32}$
6. **Effective price**: $10{,}526.32/5 = \mathbf{\$2{,}105.26}$
7. **Spot price before**: $200{,}000/100 = \$2{,}000.00$
8. **Price impact**: $(2105.26 - 2000)/2000 = \mathbf{5.26\%}$



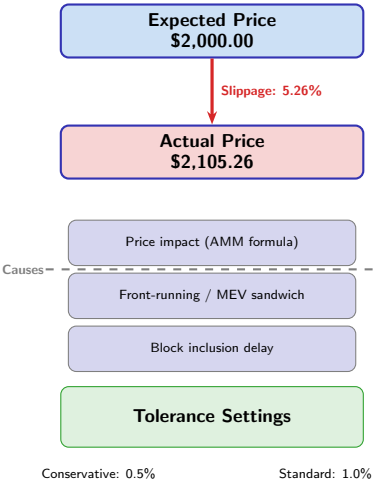
Price impact of 5.26% arises from buying 5% of the ETH reserve; larger trades relative to pool size incur more slippage

Price Impact vs. Trade Size



Price impact grows super-linearly; trades >15% of pool reserves are economically inadvisable without aggregation

Slippage: Expected vs. Actual Price



Slippage Definition

Slippage is the difference between the price quoted at trade initiation and the price at which the trade actually executes on-chain.

$$\text{Slippage} = \frac{P_{\text{actual}} - P_{\text{expected}}}{P_{\text{expected}}} \times 100\%$$

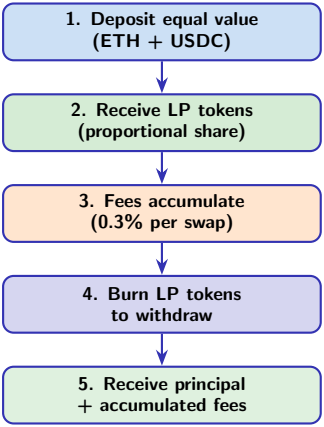
Slippage Tolerance

DEX interfaces let users set a **slippage tolerance**. If actual slippage exceeds the threshold, the transaction reverts.

- Too low (0.1%) $\rightarrow$ frequent reverts in volatile markets
- Too high (5%) $\rightarrow$ vulnerability to sandwich attacks
- Typical default: 0.5%–1%

tolerance protects users but creates a revert risk; MEV bots exploit high-tolerance transactions via sandwich attacks

Liquidity Provider (LP) Mechanics



LP Share Mathematics

When depositing $(\Delta x, \Delta y)$ into a pool with reserves (x, y) and total LP supply S:

$$\text{LP tokens received} = S \cdot \frac{\Delta x}{x} = S \cdot \frac{\Delta y}{y}$$

(Both ratios must be equal to maintain the price.)

Fee Revenue

$$r_{\text{LP}} = \frac{\text{LP share} \times \text{fee} \times \text{volume}}{\text{Total liquidity}}$$

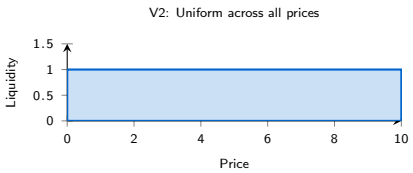
Uniswap V2: fee $= 0.3\%$ of each swap. Fees increase k, benefiting all LPs proportionally.

Risk

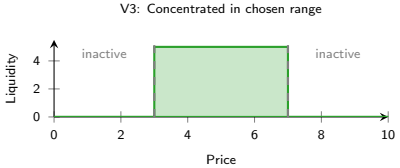
LPs face **impermanent loss** when prices diverge from

Uniswap V2 vs. V3: Concentrated Liquidity

V2: Full-Range Liquidity



V3: Concentrated Liquidity




```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

// Uniswap V3: Concentrated Liquidity
struct Position {
    uint128 liquidity;
    int24 tickLower;  // Price range start
    int24 tickUpper;  // Price range end
}

// V2: liquidity spread 0 to infinity
// V3: liquidity in [tickLower, tickUpper]
// Result: up to 4000x capital efficiency
```

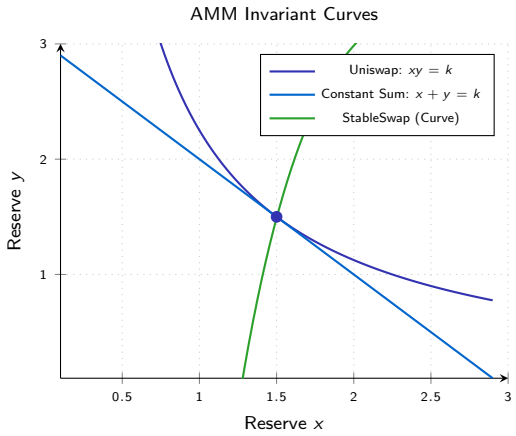
V2 vs. V3 Key Differences

	V2	V3
Range	$[0, \infty)$	$[a, b]$ chosen
Efficiency	$1\times$	up to $4000\times$
Fee tiers	0.3%	0.05/0.3/1%
IL risk	Lower	Higher (in range)

V3

concentrated liquidity dramatically improves capital efficiency but requires active management of price ranges

Other AMM Models



Constant Product (Uniswap)

$x \cdot y = k$ — Hyperbola. Works for any token pair. Price adjusts continuously.

