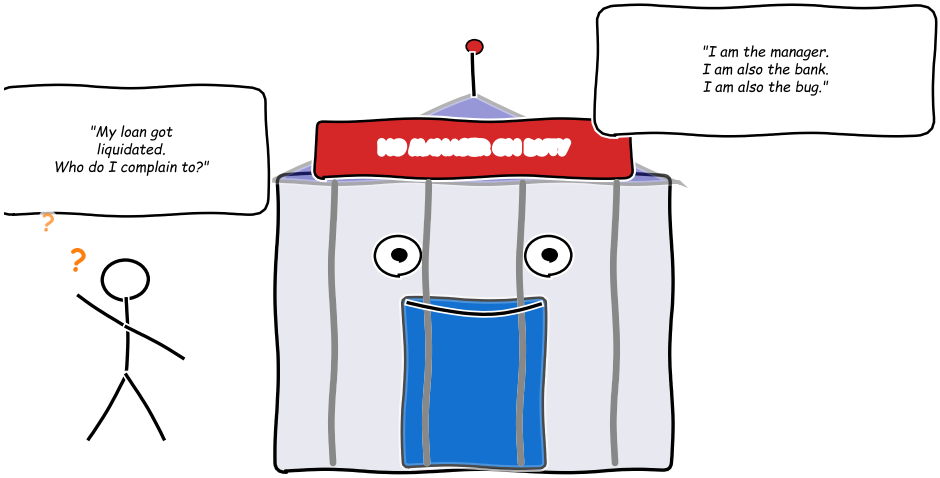
Lesson 3.4: DeFi, Stablecoins, and Tokenomics

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

The Bank With No Manager



DeFi: the bank runs itself. The exit interview is a liquidation event.

Learning Objectives

After completing this lesson, you will be able to:

1. **Explain** how an automated market maker (AMM) uses the constant product formula $x \cdot y = k$ to set prices without an order book [Understand]
2. **Calculate** impermanent loss for a liquidity provider given a price change [Apply]
3. **Trace** the lifecycle of a DeFi lending position from deposit through liquidation [Apply]
4. **Compare** the three stablecoin architectures and identify the risk profile of each [Analyze]
5. **Evaluate** how flash loans, reentrancy attacks, and oracle manipulation exploit DeFi protocols [Evaluate]

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

Objectives follow Bloom's taxonomy: Understand → Apply → Analyze → Evaluate.

From Smart Contracts to Decentralized Finance

Lesson 3.3 showed us: Smart contracts execute financial logic automatically.

This lesson asks: We can program finance. But **what happens when the code has bugs?**

DeFi recreates financial primitives without intermediaries:

- **Exchanges** → Automated market makers
- **Banks** → Lending protocols
- **Currencies** → Stablecoins
- **Stocks** → Governance tokens

But new risks emerge: smart contract bugs, oracle manipulation, governance attacks, and de-peg spirals.

DeFi is the application layer built on top of the cryptographic, consensus, and smart contract foundations from previous lessons.

What Is a Decentralized Exchange (DEX)?

Definition: Decentralized Exchange

A **decentralized exchange (DEX)** is a smart contract that allows users to swap tokens directly from their own wallets, without depositing funds with a centralized intermediary. There is no order book, no matching engine, and no custody risk.

Comparison with traditional exchanges:

Feature	Centralized Exchange	DEX
Custody	Exchange holds your funds	You keep your funds
Order matching	Limit order book	Automated market maker
KYC/AML	Required	Typically none
Counterparty risk	Exchange can fail/exit	Smart contract risk
Listing	Exchange decides	Permissionless

Key insight: DEXs eliminate custodial risk but introduce smart contract risk — a different type of trust assumption.

A DEX replaces the exchange operator with a smart contract — no custody, no permission needed.

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

Definition: Constant Product Automated Market Maker

A **constant product AMM** maintains two token reserves x and y and enforces the invariant $x \cdot y = k$ (a constant). When a trader buys token Y with token X, the contract increases x and decreases y so that the product remains k. The price emerges from the ratio $P = x/y$.

