Decentralized Finance (DeFi)

Lesson 6: Summary

Prof. Joerg Osterrieder

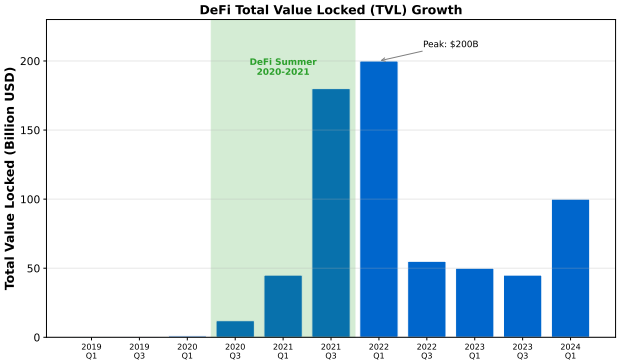
Spring 2026

What is DeFi?

Definition: Financial services on public blockchains without intermediaries.
Key Properties:

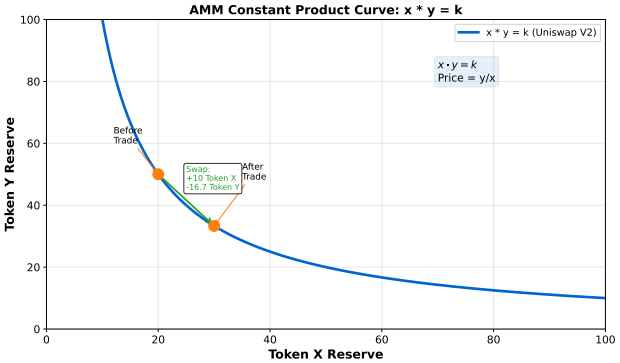
- Permissionless: Anyone can participate
- Transparent: All transactions on-chain
- Composable: "Money legos" combine protocols
- Non-custodial: Users control assets

DeFi Growth



TVL measures total assets deposited in DeFi protocols

AMM: Constant Product



$x \cdot$

$y = k$ **formula sets prices automatically based on pool reserves**

AMM Key Concepts

Liquidity Providers:

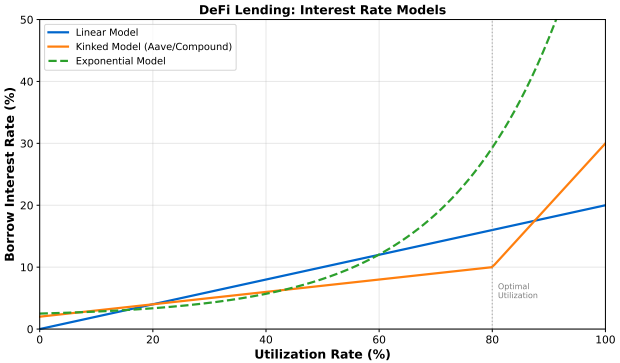
- Deposit equal value of both tokens
- Earn trading fees (0.3% typical)
- Risk: impermanent loss when prices diverge

Key AMMs: Uniswap (general), Curve (stablecoins)

LPs

earn fees but face impermanent loss risk

DeFi Lending



Overc

loans: deposit 150% to borrow 100%

Lending Mechanics

Key Features:

- Variable interest rates (supply/demand)
- Collateral factors (ETH: 80%, stables: 85%)
- Liquidation if health factor drops below 1.0

Flash Loans: Borrow millions uncollateralized, repay in same transaction.

Majo

protocols: Aave, Compound

Stablecoins

Types:

- **Fiat-backed**: USDT, USDC (centralized, USD reserves)
- **Crypto-backed**: DAI (overcollateralized by ETH)
- **Algorithmic**: High risk (Terra collapse)

Market: $150B+ total supply

Stabl

are DeFi's backbone but carry different risks

DeFi Risks

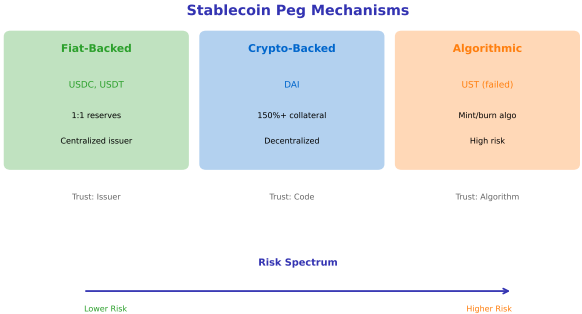
Smart Contract Risks:

- Code vulnerabilities (reentrancy, oracle manipulation)
- Billions lost to hacks (Ronin: $625M)

Mitigation: Audits, bug bounties, established protocols

DeFi offers opportunity and risk in equal measure

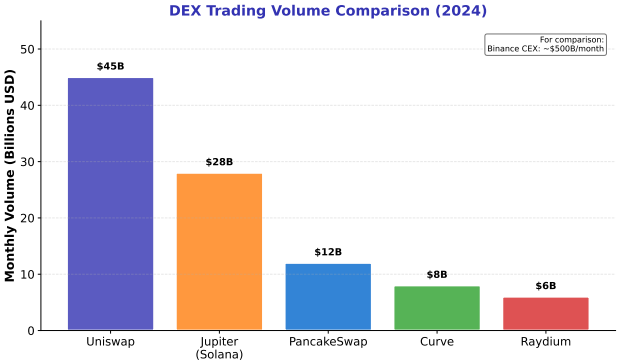
Stablecoin Peg Mechanisms



Algor

stablecoins risky (Terra collapse); fiat-backed most stable

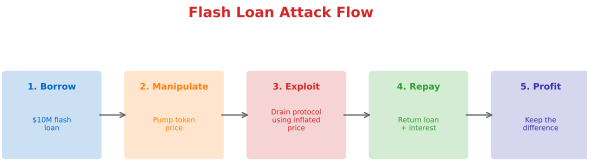
DEX Trading Volumes



Unisv

dominates; DEX volume growing relative to centralized exchanges

Flash Loan Attacks



Atom

transactions enable price manipulation without capital

Key Takeaways

1. **DeFi:** Permissionless financial services on-chain
2. **AMMs:** $x \cdot y = k$ replaces order books
3. **Lending:** Overcollateralized, algorithmic rates
4. **Stablecoins:** Bridge between crypto and fiat

Core Insight: DeFi trades complexity and risk for transparency and accessibility.

Next:

Smart Contracts and Game Theory

Thank You

Questions?