Decentralized Finance (DeFi)

Lesson 6: The New Financial System

Prof. Joerg Osterrieder

Spring 2026

Learning Objectives

After this lesson, you will be able to:

- Define DeFi and explain its core principles
- Describe how Automated Market Makers work
- Explain lending/borrowing protocols
- Analyze stablecoin mechanisms and risks

Prerequisites: Lessons 1-5 (especially Tokenomics)

recreates traditional finance using smart contracts

Lesson Outline

1. What is DeFi?
2. Automated Market Makers
3. Lending Protocols
4. Stablecoins
5. Oracles and Data Feeds
6. Yield Farming
7. DeFi Risks and Security

What is DeFi?

DeFi Definition

Decentralized Finance: Financial services built on public blockchains, operating without traditional intermediaries.

Key Characteristics:

- **Permissionless**: Anyone can participate
- **Transparent**: All transactions on-chain
- **Composable**: Protocols can be combined
- **Non-custodial**: Users control their assets

Key Terminology:

- **TVL (Total Value Locked)**: The total value of crypto assets deposited in a DeFi protocol
- **DEX (Decentralized Exchange)**: A peer-to-peer exchange operating via smart contracts without central authority

DeFi:

"banking" without banks. Note: DeFi lacks the consumer protections, deposit insurance, and regulatory oversight of traditional banking.

DeFi vs. Traditional Finance

Aspect	TradFi	DeFi
Access	Bank account required	Wallet only
Hours	Business hours	24/7/365
Settlement	Days (T+2)	Minutes
Custody	Bank holds assets	Self-custody
Transparency	Private ledgers	Public blockchain
Identity	KYC required	Pseudonymous

DeFi removes gatekeepers but also removes safety nets

The DeFi Stack

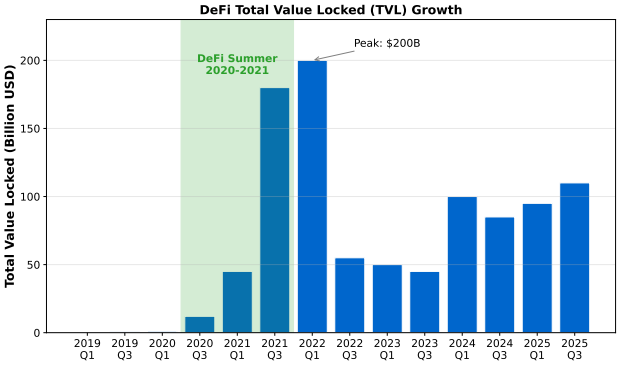
Layer Architecture:

1. **Settlement**: Blockchain (Ethereum, Solana)
2. **Asset**: Tokens (ETH, stablecoins, wrapped assets)
3. **Protocol**: Smart contracts (AMMs, lending)
4. **Application**: User interfaces (dApps)
5. **Aggregation**: Cross-protocol services

Composability: Each layer can build on layers below, creating "money legos."

modular design enables rapid innovation

DeFi Growth



Sourc

`https://defillama.com/` – **check current TVL data**

Automated Market Makers

Traditional vs. AMM Trading

Traditional (Order Book):

- Buyers and sellers place orders
- Market makers provide liquidity
- Price set by matching orders

AMM Approach:

- Liquidity pools replace order books
- Algorithm sets prices automatically
- Anyone can provide liquidity

AMM

enable permissionless, 24/7 trading without market makers

Constant Product Formula

The Core Equation:

$$x \cdot y = k$$

- x = quantity of token A in pool
- y = quantity of token B in pool
- k = constant (invariant)

How It Works:

- Buying token A decreases x, increases y
- Price adjusts to maintain k
- Larger trades = more slippage (**Slippage**: difference between expected and executed price due to trade size)

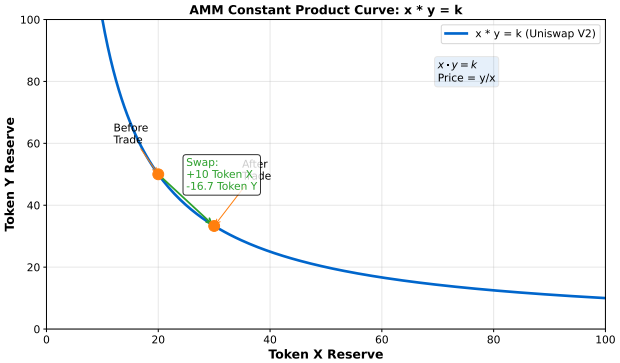
Numerical Example:

- Pool: 100 ETH + 200,000 USDC $\Rightarrow$ k = 20,000,000
- Current price: \$2,000/ETH
- Buy 1 ETH: Costs approximately \$2,020 (about 1% slippage)

Unisv

popularized the x*y=k formula

AMM Price Curves



The hyperbolic curve shows how price changes with trade size

Liquidity Provision

Becoming a Liquidity Provider (LP):

1. Deposit equal value of both tokens
2. Receive LP tokens representing your share
3. Earn trading fees (typically 0.3%)
4. Withdraw anytime by burning LP tokens

Example:

- Deposit \$500 ETH + \$500 USDC
- Earn portion of all ETH/USDC trades
- \$1B volume = \$3M in fees to split

LP

returns depend on trading volume and fee tier

Impermanent Loss

The Hidden Risk:

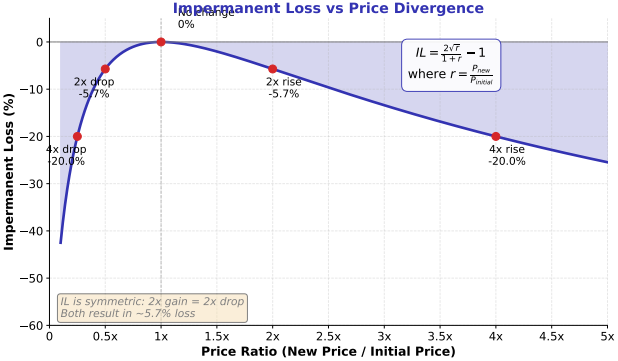
- When prices diverge, LPs may lose value
- Called "impermanent" because it reverses if prices return
- Permanent if you withdraw during divergence

Example:

- Deposit when ETH = $2000
- ETH rises to $4000
- LP position worth less than just holding
- Loss can exceed trading fee earnings

loss is real cost; "impermanent" is misleading name

Impermanent Loss: The Formula



Formula: $IL = \frac{2\sqrt{r}}{1+r} - 1$ where $r = \frac{P_{new}}{P_{initial}}$

Example Calculation (2x price change):

- If $r = 2$ (price doubles): $IL = \frac{2\sqrt{2}}{1+2} - 1 = \frac{2.828}{3} - 1 \approx -0.057$ or -5.7% loss
- If $r = 0.5$ (price halves): $IL = \frac{2\sqrt{0.5}}{1+0.5} - 1 = \frac{1.414}{1.5} - 1 \approx -0.057$ or -5.7% loss

IL is symmetric: 2x gain or 2x drop both result in 5.7% loss

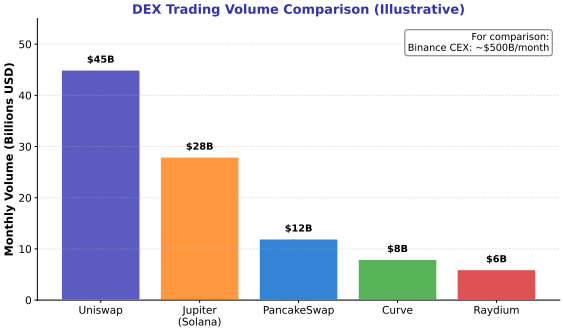
Major AMM Protocols

Uniswap (V3):

- Concentrated liquidity (custom price ranges)
- Multiple fee tiers (0.01%, 0.05%, 0.3%, 1%)
- Largest DEX by volume

Curve:

- Optimized for similar assets (stablecoins)
- Very low slippage for stable pairs
- Complex governance (veCRV)



Diffe

DEX Aggregators

What are DEX Aggregators?

