# DeFi: Finance Without Banks

## An Ultra-Simple Visual Guide with Deep-Dive Appendix

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

# Learning Objectives

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

1. **Explain** how DeFi replaces banks with code running on a blockchain [Understand]
2. **Describe** how token swaps, lending, and stablecoins work in plain English [Understand]
3. **Compare** the risks of DeFi (hacks, crashes, scams) with its benefits [Analyze]
4. **Evaluate** whether a DeFi protocol is safe using a simple risk checklist [Evaluate]

**No math required.** Main slides use only plain English and pictures.
Technical formulas are in the Appendix for those who want them.

**Bloom's levels covered: Understand, Analyze, Evaluate. The Appendix adds Apply and Create.**

# The Bank Is Closed. DeFi Is Open.

**Saturday night, 11 pm.** You need to send 50,000 dollars to a friend in another country.

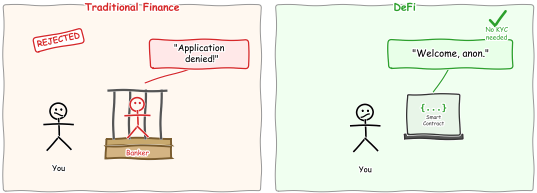
**Option A — Your Bank:**

- Closed until Monday morning
- 3–5 business days to arrive
- Wire fee: 25–50 dollars

**Option B — DeFi:**

- Open right now, always
- Arrives in 12 seconds
- Fee: under 50 cents

**Bank vs DeFi**




*Traditional finance asks for permission. DeFi asks for a wallet.*

**DeFi = Decentralized Finance. Software that does what banks do, but without the bank.**

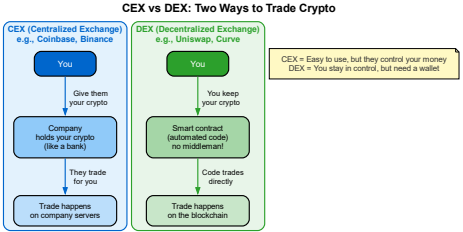
# Your Money: Bank vs DeFi

**Traditional Bank**

- Open 9–5, Monday to Friday
- The bank holds your money
- Fees on every transaction
- Requires ID, address, paperwork

**DeFi Protocol**

- Open 24 hours, 365 days
- You hold your own keys
- Low, transparent fees
- No identity required




**"Not your keys, not your coins." In DeFi, you are your own bank — and your own security guard.**

# Step Zero: Get a Wallet

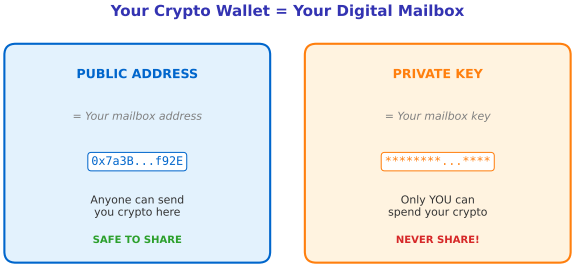
A **crypto wallet** is like a digital keychain. It stores the secret codes that prove you own your tokens.

**Hot wallet** (phone app)

- Easy to use, always connected
- Like cash in your pocket

**Cold wallet** (USB device)

- Offline, very secure
- Like a safe deposit box




*A wallet does not store coins -- it stores the keys that control them.*

**Popular hot wallets: MetaMask, Coinbase Wallet. Popular cold wallets: Ledger, Trezor.**

# What DeFi Actually Does

### Trade

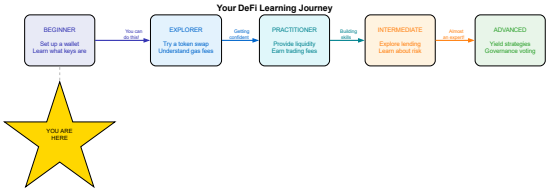
Swap one token for another instantly, like a currency exchange at the airport

### Lend

Deposit tokens and earn interest, or borrow against your crypto collateral

### Save

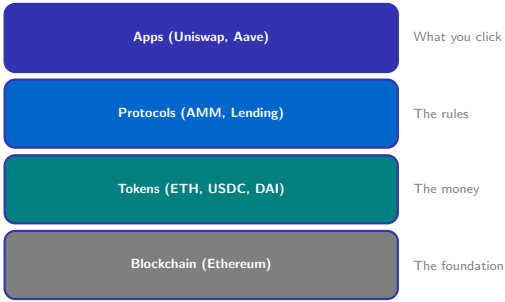
Use stablecoins pegged to the dollar so your savings do not swing wildly

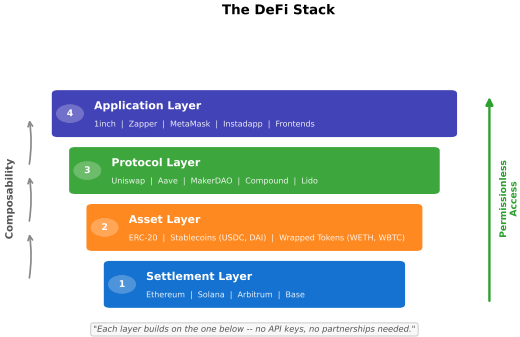



**These three actions — trade, lend, save — cover 90 percent of what people do in DeFi.**

# The DeFi Building Blocks

DeFi is built in layers, like the internet:



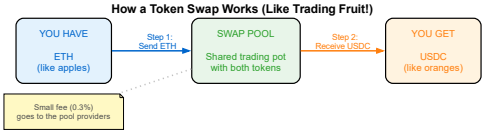

**Each layer builds on the one below. This is why DeFi is called "composable" — like LEGO bricks.**

# What Is a Token Swap?

Imagine a currency exchange booth at the airport.

- You hand over euros
- You receive dollars
- The booth keeps a small fee

A **token swap** is the same idea, but the booth is a computer program. No human involved.

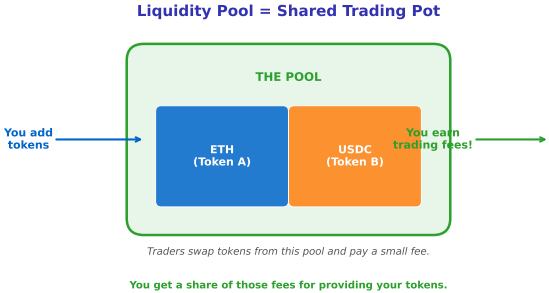



**The most popular swap protocol is Uniswap, handling billions of dollars in trades every month.**

# Behind Every Swap: A Pool of Tokens

The airport booth needs money in the register. In DeFi, that register is called a **liquidity pool**.

- A shared pot of two tokens
- Anyone can add tokens to the pot
- Traders take from one side and add to the other
- Contributors ("LPs") earn fees



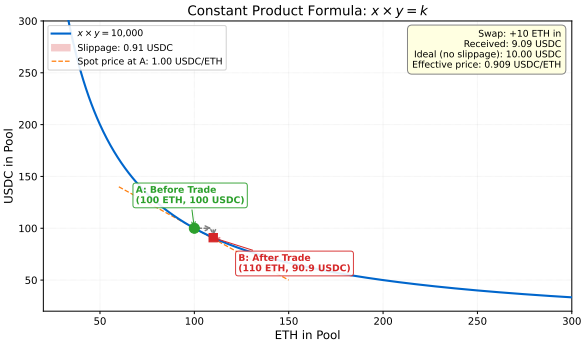

**LP = Liquidity Provider. You deposit tokens into the pool and earn a share of every trade fee.**

# How Prices Change When You Trade

Think of a **seesaw** with two buckets.

- Left bucket: ETH tokens
- Right bucket: USDC tokens
- Buy ETH: left side gets lighter, price goes up
- Sell ETH: left side gets heavier, price goes down

The pool automatically adjusts prices so the two sides always balance out. No order book, no middleman.



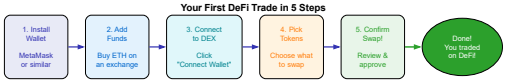

**This "automated market maker" (AMM) is the engine behind Uniswap. See Appendix A1 for the math.**

# Your First DeFi Trade

**Five steps. Under two minutes.**

1. Connect your wallet to a DEX
2. Choose which tokens to swap
3. Enter the amount
4. Review the price and fee, then confirm

That is it. The blockchain settles your trade in seconds, and the tokens appear in your wallet.