Constant Sum

$x + y = k$ — Straight line. Zero price impact but **pool drainable**: arbitrageurs empty one side entirely.

StableSwap (Curve)

Hybrid between constant sum and constant product:

$$A(x + y) + xy = A \cdot D + \left(\frac{D}{2}\right)^2$$

Near-zero slippage near the peg; reverts to

Impermanent Loss: Derivation and Magnitude

IL Derivation

Let $r = P_1/P_0$ be the price ratio (current vs. entry).

Value of LP position after price change (per unit of initial capital):

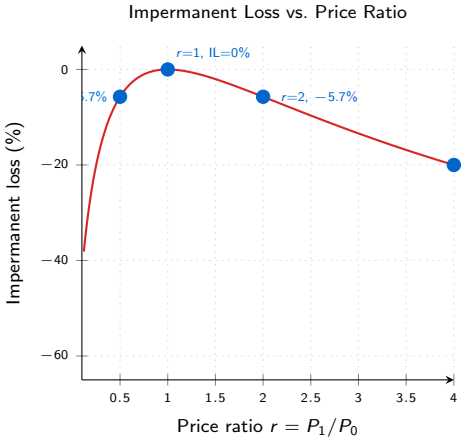
$$V_{\text{LP}} = 2\sqrt{r}$$

Value if simply held (50/50 split):

$$V_{\text{HODL}} = 1 + r$$

Impermanent Loss:

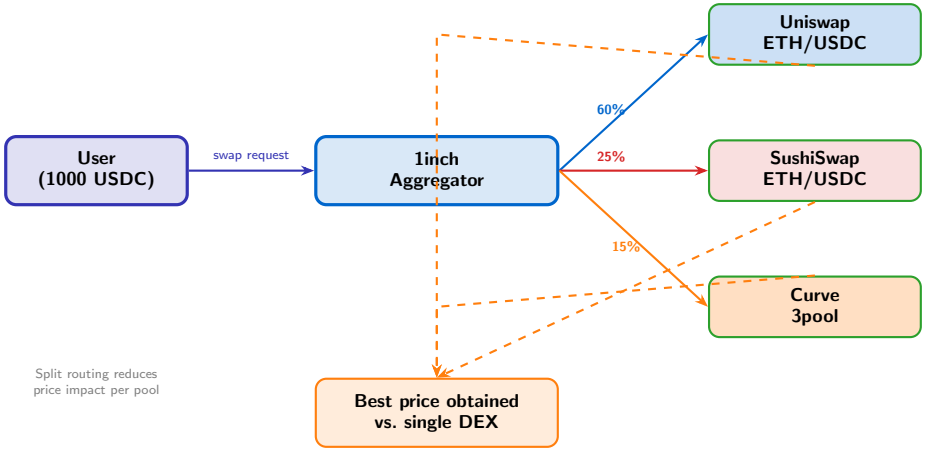
$$\boxed{IL(r) = \frac{2\sqrt{r}}{1+r} - 1}$$



Key Values

Price ratio r	IL	Example
1.0	0.00%	No change

DEX Aggregators: Optimal Order Routing



Aggr

like 1inch, Paraswap, and CoW Protocol split orders across multiple pools to minimise total price impact

Section 2 Summary: DEXs and AMMs

Key Takeaways

1. **AMMs replace order books** with pooled reserves and a mathematical invariant, enabling instant, permissionless trades against the pool
2. **Constant product** $x \cdot y = k$ sets price via reserve ratio; every trade moves along the hyperbola, causing price impact
3. **Price impact scales super-linearly** with trade size relative to pool depth; aggregators mitigate this by splitting routes
4. **Liquidity providers** earn fees proportional to their share but face impermanent loss when prices diverge from entry
5. **V3 concentrated liquidity** multiplies capital efficiency up to 4000× but requires active range management

Formulas to Remember

$$x \cdot y = k \quad \text{(constant product)}$$

$$\Delta y = y_0 - \frac{k}{x_0 + \Delta x} \quad \text{(amount out)}$$

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

$$\text{LP share} = S \cdot \frac{\Delta x}{x} \quad \text{(LP tokens)}$$

Coming Up: Section 3

Lending and Borrowing — interest rate curves, collateral mechanics, and liquidation mathematics on Aave and Compound.

Secti

2 complete — Next: Section 3 — Lending and Borrowing — Frames 27 onward

Section 3: Lending and Borrowing

Collateralisation, interest rate models, liquidation mechanics, and protocol architecture

