L42: Flash Loans and Composability

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

Why Can You Borrow Millions Without Collateral?

- Borrow $100 million with zero collateral—if you can repay it in the same transaction
- DeFi's atomic execution creates opportunities impossible in traditional finance

[COMIC: Wide-eyed developer realizing they can borrow millions for free. Speech bubble: "Wait... I can borrow $100M with ZERO collateral?!" Calculator showing astronomical numbers]

[PLACEHOLDER] — The power to borrow unlimited capital—if you can use and return it in 12 seconds

Learning Objectives

- Understand flash loan (loan borrowed and repaid in same transaction) mechanics and atomicity (all-or-nothing execution)
- Analyze legitimate flash loan use cases
- Examine flash loan attack vectors and notable exploits
- Explore DeFi composability ("money legos")
- Understand MEV—Maximal Extractable Value (profit from reordering transactions) and its relationship to flash loans

Building on L41: Layer 2 Scaling

The Problem: What new attacks does DeFi enable?

The Challenge
DeFi's composability allows any smart contract to interact with any other protocol within a single atomic transaction. This enables powerful arbitrage and refinancing strategies, but also creates a new attack surface: adversaries can borrow unlimited capital, manipulate protocol state, extract profits, and repay loans—all within one block, with zero upfront capital.

Why It Matters

- Flash loans eliminate capital requirements for large-scale attacks
- Historical examples: bZx attacks ($950K, Feb 2020), Harvest Finance ($34M, Oct 2020), Euler Finance ($197M, Mar 2023)
- Enables both arbitrage (profiting from price differences across markets) and exploits

What We Need

- Risk management and mitigation
- Understanding atomic transaction risks and oracle (external price data feed for smart contracts) manipulation vectors

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Flash Loans addresses this challenge

Continued

How Can You Borrow Millions Without Collateral?

Definition:
Uncollateralized loan borrowed and repaid within single transaction

Key Properties:

- *Atomicity*: All-or-nothing
- If repayment fails: TX reverts
- No collateral required

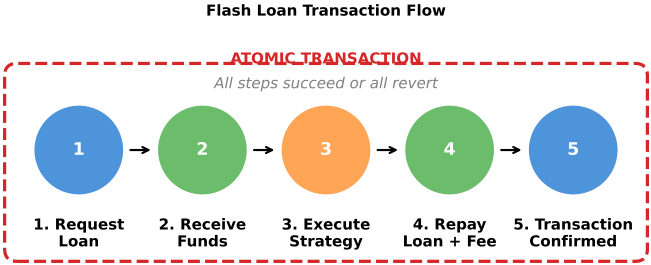
Characteristics:

- **Size**: Unlimited (pool limit)
- **Duration**: One block
- **Risk to lender**: Zero

Unique to DeFi:
Impossible in traditional finance

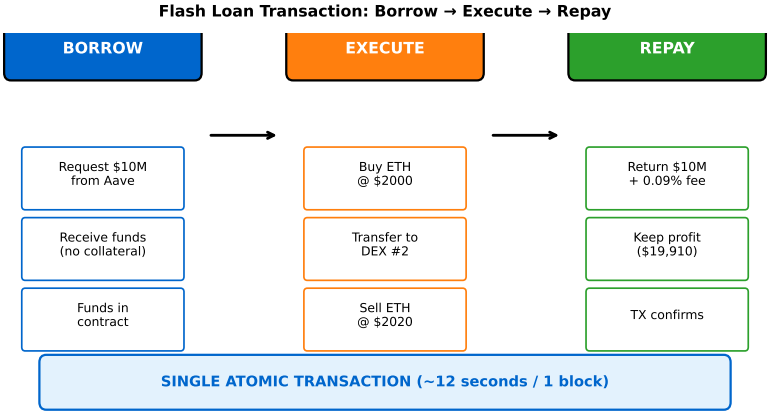
→ *Problem: What new attacks does DeFi enable? — What is a Flash Loan? shows DeFi enables borrowing unlimited capital with zero collateral—impossible in traditional finance, enabling new attack vectors*

How Does a Flash Loan Transaction Work?



If any step fails, the entire transaction reverts – zero risk to lender

What Happens in Each Phase of a Flash Loan?