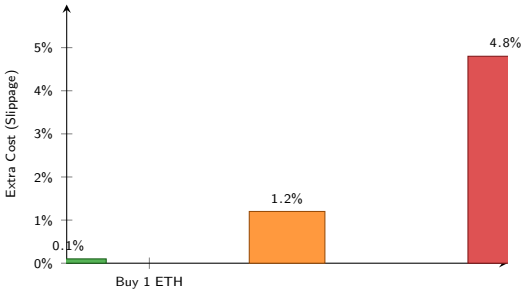

**DEX = Decentralized Exchange. Unlike Coinbase or Binance, nobody can freeze your account.**

# Why Bigger Trades Cost More

When you scoop water from a small pond, the water level drops noticeably. A big scoop moves the level a lot.

In DeFi, a big trade moves the price more than a small trade. This extra cost is called **slippage**.

- Small trade: barely notice
- Medium trade: noticeable cost
- Large trade: expensive



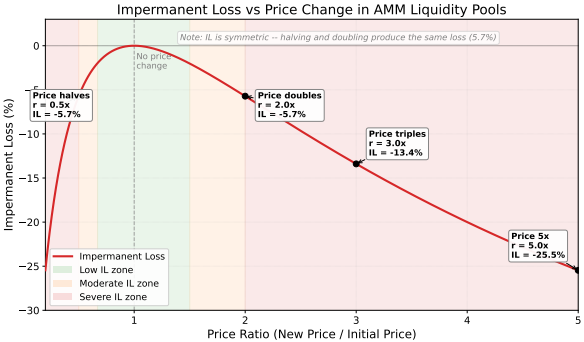

**Rule of thumb: if your trade is more than 1% of the pool, check slippage first. See Appendix A1 for details.**

# Earning Fees (and a Hidden Cost)

Liquidity providers earn a cut of every trade. Sounds like free money, right?

**The catch:** when one token's price moves a lot, the pool automatically rebalances. You end up with more of the cheaper token and less of the expensive one.

This **rebalancing cost** (called "impermanent loss") can eat into your fee earnings.



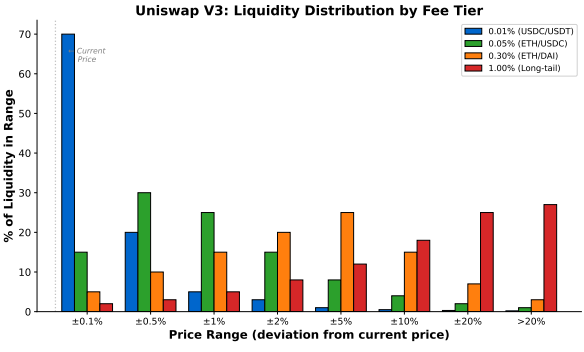

**If the price returns to where it started, the loss disappears — hence "impermanent." See Appendix A2 for the formula.**

# Concentrated Liquidity

Uniswap V3 introduced a clever upgrade: instead of spreading your money across all possible prices, you pick a **price range**.

**Analogy:** A hotel has 100 floors. Old system: one security guard patrols all 100 floors. New system: you assign your guard to floors 40–60 only, where most guests are.

- More focused = more fees earned
- But if price leaves your range, you earn nothing



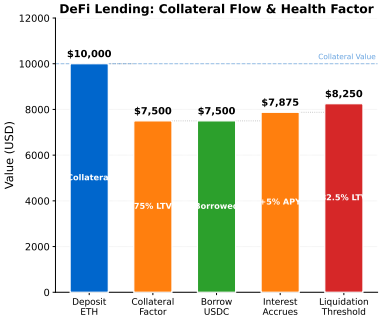

**Concentrated liquidity is more capital-efficient but requires active management. Choose your range wisely.**

# DeFi Lending: How It Works

Think of an **automated pawn shop**.

1. You deposit 150 dollars of crypto as collateral
2. The protocol lets you borrow up to 100 dollars
3. You pay interest over time
4. When you repay, you get your collateral back

No credit check. No paperwork. The smart contract enforces the rules automatically.





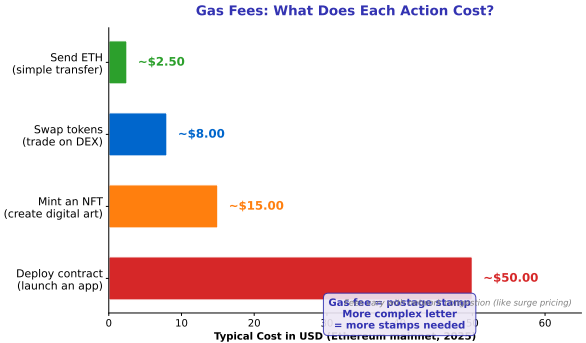
**Popular lending protocols: Aave, Compound. Over-collateralization protects lenders if borrowers default.**

# What Are Gas Fees?

Every action on Ethereum costs a small fee called **gas**.

Think of it like a **postage stamp**: you pay a small amount to have the network process and deliver your transaction.

- Simple transfer: cheap stamp
- Complex swap: more expensive stamp
- Network busy: stamps cost more
- Network quiet: stamps cost less



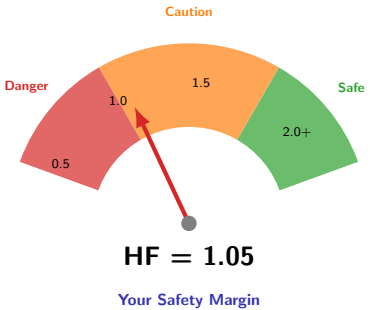

**Gas fees go to the validators who process transactions. Layer-2 networks like Arbitrum reduce fees dramatically.**

# Your Safety Margin

When you borrow in DeFi, you have a **safety margin** — the gap between your collateral value and your debt.

Think of it like a fuel gauge:

- **Green zone:** Plenty of margin. Relax.
- **Yellow zone:** Getting close. Add more collateral.
- **Red zone:** Danger. Liquidation ahead.



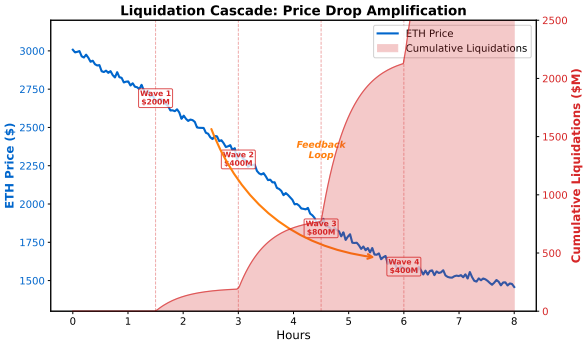

**The "Health Factor" (HF) measures how safe your loan is. Below 1.0, you get liquidated. See Appendix A3 for the formula.**

# When the Margin Runs Out

If your collateral drops too far, the protocol sells it to repay your debt. This is called **liquidation**.

Think of it like **car repossession**: if you stop making payments, the bank takes your car.

- Bots watch every loan 24/7
- They race to liquidate unhealthy loans
- They earn a bonus for doing it
- Cascading liquidations can crash prices



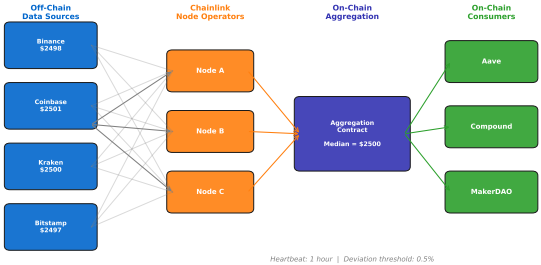

**On "Black Thursday" (March 2020), cascading liquidations wiped out over 8 million dollars on Maker in hours.**

# How DeFi Knows Prices

A lending protocol needs to know: "What is ETH worth right now?" It cannot Google it. It uses an **oracle**.

Think of an oracle like a **weather station network**: many independent stations report the temperature, and the system takes the middle value.

