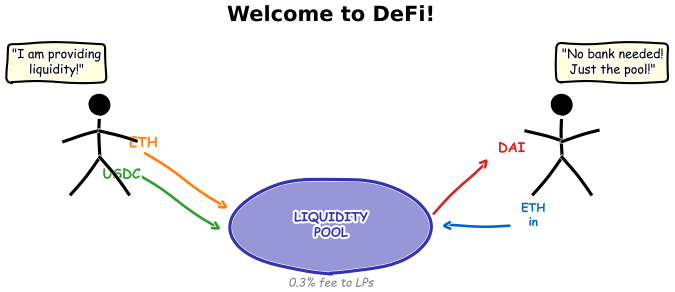
# L07: Decentralized Finance – Technical Deep Dive

BSc Blockchain Course

Digital Finance

# What If Anyone Could Be a Bank – Without a Banking License?




Imagine earning interest on your savings, borrowing against your assets, or trading currencies – all without filling out a single form, showing your passport, or waiting for a bank to open. DeFi (Decentralized Finance) makes this possible through smart contracts that run 24 hours a day, 7 days a week. Today we examine how it works, what can go wrong, and when the yield is real.

**This cartoon frames the central question of Lesson 7: can code replace banks – and should it?**

# Learning Objectives

By the end of this lesson you will be able to:

1. **Define** key DeFi primitives: AMMs (Automated Market Makers), lending protocols, flash loans, and yield aggregators. *[Understand]*
2. **Explain** how the constant product formula determines swap prices and creates slippage (price impact from large trades). *[Understand]*
3. **Calculate** impermanent loss (the cost of providing liquidity when prices move) for a given price change scenario. *[Apply]*
4. **Compare** DeFi lending mechanics with traditional bank lending on collateral, identity, and risk. *[Analyze]*
5. **Evaluate** whether a proposed DeFi yield source is sustainable or dependent on token emissions (newly created tokens used as rewards). *[Evaluate]*

**Bloom's levels covered:** Understand, Apply, Analyze, Evaluate

---

**These objectives map directly to quiz and exercise assessments.**

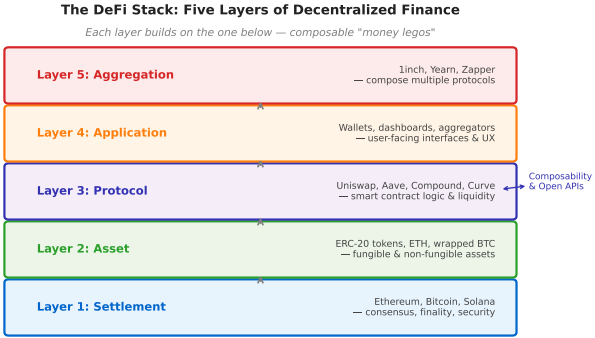
# Where DeFi Fits in the Blockchain Stack

DeFi does not exist in isolation. It sits on top of a protocol stack that you have already studied in earlier lessons.

**The layers beneath DeFi:**

- **Layer 1 – Settlement:** Ethereum, Solana, or another blockchain provides finality (irreversibility) for every transaction.
- **Smart contracts:** Self-executing programs (covered in Lesson 5) encode the rules of lending, swapping, and borrowing.
- **Token standards:** ERC-20 tokens (fungible, interchangeable) represent value inside DeFi protocols.
- **DeFi applications:** Uniswap, Aave, Compound, and others combine these layers into usable financial services.

**Key insight:** DeFi inherits both the strengths (permissionless, transparent) and the weaknesses (scalability limits, smart contract risk) of the layers below it.




- **What you see:** The DeFi protocol stack from L1 settlement up to aggregation.
- **Key pattern:** Each layer depends on the one below – a bug at the bottom breaks everything above.
- **Takeaway:** DeFi security is only as strong as its weakest layer.

**Lessons 5–6 covered Ethereum and smart contracts. DeFi is where those tools meet real money.**

# What Happened to People's Money When FTX Collapsed?

Take a moment and consider what happened in November 2022 when FTX, one of the world's largest crypto exchanges, filed for bankruptcy overnight.

**Consider these questions:**

- Over **one million customers** could not withdraw their funds. Some had their entire savings on the platform. What would you have done?
- FTX was a **centralized exchange** (CeFi) – users deposited money and trusted the company to keep it safe. The company secretly lent user funds to a sister trading firm.
- In DeFi, there is **no company holding your money**. Your assets sit in a smart contract on the blockchain. You hold the keys, and only you can move the funds.

**The core DeFi promise:** "Not your keys, not your coins." If you control the private keys (secret codes that authorize transactions), no company can freeze, steal, or lose your money.

**The trade-off:** Self-custody means *you* are responsible. If you lose your keys or approve a malicious smart contract, there is no customer support hotline to call.

---

**FTX founder Sam Bankman-Fried was convicted of fraud in 2023. Customers lost an estimated $8 billion.**

# What Is DeFi? A Definition Built on Three Pillars

## Definition: Decentralized Finance (DeFi)

**DeFi** is the delivery of financial services – lending, borrowing, trading, insurance – through **smart contracts** on public blockchains, **without centralized intermediaries** such as banks, brokers, or clearinghouses.

**Three pillars of DeFi:**

1. **Permissionless:** Anyone with an internet connection and a wallet can participate. No identity check, no minimum balance, no bank account required.
2. **Composable:** DeFi protocols are "money legos" – they can be combined. A user can deposit collateral in Aave, borrow stablecoins, and swap them on Uniswap in a single transaction.
3. **Non-custodial:** Users retain control of their assets at all times. The smart contract holds funds only as long as the rules require, and only the user can withdraw.

**What DeFi is NOT:** A centralized exchange like Coinbase or Binance. Those are CeFi (Centralized Finance) – they hold your keys and can freeze your account.

---

**As of 2024, over 1,000 DeFi protocols operate across 50+ blockchains with roughly $100 billion in deposits.**

# The AMM: How Prices Are Set Without an Order Book

In traditional finance, buyers and sellers place orders in an **order book**. A market maker (a company with lots of capital) stands in the middle, quoting buy and sell prices.

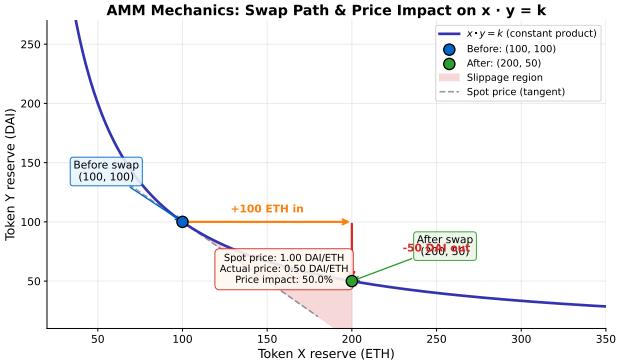
In DeFi, an **Automated Market Maker** (AMM) replaces the order book with a mathematical formula.