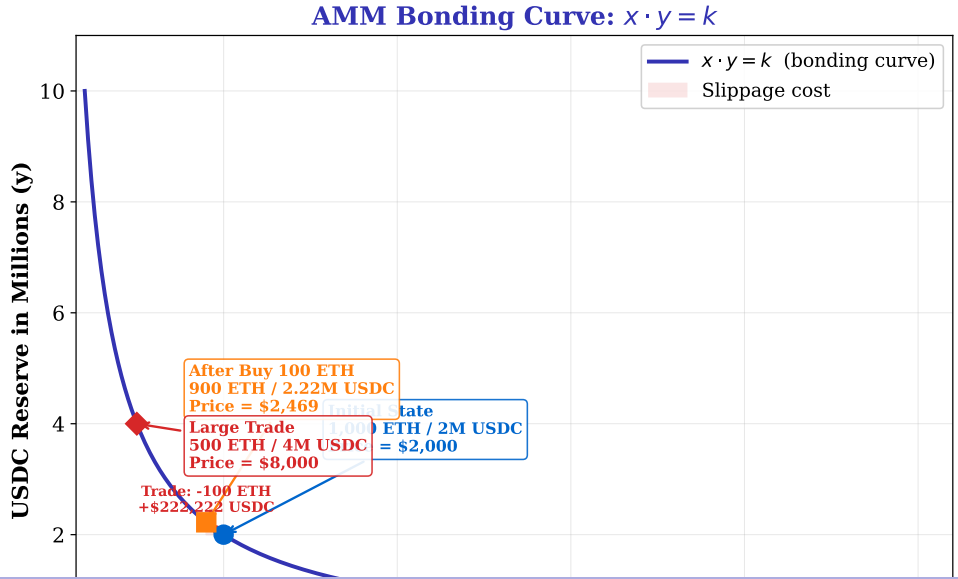
Example: A pool starts with 1,000 ETH and 2,000,000 USDC.

- $k = 1{,}000 \times 2{,}000{,}000 = 2 \times 10^9$
- Initial price: $2{,}000{,}000/1{,}000 = 2{,}000$ USDC per ETH
- A trader buys 10 ETH: the pool must now have 990 ETH
- New USDC reserve: $k/990 = 2{,}020{,}202$ USDC
- Trader pays: $2{,}020{,}202 - 2{,}000{,}000 = 20{,}202$ USDC for 10 ETH
- Effective price: $\approx 2{,}020$ USDC/ETH (higher than the starting price!)

Key property: Larger trades move the price more. The AMM never runs out of either token — it just becomes infinitely expensive.

The constant product formula replaces the order book: price is determined by reserve ratios, not by bid/ask quotes.

Visualizing the AMM Bonding Curve



Liquidity Pools: Who Provides the Tokens?

Definition: Liquidity Pool

A **liquidity pool** is a smart contract that holds reserves of two (or more) tokens. **Liquidity providers (LPs)** deposit equal-value amounts of both tokens and receive LP tokens representing their share of the pool. In return, they earn trading fees from every swap.

LP incentive structure:

- Every swap pays a fee (typically 0.3%) to the pool
- Fees accumulate in the reserves and increase the value of LP tokens
- LPs earn proportionally to their share of the pool

Example: A pool with \$10M in liquidity processes \$1M in daily volume at 0.3% fee.

- Daily fees: \$3,000
- Annual fees: $\approx$\$1,095,000
- Annualized return: $\approx$10.95% on deposited capital

Catch: This return ignores a hidden cost called **impermanent loss**.

Liquidity providers earn trading fees but face impermanent loss — the hidden cost of AMM participation.

Impermanent Loss: The Hidden Cost of Providing Liquidity

Definition: Impermanent Loss

Impermanent loss is the difference in value between holding tokens in an AMM pool versus simply holding them in a wallet. It occurs because the AMM rebalances the pool as prices change, effectively selling the appreciating token and buying the depreciating one.