- Chainlink: most popular oracle
- Dozens of independent data sources
- Median value resists manipulation




**If the oracle is wrong, bad things happen. Oracle manipulation was behind several major DeFi exploits in 2022–2023.**

# Who Does What in Lending

Three groups make DeFi lending work:

**Depositors** — Earn interest

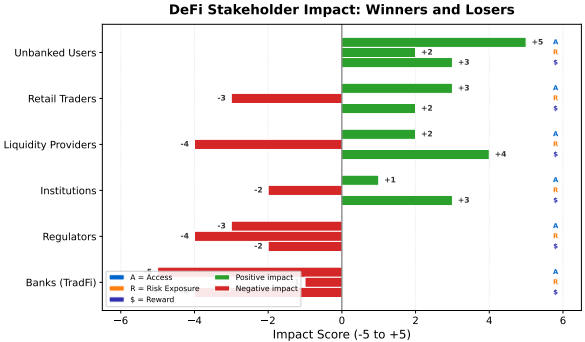
- Supply tokens to the pool
- Passive income from borrowers

**Borrowers** — Pay interest

- Lock up collateral to borrow
- Must keep safety margin healthy

**Liquidators** — Enforce safety

- Bots that close risky loans
- Earn a bonus on every liquidation



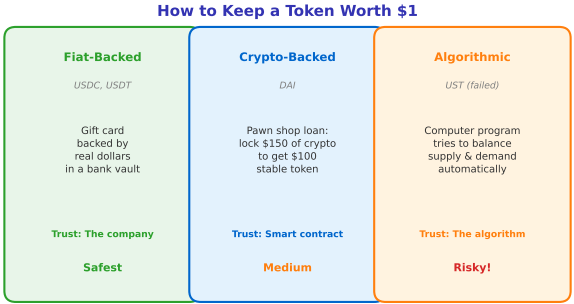

**Everyone is incentivized: depositors earn, borrowers access capital, liquidators keep the system safe.**

# Why Stable Crypto Matters

Crypto prices swing wildly. Bitcoin can drop 20 percent in a day. That makes it hard to use as everyday money.

**Stablecoins** are crypto tokens pegged to the dollar. One stablecoin always aims to be worth one dollar.

- Bridge between crypto and dollars
- Safe parking spot during volatility
- Used in nearly every DeFi protocol




**Total stablecoin market: over 300 billion dollars (2026). USDT and USDC hold about 80% of that market.**

# Three Roads to Stability

**Coat Check (Fiat-backed)**

Deposit real dollars in a bank. Mint one stablecoin per dollar. USDC, USDT.

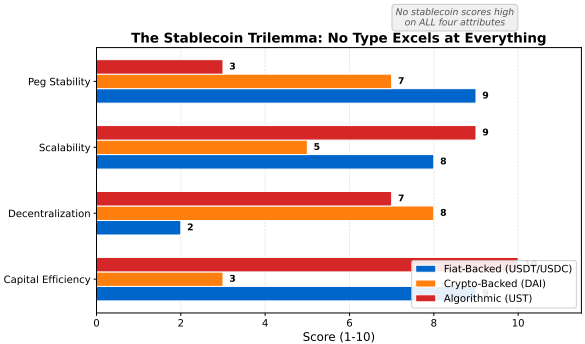
**Pawn Shop (Crypto-backed)**

Lock up 150 dollars of ETH. Mint 100 dollars of DAI. Over-collateralized.

**Promise (Algorithmic)**

No collateral. Code tries to maintain the peg with incentives alone. Very risky.

**The trilemma:** You can have two of three — stability, decentralization, capital efficiency — but not all three.




**USDC = stable + efficient but centralized. DAI = stable + decentralized but capital-heavy. Algo = efficient + decentralized but fragile.**

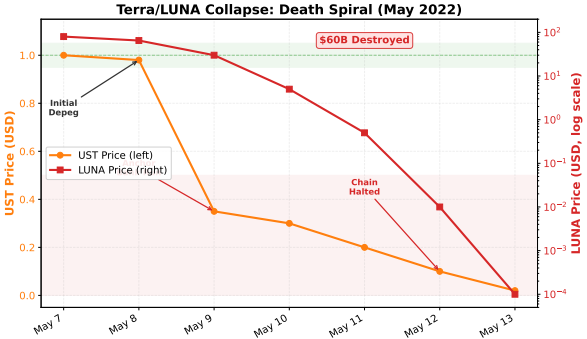
# The Terra Crash: 40 Billion Dollars Gone

In May 2022, the algorithmic stablecoin UST lost its dollar peg and never recovered.

**The two-friends analogy:** UST and LUNA promised to keep each other stable. When trust broke, both collapsed — like two drowning people pulling each other under.

**Timeline:**

- May 7: UST dips to 99 cents
- May 9: Panic selling begins
- May 12: UST hits 10 cents, LUNA near zero



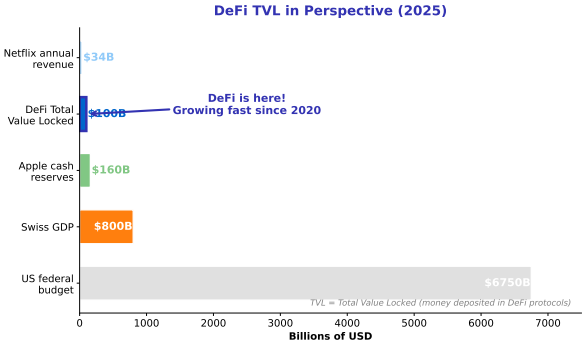

**The Terra collapse triggered a chain reaction: Three Arrows Capital, Celsius, Voyager, and eventually FTX all fell. See Appendix A5.**

# How Much Money Is in DeFi?

**Total Value Locked (TVL)** counts all the money sitting inside DeFi protocols. Think of it as DeFi's collective piggy bank.

**The journey:**

- 2020: 1 billion dollars (early days)
- 2021: 180 billion (the boom)
- 2022: 50 billion (the crash)
- 2026: about 90 billion (recovery)




**Source: DefiLlama. TVL fluctuates with crypto prices — a rising ETH price inflates TVL even without new deposits.**

# Yield Farming: Where Returns Come From

"Yield farming" means moving your tokens between protocols to earn the highest return. But where does the yield come from?

**Four real sources:**

1. Trading fees from swaps
2. Interest from borrowers
3. Token rewards from the protocol
4. Bonus incentives to attract liquidity

**Warning:** "If you cannot identify where the yield comes from, YOU are the yield."


**Sustainable yield comes from real economic activity (fees, interest). Unsustainable yield comes from printing new tokens.**

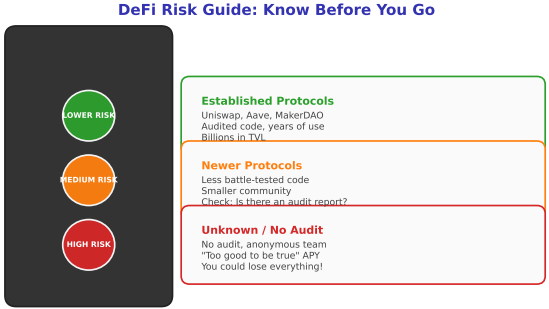
# The DeFi Risk Traffic Light

Not all DeFi protocols are equal. Use this simple traffic light:

**GREEN:** Audited code, years of operation, billions in TVL. Examples: Uniswap, Aave, MakerDAO.

**YELLOW:** Newer protocol, one audit, moderate TVL. Do your research. Check audit reports.

**RED:** No audit, anonymous team, unusually high yields. Probably a trap. Stay away.




**High yield + no audit = a red flag, not an opportunity. If it seems too good to be true, it almost certainly is.**

# Five Things That Can Go Wrong

## 1. Smart contract bugs

Code error lets hackers drain funds.

## 2. Oracle manipulation

Fake price feed tricks the protocol.

## 3. Governance attacks

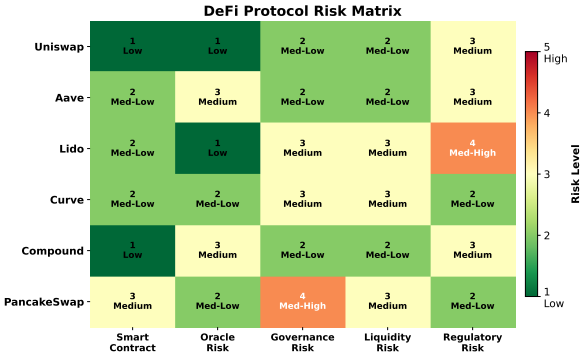
Someone buys enough votes to steal funds.

## 4. Liquidity crises

Everyone tries to withdraw at once.

## 5. Regulatory crackdown

Government shuts down access.