**The constant product formula:**

$$x \times y = k$$

- $x$ = quantity of Token A in the pool
- $y$ = quantity of Token B in the pool
- $k$ = a constant that never changes

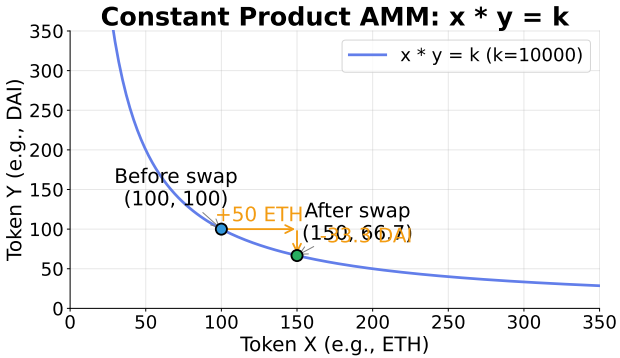
When you swap Token A for Token B, you add A to the pool and remove B. The formula ensures the product stays constant, which automatically sets the price.




- **What you see:** The constant product curve showing how removing one token requires adding more of the other.
- **Key pattern:** Large swaps move the price dramatically – this is called slippage (the difference between expected and actual price).
- **Takeaway:** AMMs work best for small trades in deep (large) pools. Large trades in shallow pools suffer heavy slippage.

# The Constant Product Curve: Visualising $x \times y = k$

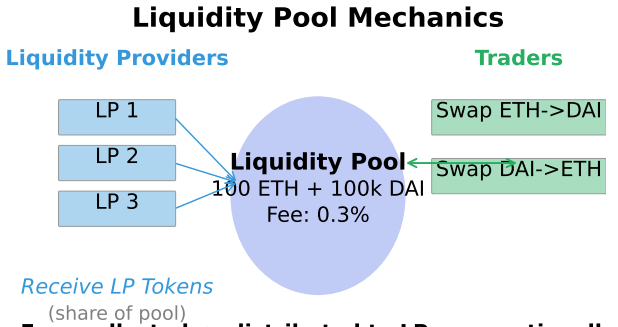
- The hyperbolic curve shows all valid $(x, y)$ combinations for a fixed constant $k$
- Adding Token X to the pool moves the price point right along the curve – you receive fewer Token Y per unit as the pool becomes unbalanced
- **Slippage** is visible as the curved slope: large trades move the price more than small ones
- The annotated "before" and "after" points show a concrete swap: adding 50 ETH yields progressively fewer DAI




**The curve is a hyperbola; it never touches the axes – the pool can never be fully drained of either token.**

# Liquidity Pools: Depositors, Traders, and Fee Flow

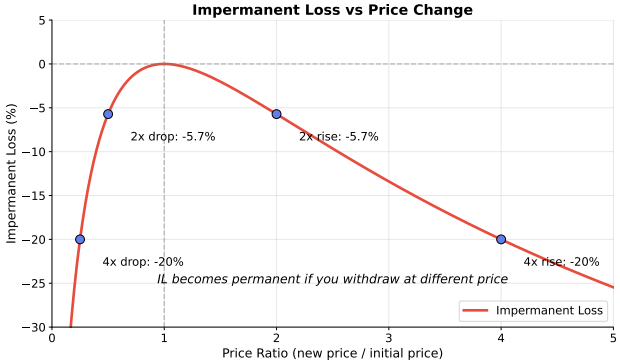
- **Liquidity providers** (LPs) deposit equal-value amounts of two tokens and receive LP tokens representing their share of the pool
- **Traders** swap tokens against the pool in exchange for paying a fee (typically 0.3% per swap)
- Fees accumulate inside the pool and are distributed to all LPs proportionally when they withdraw
- LP tokens are themselves tradeable – LPs can exit any time by burning their LP tokens for the underlying assets plus accrued fees




**A pool with $100M in TVL earning 0.3% on $10M daily volume generates $30,000 per day for its LPs.**

# Impermanent Loss: How Price Divergence Erodes LP Returns

- The IL formula $IL(r) = \frac{2\sqrt{r}}{1+r} - 1$ is symmetric: a 2x price rise and a 2x price fall both produce $-5.7\%$ IL
- IL is non-linear: a 4x move costs 20%, not $4 \times 5.7\%$ – divergence accelerates losses
- At $r = 1$ (no price change) IL is exactly zero – the only scenario with no cost to LPs
- "Impermanent" means the loss disappears if prices return to the initial ratio before withdrawal




**Stablecoin pairs (USDC/DAI) have near-zero IL because the price ratio barely moves – a key reason Curve Finance dominates stablecoin liquidity.**

# DeFi vs Traditional Finance: A Head-to-Head Comparison

How does DeFi compare to the financial system you already know? Six dimensions reveal the fundamental differences.

| Dimension | Traditional Finance | DeFi |
|---|---|---|
| **Identity required** | Yes – KYC (Know Your Customer) | No – wallet address only |
| **Operating hours** | Business hours, weekdays | 24/7/365 |
| **Custody** | Bank holds your money | You hold your own keys |
| **Intermediaries** | Banks, brokers, clearinghouses | Smart contracts only |
| **Composability** | Siloed systems, slow integration | "Money legos" – protocols snap together |
| **Regulatory status** | Licensed and insured (FDIC, etc.) | Largely unregulated, no deposit insurance |

**Key insight:** Neither system is strictly "better." Traditional finance offers consumer protection, insurance, and legal recourse. DeFi offers access, speed, and transparency. The question is which trade-offs matter most for a given use case.

**Example:** A European citizen can earn 4% interest on USDC through Aave in 30 seconds. The same person would need to open a US brokerage account, pass identity checks, and wait days to earn a comparable yield through a traditional money market fund.

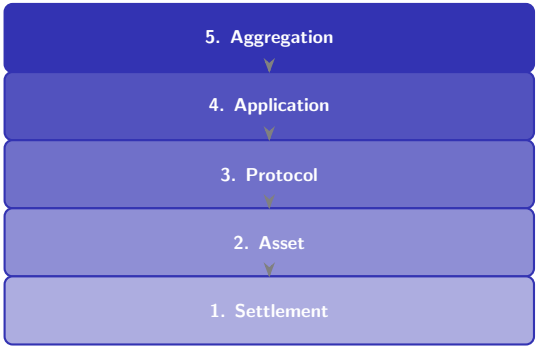
**KYC = Know Your Customer – the process banks use to verify your identity before opening an account.**

# The DeFi Composability Stack

DeFi protocols are often called **"money legos"** because they snap together like building blocks. Each layer provides a service that the layer above can use.

**Five layers of DeFi:**

1. **Settlement:** The blockchain itself (Ethereum, Solana)
2. **Asset:** Tokens – stablecoins (USDC, DAI), wrapped assets (WBTC), governance tokens (UNI)
3. **Protocol:** Core DeFi services – lending (Aave), trading (Uniswap), derivatives (dYdX)
4. **Application:** User-facing interfaces that combine protocols (e.g., Zapper, DeBank)
5. **Aggregation:** Yield optimizers (Yearn) and DEX aggregators (1inch) that route across many protocols




**Why composability matters:** A single transaction can touch five protocols – deposit into Aave, borrow DAI, swap on Uniswap, provide liquidity on Curve, and stake the LP token in Convex. All in one click.

**Risk of composability:** If a protocol at Layer 2 fails (e.g., a stablecoin depegs), every layer above it can collapse – a "DeFi domino effect."