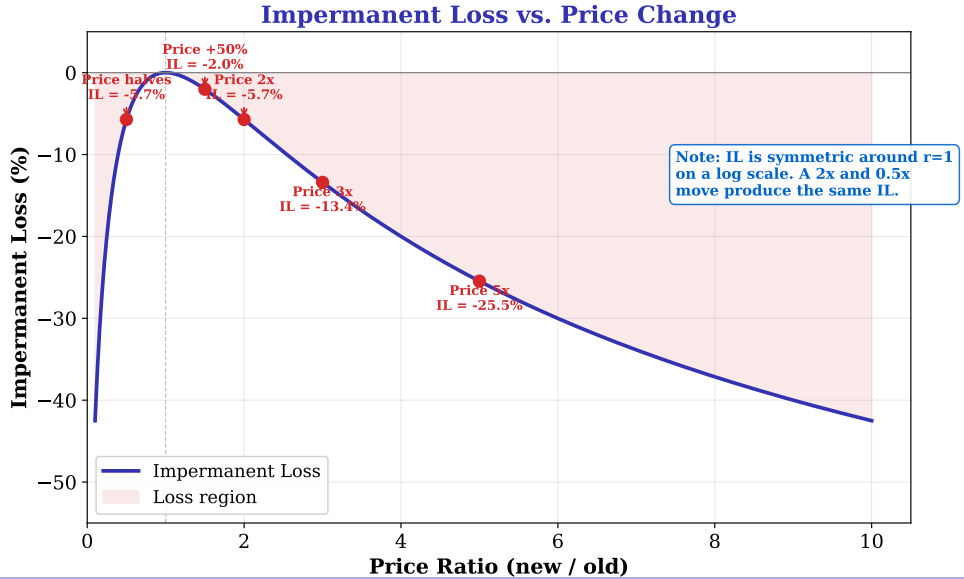
Impermanent loss formula (for constant product AMM):

$$\text{IL} = \frac{2\sqrt{r}}{1+r} - 1 \quad \text{where } r = \frac{P_{\text{new}}}{P_{\text{old}}}$$

Examples:

Price change (r)	Impermanent Loss
$\times 1.25$ (25% up)	-0.6%
$\times 1.50$ (50% up)	-2.0%
$\times 2.00$ (2x)	-5.7%
$\times 5.00$ (5x)	-25.5%

Impermanent loss grows with price divergence. LPs profit only if trading fees exceed impermanent loss.



Definition: DeFi Lending Protocol

A **DeFi lending protocol** is a smart contract that allows users to deposit crypto assets to earn interest (suppliers) or borrow crypto assets against collateral (borrowers). Interest rates are set algorithmically based on supply and demand — no bank, no credit check.

Key mechanism: Overcollateralization

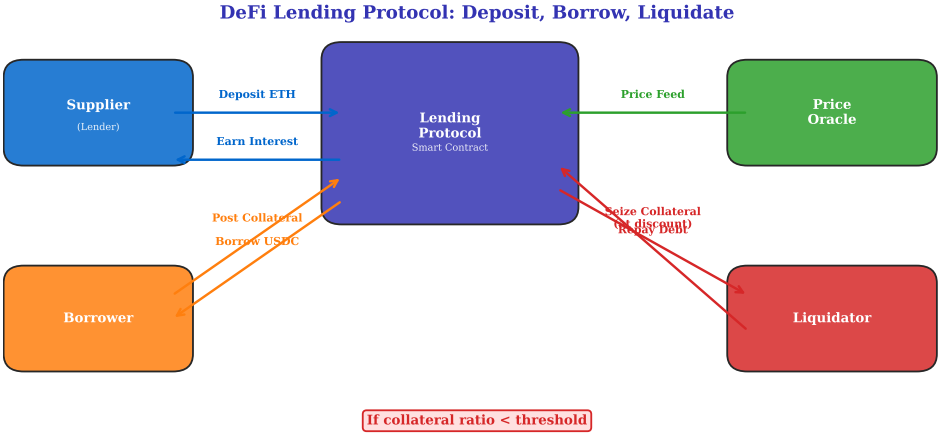
- A borrower deposits $1,500 in ETH to borrow $1,000 in stablecoins
- **Collateralization ratio:** $1{,}500/1{,}000 = 150\%$
- Why overcollateralize? Because there is no credit score, no legal recourse
- The collateral is locked in the smart contract as guarantee

Why anyone would borrow at 150%?

- Leverage: borrow stablecoins, buy more ETH (betting on price rise)
- Liquidity: access cash without selling a long-term position
- Tax optimization: borrowing is typically not a taxable event

DeFi lending replaces credit scores with overcollateralization — the collateral is the trust.