**In 2022–2023 alone, over 3 billion dollars was stolen from DeFi protocols through hacks and exploits.**

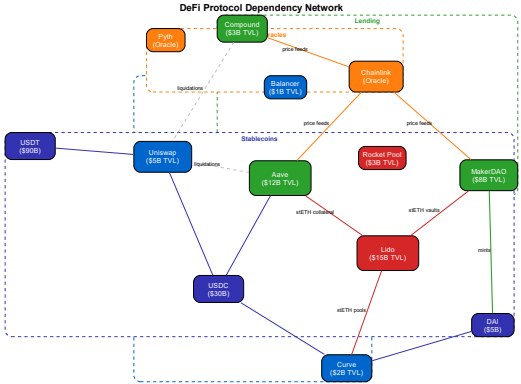
# The Domino Effect

DeFi's composability is a double-edged sword. Protocols depend on each other — when one falls, others can follow.

**2022: The year of dominoes**

- May: Terra/UST collapses
- June: Three Arrows Capital insolvent
- July: Celsius and Voyager bankrupt
- November: FTX implodes

Total losses: over 70 billion dollars across the industry.



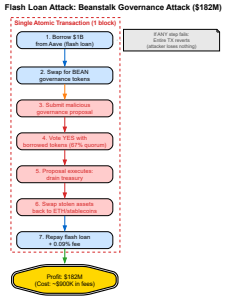

**Composability = "money LEGOs." Great for building, dangerous when one brick is rotten.**

# Flash Loans: Instant Millions

A **flash loan** lets you borrow millions of dollars for about 12 seconds — with zero collateral.

**How?** You borrow, use the money, and repay — all inside a single blockchain transaction. If you cannot repay, the entire transaction is canceled as if it never happened.

- Like time-travel money
- Used for arbitrage and liquidations
- Also used by hackers for attacks




**Flash loans are uniquely DeFi — impossible in traditional finance. See Appendix A4 for a worked example.**

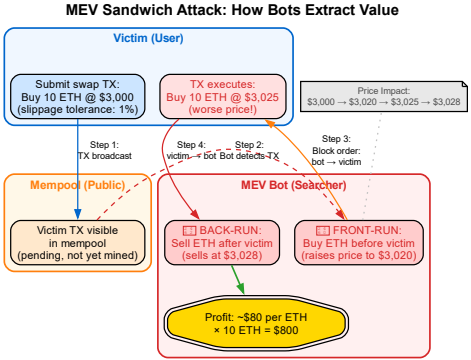
# The Invisible Tax: MEV

**MEV** (Maximal Extractable Value) is the invisible tax on your DeFi trades.

**The sandwich attack:**

1. You submit a big swap
2. A bot sees your pending trade
3. The bot buys before you (front-run)
4. Your trade executes at a worse price
5. The bot sells after you (back-run)

**Protection:** Use private mempools (Flashbots) or set tight slippage limits.




**MEV bots extracted over 600 million dollars from Ethereum users in 2022–2023. You are the prey.**

# Regulation Is Coming

### EU: MiCA

Full framework since December 2024. Stablecoin rules, exchange licensing, consumer protection.

**Status:** Active law

### US: SEC/CFTC

Enforcement-first approach. Lawsuits against exchanges. Ongoing debate in Congress.

**Status:** Uncertain

### Rest of World

Singapore, Dubai, Hong Kong building crypto hubs. China bans everything.

**Status:** Fragmented

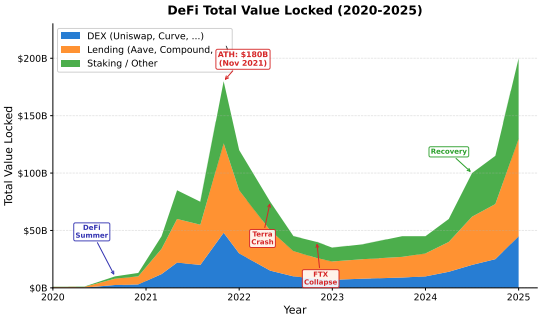
**Key question:** Can you regulate code that runs on a global, permissionless network?
DeFi protocols have no CEO to subpoena and no office to raid.

---

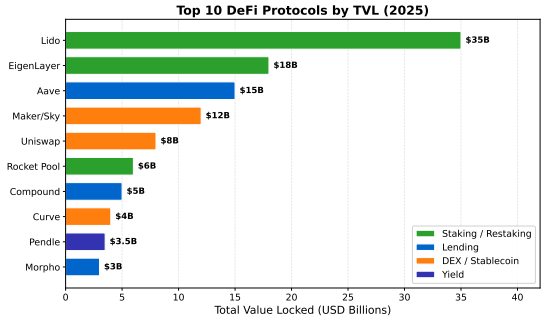
**MiCA (Markets in Crypto-Assets) is the world's first comprehensive crypto regulation. Effective December 30, 2024.**

# DeFi Market Today

## TVL Over Time




## TVL by Protocol



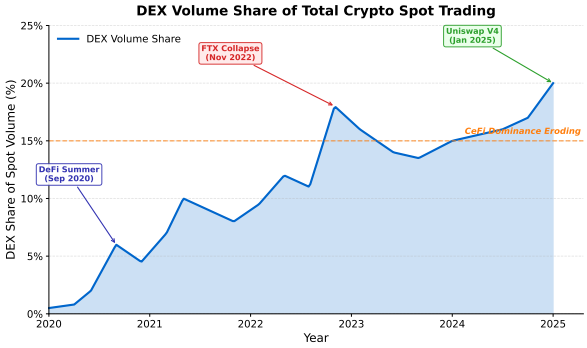

**Source: DefiLlama, January 2026. Lido, Aave, and EigenLayer are the largest protocols by TVL.**

# Who's Trading Where?

The share of trading happening on decentralized exchanges (DEXs) keeps growing.

- 2020: DEXs handled under 1% of volume
- 2023: DEXs crossed 15% of spot volume
- 2025: DEX share continues climbing

The shift is driven by self-custody, transparency, and distrust after the FTX collapse.



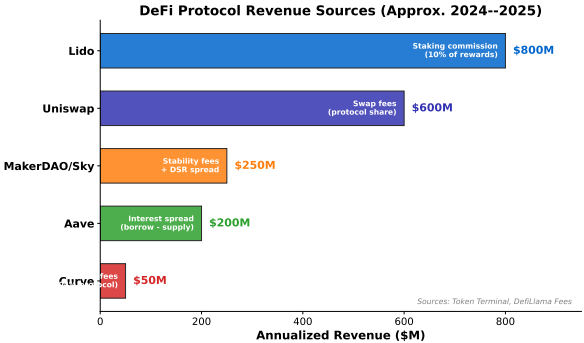

**CEX = Centralized Exchange (Binance, Coinbase). DEX = Decentralized Exchange (Uniswap, Curve). After FTX, "not your keys" hit home.**

# Is DeFi a Real Business?

Some DeFi protocols earn real revenue from real users — not just token inflation.

- Uniswap: earns fees on every swap
- Aave: earns a spread on lending
- Lido: earns a cut of staking rewards
- MakerDAO: earns interest on DAI loans

The question is no longer “Can DeFi make money?” but “Which protocols have sustainable business models?”




**MakerDAO earned over 200 million dollars in annualized revenue in 2024, partly from US Treasury exposure.**

# Key Takeaways

## What DeFi Does

Replaces banks with code. Trade, lend, and save without intermediaries. Open 24/7. Permissionless.

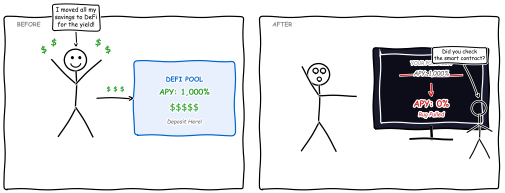
## Why It Matters

Financial access for everyone. Transparent rules. Composable building blocks. Real revenue.

## What Can Go Wrong

Smart contract bugs, oracle attacks, cascading failures, scams, and regulatory uncertainty.

DeFi Yield Farming: A Cautionary Tale




"In DeFi, if you don't understand where the yield comes from, you ARE the yield."

**DeFi is a real innovation with real risks. Understand both before you put real money in.**

# Appendix

Technical Deep Dives

The math behind the intuition

Click blue links in appendix slides to jump back to the main deck.