**Composability is DeFi's superpower and its Achilles heel – interconnected protocols share both value and risk.**

# Impermanent Loss: A Worked Example

**Problem:** You provide liquidity to an ETH/USDC pool. ETH doubles in price. How much do you lose compared to simply holding?

**Setup:**

- Deposit: 1 ETH + 2,000 USDC (50/50 split)
- Starting value: $4,000
- ETH price doubles: $2,000 $\rightarrow$ $4,000

# Impermanent Loss: A Worked Example

**Problem:** You provide liquidity to an ETH/USDC pool. ETH doubles in price. How much do you lose compared to simply holding?

**Setup:**

- Deposit: 1 ETH + 2,000 USDC (50/50 split)
- Starting value: \$4,000
- ETH price doubles: \$2,000 $\rightarrow$ \$4,000

**Impermanent loss formula:**

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

where $r$ = price ratio (new price / old price).

# Impermanent Loss: A Worked Example

**Problem:** You provide liquidity to an ETH/USDC pool. ETH doubles in price. How much do you lose compared to simply holding?

**Setup:**

- Deposit: 1 ETH + 2,000 USDC (50/50 split)
- Starting value: \$4,000
- ETH price doubles: \$2,000 $\rightarrow$ \$4,000

**Impermanent loss formula:**

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

where $r$ = price ratio (new price / old price). **At** $r = 2$ **(ETH doubles):**

$$IL = \frac{2\sqrt{2}}{1+2} - 1 = \frac{2.828}{3} - 1 = -5.7\%$$

# Impermanent Loss: A Worked Example

**Problem:** You provide liquidity to an ETH/USDC pool. ETH doubles in price. How much do you lose compared to simply holding?

**Setup:**

- Deposit: 1 ETH + 2,000 USDC (50/50 split)
- Starting value: $4,000
- ETH price doubles: $2,000 → $4,000

**Impermanent loss formula:**

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

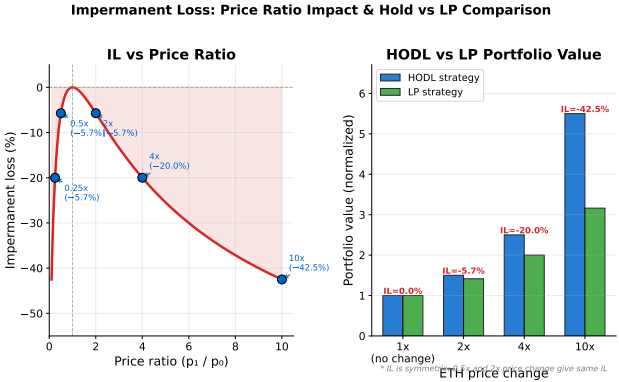
where $r$ = price ratio (new price / old price). **At $r = 2$ (ETH doubles):**

$$IL = \frac{2\sqrt{2}}{1+2} - 1 = \frac{2.828}{3} - 1 = -5.7\%$$

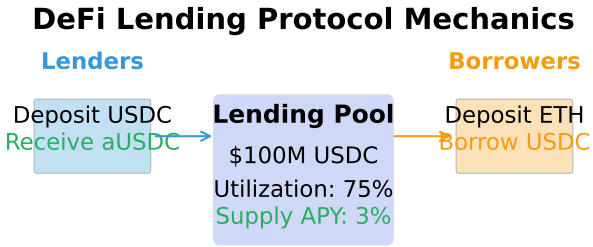
**If you had just held:** $6,000.

**In the pool:** $5,657.

**Loss from providing liquidity:** $343 (5.7%).




- **What you see:** Impermanent loss curves for different price change magnitudes.
- **Key pattern:** IL accelerates as prices diverge – a 4x move costs 20%, not 4 times 5.7%.
- **Takeaway:** Liquidity provision is profitable only when trading fees




**Five stages of a DeFi loan:**

1. **Deposit collateral:** Lock ETH into a lending smart contract (e.g., Aave or Compound).
2. **Borrow:** The protocol lets you borrow up to 75% of your collateral value in stablecoins (e.g., USDC).
3. **Monitor health factor:** The protocol continuously checks whether your collateral still exceeds the minimum ratio.
4. **Price drops:** If ETH's price falls and your health factor (a safety score) drops below 1.0, you are at risk.

# Collateral Ratio: A Worked Example

**Problem:** You deposit 10 ETH at $2,000 each into Aave and borrow USDC. At what price does your position get liquidated?

**Setup:**

- Collateral: 10 ETH $\times$ $2,000 = $20,000
- LTV (Loan-to-Value ratio): 75% maximum
- You borrow: 75% $\times$ $20,000 = $15,000 USDC
- Liquidation threshold: 80% (the point where the protocol acts)

# Collateral Ratio: A Worked Example

**Problem:** You deposit 10 ETH at $2,000 each into Aave and borrow USDC. At what price does your position get liquidated?

**Setup:**

- Collateral: 10 ETH $\times$ $2,000 = $20,000
- LTV (Loan-to-Value ratio): 75% maximum
- You borrow: 75% $\times$ $20,000 = $15,000 USDC
- Liquidation threshold: 80% (the point where the protocol acts)

**Health Factor formula:**

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Outstanding Debt}}$$

# Collateral Ratio: A Worked Example

**Problem:** You deposit 10 ETH at $2,000 each into Aave and borrow USDC. At what price does your position get liquidated?

**Setup:**

- Collateral: 10 ETH $\times$ $2,000 = $20,000
- LTV (Loan-to-Value ratio): 75% maximum
- You borrow: 75% $\times$ $20,000 = $15,000 USDC
- Liquidation threshold: 80% (the point where the protocol acts)

**Health Factor formula:**

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Outstanding Debt}}$$

**At deposit:**

$$HF = \frac{\$20{,}000 \times 0.80}{\$15{,}000} = \frac{\$16{,}000}{\$15{,}000} = 1.07 \quad \text{(safe, but barely)}$$

# Collateral Ratio: A Worked Example

**Problem:** You deposit 10 ETH at $2,000 each into Aave and borrow USDC. At what price does your position get liquidated?

**Setup:**

- Collateral: 10 ETH $\times$ $2,000 = $20,000
- LTV (Loan-to-Value ratio): 75% maximum
- You borrow: 75% $\times$ $20,000 = $15,000 USDC
- Liquidation threshold: 80% (the point where the protocol acts)

**Health Factor formula:**

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Outstanding Debt}}$$

**At deposit:**

$$HF = \frac{\$20{,}000 \times 0.80}{\$15{,}000} = \frac{\$16{,}000}{\$15{,}000} = 1.07 \quad \text{(safe, but barely)}$$

**ETH drops to $1,500:**

$$HF = \frac{(10 \times \$1{,}500) \times 0.80}{\$15{,}000} = \frac{\$12{,}000}{\$15{,}000} = 0.80 \quad \textbf{LIQUIDATED}$$

# Collateral Ratio: A Worked Example

**Problem:** You deposit 10 ETH at $2,000 each into Aave and borrow USDC. At what price does your position get liquidated?

