

L37: Lending Protocols

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

- Understand how DeFi lending protocols work (Aave, Compound)
- Analyze overcollateralization and its necessity
- Calculate health factors and liquidation thresholds
- Explore interest rate models (utilization-based)
- Compare DeFi lending to traditional finance

Traditional Lending

- Credit checks required
- Identity verification (KYC)
- Undercollateralized (borrow more than collateral)
- Long approval process
- Fixed terms and rates
- Geographic restrictions
- Intermediaries (banks)

DeFi Lending

- No credit checks
- Pseudonymous (wallet address)
- Overcollateralized (deposit \geq borrow)
- Instant approval
- Variable rates (algorithmic)
- Global access
- Smart contracts (no intermediaries)

Key Trade-off: DeFi accessibility vs. capital efficiency (must lock more than you borrow).

Core Mechanism:

① Lenders (Suppliers)

- Deposit assets (ETH, USDC, DAI, etc.) into protocol
- Earn interest on deposits (APY varies by utilization)
- Can withdraw anytime (if liquidity available)

② Borrowers

- Deposit collateral (e.g., ETH)
- Borrow up to a percentage of collateral value (e.g., 75%)
- Pay interest to lenders
- Must maintain health factor above 1

③ Protocol

- Matches lenders and borrowers via smart contracts
- Sets interest rates algorithmically
- Manages liquidations

Example: Borrowing on Aave

User Journey:

Step 1: Supply Collateral

- Deposit 10 ETH (worth \$20,000 at \$2,000/ETH)
- Receive aETH tokens (interest-bearing, 1:1 with ETH)

Step 2: Borrow

- ETH has 80% Loan-to-Value (LTV) ratio
- Max borrow: $10 \times \$2,000 \times 0.80 = \$16,000$
- User borrows \$10,000 USDC (safe margin)

Step 3: Manage Position

- Interest accrues on \$10,000 debt (e.g., 5% APY)
- User earns interest on 10 ETH deposit (e.g., 2% APY)
- Net cost: $5\% - 2\% = 3\%$ on borrowed amount

Why Overcollateralization?

Problem: No identity means no recourse if borrower defaults.

Solution: Require collateral worth more than loan.

Mechanism:

- If collateral value drops, protocol liquidates automatically
- Liquidators repay debt, seize collateral (with bonus)
- Lenders remain whole

Trade-off:

- **Capital inefficient:** Can't access full collateral value
- **Safe for lenders:** Minimal default risk

Example Use Cases:

- Leverage (borrow USDC, buy more ETH for long exposure)
- Short selling (borrow ETH, sell it, buy back cheaper)
- Liquidity without selling (keep ETH, borrow USDC for expenses)

Loan-to-Value (LTV) Ratio

Definition:

$$\text{LTV} = \frac{\text{Borrowed Value}}{\text{Collateral Value}} \times 100\%$$

Example LTV Limits (Aave):

- ETH: 80% (can borrow up to 80% of ETH value)
- WBTC: 75%
- USDC: 85% (stablecoin, less volatile)
- Low-cap tokens: 40-60% (higher risk)

Why Different LTVs?

- Volatile assets = lower LTV (more buffer for price swings)
- Stable assets = higher LTV (minimal price risk)

Calculation:

- Collateral: 10 ETH at \$2,000 = \$20,000
- Borrowed: \$12,000 USDC
- LTV: $\frac{12,000}{20,000} = 60\%$ (safe, under 80% max)

Liquidation Threshold

Definition: LTV at which liquidation occurs (always higher than max LTV).

Example (Aave):

- ETH Max LTV: 80%
- ETH Liquidation Threshold: 83%
- Buffer: 3% (gives borrower time to add collateral)

Scenario:

- User borrows at 80% LTV
- ETH price drops 5%
- New LTV: $80\% \times \frac{1}{0.95} \approx 84.2\%$ (exceeds 83% threshold)
- **Liquidation triggered**

Liquidation Penalty:

- Liquidator repays debt, receives collateral + bonus (e.g., 5%)
- Borrower loses penalty amount
- Remaining collateral returned to borrower

Definition: Metric indicating position safety.