All three phases must complete within one block (∼12 seconds on Ethereum)

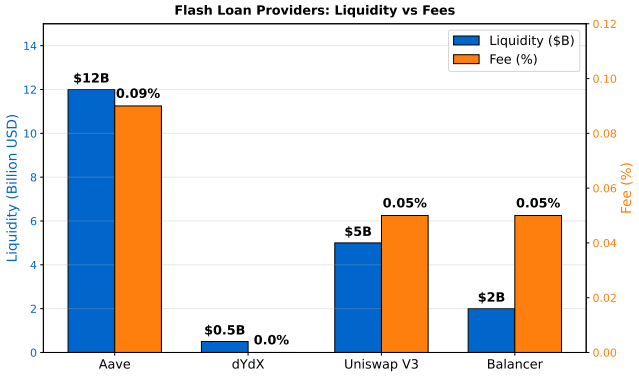
How Do Flash Loans Differ from Traditional Loans?

Property	Traditional Loan	Flash Loan
Collateral	Required (often ¿100%)	None
Duration	Days/months/years	Single transaction
Creditworthiness	Required (KYC)	Not required
Repayment Guarantee	Legal contracts	Smart contract atomicity
Risk to Lender	Default risk	Zero (reverts)

Paradigm Shift: Code execution guarantees replace legal enforcement

Compare the approaches shown above

Which Platforms Offer Flash Loans?



Aave is largest provider; dYdX offers free flash loans

Why Is DeFi Called "Money Legos"?

"Money Legos":

- Permissionless integration
- Any contract calls any contract
- Atomic multi-protocol TX

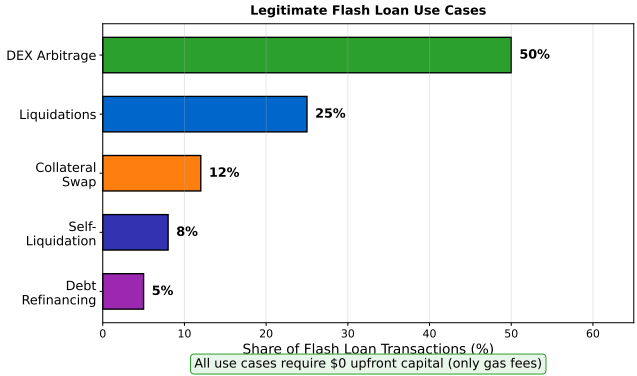
Risk:
Cascading failures, expanded attack surface

Composability Examples:

1. Uniswap → Aave → Borrow
2. Flash → Liquidate → Swap → Repay
3. Compound → Curve yield

→ *Problem: What new attacks does DeFi enable? — DeFi Composability reveals composability creates cascading risk: one protocol's weakness can be exploited via another protocol's flash loan*

What Can Flash Loans Be Used For?



All use cases democratize capital-intensive strategies to anyone

How Do Flash Loans Enable Zero-Capital Arbitrage?

Scenario:
ETH: $2000 (Uniswap) vs $2020 (SushiSwap)
Steps:

1. Borrow 1000 ETH (flash loan)
2. Buy on Uniswap ($2M)
3. Sell on SushiSwap ($2.02M)
4. Repay + fee ($2.001M)

Result:

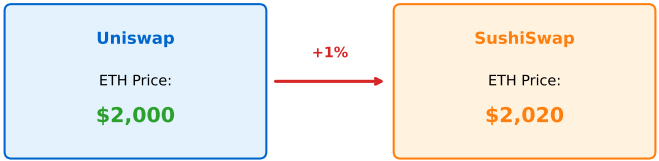
- Profit: $19,000 in one TX
- Capital needed: Gas only ($50-200)

Democratization:
Anyone can arbitrage, not just whales

Compare the approaches shown above

How Does Flash Loan Arbitrage Work in Practice?

Flash Loan Arbitrage: $18,200 Profit with Zero Capital



PROFIT CALCULATION

```
Flash borrow: 1,000 ETH (from Aave)
Buy on Uniswap: 1,000 ETH × 2,000 = 2,000,000
Sell on SushiSwap: 1,000 ETH × 2,020 = 2,020,000
Repay + Fee (0.09%): $2,000,000 + $1,800 = $2,001,800
NET PROFIT: $2,020,000 - $2,001,800 = $18,200
```

Capital Required: Only gas fees (~$50-200)

Flash loans democratize arbitrage: profit without capital, paying only gas fees

How Do Flash Loans Enable Collateral Swaps?