**Setup:**

- Collateral: 10 ETH $\times$ $2,000 = $20,000
- LTV (Loan-to-Value ratio): 75% maximum
- You borrow: 75% $\times$ $20,000 = $15,000 USDC
- Liquidation threshold: 80% (the point where the protocol acts)

**Health Factor formula:**

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Outstanding Debt}}$$

**At deposit:**

$$HF = \frac{\$20{,}000 \times 0.80}{\$15{,}000} = \frac{\$16{,}000}{\$15{,}000} = 1.07 \quad \text{(safe, but barely)}$$

**ETH drops to $1,500:**

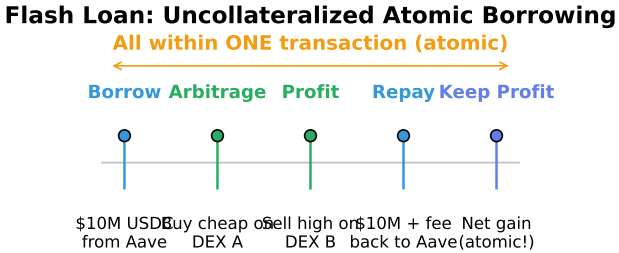
$$HF = \frac{(10 \times \$1{,}500) \times 0.80}{\$15{,}000} = \frac{\$12{,}000}{\$15{,}000} = 0.80 \quad \textbf{LIQUIDATED}$$

**Lesson:** Borrowing at maximum LTV leaves almost no safety margin. A 25% price drop triggers liquidation. Experienced users borrow well below the maximum to survive volatility.

**Health Factor above 1.0 = safe. Below 1.0 = eligible for liquidation. Most users target HF above 1.5 for safety.**

# Flash Loans Step by Step: Borrow, Arbitrage, Repay – Atomically

- All five steps – borrow, arbitrage buy, arbitrage sell, repay, keep profit – occur inside a **single Ethereum transaction**
- If the repayment step fails (e.g., arbitrage profit disappears), the entire transaction reverts as if nothing happened; the lender loses nothing
- No collateral is ever locked; the atomicity guarantee is the collateral
- Use cases include arbitrage, collateral swaps, self-liquidation to avoid penalties, and (maliciously) oracle price manipulation




**Aave charges 0.09% for flash loans. On a $10M loan that is $900 – cheap insurance for an arbitrage trade worth thousands.**

# Flash Loans: Borrowing Two Hundred Million Dollars for Twelve Seconds

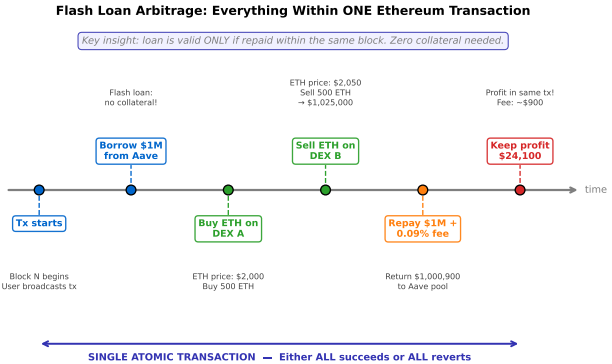
A **flash loan** is a DeFi innovation with no equivalent in traditional finance. It lets you borrow any amount – even hundreds of millions of dollars – with **zero collateral**, as long as you repay within the **same transaction** (about 12 seconds on Ethereum).

**How it works:**

1. **Borrow:** Request funds from a lending pool
2. **Use:** Execute arbitrage (buy low on one exchange, sell high on another), swap collateral, or refinance a loan
3. **Repay:** Return the borrowed amount plus a small fee (typically 0.09%)

**The atomic guarantee:** If the repayment fails – for any reason – the *entire transaction reverts*. The blockchain acts as if the loan never happened. The lender faces zero risk of losing funds.

**The dark side:** Attackers use flash loans to manipulate prices, drain liquidity pools, and exploit protocol bugs.




- **What you see:** The anatomy of a flash loan – borrow, use, and repay in one atomic block.
- **Key pattern:** Atomicity (all-or-nothing execution) is what makes uncollateralized lending possible.
- **Takeaway:** Flash loans democratize arbitrage but also democratize attacks – a double-edged sword.

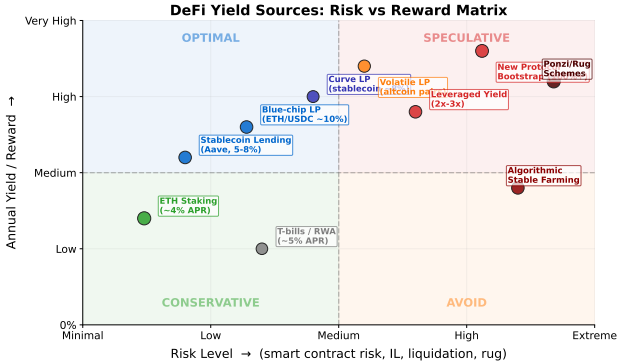
# Yield Sources: Where Does the Money Actually Come From?

When a DeFi protocol offers you 5%, 20%, or 200% annual yield, the first question should always be: **where does the money come from?**

**Two types of yield:**

1. **Real yield:** Revenue from actual economic activity
   - Trading fees (Uniswap LPs earn 0.3% per swap)
   - Borrowing interest (Aave lenders earn from borrowers)
   - Liquidation penalties (liquidators pay a bonus)
2. **Token emissions:** The protocol prints new tokens and distributes them as rewards
   - Looks like high yield, but dilutes the token price
   - Unsustainable – when emissions stop, yield drops to zero
   - Example: many "yield farms" in DeFi Summer 2020

**Rule of thumb:** If the APY (Annual Percentage Yield) exceeds 100%, ask: "Who is paying this, and for how long?"




- **What you see:** A risk-reward matrix mapping yield sources by sustainability and risk level.
- **Key pattern:** Real yield clusters in the low-risk, moderate-return quadrant. Token emissions cluster in the high-risk, high-return quadrant.
- **Takeaway:** Sustainable DeFi protocols generate revenue from fees

# DeFi Yield Strategies: Risk-Return Spectrum from Staking to Leverage

- **Staking** (3–5% APY) is the safest: rewards come from protocol inflation for securing the network
- **Lending** (2–8%) generates real yield from borrowers paying interest
- **LP fees** (5–20%) add impermanent loss risk on top of smart contract risk
- **Yield farming** (10–100%+) often pays in governance tokens whose value can collapse overnight – classic unsustainable emission yield
- **Leveraged yield** compounds risk recursively: one liquidation unwinds the entire stack

**DeFi Yield Strategies Comparison**

| Strategy | Example | APY Range | Risk Level |
|---|---|---|---|
| Staking | ETH, SOL | 3–5% | Native |
| Lending | Aave, Compound | 2–8% | Low–Med |
| LP Fees | Uniswap, Curve | 5–20% | Medium |
| Yield Farming | Token incentives | 10–100%+ | High |
| Leveraged | Recursive loops | 20–500%+ | Very High |

***Higher APY = Higher Risk (smart contract, IL, liquidation, token devaluation)***

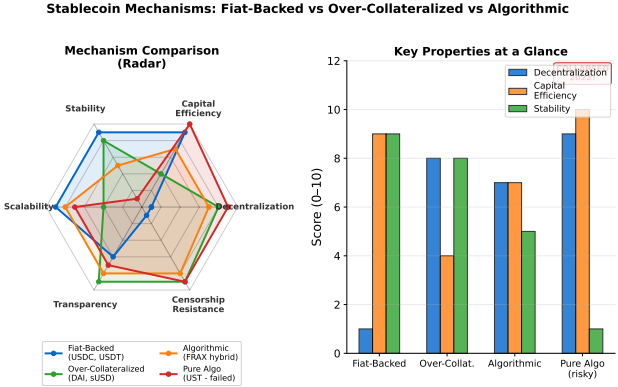
**Rule: if strategy complexity or APY increases, ask which risk category is funding the extra return.**

# Stablecoins: The Backbone of DeFi

A **stablecoin** is a cryptocurrency designed to maintain a 1:1 peg (fixed exchange rate) with a fiat currency, usually the US dollar. Stablecoins are the "cash" of DeFi – nearly every protocol uses them.