Formula (Aave):

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Borrowed Value}}$$

Interpretation:

- Health Factor > 1 : Safe (no liquidation)
- Health Factor = 1: At liquidation threshold
- Health Factor < 1 : Liquidation occurs

Example:

- Collateral: \$20,000 (ETH)
- Borrowed: \$12,000 (USDC)
- Liquidation threshold: 83%

$$\text{HF} = \frac{20,000 \times 0.83}{12,000} = 1.38$$

Safe: 38% buffer before liquidation.

Initial State:

- 10 ETH at \$2,000 = \$20,000 collateral
- \$12,000 USDC borrowed
- Liquidation threshold: 83%
- Health Factor: $\frac{20,000 \times 0.83}{12,000} = 1.38$

ETH drops to \$1,600:

- New collateral value: $10 \times \$1,600 = \$16,000$
- Borrowed still: \$12,000
- New HF: $\frac{16,000 \times 0.83}{12,000} = 1.11$ (still safe)

ETH drops to \$1,446:

- New collateral value: $10 \times \$1,446 = \$14,460$
- New HF: $\frac{14,460 \times 0.83}{12,000} = 1.00$ (liquidation threshold)
- **Position liquidated**

When Health Factor ≤ 1 :

- 1 **Liquidator Bot Detects** unhealthy position
- 2 **Liquidator Repays** portion of debt (up to 50%)
- 3 **Liquidator Receives** equivalent collateral + bonus (5-10%)
- 4 **Borrower Loses** liquidation penalty
- 5 **Remaining Collateral** returned to borrower

Example:

- Debt: \$12,000 USDC
- Collateral: \$14,460 ETH (at \$1,446/ETH)
- Liquidator repays 50%: \$6,000
- Liquidator receives: $\$6,000 \times 1.05 = \$6,300$ in ETH
- Borrower left with: $\$14,460 - \$6,300 = \$8,160$ collateral and \$6,000 debt

Penalty: Borrower lost \$300 (5% of liquidated amount).

Key Concept: Rates adjust based on utilization.

Utilization Rate:

$$U = \frac{\text{Total Borrowed}}{\text{Total Supplied}}$$

Interest Rates:

- Low utilization (0-60%): Low borrow rates (encourage borrowing)
- Optimal utilization (80%): Moderate rates (balanced)
- High utilization (>90%): High rates (encourage repayment, discourage borrowing)

Example (USDC on Aave):

- 0% utilization: 1% borrow APY
- 80% utilization: 5% borrow APY
- 95% utilization: 20% borrow APY (sharp increase)

Why? Prevents bank runs (always keep some liquidity for withdrawals).

Supply and Borrow APY Relationship

Lenders earn a portion of what borrowers pay.

Formula:

$$\text{Supply APY} = \text{Borrow APY} \times U \times (1 - \text{Reserve Factor})$$

where Reserve Factor is protocol fee (e.g., 10%).

Example:

- Borrow APY: 5%
- Utilization: 80%
- Reserve Factor: 10%

$$\text{Supply APY} = 5\% \times 0.80 \times 0.90 = 3.6\%$$

Observation: Supply APY always lower than borrow APY (protocol takes cut, not everyone borrows).

Key Features:

- **Flash Loans:** Borrow without collateral if repaid in same transaction
- **Rate Switching:** Choose stable or variable interest rates
- **Credit Delegation:** Lend your credit line to others
- **Isolation Mode:** New assets isolated to reduce systemic risk
- **E-Mode:** Higher LTV for correlated assets (e.g., ETH/stETH)

Governance:

- AAVE token holders vote on protocol changes
- Risk parameters (LTV, liquidation thresholds)
- Asset listings
- Treasury management

TVL: \$4B (Dec 2024), deployed on Ethereum, Polygon, Avalanche, Arbitrum, Optimism.

Key Features:

- **cTokens:** Interest-bearing tokens (cUSDC, cETH)
- **Algorithmic Rates:** Fully automated interest rate model
- **Governance:** COMP token holders control protocol
- **Simplicity:** Fewer features than Aave, easier to understand

cToken Mechanism:

- Supply 100 USDC, receive 5,000 cUSDC
- cUSDC exchange rate increases over time (accrues interest)
- Redeem cUSDC for USDC + interest anytime

Historical Significance:

- Pioneered DeFi lending (launched 2018)
- Introduced COMP governance token (2020)
- Sparked “DeFi Summer” via liquidity mining

TVL: \$1.5B (Dec 2024).

