DeFi-Protokolle

Learning Outcome: DeFi-Protokolle (AMMs, Lending) beschreiben — Bloom's: Understand

Prof. Dr. J. Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

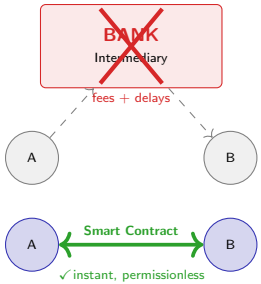
What If You Could Be Your Own Bank?

Traditional Finance Requires Intermediaries:

- Banks hold your deposits and approve loans
- Brokers match buyers and sellers in markets
- Clearing houses settle trades between parties
- Each step adds fees, delays, and gatekeeping
- Geographic and credit limits exclude millions

DeFi removes the middlemen:

- Smart contracts replace banks, brokers, and clearing
- Anyone with a wallet can trade or lend instantly
- Rules are code – transparent and permissionless



DeFi = financial services encoded in smart contracts; no central authority controls funds or access.

How Does a Pool Replace an Order Book?

Definition: Automated Market Maker (AMM)

A smart contract holding two tokens in a pool, pricing trades via formula – no order book or counterparty required.

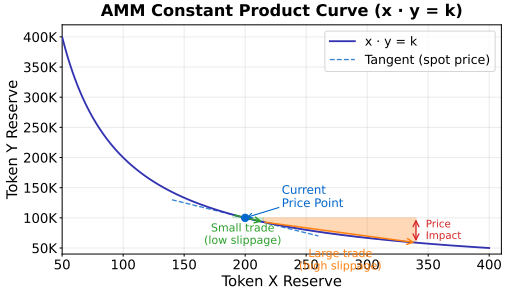
Constant Product Formula:

$$\underbrace{x \cdot y = k}_{\text{invariant after every trade}}$$

- x = token A quantity in pool
- y = token B quantity in pool
- k = constant – never changes
- Buying A reduces x, pushes price up

Liquidity Providers (LPs):

- Deposit both tokens to earn fees
- Permissionless – no KYC required



Uniswap V2 pioneered $x \cdot y = k$; Curve uses a flatter variant for stablecoins; Uniswap V3 concentrates liquidity in price ranges.

How Does Lending Work Without a Bank?

Overcollateralization:

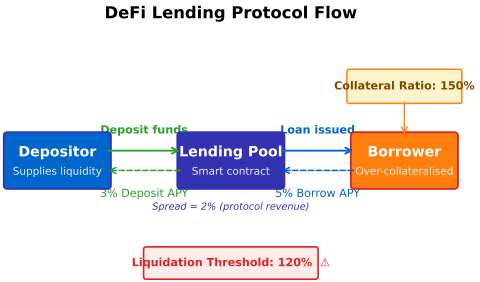
- Borrow less than you deposit as collateral
- Typical ratio: 150%–200% collateral required
- No credit score – the collateral is the guarantee

Interest Rate Models:

- Rates adjust automatically with utilization
- High demand to borrow $\Rightarrow$ rates rise, incentivizing supply
- Low demand $\Rightarrow$ rates fall, incentivizing borrowing

Liquidation:

- Triggered when collateral value falls below threshold
- Liquidators repay debt, receive collateral at discount
- Automatic, on-chain – no human approval needed



Aave and Compound are the leading lending protocols; both use overcollateralized models with algorithmic interest rates and on-chain liquidation.

What Are the Five Layers of the DeFi Stack?

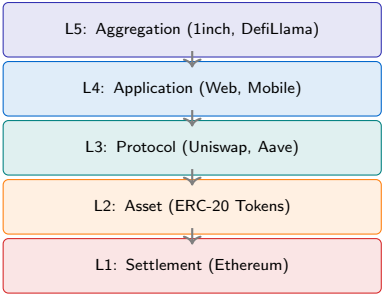
Layer 1 – Settlement: Base blockchain (Ethereum, Solana, Avalanche). Provides finality and security for all layers above.

Layer 2 – Asset: Native and bridged tokens (ERC-20, wrapped assets). Define what value can flow through protocols.

Layer 3 – Protocol: Core DeFi applications (Uniswap, Aave, Compound, MakerDAO). Encode financial logic in smart contracts.

Layer 4 – Application: Frontend interfaces (web apps, mobile). Abstract complexity for end users.

Layer 5 – Aggregation: Routing and analytics (1inch, DefiLlama, Zapper). Combine protocols for best execution.



Each layer depends on the one below; a vulnerability at Layer 1 or 2 propagates upward – understanding the stack identifies systemic risk.

Worked Example: What Is the Price Impact of One Swap?