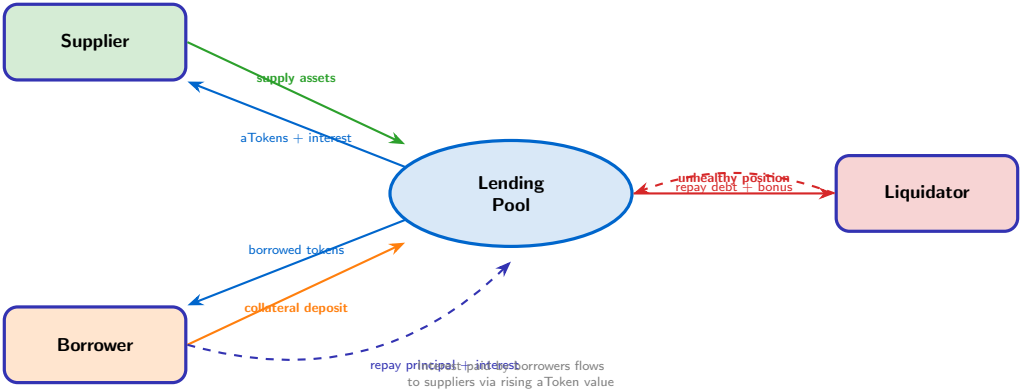
What you will learn

- How DeFi lending pools work end-to-end
- Collateralisation ratios and loan-to-value limits
- Kinked interest rate models and utilisation-driven pricing
- Health factor computation and liquidation triggers
- Aave vs. Compound architecture differences

Frames in this section

- Frame 28 – How DeFi Lending Works
- Frame 29 – Collateralisation Ratios
- Frames 30–31 – Interest Rate Models
- Frames 32–33 – Liquidation Mechanics, Health Factor
- Frames 34–38 – Protocol Architecture, Stablecoins, Summary

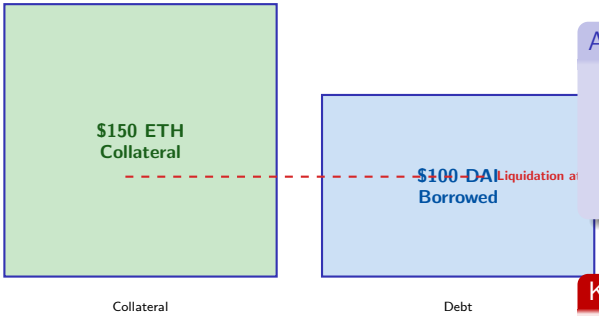
How DeFi Lending Works



Lendi

pools intermediary-free: suppliers earn yield while borrowers access liquidity against locked collateral

Collateralisation Ratios



Aave V3 Risk Parameters (illustrative)

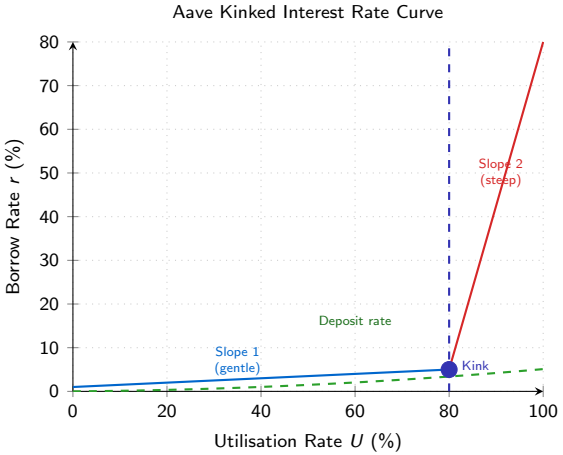
Asset	Max LTV	Liq. Threshold	Liq. Penalty
ETH	80.0%	82.5%	5.0%
WBTC	70.0%	75.0%	6.25%
USDC	77.0%	80.0%	4.5%
DAI	77.0%	80.0%	4.5%
LINK	65.0%	70.0%	7.5%

Key Insight

The **liquidation threshold** is always above the **max LTV**, giving a safety buffer. A borrower depositing \$100 of ETH can borrow at most \$80 (80% LTV) but faces liquidation only if the position degrades past the 82.5% threshold.

$$CR = \frac{V_{\text{collateral}}}{V_{\text{debt}}} \qquad \text{LTV} = \frac{V_{\text{debt}}}{V_{\text{collateral}}}$$

Over-collateralisation is the primary solvency mechanism in DeFi lending; there is no recourse for undercollateralised default



Kinked Rate Rationale

The two-slope model achieves three goals simultaneously:

1. **Low rates at low utilisation** attract borrowers and grow the market
2. **Moderate rates near optimal** balance supply and demand efficiently
3. **Steep rates above optimal** act as an automatic brake, incentivising repayment and new deposits before liquidity is exhausted

Rate Parameters (Aave style)

Parameter	Value
Base rate	1%
Optimal util. U^*	80%
Slope 1 (below U^*)	4%
Slope 2 (above U^*)	75%

Interest Rate Formula: Mathematics

Piecewise Rate Function

Let U = utilisation rate, U^* = optimal utilisation.

$$r_{\text{borrow}}(U) = \begin{cases} r_{\text{base}} + \dfrac{U}{U^*} \cdot s_1 & \text{if } U \le U^* \\ r_{\text{base}} + s_1 + \dfrac{U - U^*}{1 - U^*} \cdot s_2 & \text{if } U > U^* \end{cases}$$

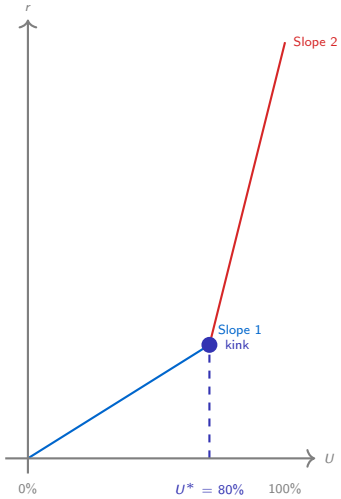
where s_1 = slope 1, s_2 = slope 2.