**Three types:**

1. **Fiat-backed:** Each token is backed by $1 in a bank account.
   - Examples: USDC (Circle), USDT (Tether)
   - Risk: Centralized – issuer can freeze your coins
2. **Over-collateralized:** Backed by crypto worth more than the stablecoin issued.
   - Example: DAI (MakerDAO) – $1.50 of ETH backs each $1 of DAI
   - Risk: Liquidation cascades if collateral crashes
3. **Algorithmic:** Uses code to expand/contract supply, no collateral backing.
   - Example: UST (Terra) – **collapsed in May 2022**, wiping out $40 billion
   - Risk: "Death spiral" when confidence breaks




**Market share (2024):**
USDT: $110B – USDC: $33B – DAI: $5B

**Key insight:** After UST's collapse, the market decisively shifted toward fiat-backed stablecoins. Algorithmic designs are now viewed with extreme skepticism.

# Impermanent Loss Calculation: The Full Formula

**Review:** Impermanent loss (IL) is the cost a liquidity provider pays when the price ratio between two tokens in a pool changes. Here is the complete calculation.

**Formula:**

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

where $r$ = new price / old price of the volatile asset.

# Impermanent Loss Calculation: The Full Formula

**Review:** Impermanent loss (IL) is the cost a liquidity provider pays when the price ratio between two tokens in a pool changes. Here is the complete calculation.

**Formula:**

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

where $r$ = new price / old price of the volatile asset.

| Price Change | $r$ | IL | Interpretation |
|---|---|---|---|
| +25% | 1.25 | −0.6% | Barely noticeable |
| +50% | 1.50 | −2.0% | Fees likely compensate |
| +100% (2x) | 2.00 | −5.7% | Significant – need high volume |
| +200% (3x) | 3.00 | −13.4% | Painful unless fees are exceptional |
| +300% (4x) | 4.00 | −20.0% | One-fifth of your gains lost to IL |

# Impermanent Loss Calculation: The Full Formula

**Review:** Impermanent loss (IL) is the cost a liquidity provider pays when the price ratio between two tokens in a pool changes. Here is the complete calculation.

**Formula:**

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

where $r$ = new price / old price of the volatile asset.

| Price Change | $r$ | IL | Interpretation |
|---|---|---|---|
| +25% | 1.25 | −0.6% | Barely noticeable |
| +50% | 1.50 | −2.0% | Fees likely compensate |
| +100% (2×) | 2.00 | −5.7% | Significant – need high volume |
| +200% (3×) | 3.00 | −13.4% | Painful unless fees are exceptional |
| +300% (4×) | 4.00 | −20.0% | One-fifth of your gains lost to IL |

**Worked verification ($r = 1.5$):**

$$IL = \frac{2\sqrt{1.5}}{1+1.5} - 1 = \frac{2 \times 1.2247}{2.5} - 1 = \frac{2.4495}{2.5} - 1 = 0.9798 - 1 = -2.0\%$$

# Impermanent Loss Calculation: The Full Formula

**Review:** Impermanent loss (IL) is the cost a liquidity provider pays when the price ratio between two tokens in a pool changes. Here is the complete calculation.

**Formula:**

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

where $r$ = new price / old price of the volatile asset.

| Price Change | $r$ | IL | Interpretation |
|---|---|---|---|
| +25% | 1.25 | −0.6% | Barely noticeable |
| +50% | 1.50 | −2.0% | Fees likely compensate |
| +100% (2×) | 2.00 | −5.7% | Significant – need high volume |
| +200% (3×) | 3.00 | −13.4% | Painful unless fees are exceptional |
| +300% (4×) | 4.00 | −20.0% | One-fifth of your gains lost to IL |

**Worked verification ($r = 1.5$):**

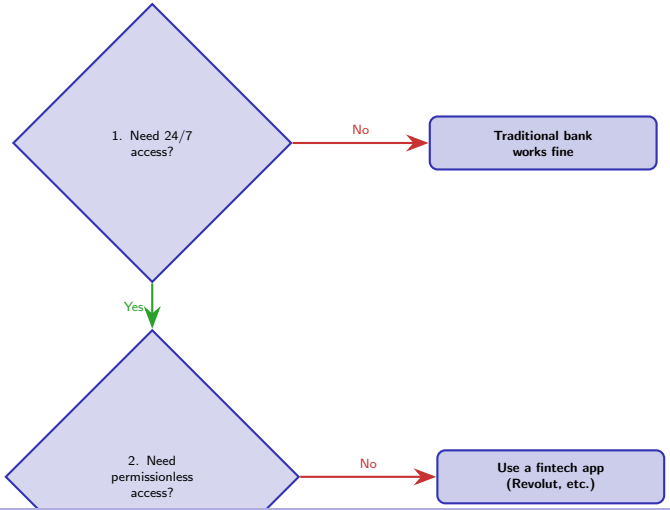
$$IL = \frac{2\sqrt{1.5}}{1+1.5} - 1 = \frac{2 \times 1.2247}{2.5} - 1 = \frac{2.4495}{2.5} - 1 = 0.9798 - 1 = -2.0\%$$

**Decision rule:** Provide liquidity only when expected trading fees exceed the expected impermanent loss over your holding period.

**IL is symmetric: a 50% price decrease ($r = 0.5$) also produces -2.0% IL. The formula depends on magnitude, not direction.**

# When to Use DeFi: A Decision Framework

Not every financial need benefits from DeFi. Before using a DeFi protocol, walk through these five questions. If any answer is "no," traditional finance may be the better choice.



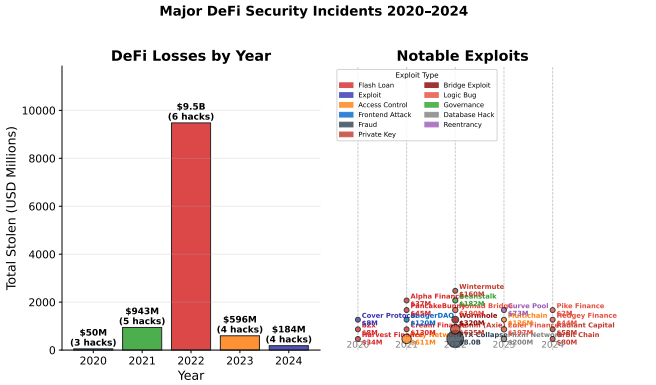
# The DeFi Hack Hall of Shame

DeFi's permissionless nature means anyone can build a protocol – but also anyone can attack one. Over $6 billion has been stolen from DeFi protocols since 2020.