Problem:
User has debt with Asset A collateral, wants Asset B
Steps:

1. Flash borrow Asset A
2. Repay existing debt
3. Withdraw collateral A
4. Deposit collateral B
5. Re-borrow Asset A
6. Repay flash loan

Result:

- Collateral swapped atomically
- Zero liquidation risk
- Fee: 0.05-0.09% only

Key Benefit:
Atomicity ensures no risk during swap

Compare the approaches shown above

Problem Check-In: Flash Loans

Recall Our Problem

What new attacks does DeFi enable?

What We've Learned So Far

- Flash loans are uncollateralized loans repaid within one transaction—if repayment fails, everything reverts
- DeFi composability lets any smart contract call any other protocol atomically ("money legos")
- Together these enable zero-capital attacks: borrow millions, exploit vulnerability, profit, repay—all in one block

Still to Address

- Specific attack patterns (oracle manipulation, governance attacks) and defense mechanisms
- Can protocols be designed to be flash-loan-resistant without sacrificing the composability that makes DeFi powerful?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "What new attacks does DeFi enable?"?

What Makes Flash Loans Dangerous?

Dark Side:
Enable large-scale attacks with zero capital
Attack Pattern:

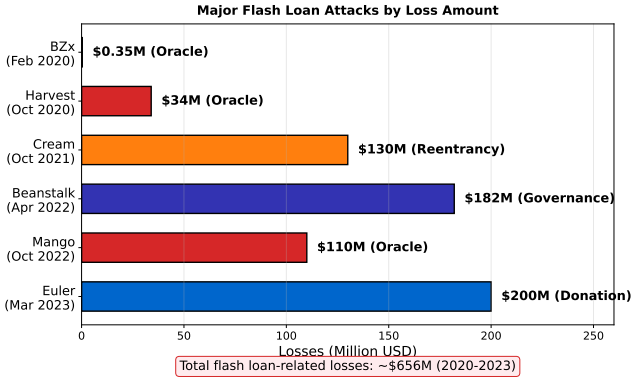
1. Flash borrow massive amount
2. Manipulate state (oracle/gov)
3. Exploit for profit
4. Repay flash loan

Impact:
$500M+ stolen (2020-2023)

Key Insight:
Flash loans *amplify* existing vulnerabilities — they are not the root cause

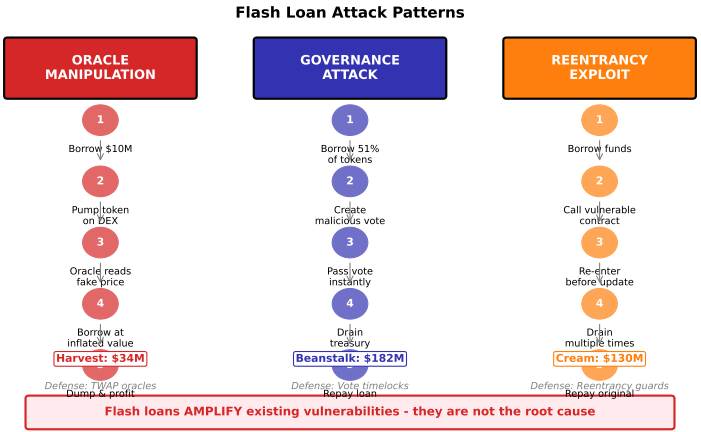
→ *Problem: What new attacks does DeFi enable? — Flash Loan Attacks: Overview demonstrates flash loans amplify existing vulnerabilities: attackers need only gas fees to execute million-dollar exploits*

What Were the Major Flash Loan Attacks?



Oracle manipulation is most common attack vector

What Are the Common Flash Loan Attack Patterns?



Each attack exploits a different vulnerability; defenses exist but trade-offs apply

How Do Attackers Manipulate Price Oracles?

Vulnerability:
Protocol uses single DEX (Decentralized Exchange) as oracle

Attack Steps:

1. Flash borrow 10K ETH
2. Buy all TOKEN (10x pump)
3. Oracle reads inflated price
4. Borrow stables at fake price
5. Sell TOKEN (price normalizes)
6. Repay flash loan

Real Example:
Harvest Finance: $34M stolen

Mitigation:

- Use TWAP (time-weighted)
- Use Chainlink oracles
- Multiple price sources

Compare the approaches shown above

How Can Protocols Defend Against Flash Loan Attacks?