Deposit Rate

$$r_{\text{deposit}} = r_{\text{borrow}} \cdot U \cdot (1 - \text{reserveFactor})$$

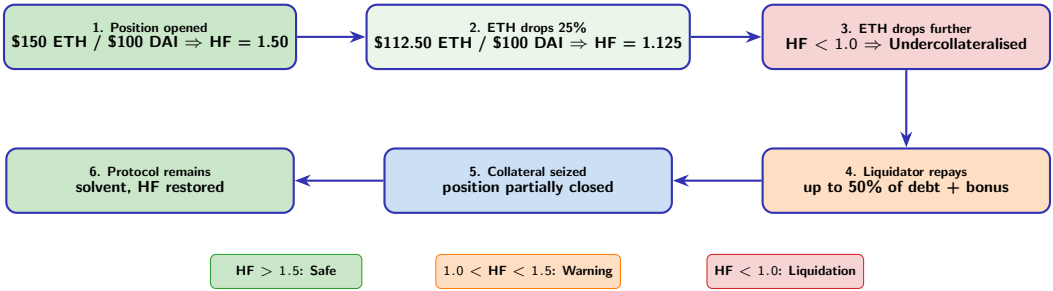
The reserve factor (e.g., 10%) accrues to the protocol treasury.

Worked Example ($U = 60\%$)



Below U^*:
base + linear

Liquidation Mechanics



Liqui

are permissionless: any wallet can repay a borrower's debt and claim collateral at a discount; this incentivises rapid execution

Health Factor: Deep Dive

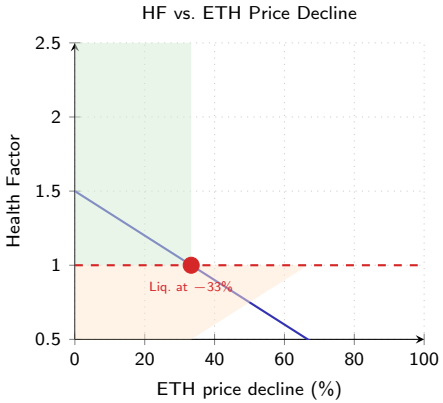
Health Factor Formula

$$HF = \frac{\sum_i V_{c,i} \cdot LT_i}{V_{\text{debt,total}}}$$

where $V_{c,i}$ is the USD value of collateral asset i and LT_i is its liquidation threshold. Liquidation is triggered when $HF < 1$.

Multi-Asset Example

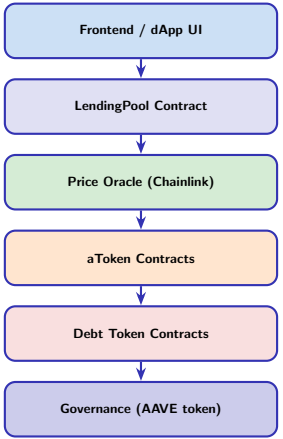
Asset	Value	LT	Weighted
ETH	\$1,000	82.5%	\$825.00
WBTC	\$500	75.0%	\$375.00
Total weighted collateral			\$1,200.00
Total debt (DAI)			\$800.00
Health Factor			**1.50**



Healt

factor aggregates multiple collateral assets with asset-specific thresholds; monitoring HF is essential for active borrowers

Aave Protocol Architecture




```solidity
// Simplified Aave Lending Pool
interface ILendingPool {
    // Supply assets to earn interest
    function supply(
        address asset,
        uint256 amount,
        address onBehalfOf
    ) external;

    // Borrow against collateral
    function borrow(
        address asset,
        uint256 amount,
        uint256 interestRateMode  // 1=stable, 2=variable
    ) external;
}
```

aToken Mechanics

When you supply 100 DAI, you receive 100 aDAI. The aDAI balance increases every block as interest accrues. Redeeming 1 aDAI always yields ≥ 1 DAI.

Aave

modular architecture separates concerns: core pool logic, oracle pricing, yield tokens, and governance are independent contracts

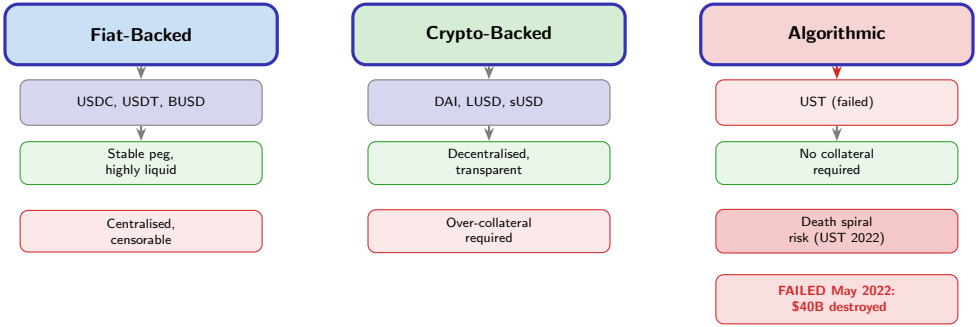
Compound vs. Aave: Protocol Comparison

Feature	Compound	Aave
Governance token	COMP	AAVE
Rate model	Kinked (per market)	Kinked + stable rate
Multi-chain	Ethereum + limited	8+ chains (Portal)
Flash loans	No (native)	Yes (0.09% fee)
Yield token	cToken (exchange rate)	aToken (rebasing)
Liquidation cap	50% of position	50% (default)