- Route trades across multiple DEXs to find the best execution price
- Split large orders across venues to minimize slippage
- Automatically optimize for price, gas fees, and slippage

Leading Aggregators:

- **1inch**: Pathfinder algorithm for multi-hop routing
- **Paraswap**: Supports 30+ DEXs across multiple chains
- **0x**: Professional-grade API for DEX aggregation

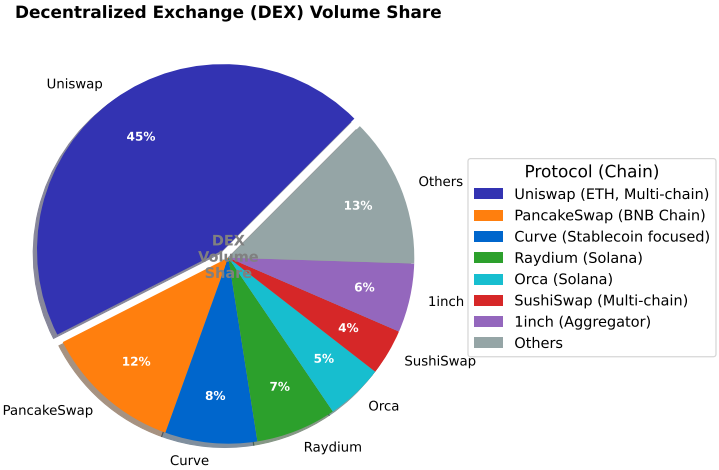
Why Use Aggregators?

- Better prices than single DEX for large trades
- Reduced slippage through order splitting
- Gas optimization across multiple swaps

Aggr

are essential for efficient DeFi trading at scale

DEX Volume Market Share

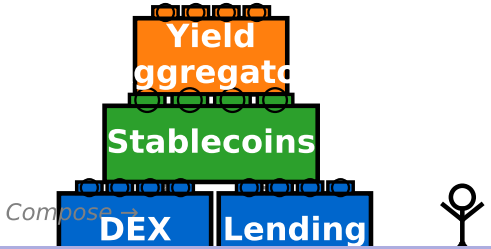


Sourc

DeFiLlama – Uniswap dominates DEX volume across multiple chains

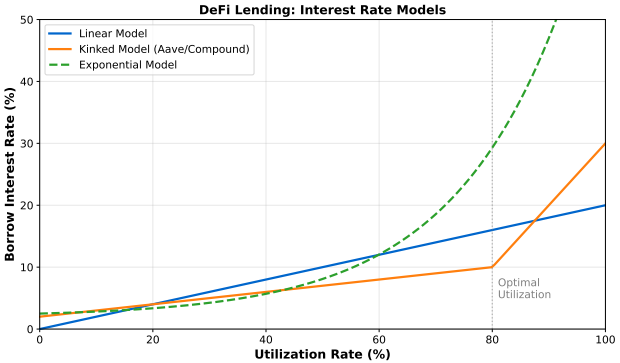
DeFi: Money Legos

Composable Financial Protocols



Lending Protocols

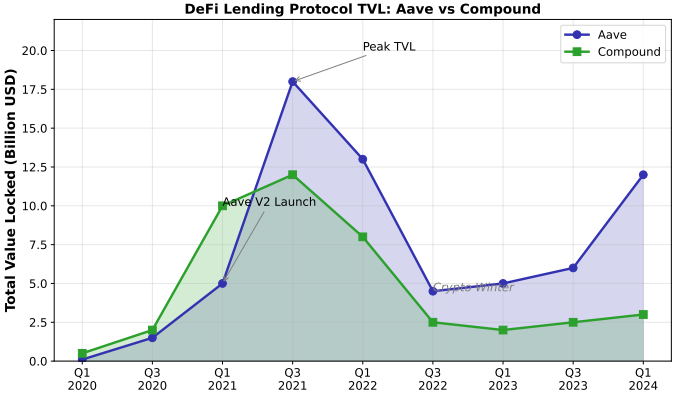
DeFi Lending Overview



Lendi

protocols match depositors with borrowers algorithmically

Lending Protocol TVL Growth



Sourc

DeFiLlama – Aave surpassed Compound as leading lending protocol

How DeFi Lending Works

Depositors (Lenders):

- Deposit assets into lending pool
- Earn variable interest (supply APY)
- Can withdraw anytime (if liquidity available)

Borrowers:

- Deposit collateral (150%+ of loan)
- Borrow up to collateral factor
- Pay variable interest (borrow APY)
- Risk liquidation if collateral falls

loans are overcollateralized; no credit checks needed

Interest Rate Models

Utilization-Based Rates:

$$\text{Interest Rate} = f(\text{Utilization Rate})$$

- Low utilization = low rates (encourage borrowing)
- High utilization = high rates (attract deposits)
- "Kink" point where rates spike

Example (Aave):

- Below 80% utilization: gradual increase
- Above 80%: steep rate increase
- Ensures liquidity for withdrawals

rates algorithmically balance supply and demand

Collateral and Liquidation

Collateral Factors:

- ETH: 80% (borrow up to 80% of value)
- Stablecoins: 85%
- Volatile tokens: 50-70%

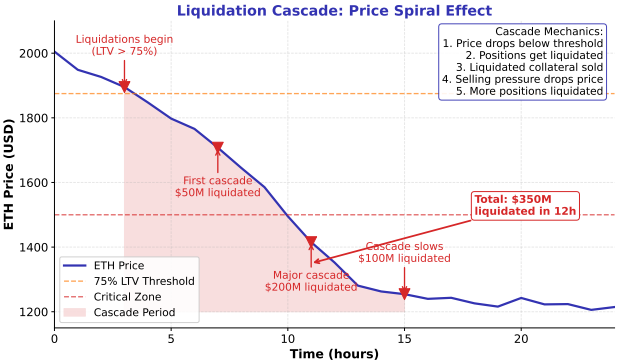
Liquidation Process:

- Health factor drops below 1.0
- Liquidators repay portion of debt
- Receive collateral at discount (5-10%)
- Automated, permissionless process

Liqui

protects lenders; liquidators profit from unhealthy positions

Liquidation Cascades



The Spiral: Liquidations → forced selling → price drop → more liquidations

liquidations can amplify price crashes; $350M+ liquidated in hours during crashes

Flash Loans

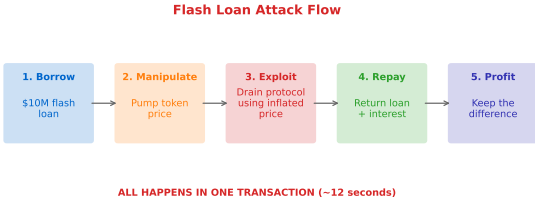
Definition: Uncollateralized loans that must be repaid in same transaction.

How They Work:

1. Borrow any amount (millions possible)
2. Use funds within single transaction
3. Repay principal + fee
4. If not repaid, entire transaction reverts

Use Cases:

- Arbitrage between DEXs
- Collateral swaps
- Self-liquidation



No collateral needed - loan must be repaid in same block or transaction reverts

Stablecoins

Why Stablecoins Matter

The Problem:

- Crypto volatility makes it hard to use as money
- Need stable unit of account for DeFi
- Bridge between crypto and fiat

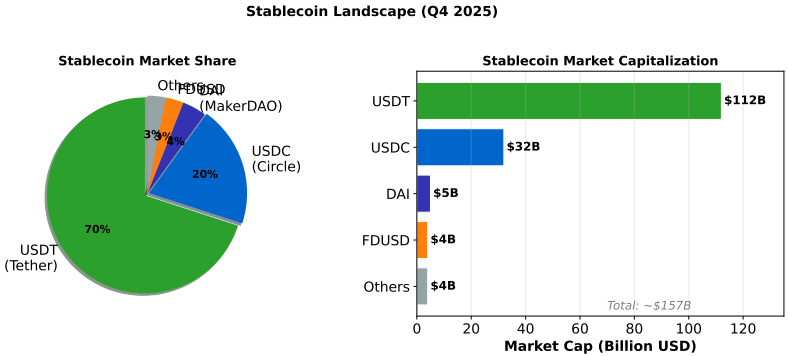
Market Leaders:

- Stablecoin supply dominates DeFi liquidity
- USDT: Largest by market cap (Tether)
- USDC: Second largest (Circle)
- DAI: Leading decentralized stablecoin (MakerDAO)

Curre

supply: `https://defillama.com/stablecoins`

Stablecoin Market Share



Sourc

CoinGecko – USDT dominates with 70% market share

Types of Stablecoins

Fiat-Collateralized:

- Backed by USD in bank accounts
- Examples: USDT, USDC
- Centralized, requires trust