# A1: The Constant Product Rule

The AMM uses one elegant equation to set prices automatically:

$$x \cdot y = k$$

- $x$ = quantity of Token A in the pool (e.g., ETH)
- $y$ = quantity of Token B in the pool (e.g., USDC)
- $k$ = a constant that never changes during a trade
- When traders remove Token A, they must add enough Token B to keep $k$ the same

# A1: The Constant Product Rule

The AMM uses one elegant equation to set prices automatically:

$$x \cdot y = k$$

- $x$ = quantity of Token A in the pool (e.g., ETH)
- $y$ = quantity of Token B in the pool (e.g., USDC)
- $k$ = a constant that never changes during a trade
- When traders remove Token A, they must add enough Token B to keep $k$ the same

**Spot price** at any moment: Price of A in terms of B = $\frac{y}{x}$

← Back to main slide: How Prices Change

---

**Uniswap V2 uses this exact formula. V3 adds concentrated liquidity ranges on top of it.**

# A1: Worked Example — Buying 5 ETH

**Pool:** 100 ETH and 200,000 USDC. $k = 100 \times 200{,}000 = 20{,}000{,}000$

**Spot price before trade:** $\frac{200{,}000}{100} = 2{,}000$ USDC per ETH

# A1: Worked Example — Buying 5 ETH

**Pool:** 100 ETH and 200,000 USDC. $k = 100 \times 200{,}000 = 20{,}000{,}000$

**Spot price before trade:** $\frac{200{,}000}{100} = 2{,}000$ USDC per ETH

**You want to buy 5 ETH.** After the trade, the pool has $100 - 5 = 95$ ETH.

New USDC amount: $y' = \frac{k}{x'} = \frac{20{,}000{,}000}{95} = 210{,}526.32$

# A1: Worked Example — Buying 5 ETH

**Pool:** 100 ETH and 200,000 USDC. $k = 100 \times 200{,}000 = 20{,}000{,}000$

**Spot price before trade:** $\frac{200{,}000}{100} = 2{,}000$ USDC per ETH

**You want to buy 5 ETH.** After the trade, the pool has $100 - 5 = 95$ ETH.

New USDC amount: $y' = \frac{k}{x'} = \frac{20{,}000{,}000}{95} = 210{,}526.32$

**You pay:** $210{,}526.32 - 200{,}000 = \mathbf{10{,}526.32}$ USDC for 5 ETH

**Average price:** $\frac{10{,}526.32}{5} = \mathbf{2{,}105.26}$ USDC per ETH

# A1: Worked Example — Buying 5 ETH

**Pool:** 100 ETH and 200,000 USDC. $k = 100 \times 200{,}000 = 20{,}000{,}000$

**Spot price before trade:** $\frac{200{,}000}{100} = 2{,}000$ USDC per ETH

**You want to buy 5 ETH.** After the trade, the pool has $100 - 5 = 95$ ETH.

New USDC amount: $y' = \frac{k}{x'} = \frac{20{,}000{,}000}{95} = 210{,}526.32$

**You pay:** $210{,}526.32 - 200{,}000 = \mathbf{10{,}526.32}$ USDC for 5 ETH

**Average price:** $\frac{10{,}526.32}{5} = \mathbf{2{,}105.26}$ USDC per ETH

**Slippage:** $\frac{2{,}105.26 - 2{,}000}{2{,}000} = \mathbf{5.26\%}$ above spot price

Buying just 5% of the pool's ETH already costs you 5.26% extra. This is why pool size matters.

**Larger pools = less slippage. A pool with 10,000 ETH would give only 0.05% slippage for the same trade.**

# A1: Slippage Formula

For a trade of size $\Delta x$ in a pool of size $x$:

$$\text{Slippage} = \frac{\Delta x}{x - \Delta x}$$

# A1: Slippage Formula

For a trade of size $\Delta x$ in a pool of size $x$:

$$\text{Slippage} = \frac{\Delta x}{x - \Delta x}$$

**Examples with a 100 ETH pool:**

| Trade Size | $\Delta x$ | Pool After | Slippage |
|---|---|---|---|
| Buy 1 ETH | 1 | 99 ETH | $\frac{1}{99} = 1.01\%$ |
| Buy 5 ETH | 5 | 95 ETH | $\frac{5}{95} = 5.26\%$ |
| Buy 10 ETH | 10 | 90 ETH | $\frac{10}{90} = 11.11\%$ |
| Buy 50 ETH | 50 | 50 ETH | $\frac{50}{50} = 100\%$ |

← Back to main slide: Why Bigger Trades Cost More

**Slippage grows exponentially with trade size. Never buy more than 1–2% of a pool in a single trade.**

# A1: Trading Fees in AMMs

Uniswap charges a fee on every swap that goes to liquidity providers:

| Fee Tier | Fee | Best For |
|---|---|---|
| Stablecoin pairs | 0.01% | USDC/USDT |
| Standard pairs | 0.05% or 0.30% | ETH/USDC |
| Exotic pairs | 1.00% | Low-liquidity tokens |

# A1: Trading Fees in AMMs

Uniswap charges a fee on every swap that goes to liquidity providers:

| Fee Tier | Fee | Best For |
|---|---|---|
| Stablecoin pairs | 0.01% | USDC/USDT |
| Standard pairs | 0.05% or 0.30% | ETH/USDC |
| Exotic pairs | 1.00% | Low-liquidity tokens |

**Fee calculation:** On a 10,000 USDC swap at 0.30% fee:

- Fee paid: $10{,}000 \times 0.003 = 30$ USDC
- You receive tokens worth: $10{,}000 - 30 = 9{,}970$ USDC equivalent
- The 30 USDC is added to the pool (increases $k$ slightly)

# A1: Trading Fees in AMMs

Uniswap charges a fee on every swap that goes to liquidity providers:

| Fee Tier | Fee | Best For |
|---|---|---|
| Stablecoin pairs | 0.01% | USDC/USDT |
| Standard pairs | 0.05% or 0.30% | ETH/USDC |
| Exotic pairs | 1.00% | Low-liquidity tokens |

**Fee calculation:** On a 10,000 USDC swap at 0.30% fee:

- Fee paid: $10{,}000 \times 0.003 = 30$ USDC
- You receive tokens worth: $10{,}000 - 30 = 9{,}970$ USDC equivalent
- The 30 USDC is added to the pool (increases $k$ slightly)

**Uniswap V4** (launched January 2025) introduces "hooks" — custom code that runs before or after swaps, enabling dynamic fees, limit orders, and more.

**Fees compound over time. A busy pool at 0.30% can generate 20–50% annualized returns for LPs.**

# A2: Impermanent Loss — The Formula

If the price ratio between two tokens changes by a factor $r$:

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

Where $r = \frac{\text{new price}}{\text{original price}}$.

# A2: Impermanent Loss — The Formula

If the price ratio between two tokens changes by a factor $r$:

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

Where $r = \frac{\text{new price}}{\text{original price}}$.

**Key insight:** IL depends only on the *magnitude* of price change, not the direction. A 2x increase and a 2x decrease produce the same IL.

← Back to main slide: Earning Fees (and a Hidden Cost)

**IL is "impermanent" because it reverses if the price returns to the original ratio. But if you withdraw, the loss is locked in.**

# A2: Worked Example — ETH Doubles in Price

**Start:** You deposit 1 ETH + 2,000 USDC (total value: 4,000 USDC).

**ETH doubles** from 2,000 to 4,000 USDC. Price ratio $r = 2$.

# A2: Worked Example — ETH Doubles in Price

**Start:** You deposit 1 ETH + 2,000 USDC (total value: 4,000 USDC).

**ETH doubles** from 2,000 to 4,000 USDC. Price ratio $r = 2$.

**If you just held (no pool):**

- 1 ETH at 4,000 + 2,000 USDC = **6,000 USDC total**

# A2: Worked Example — ETH Doubles in Price

**Start:** You deposit 1 ETH + 2,000 USDC (total value: 4,000 USDC).

**ETH doubles** from 2,000 to 4,000 USDC. Price ratio $r = 2$.

**If you just held (no pool):**

- 1 ETH at 4,000 + 2,000 USDC = **6,000 USDC total**

**In the pool (constant product rebalances):**

- Pool rebalances to: 0.707 ETH + 2,828 USDC
- Value: $(0.707 \times 4{,}000) + 2{,}828 = \mathbf{5{,}656}$ USDC

# A2: Worked Example — ETH Doubles in Price

**Start:** You deposit 1 ETH + 2,000 USDC (total value: 4,000 USDC).

**ETH doubles** from 2,000 to 4,000 USDC. Price ratio $r = 2$.

**If you just held (no pool):**

- 1 ETH at 4,000 + 2,000 USDC = **6,000 USDC total**

**In the pool (constant product rebalances):**

- Pool rebalances to: 0.707 ETH + 2,828 USDC
- Value: $(0.707 \times 4{,}000) + 2{,}828 = \mathbf{5{,}656}$ USDC