DeFi Lending: Deposit, Borrow, Liquidate



Suppliers earn interest from borrowers. If collateral falls below threshold, liquidators seize it automatically.

Collateralization Ratio and Liquidation

Definition: Liquidation

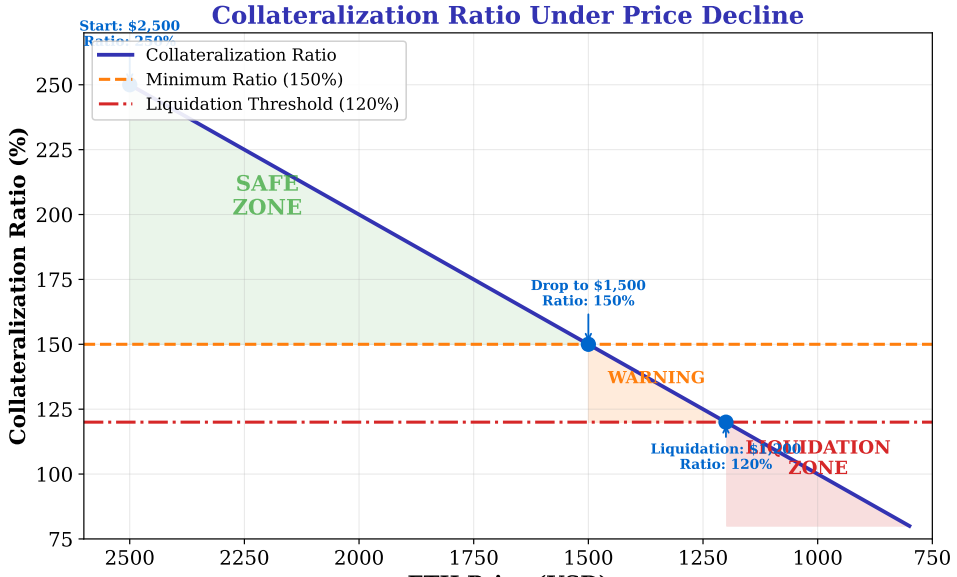
Liquidation occurs when a borrower's collateral value falls below the protocol's minimum collateralization ratio (e.g., 150% $\rightarrow$ liquidation at $\leq$120%). A third-party **liquidator** repays part of the debt and receives the collateral at a discount (the "liquidation bonus").

Worked example:

- Borrower deposits 1 ETH at \$2,000, borrows 1,000 USDC (200% ratio)
- ETH drops to \$1,200 $\rightarrow$ ratio = 1,200/1,000 = 120%
- Protocol triggers liquidation at $\leq$120%
- Liquidator repays 500 USDC of the debt
- Liquidator receives ETH worth \$500 + 5% bonus = \$525 in ETH
- Borrower keeps their 1,000 USDC but loses $\approx$0.44 ETH

Cascade risk: In a market crash, mass liquidations sell collateral $\rightarrow$ price drops further $\rightarrow$ more liquidations. This positive feedback loop is called a **liquidation cascade**.

Liquidation is the enforcement mechanism of DeFi lending — automated, instant, and unforgiving.



What Is a Flash Loan?

Definition: Flash Loan

A **flash loan** is an uncollateralized loan that must be borrowed and repaid within a *single blockchain transaction*. If the borrower fails to repay, the entire transaction reverts as if it never happened. No collateral, no credit check, no risk to the lender.

Why flash loans exist:

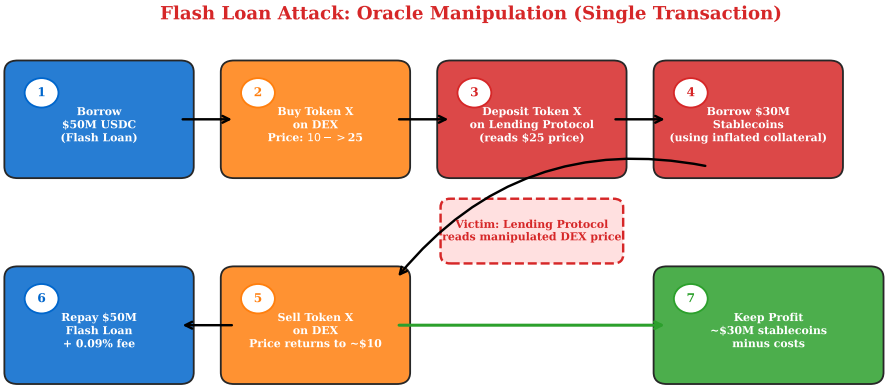
- Atomic execution: the blockchain guarantees all-or-nothing
- If repayment fails $\rightarrow$ the loan never happened $\rightarrow$ lender loses nothing
- Enables: arbitrage, collateral swaps, self-liquidation, governance attacks