Crypto-Collateralized:

- Backed by crypto (overcollateralized)
- Example: DAI (ETH backing)
- Decentralized, transparent

Algorithmic:

- Maintain peg via algorithms/incentives
- High risk (see Terra collapse)

Differ

stablecoin types have different trust assumptions

MakerDAO and DAI

How DAI Works:

1. Deposit ETH into Maker Vault
2. Mint DAI up to collateral ratio
3. Pay stability fee (interest)
4. Repay DAI to unlock collateral

Peg Maintenance:

- DAI $>$ \$1: Incentive to mint and sell
- DAI $<$ \$1: Incentive to buy and repay
- Liquidations if collateral ratio falls

DAI

is the largest decentralized stablecoin

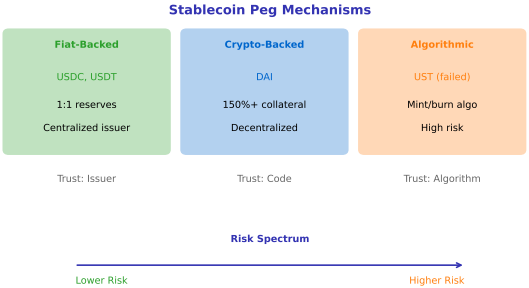
Stablecoin Risks

Fiat-Backed Risks:

- Counterparty risk (issuer failure)
- Regulatory risk (asset freezing)
- Reserve quality concerns

Crypto-Backed Risks:

- Collateral volatility (mass liquidations)
- Smart contract bugs
- Oracle failures



Oracles and Data Feeds

The Oracle Problem

What are Oracles?

- **Oracle**: A service that provides external data to smart contracts on the blockchain
- Blockchains are isolated systems that cannot natively access off-chain information

The Challenge:

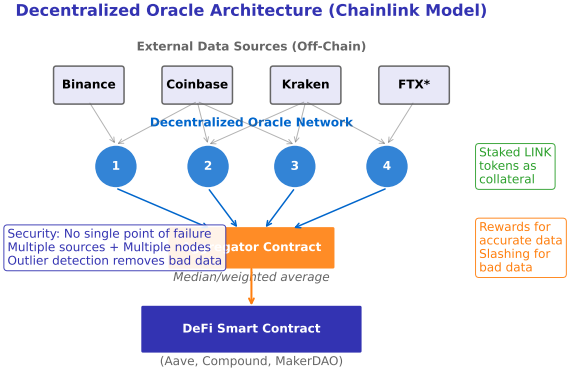
- Smart contracts cannot access external data
- Need real-world prices for DeFi to function
- Single data source = single point of failure

What Oracles Provide:

- Asset prices (ETH/USD, BTC/USD)
- Interest rates and yield data
- Random numbers for games/NFTs
- Real-world event outcomes

are the bridge between blockchain and real world

Decentralized Oracle Architecture



Chain

TVS: `https://data.chain.link/` – **leading oracle by value secured**

Oracle Economics

Incentive Design:

- Node operators stake tokens as collateral
- Rewards for providing accurate data
- Slashing for incorrect or delayed data
- Reputation system tracks performance

Attack Vectors:

- Flash loan oracle manipulation
- Spot price vs. TWAP attacks
- Low-liquidity asset manipulation

security is critical; many DeFi hacks exploit oracle weaknesses

Yield Farming

What is Yield Farming?

Definition: Strategy of moving assets between DeFi protocols to maximize returns.

Yield Sources:

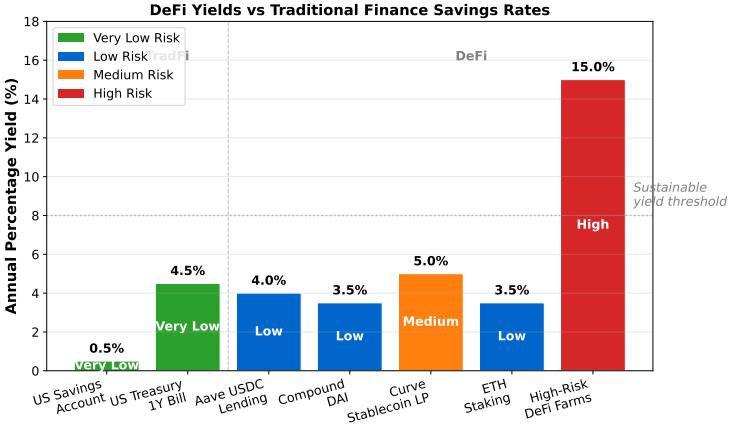
- Trading fees (LP positions)
- Lending interest (supply APY)
- Protocol token rewards (incentives)
- Governance token distributions