Comp

pioneered DeFi lending in 2018; Aave extended the model with stable rates, flash loans, and multi-chain support

Stablecoins in DeFi

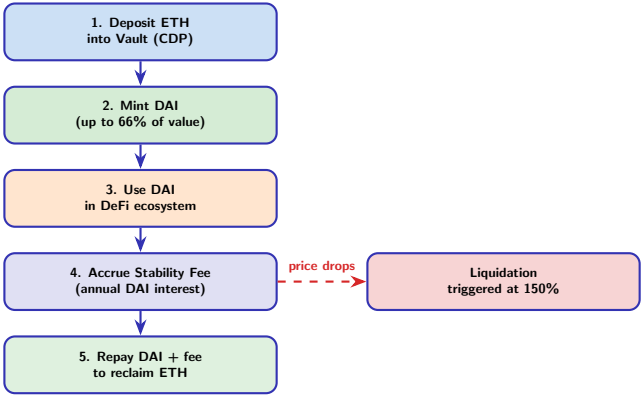


Stablecoins are the primary collateral and liquidity medium across all DeFi protocols

Stabl

choice involves a trust-decentralisation tradeoff; the 2022 Terra/LUNA collapse remains the largest algorithmic failure

MakerDAO and DAI: Crypto-Backed Stablecoin



Peg maintained via over-collateralisation + stability fee + DSR (DAI Savings Rate)

Key Parameters

Parameter	Value
Min collateral ratio	150%
Liquidation penalty	13%
Stability fee (APR)	0–10% (variable)
DAI Savings Rate	governance-set

Peg Stability Mechanisms

- **Over-collateralisation** ensures DAI is always backed
- **Stability fee** controls minting incentive (DAI supply)
- **DSR** controls holding incentive (DAI demand)
- **PSM** (Peg Stability Module) allows 1:1 USDC swap at zero fee

Section 3 Summary: Lending and Borrowing

Key Takeaways

1. **DeFi lending** is permissionless and overcollateralised: borrowers lock crypto collateral to access liquidity without credit checks
2. **Kinked interest rate models** dynamically price credit by utilisation rate, automatically incentivising liquidity at both extremes
3. **Liquidation** is the protocol's solvency backstop: unhealthy positions are closed by profit-seeking liquidators who repay debt and claim collateral at a discount
4. **Health factor** aggregates multi-asset collateral with asset-specific liquidation thresholds into a single solvency signal
5. **Stablecoins** — fiat-backed, crypto-backed, and algorithmic — each carry distinct trust assumptions and failure modes

Formulas to Remember

$$HF = \frac{\sum_i V_{c,i} \cdot LT_i}{V_{\text{debt,total}}}$$

$$r(U) = r_{\text{base}} + \frac{U}{U^*} s_1 \quad (U \leq U^*)$$

$$r(U) = r_{\text{base}} + s_1 + \frac{U - U^*}{1 - U^*} s_2 \quad (U > U^*)$$

$$CR = \frac{V_{\text{collateral}}}{V_{\text{debt}}} \geq CR_{\min}$$

Coming Up: Section 4

Yield Farming — liquidity mining, token emissions, APY calculation, and impermanent loss under incentivised pools.

Secti

3 complete — Next: Section 4 — Yield Farming — Frames 39 onward

Section 4: Yield Farming and Liquidity Mining

LP tokens, APR vs APY, impermanent loss, yield strategies, and real yield analysis

What you will learn

- What is yield farming?
- LP token mechanics
- APR vs APY calculations
- Impermanent loss in practice
- Yield farming strategies
- Real yield vs token emissions
- Yield aggregators (Yearn)

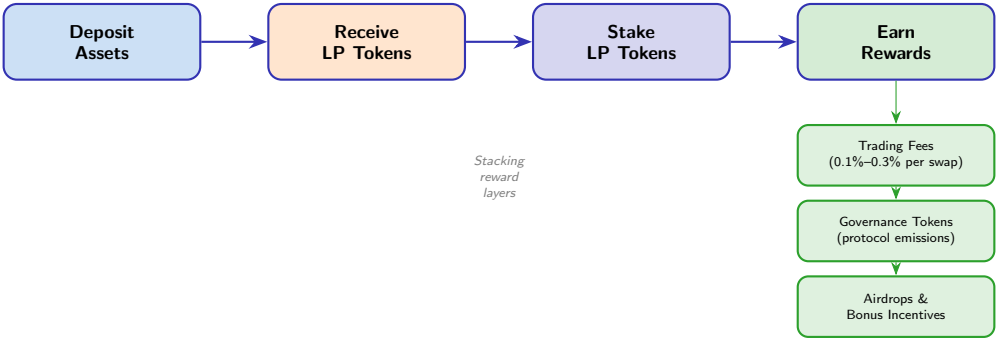
Frames in this section

- Frame 40 – What is Yield Farming?
- Frame 41 – LP Token Mechanics
- Frames 42–43 – APR vs APY, Compounding
- Frames 44–45 – Impermanent Loss, Strategies
- Frames 46–48 – Real Yield, Aggregators, Summary

Secti

4 of 5 — Yield Farming & Liquidity Mining — Frames 39–48

What is Yield Farming?