Legitimate use — arbitrage:

1. Borrow 1,000,000 USDC (flash loan, 0.09% fee)
2. Buy ETH on DEX A where price is \$1,990
3. Sell ETH on DEX B where price is \$2,010
4. Repay loan + fee; keep $\approx$\$9,100 profit
5. Total time: one transaction ($\approx$12 seconds)

Flash loans give anyone access to unlimited capital for one transaction — a capability that does not exist in traditional finance.

Flash Loan Attack: Anatomy of an Exploit



Flash loan attacks exploit price oracles: borrow → manipulate price → profit → repay, all in one transaction.

Reentrancy Attacks: The DAO Hack Pattern

Definition: Reentrancy Attack

A **reentrancy attack** exploits a smart contract that calls an external contract *before* updating its own state. The attacker's contract "re-enters" the vulnerable function repeatedly, draining funds before the balance is updated.

The pattern (simplified):

1. Victim contract has a `withdraw()` function
2. Step 1: Check balance → Step 2: Send ETH → Step 3: Update balance
3. **Bug:** The ETH transfer (Step 2) triggers the attacker's fallback function
4. The attacker's fallback calls `withdraw()` again → **re-enters** before Step 3
5. The balance has not been updated, so the check passes again
6. Repeat until the contract is drained

The fix — Checks-Effects-Interactions pattern:

- **Checks:** Verify conditions (sufficient balance)
- **Effects:** Update state (set balance to zero)
- **Interactions:** Transfer funds (external call last)

Reentrancy is the most infamous smart contract vulnerability — the 2016 DAO exploit used exactly this pattern.

Oracle Manipulation: Corrupting the Price Feed

Definition: Oracle Manipulation

Oracle manipulation is an attack where an adversary artificially moves the price reported by an on-chain oracle (e.g., a DEX spot price) to exploit a protocol that depends on that price for collateral valuation, liquidation, or swap rates.

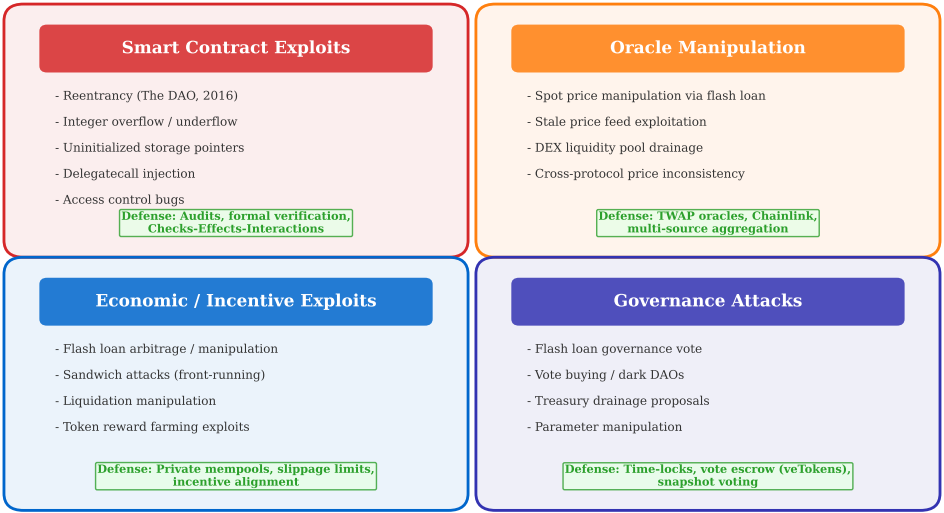
Attack pattern:

1. Protocol uses a DEX spot price as its oracle
2. Attacker takes a flash loan of \$50M
3. Attacker makes a massive trade on the DEX, moving the spot price 40%
4. Attacker interacts with the victim protocol, which reads the manipulated price
5. Attacker borrows underpriced assets or avoids liquidation
6. Attacker reverses the trade on the DEX and repays the flash loan

Defense: Time-weighted average price (TWAP)

- Use the average price over the last N blocks, not the spot price
- Manipulating a TWAP requires sustaining the price distortion across multiple blocks — much more expensive

Spot price oracles are the single biggest attack surface in DeFi. TWAP oracles dramatically increase the cost of manipulation.