Definition: Borrow any amount without collateral, repay in same transaction.

How It Works:

- 1 Borrow \$1M USDC from Aave
- 2 Use \$1M for arbitrage, collateral swap, or liquidation
- 3 Repay \$1M + 0.09% fee
- 4 All in one atomic transaction (either all succeeds or all reverts)

Use Cases:

- **Arbitrage:** Exploit price differences across DEXs
- **Collateral Swap:** Switch collateral without closing position
- **Self-Liquidation:** Repay debt before liquidation penalty
- **Exploits:** Unfortunately, used in many DeFi hacks

Fee: 0.09% of borrowed amount.

Risk: If transaction fails, borrow is reversed (no loss to lenders).

Historical Attack: bZx (2020)

Attack Steps:

- 1 Flash loan 10,000 ETH from dYdX
- 2 Deposit 5,500 ETH into Compound as collateral
- 3 Borrow 112 WBTC from Compound
- 4 Swap 112 WBTC on Uniswap for 6,871 ETH (manipulating price)
- 5 Use pumped ETH price to borrow max from bZx
- 6 Repay flash loan, keep profit (\$350k)

Root Cause: bZx used Uniswap as sole price oracle (manipulable).

Lesson: Flash loans amplify oracle manipulation attacks. Protocols must use decentralized, manipulation-resistant oracles.

Aave offers borrowers a choice:

Variable Rate

- Changes with utilization
- Usually lower (on average)
- Unpredictable
- Can spike during high demand

Best for:

- Short-term borrowing
- Users who monitor actively

Switching: Borrowers can switch between rate types anytime.

Stable Rate

- Fixed for duration
- Higher than variable (premium for stability)
- Predictable
- Can be rebalanced by protocol if too far from market

Best for:

- Long-term borrowing
- Risk-averse users

1. Smart Contract Risk

- Bugs or exploits in protocol code
- Historical hacks: Rari Capital, Cream Finance

2. Liquidation Risk

- Volatile markets can trigger liquidations
- Network congestion may prevent adding collateral

3. Oracle Risk

- Price feed manipulation
- Stale prices during network issues

4. Governance Risk

- Malicious proposals changing parameters
- Low voter participation

5. Liquidity Risk

- High utilization prevents withdrawals
- Bank run scenarios (rare but possible)

DeFi (Aave, Compound)

- Non-custodial
- Transparent reserves
- Overcollateralized
- Instant settlement
- Smart contract risk
- No insurance (usually)
- Permissionless

CeFi (BlockFi, Celsius)

- Custodial
- Opaque reserves
- Can be undercollateralized
- T+1 settlement
- Counterparty risk
- Some insurance
- KYC required

2022 Lesson: CeFi lenders (Celsius, Voyager, BlockFi) collapsed. DeFi protocols (Aave, Compound) survived intact, demonstrating transparency advantage.

Current Limitation: DeFi lending is capital inefficient (overcollateralization).

Emerging Solutions:

① On-Chain Credit Scores

- Track repayment history, wallet activity
- Examples: Credora, ARCx

② Real-World Identity

- Link wallet to verified identity (KYC)
- Legal recourse if default
- Examples: Goldfinch, TrueFi

③ Social Collateral

- Community vouching, reputation staking
- Example: Teller Protocol

Trade-off: Undercollateralization requires identity or trust, reducing permissionlessness.

Key Takeaways:

- DeFi lending is permissionless but requires overcollateralization
- LTV ratios vary by asset risk (ETH 80%, low-cap tokens 40%)
- Health factor must stay above 1 to avoid liquidation
- Interest rates adjust algorithmically based on utilization
- Flash loans enable zero-collateral borrowing within one transaction
- Aave and Compound dominate DeFi lending (\$5.5B+ combined TVL)
- Risks: smart contract bugs, liquidations, oracle manipulation
- Future: undercollateralized lending via on-chain credit scoring

Next Lecture: Stablecoin Mechanisms - How stablecoins maintain price stability.

- 1 Calculate health factor for: \$30k collateral, \$20k borrowed, 85% liquidation threshold.
- 2 Why is overcollateralization necessary in DeFi lending?
- 3 How do interest rates adjust to prevent bank runs?
- 4 What risks do flash loans pose to DeFi protocols?
- 5 Would you prefer variable or stable interest rates for a 1-year borrow?