APY Range: 5% to 1000%+ (higher = higher risk)

"DeF

Summer 2020" saw explosive yield farming growth

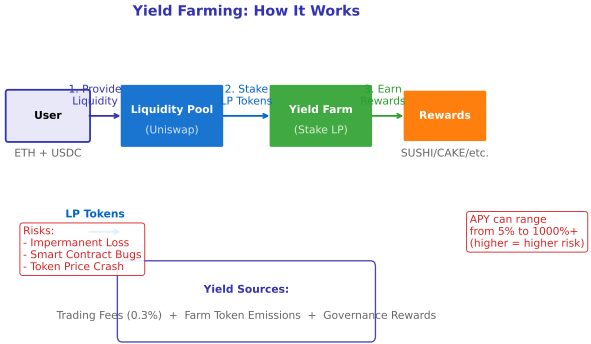
DeFi Yields vs Traditional Finance



Sourc

DeFiLlama, Federal Reserve – Higher yields come with higher risks

Yield Farming Mechanics



Yield farming combines multiple DeFi primitives for compounded returns

Yield Farming Risks

Key Risks:

- **Impermanent Loss**: Price divergence erodes LP value
- **Smart Contract Risk**: Protocol exploits
- **Token Price Risk**: Reward tokens may crash
- **Rug Pulls**: Malicious projects steal funds

Due Diligence:

- Check audit reports
- Verify team and backers
- Understand token emission schedule
- Start with small amounts

High

APY = high risk; sustainable yields are typically 5-20%

DeFi Risks and Security

Smart Contract Risks

Common Vulnerabilities:

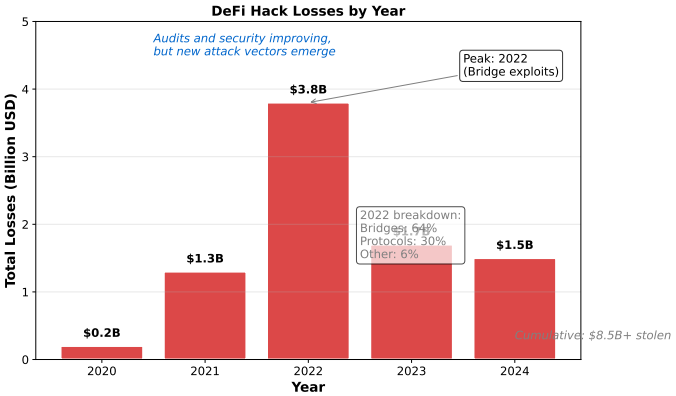
- Reentrancy attacks
- Oracle manipulation
- Flash loan exploits
- Access control bugs

Major Bridge Hacks (2022):

- Ronin Bridge
- Wormhole
- Nomad

Full leaderboard: `https://rekt.news/leaderboard/`

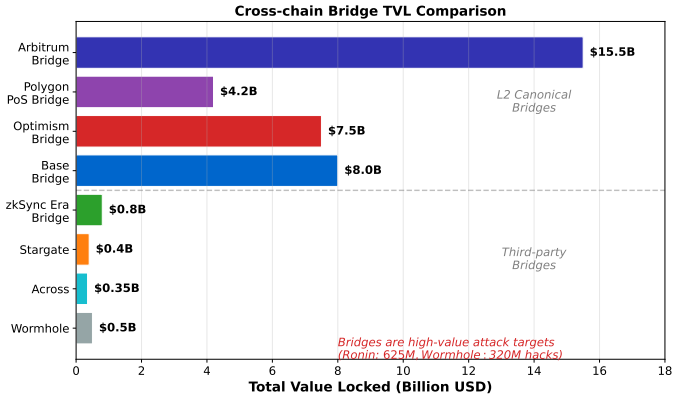
DeFi Hack Losses by Year



Sourc

Rekt.news, DeFiLlama – 2022 peak driven by bridge exploits

Cross-chain Bridge TVL



Sourc

L2Beat – Bridges hold billions but are high-value attack targets

Risk Mitigation

Protocol-Level:

- Code audits (multiple firms)
- Bug bounty programs
- Formal verification
- Time-locked upgrades

User-Level:

- Use established protocols
- Start with small amounts
- Understand what you're signing
- Revoke unused approvals

security requires vigilance from both builders and users

Key Takeaways

What You Learned Today:

1. DeFi enables permissionless financial services
2. AMMs use formulas instead of order books
3. Lending protocols match depositors with borrowers
4. Stablecoins bridge volatility gap

Core Insight: DeFi recreates traditional finance with smart contracts, offering transparency and accessibility at the cost of complexity and risk.

Next lesson: Smart Contracts and Game Theory

Questions for Reflection

1. Why do AMMs need impermanent loss?
2. What makes flash loans possible only in DeFi?
3. How does overcollateralization enable trustless lending?
4. What are the trade-offs between stablecoin types?

Discussion: Will DeFi replace traditional finance?

Consi

these questions before our next session

Thank You

Questions?

Appendix: Case Studies

Case Study: Terra/Luna Collapse (May 2022)

What Happened:

- UST: algorithmic stablecoin backed by LUNA
- $18B UST + $40B LUNA market cap at peak
- May 7-13, 2022: Death spiral collapse
- UST lost peg; LUNA hyperinflated to zero

The Mechanism Failure:

- UST redeemable for $1 of LUNA
- Large withdrawals triggered panic
- LUNA minting couldn't keep pace
- Approximately $60B in market cap lost (market cap loss, not necessarily invested capital)

Sourc

https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/

Terra Collapse: Lessons Learned

Why It Failed:

- Reflexive design: confidence collapse = system collapse
- No external collateral backing
- Anchor Protocol's 20% yield was unsustainable
- "Bank run" dynamics in algorithmic systems

Key Lessons:

- Algorithmic stablecoins carry extreme tail risk
- High yields require sustainable sources
- Decentralization doesn't prevent collapse
- Market cap doesn't equal safety

Do

Kwon later charged with fraud; extradited to US (2024)

Case Study: Aave Protocol

Overview:

- Launched 2020 (evolved from ETHLend 2017)
- Leading DeFi lending protocol
- Multi-chain: Ethereum, Polygon, Avalanche, etc.
- Governance token: AAVE

Key Innovations:

- Flash loans (invented by Aave)
- Variable + stable rate borrowing
- Credit delegation
- Safety Module for protocol insurance

stats: `https://defillama.com/protocol/aave` — **Docs:** `https://aave.com/`

Interest Rate Model:

$$R = R_0 + \frac{U}{U_{optimal}} \cdot R_{slope1} + \max(0, \frac{U - U_{optimal}}{1 - U_{optimal}}) \cdot R_{slope2}$$

- U = utilization rate (percent of pool borrowed)
- R_0 = base rate (minimum interest)
- $U_{optimal}$ = target utilization (typically 80%)
- R_{slope1} = interest rate slope below optimal utilization
- R_{slope2} = interest rate slope above optimal utilization (steep)

Health Factor:

$$HF = \frac{\sum(Collateral_i \times LiquidationThreshold_i)}{TotalBorrows}$$

- $Collateral_i$ = value of asset i deposited as collateral
- $LiquidationThreshold_i$ = maximum borrowable percentage for asset i
- $TotalBorrows$ = total value borrowed
- $HF < 1$: Position can be liquidated; liquidation bonus: 5-10% for liquidators

V3 introduced efficiency mode, isolation mode, and portals for cross-chain

Appendix: DeFi Data Sources

Live Data Dashboards:

- **TVL**: `https://defillama.com/`
- **Stablecoins**: `https://defillama.com/stablecoins`
- **DEX Volumes**: `https://defillama.com/dexs`
- **Lending**: `https://defillama.com/protocols/Lending`

Security Resources:

- **Hack Database**: `https://rekt.news/leaderboard/`
- **Audit Reports**: `https://de.fi/rekt-database`

Alway

verify current data – crypto markets move fast