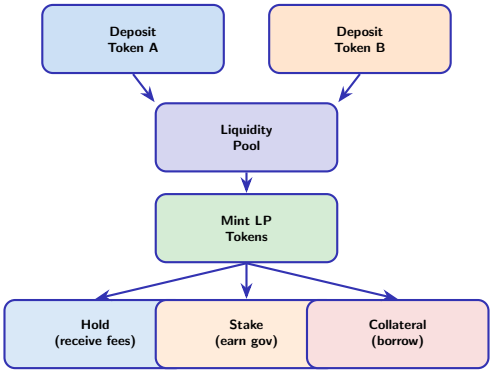


Definition

Yield farming is the practice of deploying crypto assets into DeFi protocols to generate returns from multiple stacked incentive layers simultaneously. Farmers optimise across protocols seeking the highest risk-adjusted yield.

Yield farming = deposit + stake + earn; rewards stack across fees, governance tokens, and airdrops

LP Token Mechanics



LP Token Formula

For a constant-product pool:

$$\text{LP}_{\text{minted}} = \sqrt{x \cdot y}$$

where x = amount of Token A deposited, y = amount of Token B deposited.

Redemption share:

$$\text{share} = \frac{\text{LP}_{\text{held}}}{\text{LP}_{\text{total}}}$$

You withdraw `share` $\times$ pool balance of each token.

Key Property

LP tokens are composable — they can be staked, used as collateral, or bridged, enabling nested yield strategies.

LP tokens represent proportional pool ownership; formula: $\sqrt{A \times B}$; composable across DeFi protocols

APR vs APY

Definitions

APR — Annual Percentage Rate (simple, no compounding):

$$\text{APR} = r \times n$$

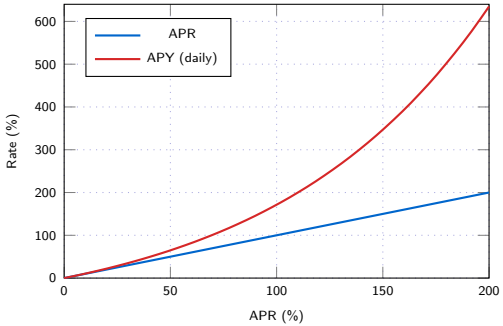
APY — Annual Percentage Yield (with compounding n times/year):

$$\text{APY} = \left(1 + \frac{\text{APR}}{n}\right)^n - 1$$

Example: 50% APR

- Weekly ($n = 52$): APY $= 64.5\%$
- Daily ($n = 365$): APY $= 64.8\%$
- Hourly ($n = 8760$): APY $= 64.87\%$
- Continuous: APY $= e^{0.5} - 1 = 64.87\%$

Gap grows dramatically at high APR.



Warning

DeFi protocols advertise APY, but token emissions may decline — actual returns are lower than headline figures suggest.

APY $= (1 + \text{APR}/n)^n - 1$; **divergence accelerates above 100% APR; always check emission schedules**

Impermanent Loss in Practice

Real Scenario

Initial deposit:

- 1 ETH at \$2,000 + 2,000 USDC
- Total value: \$4,000
- $k = 1 \times 2000 = 2000$

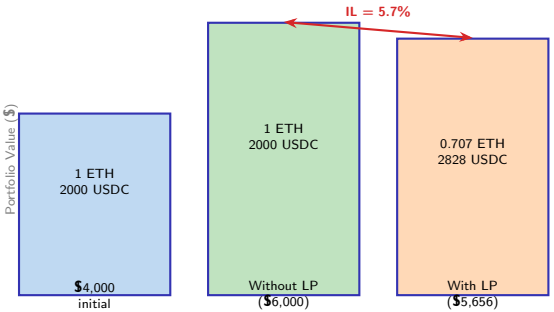
ETH price rises to \$4,000:

- New pool state: $\sqrt{2000/4000} \approx 0.707$ ETH, 2828 USDC
- Pool value: $0.707 \times 4000 + 2828 = \$5{,}656$
- *Without LP*: $1 \times 4000 + 2000 = \$6{,}000$

Impermanent Loss

$$\text{IL} = \frac{5656 - 6000}{6000} \approx -5.7\%$$

You hold *less* of the appreciating asset.



IL

formula: $\frac{2\sqrt{r}}{1+r} - 1$ **where** r **= price ratio; IL is temporary only if prices revert**

Impermanent Loss Table

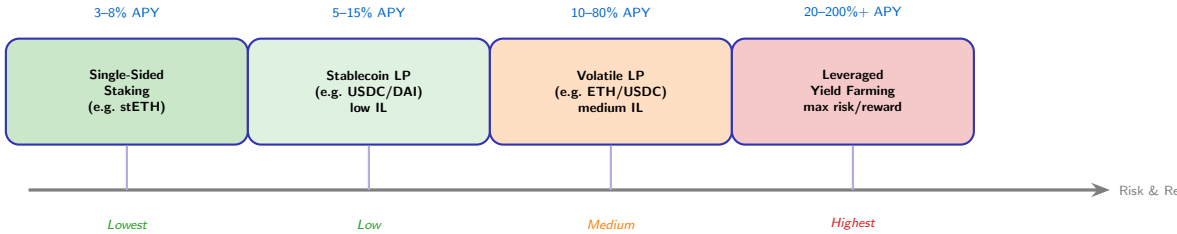
Price Change	IL (%)	Break-even Fees
1.25×	0.6%	Low
1.50×	2.0%	Moderate
2.00×	5.7%	Significant
3.00×	13.4%	High
5.00×	25.5%	Very High
10.00×	42.5%	Extreme