Oracle Protection:

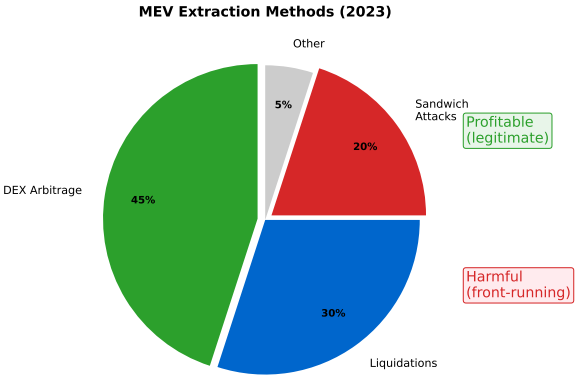
- Decentralized oracles (Chainlink)
- TWAP: Average over blocks
- Multiple price sources

Protocol Protection:

- Reentrancy guards
- Governance timelocks
- Vote locking periods
- Circuit breakers

Compare the approaches shown above

How Do Flash Loans Enable MEV Extraction?



Flash loans amplify both legitimate arbitrage and harmful MEV extraction | → Problem: What new attacks does DeFi enable? — MEV and Flash Loans shows MEV extractors use flash loans to profit from transaction ordering, harming regular users via front-running

How Do Bots Extract MEV from Flash Loans?

MEV: Maximal Extractable Value
Profit from transaction ordering
Techniques:

- **Front-running (placing your transaction ahead of someone else's to profit)**: TX before victim
- **Back-running**: TX after victim
- **Sandwich**: Front + back-run

Flash Loans + MEV:
Amplify arbitrage and liquidation profits
Scale:

- $600M+ extracted (2023)
- Flashbots: Democratize MEV
- Reduces gas wars

Compare the approaches shown above

What Is the Economic Impact of Flash Loans?

Positive Effects

- Democratize arbitrage
- Increase market efficiency
- Enable capital-efficient refinancing
- Liquidation bots improve protocol health

Negative Effects

- Enable zero-capital attacks
- Amplify protocol vulnerabilities
- MEV extraction harms users
- Governance manipulation risk

Net Assessment: Powerful tool that magnifies both good and bad protocol design

Compare the approaches shown above

Are Flash Loan Exploits Legal or Illegal?

Legal Gray Area:
No clear regulatory framework
Key Questions:

- Theft or code exploitation?
- Protocol or attacker liable?
- Code is law vs legal?

Precedent:
Mango Markets attacker arrested (Dec 2022)

- Charged: market manipulation
- Not: flash loan use itself

Protocol Responsibility:
Bug bounties, audits, insurance

Compare the approaches shown above

Problem Solved? Flash Loans

The Original Problem

What new attacks does DeFi enable?

How Flash Loans Solves It

- Atomic transactions enable instant arbitrage and liquidations, democratizing capital-intensive strategies
- All-or-nothing execution ensures zero risk to lenders via transaction reversion
- Composability allows permissionless integration across protocols

Remaining Limitations

- Oracle manipulation: Single-block price feeds can be distorted to exploit lending protocols
- Governance attacks: Flash-borrowed tokens enable malicious proposal execution without long-term commitment

Open Questions

- How do we design flash-loan-resistant protocols without sacrificing composability?
- Risk: Black swan events, cascading failures

Flash Loans partially solves "What new attacks does DeFi enable" but introduces new trade-offs

Cryptoeconomics

The Economics of Flash Loans

Incentive Structure

- Managing systemic and idiosyncratic risks
- Risk-adjusted returns, insurance mechanisms
- Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Flash Loans

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Flash Loans

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

What Does Flash Loan Arbitrage Really Look Like?