**Largest DeFi exploits:**

1. **Ronin Bridge** (Mar 2022): $625M stolen via compromised validator keys on Axie Infinity's bridge
2. **Wormhole** (Feb 2022): $320M – attacker forged a verification signature to mint tokens from nothing
3. **Euler Finance** (Mar 2023): $197M – a flash loan attack exploiting a missing health check
4. **Nomad Bridge** (Aug 2022): $190M – a bug let anyone copy-paste the exploit transaction

**Pattern:** Bridges (protocols connecting two blockchains) are the most vulnerable targets because they hold large pools of locked assets.




- **What you see:** A timeline of major DeFi hacks showing the amount stolen per incident.
- **Key pattern:** Bridge exploits dominate the largest losses. Protocol-level hacks tend to be smaller but more frequent.
- **Takeaway:** Audits reduce risk but do not eliminate it – several

# Oracle Manipulation: When the Price Feed Lies

A **price oracle** is a service that tells a smart contract the current market price of an asset. DeFi protocols rely on oracles to decide liquidations, set swap prices, and calculate collateral ratios. If the oracle reports a wrong price, the protocol makes wrong decisions.

**How oracle manipulation works:**

1. **The attacker** takes a flash loan of millions of dollars
2. **Trades aggressively** on a low-liquidity pool to move the on-chain price of an asset
3. **A vulnerable protocol** reads this manipulated price and executes at the wrong rate – enabling the attacker to borrow more than their collateral is worth, or buy assets below market value
4. **The attacker** repays the flash loan and keeps the profit

**Mitigation strategies:**

- **Chainlink oracles:** Aggregate prices from multiple off-chain sources – much harder to manipulate
- **TWAP** (Time-Weighted Average Price): Average the price over multiple blocks instead of using a single spot price
- **Circuit breakers:** Pause the protocol if prices move more than a threshold in a single block

**Over $400M was lost to oracle manipulation attacks in 2021–2023. Chainlink now secures over $75B in DeFi value.**

# Smart Contract Risk, Regulatory Risk, and Economic Risk

DeFi risk comes in three distinct categories. A responsible user must evaluate all three before depositing funds.

| Risk Category | Severity | Example | Mitigation |
|---|---|---|---|
| **Smart contract risk** | High | Bug in code drains funds (e.g., Euler $197M exploit) | Multiple audits, bug bounties, formal verification, timelocks |
| **Regulatory risk** | Medium | Government bans DeFi access or requires KYC on-chain | Use protocols with regulatory compliance options (Aave Arc) |
| **Economic risk** | High | Stablecoin depeg, oracle failure, liquidity crisis, bank run on a lending protocol | Diversify across protocols, monitor health factor, use conservative LTV ratios |

**Key insight:** Traditional finance distributes these risks across regulated institutions with insurance and legal recourse. In DeFi, **you bear all three risks directly**. There is no FDIC insurance, no ombudsman, and no refund button.

**Practical rule:** Never deposit more in DeFi than you can afford to lose entirely. Treat it like a high-risk investment, not a savings account.

**The EU's MiCA regulation (2024) begins to address regulatory risk by requiring stablecoin issuers to hold reserves.**

# DeFi vs TradFi: Who Is Winning the Comparison?

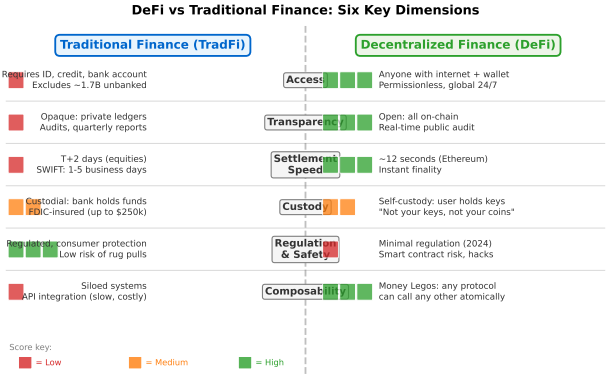
DeFi and traditional finance (TradFi) each excel on different dimensions. Neither dominates across the board.

**Where DeFi wins:**

- **Speed:** Settlement in seconds vs days
- **Access:** No identity check, no minimum balance
- **Transparency:** All transactions publicly verifiable
- **Cost:** Often lower fees for cross-border transfers

**Where TradFi wins:**

- **Regulation:** Consumer protection, deposit insurance
- **User protection:** Fraud reversal, dispute resolution
- **Scale:** Handles millions of transactions per second
- **Usability:** Decades of UX refinement




- **What you see:** A multi-dimensional comparison of DeFi and TradFi across speed, cost, access, transparency, regulation, and user protection.
- **Key pattern:** DeFi leads on efficiency and access; TradFi leads on safety and scale.

# DeFi Adoption: Who Is Using It and Where?

DeFi adoption is growing but remains concentrated among a relatively small, technically sophisticated user base.

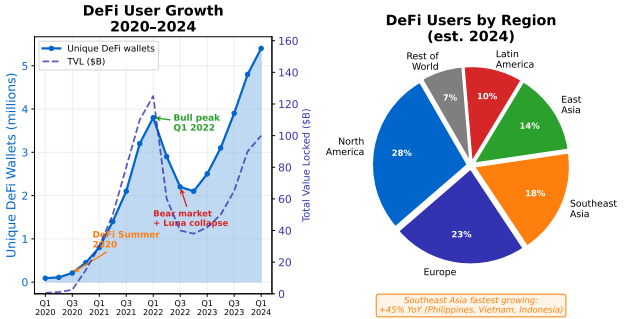
**User statistics (2024):**

- Approximately **7 million** unique DeFi wallet addresses active monthly (vs 5.5 billion traditional bank account holders)
- Average DeFi user age: 25–40 years old
- Median deposit size: approximately $5,000

**Geographic concentration:**

- **Highest adoption:** Southeast Asia, Sub-Saharan Africa (often driven by weak local currencies and limited banking)
- **Largest volume:** North America, Western Europe (institutional and whale-driven)
- **Fastest growth:** Latin America (remittance corridor demand)

**DeFi Adoption: User Growth & Global Distribution**




- **What you see:** DeFi adoption metrics by region, showing user growth and geographic distribution.
- **Key pattern:** The highest adoption rates are in developing countries where traditional banking fails the most people.
- **Takeaway:** DeFi's greatest impact may not be replacing Western

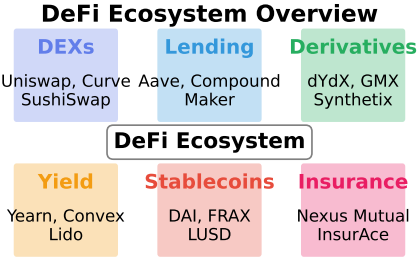
# The DeFi Ecosystem: Protocols Build on Protocols

The DeFi ecosystem is not a collection of isolated protocols – it is a **web of dependencies** where each protocol builds on and interacts with others.