What Is a Stablecoin?

Definition: Stablecoin

A **stablecoin** is a cryptocurrency designed to maintain a stable value relative to a reference asset (typically the US dollar). It achieves this through one of three mechanisms: fiat reserves, crypto overcollateralization, or algorithmic supply adjustment.

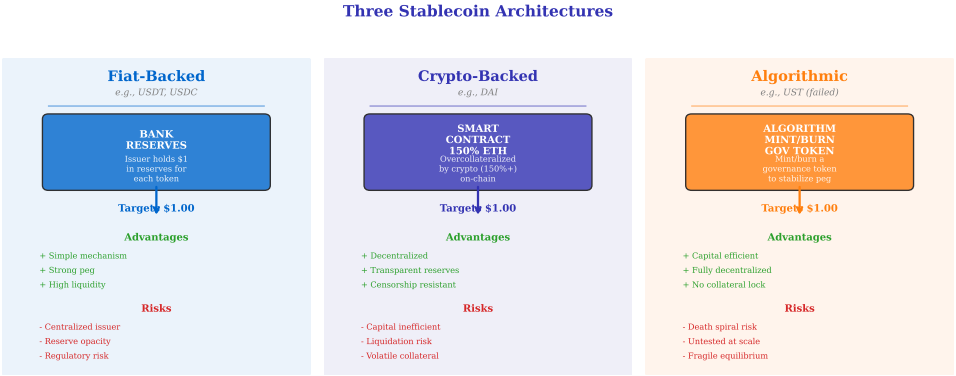
Why stablecoins matter:

- Crypto is volatile — you cannot price a loan in ETH if ETH moves 10% daily
- Stablecoins provide the **unit of account** needed for DeFi to function
- They bridge the fiat and crypto worlds: on-ramp and off-ramp
- As of 2024, total stablecoin supply exceeds $150 billion

The impossible trinity of stablecoins: You cannot simultaneously achieve full decentralization, capital efficiency, and perfect peg stability. Every design makes trade-offs.

Stablecoins are the backbone of DeFi — without a stable unit of account, lending, trading, and payments are impractical.

Three Stablecoin Architectures



Fiat-backed is simplest but centralized; crypto-backed is decentralized but capital-inefficient; algorithmic is efficient but fragile.

De-Peg Risk: When Stablecoins Break

Definition: De-Peg Event

A **de-peg event** occurs when a stablecoin's market price deviates significantly from its target value (e.g., \$1.00). De-pegs can be temporary (arbitrage restores the peg within hours) or permanent (the stablecoin collapses to near-zero).

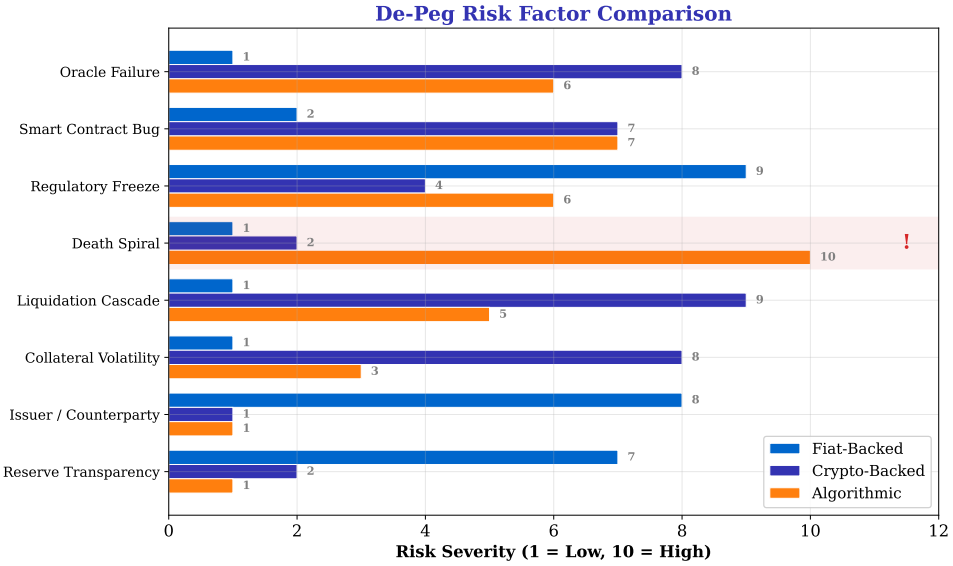
De-peg risk factors by type:

Type	Primary De-Peg Risk
Fiat-backed	Reserve transparency, issuer insolvency, regulatory freeze
Crypto-backed	Collateral crash (liquidation cascade), oracle failure
Algorithmic	Death spiral: sell pressure $\rightarrow$ mint governance token $\rightarrow$ governance token crashes $\rightarrow$ more sell pressure

Case study: The algorithmic stablecoin UST lost its peg in May 2022, dropping from \$1.00 to \$0.02 in five days, destroying $\approx$\$40 billion in value.

The UST collapse demonstrated that algorithmic stability without sufficient reserves is an unstable equilibrium.

De-Peg Risk Factor Comparison



Definition: Tokenomics

Tokenomics (token + economics) is the study of a crypto token's supply schedule, distribution, utility, and incentive mechanisms. It determines how tokens are created, allocated, earned, spent, and burned — and how these flows affect the token's value.

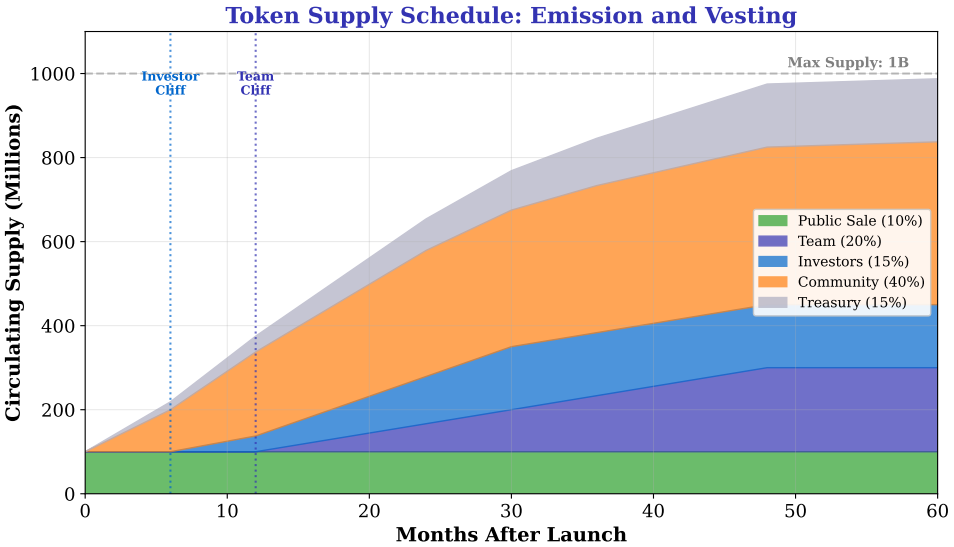
Key tokenomics parameters:

Parameter	Description
Total supply	Maximum tokens that will ever exist
Circulating supply	Tokens currently tradeable
Emission schedule	Rate at which new tokens enter circulation
Vesting	Lock-up periods for team/investor tokens
Burn mechanism	Permanent removal of tokens from supply
Governance rights	Voting power over protocol parameters

Key insight: Tokenomics is protocol-level monetary policy. Unlike central banks, the rules are transparent and (usually) immutable.

Tokenomics determines a protocol's long-term economic sustainability — bad tokenomics kills good protocols.