- Profitable arbitrage requires finding price discrepancies, writing exploit code, and competing with MEV bots—all in milliseconds
- The gap between "borrow millions for free" and "profitable arbitrage" is filled with failed transactions and gas costs

[COMIC: Developer surrounded by multiple monitors showing complex arbitrage calculations, failed transactions, and MEV bot competition. Speech bubble: "The arbitrage looked so simple in the tutorial..." Red "TX FAILED" messages scattered around]

[PLACEHOLDER] — Flash loans democratize capital access but not the expertise needed to profit from it

Summary

Summary

Flash Loans:

- Uncollateralized, atomic
- Zero lender risk (reverts)
- Use: Arbitrage, collateral swap
- Composability: "Money legos"

Next Lesson: L43 – Smart Contract Security

Security:

- Attacks: $500M+ stolen
- Amplify vulnerabilities
- Defenses: TWAP, Chainlink
- Circuit breakers, timelocks

Flash loans are a powerful tool that magnifies both good and bad protocol design

Questions for Reflection

1. Why can flash loans exist in DeFi but not in traditional finance?
2. How do flash loans democratize arbitrage opportunities?
3. What makes oracle manipulation the most common attack vector?
4. Should flash loan attackers be prosecuted if they exploit code bugs?
5. How can protocols defend against flash loan governance attacks?

Key point: Questions for Reflection

Quiz Questions (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which flash loan provider offers free flash loans (0% fee)?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers 0% fee; Aave charges 0.09%.

Q4. In the arbitrage example, ETH is $2000 on Uniswap and $2020 on SushiSwap. What is the profit from a 1000 ETH flash loan arbitrage (before fees)?
A) $10,000 B) $19,000 C) $20,000 D) $2,000
Answer: C – Buy for $2M, sell for $2.02M = $20,000 profit.

Q5. What does DeFi composability refer to?
A) Combining multiple cryptocurrencies B) Permissionless integration like "money legos"
C) Creating new tokens D) Merging blockchain networks
Answer: B – Composability allows atomic transactions across multiple protocols.

Quiz Questions (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q7. Which of the following is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q8. How much was stolen via flash loan attacks between 2020-2023?
A) $50M+ B) $100M+ C) $500M+ D) $1B+
Answer: C – Over $500M stolen during this period.

Q9. In the Harvest Finance attack, what was the primary vulnerability exploited?
A) Reentrancy bug B) Single DEX price oracle C) Governance takeover D) Smart contract bug
Answer: B – Single DEX oracle allowed price manipulation.

Q10. What is TWAP and how does it defend against flash loan attacks?
A) Total Weighted Asset Pool B) Time-Weighted Average Price
C) Token Withdrawal Attack Prevention D) Trusted Wallet Authentication
Answer: B – TWAP averages prices over blocks, preventing single-transaction manipulation.

Quiz

Quiz Questions (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital
Answer: C – Flash loans democratize arbitrage by requiring only gas fees.

Q12. What does MEV stand for?
A) Maximum Extractable Value B) Miner Extractable Value
C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

Q13. Which defense mechanism requires tokens to be locked before voting?
A) Circuit breakers B) Reentrancy guards C) Vote locking D) TWAP oracles
Answer: C – Vote locking prevents flash loan governance attacks.

Q14. What was the approximate MEV volume extracted in 2023?
A) $60M+ B) $200M+ C) $600M+ D) $2B+
Answer: C – Over $600M extracted via MEV in 2023.

Q15. In a sandwich attack, what does the attacker do?
A) Front-run and back-run a victim's transaction B) Split transaction into parts
C) Surround smart contract with malicious code D) Execute trades on multiple DEXs
Answer: A – Sandwich attacks place transaction before and after victim's transaction.

Quiz Questions (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys
Answer: B – Flashbots democratizes MEV extraction and reduces network congestion.

Q17. What was the charge against the Mango Markets attacker in December 2022?
A) Flash loan abuse B) Market manipulation C) Smart contract hacking D) Money laundering
Answer: B – Charged with market manipulation, not specifically flash loan use.

Q18. Which oracle solution is recommended to prevent flash loan price manipulation?
A) Single DEX price feed B) Centralized price API
C) Chainlink decentralized oracles D) On-chain voting
Answer: C – Chainlink aggregates prices from multiple sources, preventing manipulation.

Q19. What is the primary reason flash loans amplify protocol vulnerabilities?
A) They are free to execute B) They provide unlimited capital for exploitation
C) They bypass security checks D) They cannot be traced
Answer: B – Flash loans allow borrowing unlimited amounts to exploit vulnerabilities at scale.

Q20. In a collateral swap using flash loans, what is the main benefit?
A) Lower interest rates B) Zero liquidation risk during swap
C) No transaction fees D) Increased borrowing capacity
Answer: B – Atomicity ensures instant swap with zero liquidation risk.