**Composability in action:**

- **Yearn Finance** deposits user funds into whichever lending protocol (Aave, Compound) currently offers the best rate
- **Aave** uses **Chainlink** price oracles to determine when to liquidate undercollateralized loans
- **Chainlink** reads prices from centralized exchanges and on-chain DEXs (Decentralized Exchanges like Uniswap)
- **All of them** settle on **Ethereum** Layer 1

**Systemic risk:** A failure in any widely-used protocol can cascade through the entire ecosystem. When UST collapsed in May 2022, it triggered liquidations across dozens of protocols that held UST as collateral.




***Composability: "Money Legos" - protocols can be combined***

**Major protocol categories:**

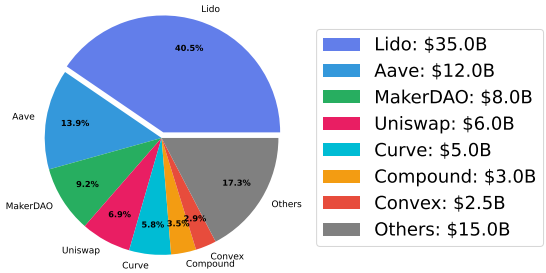
- **DEXs:** Uniswap, Curve, SushiSwap
- **Lending:** Aave, Compound, MakerDAO
- **Derivatives:** dYdX, GMX, Synthetix
- **Aggregators:** 1inch, Yearn, Convex
- **Oracles:** Chainlink, Pyth, UMA

**Over 80% of DeFi TVL is concentrated in the top 10 protocols – composability amplifies both value and risk.**

# DeFi TVL Distribution: Where the $86 Billion Is Parked

- **Lido** dominates with $35B: users deposit ETH and receive stETH (liquid staking token) while earning staking rewards
- **Aave** and **MakerDAO** together hold $20B – lending protocols attract deep capital because yields are predictable
- The "Others" slice ($15B) captures hundreds of smaller protocols – high yield, high risk
- Concentration in a few protocols reduces systemic diversity; a Lido exploit would ripple through all protocols that accept stETH as collateral

**DeFi TVL Distribution (~$86B Total)**




**TVL peaked at $180B in Nov 2021, fell to $37B by mid-2023, and recovered to $86B by 2024 – tracking crypto market cycles closely.**

# DEX vs CEX: Self-Custody vs Convenience

- **DEX** (e.g., Uniswap): trades settle on-chain; you never relinquish your private key; no KYC required; vulnerable to smart contract bugs
- **CEX** (e.g., Binance): fast off-chain matching engine; supports fiat on-ramps and complex order types; requires identity verification; counterparty risk (as FTX demonstrated)
- DEX fees (fixed 0.3%) are simpler than CEX maker/taker structures but do not support limit orders
- Most retail users start on a CEX for ease, then move assets to a DEX for DeFi composability

**DEX vs CEX Comparison**

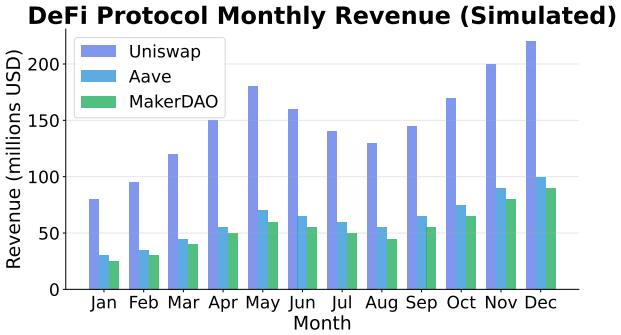
| Feature | DEX (Uniswap) | CEX (Binance) |
|---|---|---|
| **Custody** | Self-custody | Exchange holds |
| **KYC** | None | Required |
| **Speed** | Slower (on-chain) | Fast (off-chain) |
| **Liquidity** | Growing | High |
| **Fees** | 0.3% swap | Maker/taker |
| **Security** | Smart contract risk | Counterparty risk |

***DEX: "Not your keys, not your coins" | CEX: Better UX, more features***

**DEX spot volume reached 15% of CEX volume in 2023 – up from under 1% in 2019. The gap is narrowing but CEXs still dominate.**

# Protocol Revenue: Which DeFi Protocols Earn Real Money?

- **Uniswap** consistently earns the most – its revenue is purely from swap fees (real yield), growing with trading volume
- **Aave** earns from the spread between borrowing and lending rates; revenue is more stable but lower peak than Uniswap
- **MakerDAO** earns stability fees on DAI loans – a bond-like revenue model
- All three show seasonal growth patterns, with peaks in bull markets when trading volume and borrowing demand surge




**Protocols that earn real fee revenue can sustain token holders without dilutive emissions – the key sign of a financially mature DeFi protocol.**

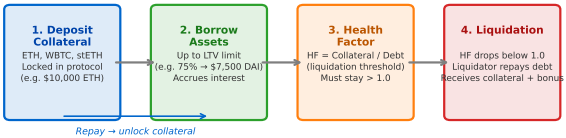
# Who Wins and Who Loses When Finance Goes Permissionless?

DeFi does not create value from nothing – it **redistributes** who captures value and who loses it.

| Stakeholder | Impact |
|---|---|
| Unbanked populations | + Financial inclusion |
| Yield seekers | + Higher returns (and risk) |
| Developers | + New revenue models |
| Traditional banks | – Disintermediation |
| Unsophisticated users | – No safety net |
| Regulators | +/– New tools, new risks |

**The inclusion paradox:** DeFi claims to serve the unbanked, but most current users are already wealthy, tech-savvy individuals in developed countries. The gas fees (transaction costs on Ethereum) alone can exceed a day's wage in many developing nations.

**DeFi Lending: Collateral → Borrow → Health Factor → Liquidation**




**The path forward:**

- **Layer-2 solutions** (Arbitrum, Optimism) reduce fees from $5–50 to $0.01–0.10
- **Account abstraction** (ERC-4337) simplifies wallet management – no more memorizing 24-word seed phrases
- **Fiat on-ramps** (MoonPay, Transak) let users enter DeFi with a credit

# The DeFi Generation Gap: Degens vs Institutions

Two fundamentally different groups use DeFi – and they approach it with completely different assumptions, risk appetites, and goals.

| Dimension | Retail "Degens" | Institutional DeFi |
|---|---|---|
| **Goal** | Maximize yield, speculate | Reduce costs, increase efficiency |
| **Risk appetite** | High – "ape in" culture | Low – fiduciary duty to clients |
| **Identity** | Pseudonymous (wallet only) | Full KYC required |
| **Protocols used** | Any – new forks, meme tokens | Permissioned pools (Aave Arc) |
| **Time horizon** | Days to weeks | Months to years |
| **Loss tolerance** | "I knew the risk" | Legal liability if funds lost |
| **Regulatory view** | Regulation = enemy | Regulation = enabler |

**Convergence trend:** Institutional DeFi is growing rapidly.

- JPMorgan tested tokenized repo transactions on a public blockchain (Project Guardian, 2023)
- BlackRock launched BUIDL, a tokenized money market fund on Ethereum
- Goldman Sachs explored bond issuance on blockchain rails

**Key insight:** "Degen" (short for "degenerate gambler") is a self-adopted term in crypto culture. It reflects high risk tolerance, not financial sophistication.