**Impermanent loss:** $6{,}000 - 5{,}656 = \mathbf{344}$ USDC $(-5.72\%)$

**Check with formula:** $\text{IL} = \frac{2\sqrt{2}}{1+2} - 1 = \frac{2.828}{3} - 1 = -5.72\%$ ✓

---

**You still made money (4,000 → 5,656) but you made LESS than if you had simply held your tokens.**

# A2: Impermanent Loss Reference Table

| Price Change | Ratio $r$ | Impermanent Loss |
|---|---|---|
| $+25\%$ | 1.25 | $-0.60\%$ |
| $+50\%$ | 1.50 | $-2.02\%$ |
| $+100\%$ (2x) | 2.00 | $-5.72\%$ |
| $+200\%$ (3x) | 3.00 | $-13.40\%$ |
| $+400\%$ (5x) | 5.00 | $-25.46\%$ |
| $-50\%$ (halved) | 0.50 | $-5.72\%$ |
| $-75\%$ | 0.25 | $-20.00\%$ |

# A2: Impermanent Loss Reference Table

| Price Change | Ratio $r$ | Impermanent Loss |
|---|---|---|
| +25% | 1.25 | −0.60% |
| +50% | 1.50 | −2.02% |
| +100% (2x) | 2.00 | −5.72% |
| +200% (3x) | 3.00 | −13.40% |
| +400% (5x) | 5.00 | −25.46% |
| −50% (halved) | 0.50 | −5.72% |
| −75% | 0.25 | −20.00% |

**Rules of thumb:**

- Small price moves (under 25%): IL is negligible, fees likely cover it
- Moderate moves (25–100%): IL matters, check if fees compensate
- Large moves (over 200%): IL is severe, you would have been better off holding

← Back to main slide

**Concentrated liquidity (V3) amplifies both fees AND impermanent loss. Higher reward, higher risk.**

# A3: Health Factor — The Formula

$$\text{HF} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Total Debt}}$$

- $\text{HF} > 1.0$: Loan is safe
- $\text{HF} = 1.0$: Liquidation can begin
- $\text{HF} < 1.0$: Protocol is losing money (should not happen)

# A3: Health Factor — The Formula

$$\text{HF} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Total Debt}}$$

- $\text{HF} > 1.0$: Loan is safe
- $\text{HF} = 1.0$: Liquidation can begin
- $\text{HF} < 1.0$: Protocol is losing money (should not happen)

**Liquidation Threshold (LT)** varies by asset:

| Asset | LT | Max Borrow |
|---|---|---|
| ETH | 82.5% | 82.5% of collateral |
| WBTC | 75% | 75% of collateral |
| LINK | 65% | 65% of collateral |

← Back to main slide: Your Safety Margin

**Source: Aave V3 risk parameters. More volatile assets get lower LTs to protect the protocol.**

# A3: Worked Example — ETH Drops, HF Drops

**Setup:** You deposit 5 ETH at \$2,000 each. LT = 82.5%. You borrow \$5,200 USDC.

# A3: Worked Example — ETH Drops, HF Drops

**Setup:** You deposit 5 ETH at \$2,000 each. LT = 82.5%. You borrow \$5,200 USDC.

**Initial HF:** $\frac{(5 \times 2{,}000) \times 0.825}{5{,}200} = \frac{8{,}250}{5{,}200} = \mathbf{1.587}$ **Safe**

# A3: Worked Example — ETH Drops, HF Drops

**Setup:** You deposit 5 ETH at \$2,000 each. LT = 82.5%. You borrow \$5,200 USDC.

**Initial HF:** $\frac{(5 \times 2{,}000) \times 0.825}{5{,}200} = \frac{8{,}250}{5{,}200} = \mathbf{1.587}$ **Safe**

**ETH drops to \$1,500:** $\frac{(5 \times 1{,}500) \times 0.825}{5{,}200} = \frac{6{,}187.50}{5{,}200} = \mathbf{1.190}$ **Caution**

# A3: Worked Example — ETH Drops, HF Drops

**Setup:** You deposit 5 ETH at \$2,000 each. LT = 82.5%. You borrow \$5,200 USDC.

**Initial HF:** $\frac{(5 \times 2{,}000) \times 0.825}{5{,}200} = \frac{8{,}250}{5{,}200} = \mathbf{1.587}$ **Safe**

**ETH drops to \$1,500:** $\frac{(5 \times 1{,}500) \times 0.825}{5{,}200} = \frac{6{,}187.50}{5{,}200} = \mathbf{1.190}$ **Caution**

**ETH drops to \$1,300:** $\frac{(5 \times 1{,}300) \times 0.825}{5{,}200} = \frac{5{,}362.50}{5{,}200} = \mathbf{1.031}$ **Danger!**

# A3: Worked Example — ETH Drops, HF Drops

**Setup:** You deposit 5 ETH at \$2,000 each. LT = 82.5%. You borrow \$5,200 USDC.

**Initial HF:** $\frac{(5 \times 2{,}000) \times 0.825}{5{,}200} = \frac{8{,}250}{5{,}200} = \mathbf{1.587}$ **Safe**

**ETH drops to \$1,500:** $\frac{(5 \times 1{,}500) \times 0.825}{5{,}200} = \frac{6{,}187.50}{5{,}200} = \mathbf{1.190}$ **Caution**

**ETH drops to \$1,300:** $\frac{(5 \times 1{,}300) \times 0.825}{5{,}200} = \frac{5{,}362.50}{5{,}200} = \mathbf{1.031}$ **Danger!**

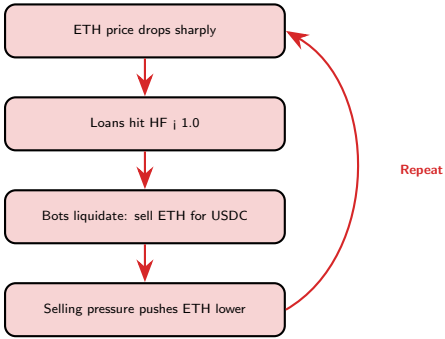
**ETH drops to \$1,260:** $\frac{(5 \times 1{,}260) \times 0.825}{5{,}200} = \frac{5{,}197.50}{5{,}200} = \mathbf{0.9995}$ **LIQUIDATED**

A bot seizes part of your ETH, sells it, and repays your debt. You lose a 5% liquidation penalty.

**Liquidation penalty: the bot gets a 5% bonus for liquidating you. On \$5,200 debt, that is \$260 lost.**

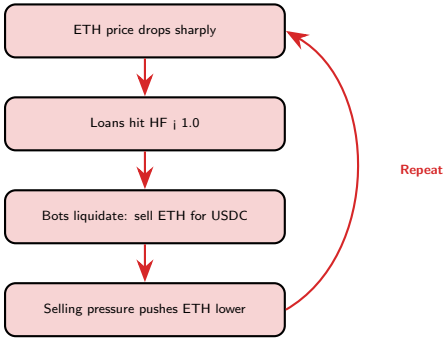
# A3: Liquidation Cascades

When many loans get liquidated at once, it creates a dangerous feedback loop:



# A3: Liquidation Cascades

When many loans get liquidated at once, it creates a dangerous feedback loop:



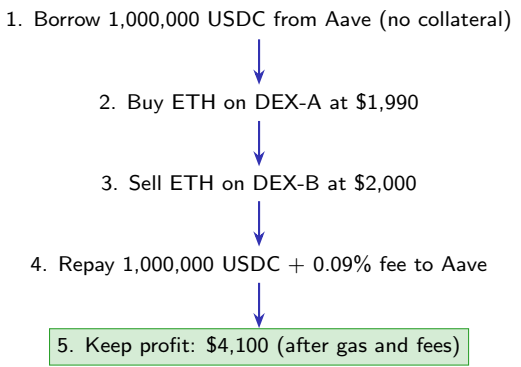

**March 12, 2020 ("Black Thursday"):** ETH fell 43% in one day. Over $8.3M liquidated on MakerDAO. Some vaults were liquidated for zero due to network congestion.