Pool state before swap: 100 ETH + 200,000 USDC $\Rightarrow$ $k = 100 \times 200{,}000 = 20{,}000{,}000$

Step-by-step: Swap 1 ETH for USDC

1. New ETH in pool: $100 + 1 = 101$
2. New USDC: $k/101 = 20{,}000{,}000/101 \approx 198{,}019.80$
3. USDC received: $\underbrace{200{,}000 - 198{,}019.80}_{= 1{,}980.20 \text{ USDC}}$
4. Effective price: $\underbrace{1{,}980.20 \text{ USDC/ETH}}_{\text{vs. spot } 2{,}000}$
5. Slippage: $\underbrace{(2{,}000 - 1{,}980.20)/2{,}000}_{\approx 0.99\% \text{ price impact}}$

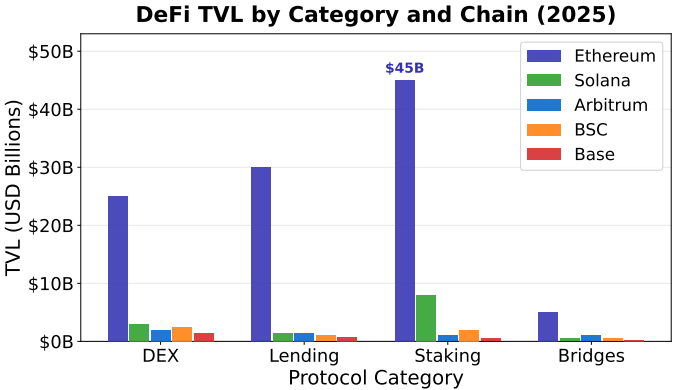
Key Insight: Why Slippage Grows with Trade Size

- Small trades: curve barely moves, slippage $< 0.1\%$
- Large trades: curve moves sharply, slippage can exceed 5%
- Deep pools (more liquidity) reduce slippage for all sizes
- Aggregators split orders across multiple pools to minimise impact

In practice, Uniswap also charges a 0.3% fee deducted before the swap, paid to liquidity providers.

The constant product formula creates a hyperbolic price curve: infinite liquidity at any price, but always with increasing slippage for larger trades.

How Big Has DeFi Become?



- **Ethereum dominates** with over 70% of DeFi TVL – ecosystem depth attracts the most capital
- **Lending protocols** (Aave, Compound, MakerDAO) hold more TVL than DEXs, reflecting strong on-chain credit demand
- **Layer 2 chains** (Arbitrum, Base, Optimism) are the fastest-growing segment at lower transaction cost

TVL (Total Value Locked) = USD value deposited in smart contracts; primary DeFi size metric but does not capture protocol revenue or user count.

What Are the Main Traps for DeFi Participants?

Impermanent Loss (LP Risk):

- Providing liquidity can underperform simply holding tokens
- Occurs when the price ratio of the two tokens diverges
- Example: one token doubles in price in a 50/50 pool
- Mathematical loss vs. holding: approximately 5.7%
- Fee income must exceed this loss for LPs to profit

Additional Protocol Risks:

- **Oracle manipulation** – price feed attacks distort collateral values
- **Smart contract bugs** – audited code can still contain exploits
- **Flash loan exploits** – atomic, uncollateralised loans enable complex attacks
- **Regulatory uncertainty** – classification of tokens and protocols varies by jurisdiction
- **Governance attacks** – large token holders can pass malicious proposals

Risk in DeFi is multidimensional: market risk (impermanent loss), protocol risk (smart contract), systemic risk (oracle/governance). Diversification across protocols reduces but does not eliminate exposure.

Three Questions to Describe Any DeFi Protocol

The Three Diagnostic Questions:

1. **What is the liquidity source?**
   Who supplies the capital, and what do they earn?
2. **How is price discovered?**
   Formula-based, oracle-fed, or order-book?
3. **What is the collateral mechanism?**
   Overcollateralised, algorithmic, or uncollateralised?

How to Answer – Examples:

- **Uniswap V3:**
  LP pools / constant product formula / no collateral (spot swap)
- **Aave:**
  Depositors / oracle price feeds / overcollateralisation (150%+)
- **Curve Finance:**
  LP pools / stableswap invariant / no collateral (stablecoin swap)
- **MakerDAO:**
  Protocol-minted / oracle / overcollateralised CDP (150%+)

Applying these three questions to any protocol immediately reveals its economic structure, risk profile, and how it compares to traditional finance equivalents.

Key Takeaways

What You Have Learned:

- **DeFi** replaces financial intermediaries with smart contracts operating on public blockchains
- **AMMs** use the constant product formula $x \cdot y = k$ to price trades from pooled liquidity – no order book required
- **Lending protocols** rely on overcollateralisation and algorithmic interest rates; liquidation is automatic and on-chain
- **The DeFi stack** has five layers: settlement, asset, protocol, application, and aggregation
- **Key risks** include impermanent loss, smart contract bugs, oracle attacks, and governance vulnerabilities

You Can Now Describe:

- How AMMs price trades using $x \cdot y = k$ and why slippage increases with trade size
- How lending protocols manage risk through overcollateralisation and liquidation
- The role of each layer in the DeFi stack
- The three diagnostic questions for any DeFi protocol (liquidity, price, collateral)
- Why impermanent loss and flash loan exploits matter for DeFi participants

Next step: Analyse a specific protocol's tokenomics and governance model using these frameworks.