IL Formula

$$\text{IL}(r) = \frac{2\sqrt{r}}{1+r} - 1, \quad r = \frac{P_{\text{new}}}{P_{\text{initial}}}$$

IL is *permanent* if you withdraw when prices diverge; fees must exceed IL to be profitable.

Yield Farming Strategies



Strategy Selection Principle

Match strategy to risk tolerance. Leveraged farming amplifies IL and liquidation risk; stablecoin pools sacrifice upside for consistency. *Higher APY always implies higher risk.*

Strat

spectrum: single-sided (safest) → stablecoin LP → volatile LP → leveraged (highest risk)

Real Yield vs Token Emissions

Real Yield

Source: Protocol revenue (trading fees, liquidation fees, interest spreads).

Properties:

- Sustainable long-term
- Denominated in established tokens (ETH, stables)
- Grows with protocol usage
- Examples: GMX, dYdX, Curve (3CRV fees)

Token Emissions

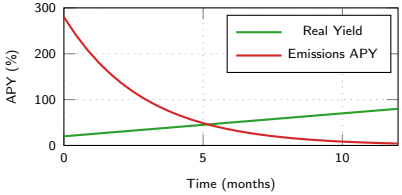
Source: Protocol mints new governance tokens for LPs.

Properties:

- Inflationary by design
- Token value may decline faster than yield accrues
- Mercenary capital: LPs exit when emissions end
- Examples: early Sushiswap, OlympusDAO forks

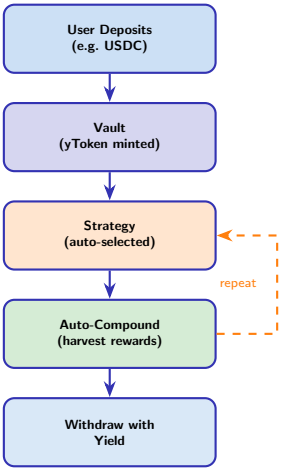
Evaluation

Always compute: **Real Yield** = Total APY − Emission APY. If real yield is near zero, the protocol subsidises LPs unsustainably.



Real yield = fee revenue; token emissions are inflationary subsidies; distinguish before committing capital

Yield Aggregators (e.g. Yearn Finance)



Benefits of Aggregators

- **Gas savings**: Socialised harvest costs across many depositors
- **Strategy expertise**: Professionals manage complex DeFi positions
- **Auto-compounding**: Rewards reinvested without manual action
- **Diversification**: Vault can rotate among strategies
- **Risk management**: Strategies audited; loss limits enforced

Cost

Performance fee (typically 20%) on yields. Smart contract and strategy risk remain.

Yearn

pattern: deposit → vault → strategy → auto-compound; socialises gas and expertise costs

Section 4 Summary

LP Tokens represent proportional pool ownership; LP $= \sqrt{A \times B}$; composable in DeFi

APY vs APR: Daily compounding at 50% APR yields 64.8% APY; advertised figures are often APY

Impermanent Loss: $\text{IL}(r) = \frac{2\sqrt{r}}{1+r} - 1$; $2\times$ price move costs 5.7%; grows nonlinearly

Strategies: spectrum from single-sided staking (safe) to leveraged farming (highest risk)

Real Yield: always distinguish fee revenue from inflationary token emissions

Key Insight

Headline APYs combine fees, emissions, and compounding. Decompose each component and account for IL before comparing yield farming opportunities.

Secti

4 complete — Next: Section 5 — Advanced Topics — Frames 49–55

Section 5: Advanced Topics and Summary

Flash loans, MEV, DeFi security, attack anatomy, regulation, and course summary

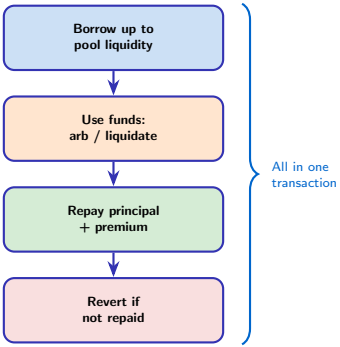
What you will learn

- Flash loans
- MEV — Maximal Extractable Value
- DeFi security best practices
- Flash loan attack anatomy
- Regulatory landscape
- Course summary and key takeaways

Frames in this section

- Frame 50 – Flash Loans
- Frame 51 – MEV
- Frame 52 – DeFi Security Best Practices
- Frames 53–54 – Flash Loan Attacks, Regulation
- Frame 55 – Key Takeaways and Course Summary