← Back to main slide

**Protocols now use "gradual liquidation" (liquidate 50% of position, not 100%) to reduce cascade risk.**

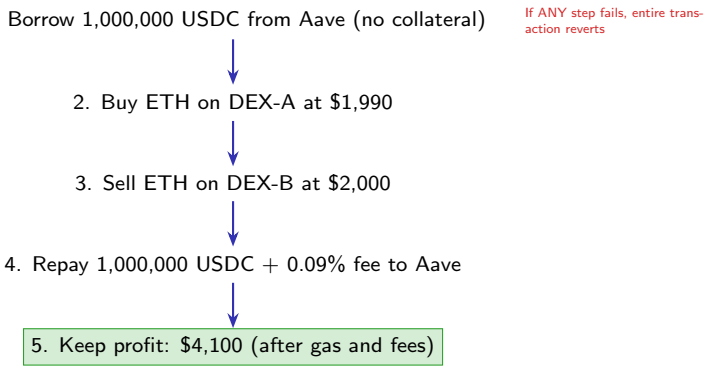
# A4: Flash Loan — How It Works

A flash loan is an **atomic transaction**: everything happens in one block, or nothing happens at all.



# A4: Flash Loan — How It Works

A flash loan is an **atomic transaction**: everything happens in one block, or nothing happens at all.




**Fee:** Aave charges 0.09% (= 900 USDC on a 1M loan). Gas: about $50. Net profit: $4,100.

**Flash loans democratize arbitrage: you do not need capital, just a smart contract and a price discrepancy.**

# A4: Flash Loan Attack — Price Manipulation

Flash loans can also be used maliciously to manipulate prices:

1. **Borrow** 10M USDC via flash loan
2. **Dump** tokens on DEX-A, crashing the price
3. **Exploit** a lending protocol that reads DEX-A's price as an oracle
4. **Borrow** underpriced collateral at the manipulated price
5. **Repay** flash loan, keep the extra collateral

# A4: Flash Loan Attack — Price Manipulation

Flash loans can also be used maliciously to manipulate prices:

1. **Borrow** 10M USDC via flash loan
2. **Dump** tokens on DEX-A, crashing the price
3. **Exploit** a lending protocol that reads DEX-A's price as an oracle
4. **Borrow** underpriced collateral at the manipulated price
5. **Repay** flash loan, keep the extra collateral

**Real example — bZx (Feb 2020):**

- Attacker borrowed 10,000 ETH via flash loan
- Manipulated the sUSD price on Kyber
- Profited approximately $350,000 in a single transaction
- Total time: about 15 seconds (one Ethereum block)

---

**Defense: use time-weighted average prices (TWAP) instead of spot prices. Chainlink oracles resist flash loan manipulation.**

# A4: MEV Sandwich Attack — Step by Step

**You** want to buy 50 ETH on Uniswap. A **MEV bot** sees your pending transaction:

| Order | Action | ETH Price | Who Profits |
|---|---|---|---|
| 1 | Bot buys 20 ETH (front-run) | \$2,000 $\rightarrow$ \$2,020 | — |

# A4: MEV Sandwich Attack — Step by Step

**You** want to buy 50 ETH on Uniswap. A **MEV bot** sees your pending transaction:

| Order | Action | ETH Price | Who Profits |
|---|---|---|---|
| 1 | Bot buys 20 ETH (front-run) | \$2,000 → \$2,020 | — |
| 2 | Your trade: buy 50 ETH | \$2,020 → \$2,080 | — |

# A4: MEV Sandwich Attack — Step by Step

**You** want to buy 50 ETH on Uniswap. A **MEV bot** sees your pending transaction:

| Order | Action | ETH Price | Who Profits |
|---|---|---|---|
| 1 | Bot buys 20 ETH (front-run) | \$2,000 → \$2,020 | — |
| 2 | Your trade: buy 50 ETH | \$2,020 → \$2,080 | — |
| 3 | Bot sells 20 ETH (back-run) | \$2,080 → \$2,060 | Bot: +\$60/ETH |
| | **Bot profit:** | | ∼\$1,200 |
| | **Your extra cost:** | | ∼\$20/ETH |

# A4: MEV Sandwich Attack — Step by Step

**You** want to buy 50 ETH on Uniswap. A **MEV bot** sees your pending transaction:

| Order | Action | ETH Price | Who Profits |
|---|---|---|---|
| 1 | Bot buys 20 ETH (front-run) | \$2,000 → \$2,020 | — |
| 2 | Your trade: buy 50 ETH | \$2,020 → \$2,080 | — |
| 3 | Bot sells 20 ETH (back-run) | \$2,080 → \$2,060 | Bot: +\$60/ETH |
| | **Bot profit:** | | ∼\$1,200 |
| | **Your extra cost:** | | ∼\$20/ETH |

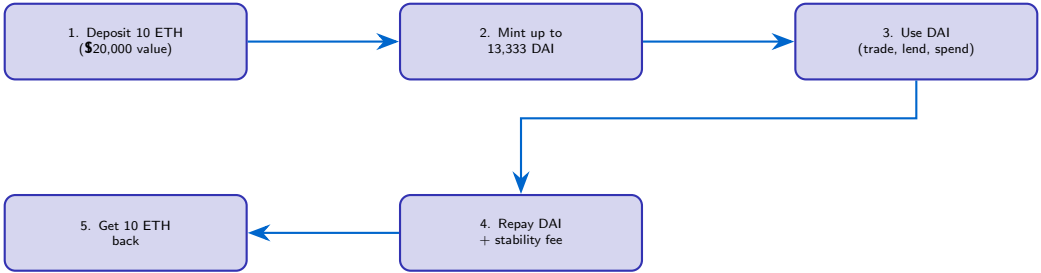
**Protection strategies:**

- Use Flashbots Protect (private mempool — bots cannot see your trade)
- Set tight slippage tolerance (reject trades above your max price)
- Break large trades into smaller pieces

**Flashbots Protect:** `rpc.flashbots.net`**. Free to use. Hides your transactions from sandwich bots.**

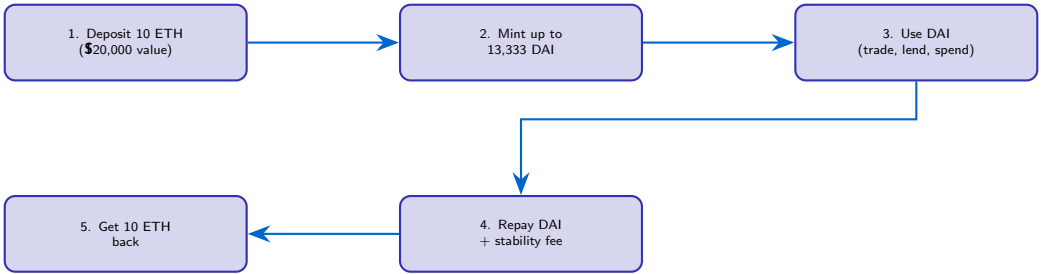
# A5: How DAI Works — Vault Mechanics

DAI is minted through MakerDAO "vaults" (previously called CDPs):



# A5: How DAI Works — Vault Mechanics

DAI is minted through MakerDAO "vaults" (previously called CDPs):




**Key numbers:**

- Minimum collateral ratio: 150% (deposit $150 to borrow $100)
- Stability fee: variable (currently 3–8% APR, set by governance)
- Liquidation penalty: 13% if your vault falls below 150%

**DAI is "decentralized" because anyone can mint it, and the rules are enforced by code, not a company.**

# A5: How DAI Stays at One Dollar

MakerDAO uses interest rates to push DAI back to $1.00:

| Condition | Governance Action | Effect |
|---|---|---|

# A5: How DAI Stays at One Dollar

MakerDAO uses interest rates to push DAI back to \$1.00:

| Condition | Governance Action | Effect |
|---|---|---|
| DAI $>$ \$1.00 | Lower stability fee | Cheaper to borrow $\rightarrow$ more DAI minted $\rightarrow$ price drops |

# A5: How DAI Stays at One Dollar

MakerDAO uses interest rates to push DAI back to \$1.00:

| Condition | Governance Action | Effect |
|---|---|---|
| DAI $>$ \$1.00 | Lower stability fee | Cheaper to borrow $\rightarrow$ more DAI minted $\rightarrow$ price drops |
| DAI $<$ \$1.00 | Raise stability fee | Expensive to borrow $\rightarrow$ DAI repaid $\rightarrow$ supply shrinks $\rightarrow$ price rises |