**Aave Arc launched in 2022 as the first permissioned (KYC-gated) DeFi lending pool for institutions.**

# Five Red Flags in Any DeFi Protocol

Before depositing funds into any DeFi protocol, check for these five warning signs. Even one red flag should make you pause; three or more should make you walk away.

**The Five Red Flags:**

1. **Anonymous team:** No identifiable founders or developers. If the team cannot be held accountable, they have no reason to act responsibly.
2. **Unaudited contracts:** The smart contract code has not been reviewed by a reputable security firm (Trail of Bits, OpenZeppelin, Certik). Bugs in unaudited code are essentially guaranteed.
3. **APY from token emissions only:** The yield comes entirely from newly minted governance tokens, not from fees or real economic activity. When emissions stop, the yield drops to zero and the token price crashes.
4. **No timelock on admin keys:** The team can change the smart contract rules instantly, without giving users time to withdraw. A timelock (typically 24–48 hours) gives users an exit window.
5. **Single oracle dependency:** The protocol relies on one price source. If that source is manipulated (via flash loan or data error), the entire protocol can be drained.

**Evaluation rule:** 0 red flags = blue-chip DeFi. 1–2 = proceed with caution. 3+ = stay away.

---

**Even "blue-chip" protocols like Aave and Uniswap have had minor vulnerabilities – no smart contract is 100% safe.**

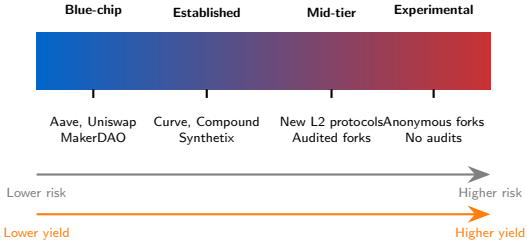
# The DeFi Risk Spectrum: Where Does Your Protocol Fall?

Not all DeFi protocols carry the same risk. The ecosystem ranges from battle-tested "blue-chip" protocols to experimental new projects that could disappear overnight.

**Risk tiers:**

1. **Blue-chip:** Aave, Uniswap, MakerDAO – multiple audits, billions in TVL, years of operation, known teams
2. **Established:** Curve, Compound, Synthetix – well-audited, significant TVL, but occasionally exploited
3. **Mid-tier:** Newer protocols with audits but limited track record – higher yield, higher risk
4. **Experimental:** Unaudited forks, anonymous teams, exotic mechanisms – "degen" territory

**Portfolio approach:** Allocate most capital to blue-chip, a small portion to established, and only "play money" to experimental.




**Key insight:** Higher yield almost always means higher risk. If a new protocol offers 500% APY while Aave offers 3%, ask yourself: "Why would anyone leave Aave for this?" The answer is usually "because the risk is 100 times higher."

**A "rug pull" is when a protocol's anonymous team drains all user funds and disappears. Over $2.8B was lost to rug pulls in 2021.**

# What Comes Next: NFTs and Token Standards

Today you learned how DeFi moves *fungible* value – tokens where one unit is identical to another (1 USDC = 1 USDC). In Lesson 8, we explore *non-fungible* tokens (NFTs) – tokens where every unit is unique.

**Lesson 8 will cover:**

- **Token standards:** ERC-20 (fungible, used in DeFi today), ERC-721 (non-fungible, one-of-a-kind), and ERC-1155 (multi-token, combining both)
- **NFT mechanics:** How ownership of a digital asset is recorded on-chain, what "owning an NFT" actually means (and does not mean), and how marketplaces work
- **Beyond art:** Real-world applications of NFTs – event tickets, academic credentials, real estate title deeds, and gaming items
- **The NFT market cycle:** From $25 billion in 2021 sales to 95% value decline – what survived, what did not, and why

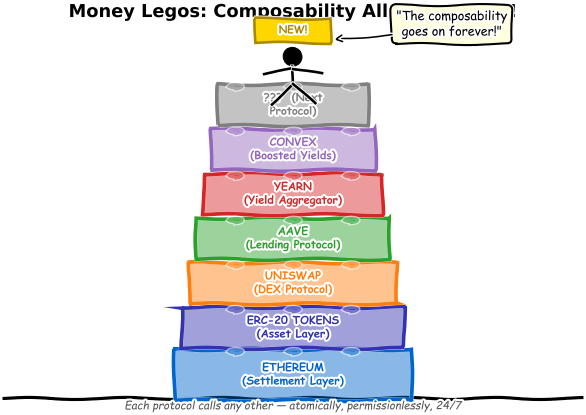
**Bridge:** Now you know how DeFi moves value. Next week you learn how tokens represent *ownership* – and why that distinction changes everything from art markets to supply chains.

**Preparation:** Think about what makes a concert ticket or a university diploma valuable. Is it the paper (or PDF), or the fact that it is uniquely yours and verifiable?

---

**Lesson 8 builds directly on the token standards and smart contract concepts from Lessons 5–7.**

# One Last Thought...




Now you understand why "just earn yield on DeFi" is not as simple as it sounds – and when the technology genuinely delivers on its promise of open, permissionless finance. The yields are real, but so are the risks. The key is knowing which is which.

**The best DeFi users start with the question "where does the yield come from?" – not "how high is the APY?"**

# Key Takeaways

1. **DeFi defined:** Financial services delivered by smart contracts on public blockchains – permissionless, composable, and non-custodial.
2. **AMM mechanics:** The constant product formula ($x \times y = k$) eliminates order books but introduces slippage and impermanent loss as trade-offs.
3. **Lending without identity:** DeFi lending replaces credit scores with over-collateralization – your deposited assets are the only trust signal the protocol needs.
4. **Yield reality:** Real yield comes from trading fees and borrowing interest. Token emissions create the illusion of high returns but dilute value over time.
5. **Risk trifecta:** Smart contract bugs, oracle manipulation, and regulatory uncertainty are the three risk categories every DeFi user must evaluate before depositing funds.
6. **Five red flags:** Anonymous team, unaudited code, emission-only yield, no admin timelock, and single oracle dependency – any three of these should disqualify a protocol from serious consideration.

**Review question: Calculate the impermanent loss for a 3x price change and decide if a 15% annual fee income justifies providing liquidity.**

# Summary / Next Lesson Preview

DeFi replaces banks, brokers, and clearinghouses with smart contracts that execute automatically on public blockchains. Its three pillars – permissionless access, composability, and non-custodial design – make it the most significant application of blockchain technology to date. But this power comes with real risks: smart contract bugs, oracle manipulation, stablecoin collapses, and a complete absence of deposit insurance. The key skill is distinguishing sustainable yield from unsustainable token emissions.

**Key Vocabulary:**

- DeFi (Decentralized Finance)
- AMM (Automated Market Maker)
- Impermanent Loss
- Flash Loan
- Stablecoin
- TVL (Total Value Locked)
- Collateral Ratio / LTV
- Health Factor
- Oracle
- Composability (Money Legos)

**Next lesson:** *NFTs and Token Standards* – how tokens represent unique ownership, why ERC-721 changed digital art, and what happens when speculation meets verifiable scarcity.

---

**Try this before Lesson 8: visit Uniswap (app.uniswap.org) and simulate a token swap. Note the estimated slippage and gas fee.**