Flash Loans

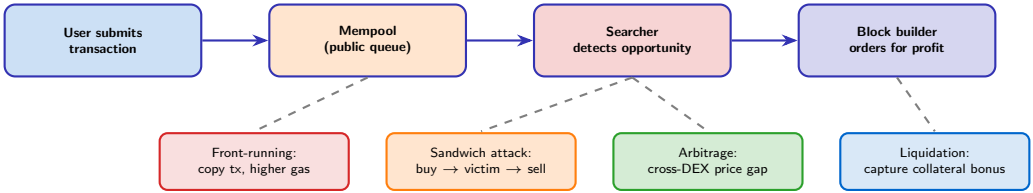


Listing 1: Flash Loan Receiver Pattern

```solidity
// Flash Loan Receiver Pattern
contract MyFlashLoan {
    function executeOperation(
        address asset,
        uint256 amount,
        uint256 premium,  // fee
        address initiator
    ) external returns (bool) {
        // 1. Receive borrowed funds
        // 2. Execute arbitrage/liquidation
        // 3. Repay amount + premium
        IERC20(asset).approve(
            msg.sender, amount + premium
        );
        return true;
    }
}
```

Flash loans: uncollateralised; must repay in same tx or revert; enable arbitrage, liquidations, collateral swaps

MEV — Maximal Extractable Value



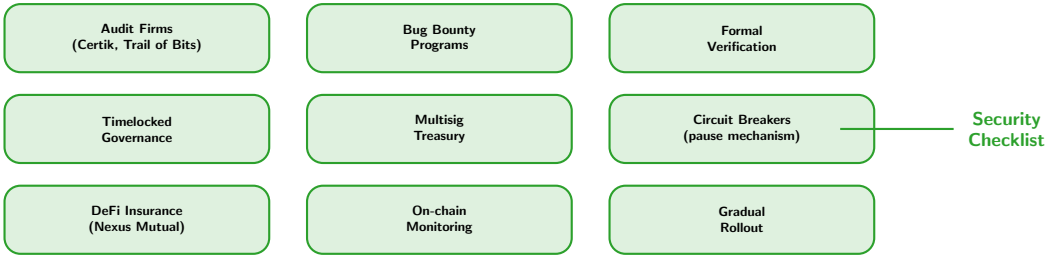
Scale of MEV

Over $500M in MEV extracted since Ethereum's genesis. **Flashbots** and **MEV-Boost** have shifted extraction to off-chain block building, reducing on-chain gas wars but concentrating power in block builders.

MEV

= value extracted by reordering/inserting/censoring txs; front-run, sandwich, arb, liquidation are main types

DeFi Security Best Practices



Major Attack Vectors

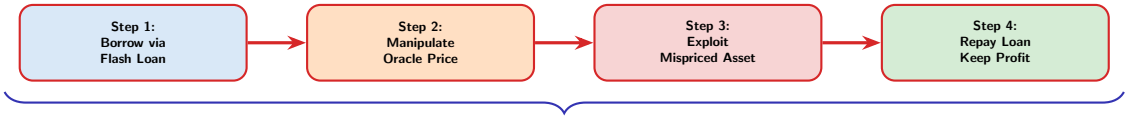
- Reentrancy (DAO hack, $60M)
- Flash loan oracle manipulation
- Access control vulnerabilities
- Integer overflow / underflow

Total DeFi Hacks (cumulative)

>$7 billion lost to exploits since 2020. Audits reduce but do not eliminate risk — bugs remain in audited code.

No audit guarantees safety; defence-in-depth: audits + bug bounties + monitoring + insurance + circuit breakers

Flash Loan Attack Anatomy



Example: bZx Attack (2020) — Borrow ETH → short on Fulcrum → dump on Uniswap → trigger undercollateralised loan → profit $350k

Flash loan attacks exploit atomic composability; defence: TWAP oracles, circuit breakers, reentrancy guards

DeFi Regulation Landscape

United States

SEC enforcement (securities law)

CFTC (derivatives)

No DeFi-specific framework yet

European Union

MiCA Regulation (Markets in Crypto)

Effective 2024–2025

DeFi carve-out under review

Singapore

MAS regulatory sandbox

Licensing under Payment Services Act

Innovation-friendly

China

All crypto transactions banned (Sept 2021)

State-run CBDC (e-CNY) only

Key questions: Who is liable for a DAO? Are governance tokens securities? How to enforce KYC on permissionless protocols?

Regulatory Trajectory

Most jurisdictions are moving toward **activity-based regulation** (what you do, not what technology you use). Centralised interfaces (front-ends) are increasingly targeted, even when underlying smart contracts remain permissionless.

Regu

varies: US (enforcement), EU (MiCA), Singapore (sandbox), China (banned); DAO liability unresolved

Key Takeaways and Course Summary

1. Permissionless Finance: DeFi removes intermediaries via open, auditable smart contracts

2. AMMs: $x \cdot y = k$ enables trustless trading; price impact and IL are fundamental tradeoffs

3. Overcollateralised Lending: health factor > 1 prevents insolvency; interest rate curves balance supply/demand

4. Yield Farming: stack fees + emissions + compounding; always decompose APY and quantify IL

5. Flash Loans, MEV, & Security: atomic composability creates both opportunities and systemic risks

Course Complete — DeFi Fundamentals: A Quantitative Deep Dive

5 Sections | 55 Frames | Prof. Dr. Joerg Osterrieder

Cours

complete — All 5 sections delivered — Continue with Lesson 6: DeFi Risk Management