# A5: How DAI Stays at One Dollar

MakerDAO uses interest rates to push DAI back to $1.00:

| Condition | Governance Action | Effect |
|---|---|---|
| DAI $>$ \$1.00 | Lower stability fee | Cheaper to borrow $\rightarrow$ more DAI minted $\rightarrow$ price drops |
| DAI $<$ \$1.00 | Raise stability fee | Expensive to borrow $\rightarrow$ DAI repaid $\rightarrow$ supply shrinks $\rightarrow$ price rises |
| DAI $\ll$ \$1.00 | Emergency shutdown | All vaults unwound, DAI redeemed at \$1 from collateral |

**Additional tool — the DAI Savings Rate (DSR):**

- When DAI is above \$1: lower DSR (less demand to hold DAI)
- When DAI is below \$1: raise DSR (more demand to hold DAI)

**MakerDAO rebranded to "Sky" in 2024 (DAI $\rightarrow$ USDS, MKR $\rightarrow$ SKY), but the core mechanics remain identical.**

# A5: Terra/Luna Death Spiral — Day by Day

| Date | UST Price | What Happened |
|---|---|---|
| May 7 | $0.985 | Large withdrawals from Anchor protocol ($2B in 2 days) |

# A5: Terra/Luna Death Spiral — Day by Day

| Date | UST Price | What Happened |
|---|---|---|
| May 7 | $0.985 | Large withdrawals from Anchor protocol ($2B in 2 days) |
| May 8 | $0.98 | Luna Foundation Guard deploys $1.5B Bitcoin reserves to defend peg |

# A5: Terra/Luna Death Spiral — Day by Day

| Date | UST Price | What Happened |
|---|---|---|
| May 7 | $0.985 | Large withdrawals from Anchor protocol ($2B in 2 days) |
| May 8 | $0.98 | Luna Foundation Guard deploys $1.5B Bitcoin reserves to defend peg |
| May 9 | $0.90 | Mint/burn mechanism floods market with LUNA; LUNA price collapses |

# A5: Terra/Luna Death Spiral — Day by Day

| Date | UST Price | What Happened |
|---|---|---|
| May 7 | \$0.985 | Large withdrawals from Anchor protocol (\$2B in 2 days) |
| May 8 | \$0.98 | Luna Foundation Guard deploys \$1.5B Bitcoin reserves to defend peg |
| May 9 | \$0.90 | Mint/burn mechanism floods market with LUNA; LUNA price collapses |
| May 10 | \$0.60 | Death spiral: UST depeg $\rightarrow$ mint LUNA $\rightarrow$ LUNA crashes $\rightarrow$ UST depegs further |

# A5: Terra/Luna Death Spiral — Day by Day

| Date | UST Price | What Happened |
|---|---|---|
| May 7 | \$0.985 | Large withdrawals from Anchor protocol (\$2B in 2 days) |
| May 8 | \$0.98 | Luna Foundation Guard deploys \$1.5B Bitcoin reserves to defend peg |
| May 9 | \$0.90 | Mint/burn mechanism floods market with LUNA; LUNA price collapses |
| May 10 | \$0.60 | Death spiral: UST depeg $\rightarrow$ mint LUNA $\rightarrow$ LUNA crashes $\rightarrow$ UST depegs further |
| May 11 | \$0.30 | LUNA supply explodes from 350M to 6.5 trillion tokens |

# A5: Terra/Luna Death Spiral — Day by Day

| Date | UST Price | What Happened |
|---|---|---|
| May 7 | \$0.985 | Large withdrawals from Anchor protocol (\$2B in 2 days) |
| May 8 | \$0.98 | Luna Foundation Guard deploys \$1.5B Bitcoin reserves to defend peg |
| May 9 | \$0.90 | Mint/burn mechanism floods market with LUNA; LUNA price collapses |
| May 10 | \$0.60 | Death spiral: UST depeg $\rightarrow$ mint LUNA $\rightarrow$ LUNA crashes $\rightarrow$ UST depegs further |
| May 11 | \$0.30 | LUNA supply explodes from 350M to 6.5 trillion tokens |
| May 12 | \$0.10 | Chain halted. \$40B market cap destroyed. |

**Root cause:** Anchor offered 20% APY on UST deposits, attracting \$14B. When withdrawals exceeded reserves, the algorithm could not mint enough LUNA fast enough, and both tokens entered a hyperinflationary death spiral.

**Do Kwon was extradited to the US in 2024. Algorithmic stablecoins without external collateral remain widely distrusted.**

# A6: APR vs APY — The Compounding Effect

**APR** = Annual Percentage Rate (simple interest, no compounding)
**APY** = Annual Percentage Yield (with compounding)

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

Where $n$ = number of compounding periods per year.

# A6: APR vs APY — The Compounding Effect

**APR** = Annual Percentage Rate (simple interest, no compounding)
**APY** = Annual Percentage Yield (with compounding)

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

Where $n$ = number of compounding periods per year.

**Example:** 12% APR compounded at different frequencies:

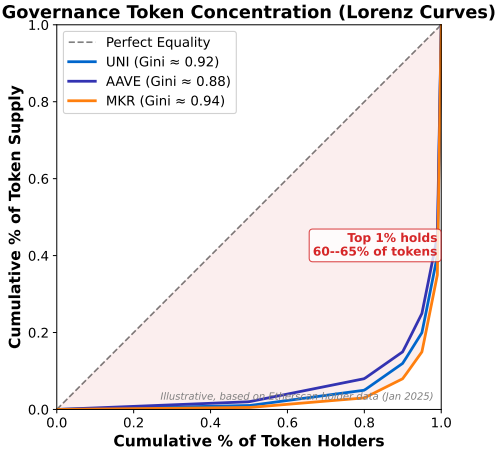
| **Compounding** | $n$ | **APY** |
|---|---|---|
| Yearly | 1 | 12.00% |
| Monthly | 12 | 12.68% |
| Daily | 365 | 12.75% |
| Per block ($\sim$12 sec) | 2,628,000 | 12.75% |

**DeFi protocols often auto-compound. A "12% APR" vault that compounds daily is really 12.75% APY.**

**“Governance theater”: many protocols are effectively controlled by the founding team and a few large investors.**

**The reality of governance:**

- Uniswap (UNI): top 10 wallets control over 40% of voting power
- Typical voter turnout: 2–5% of token supply
- Most governance tokens have no revenue share — they only grant voting rights




**"Governance theater": many protocols are effectively controlled by the founding team and a few large investors.**

Most DeFi protocols are governed by token holders who vote on proposals:

# A7: The Cryptoeconomics Lens Applied to DeFi

c

| Question | Applied to DeFi |
|---|---|
| 1. Problem | How do we provide financial services (trading, lending, saving) without trusted intermediaries like banks? |
| 2. Incentives | LPs earn fees, depositors earn interest, liquidators earn bonuses, validators earn gas fees. Everyone profits by keeping the system running. |
| 3. Benefits/Costs | Benefits: permissionless access, transparency, composability. Costs: smart contract risk, gas fees, complexity. |
| 4. Failure Mode | Terra collapse ($40B), smart contract hacks ($3B+ in 2022–2023), oracle manipulation, governance attacks. |
| 5. Design | AMM vs. order book, over-collateralized vs. algorithmic stablecoins, on-chain vs. off-chain oracles. |
| 6. Alternatives | Layer-2 scaling, intent-based trading, real-world asset tokenization, centralized hybrid models. |

**These six questions are the "Cryptoeconomics Lens" — apply them to every blockchain topic you study.**

# A7: The DeFi Design Space

Every DeFi protocol navigates fundamental trade-offs:

**Trading:**

- AMM (simple, always liquid) vs. Order book (efficient, complex)
- Constant product vs. concentrated liquidity
- On-chain execution vs. off-chain matching

**Lending:**

- Over-collateralized (safe, capital-heavy) vs. under-collateralized (efficient, risky)
- Pool-based (Aave) vs. peer-to-peer (Morpho)
- Fixed rate vs. variable rate

**Stablecoins:**

- Fiat-backed (stable, centralized) vs. crypto-backed (decentralized, over-collateralized)
- Algorithmic (capital-efficient, fragile)
- Hybrid approaches (FRAX, RAI)

**Governance:**

- Token voting (plutocratic) vs. reputation (meritocratic)
- On-chain (transparent, slow) vs. multi-sig (fast, centralized)
- Optimistic (default approve) vs. active (default reject)

---

**There is no "best" design — only trade-offs. The art of cryptoeconomics is choosing the right trade-off for your use case.**