Token Supply Schedule: Emission and Vesting

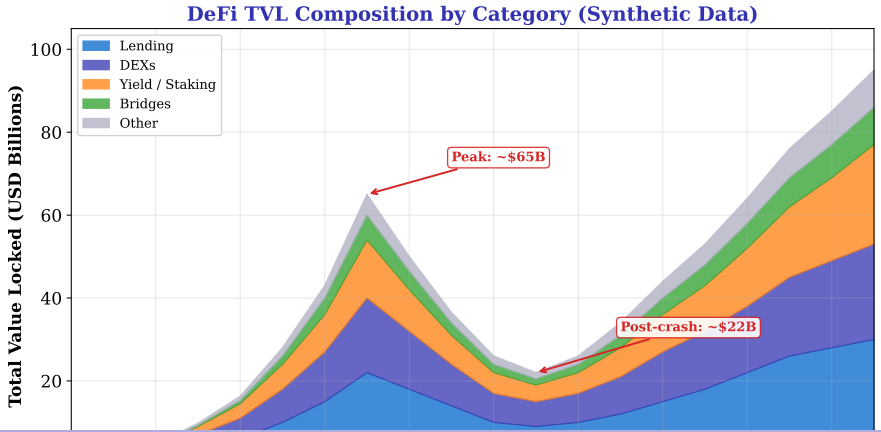


Vesting cliffs and emission halving create predictable supply shocks — savvy investors watch these schedules closely.

Total Value Locked (TVL): The DeFi Scoreboard

Definition: Total Value Locked

Total Value Locked (TVL) is the aggregate value of crypto assets deposited in a DeFi protocol's smart contracts. It is the most widely used metric for measuring the size and adoption of DeFi protocols.



Governance Attacks: When Voting Power Is for Sale

Most DeFi protocols are governed by token holders:

- 1 token = 1 vote on protocol parameters (fees, collateral ratios, new assets)
- Proposals pass with a quorum (e.g., 4% of total supply)
- Execution is automatic: the smart contract implements the vote result

Attack vectors:

Attack	Mechanism
Flash loan governance	Borrow tokens, vote, return tokens — all in one transaction
Vote buying	Offer bribes to token holders ("dark DAOs")
Treasury drain	Propose to send the protocol treasury to the attacker's address
Parameter manipulation	Change collateral ratios to enable under-collateralized borrowing

Defense mechanisms: Time-locked voting, vote escrow (lock tokens for longer = more voting power), snapshot-based voting (use token balances from a past block).

Token-based governance is transparent but fragile — concentrated token holdings can hijack protocol decisions.

Key Takeaways

1. **AMMs** replace order books with the constant product formula $x \cdot y = k$, where price emerges from reserve ratios
2. **Impermanent loss** is the hidden cost of providing liquidity — LPs lose relative to holding when prices diverge
3. **DeFi lending** replaces credit scores with overcollateralization; falling collateral triggers automatic **liquidation**
4. **Flash loans** provide uncollateralized capital within a single transaction — enabling both arbitrage and attacks
5. **Reentrancy** and **oracle manipulation** are the most common smart contract vulnerabilities
6. **Stablecoins** come in three types (fiat-backed, crypto-backed, algorithmic), each with distinct de-peg risks
7. **Tokenomics** defines a protocol's monetary policy: supply, emission, vesting, and governance rights
8. DeFi eliminates intermediaries but introduces **new risks**: code bugs, economic exploits, and governance attacks

DeFi is a new financial system with new risk categories — understanding the mechanisms is the first step to managing the risks.

Summary / Next Lesson Preview

This lesson: We explored DeFi primitives (AMMs, lending, stablecoins, tokenomics) and the attack surfaces they create (flash loans, reentrancy, oracle manipulation, governance attacks).

Key vocabulary:

- Automated market maker (AMM)
- Constant product formula
- Impermanent loss
- Liquidity pool / LP tokens
- Overcollateralization
- Liquidation cascade
- Flash loan
- Reentrancy attack
- Oracle manipulation
- TWAP oracle
- Stablecoin (3 types)
- De-peg risk
- Tokenomics
- Total value locked (TVL)
- Governance attack

Next module (M4): *The Risk Problem* — How do we measure, model, and manage risk in both traditional and digital financial systems?

Review: Can you calculate impermanent loss for a 2x price change? Can you explain why flash loans enable oracle manipulation?