L42: Flash Loans and Composability

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand flash loan mechanics and atomicity
- Analyze legitimate flash loan use cases
- Examine flash loan attack vectors and notable exploits
- Explore DeFi composability ("money legos")
- Understand MEV and its relationship to flash loans

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)

What We Need

- Risk management and mitigation
- Understanding atomic transaction risks and oracle manipulation vectors

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Flash Loans addresses this challenge

What is a Flash Loan?

Definition:
Uncollateralized loan borrowed and repaid within single transaction

Key Properties:

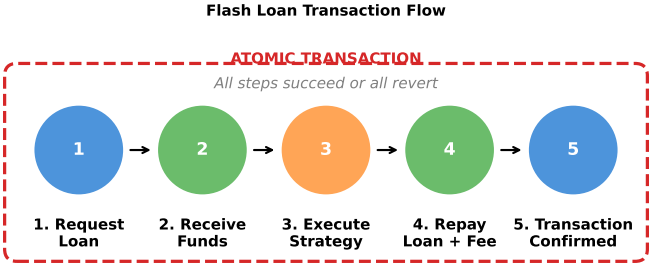
- *Atomicity*: All-or-nothing
- If repayment fails: TX reverts
- No collateral required

Characteristics:

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

Unique to DeFi:
Impossible in traditional finance

Flash Loan Transaction Flow



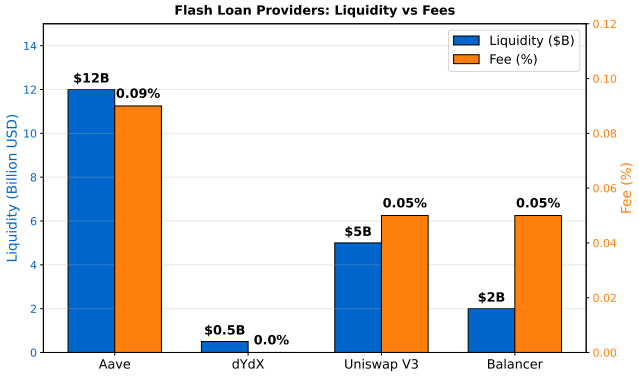
If any step fails, the entire transaction reverts – zero risk to lender

Traditional Loans vs Flash 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

Flash Loan Providers



Aave is largest provider; dYdX offers free flash loans

DeFi Composability

“Money Legos”:

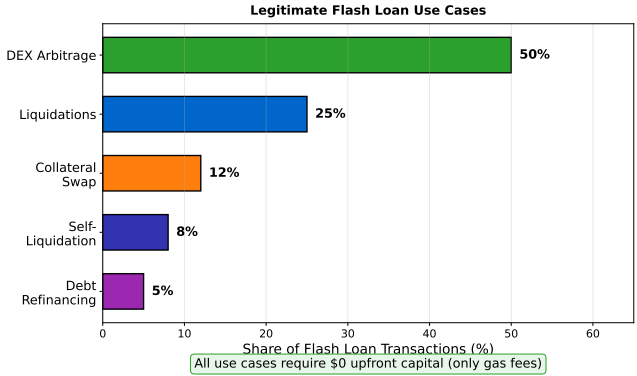
- Permissionless integration
- Any contract calls any contract
- Atomic multi-protocol TX

Risk:
Cascading failures, expanded attack surface

Composability Examples:

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

Legitimate Use Cases



All use cases democratize capital-intensive strategies to anyone

Flash Loan Use Case: 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

Flash Loan Use Case: Collateral Swap

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

Flash Loan Attacks: Overview

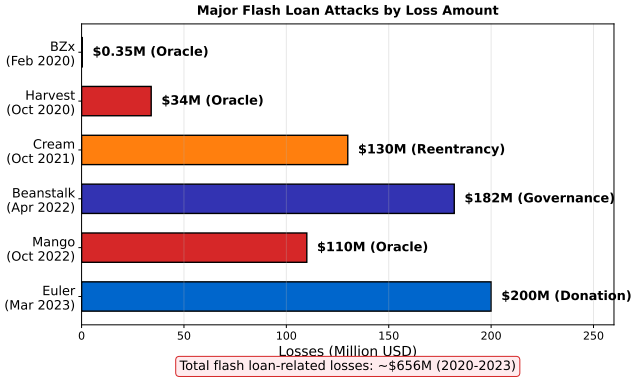
Dark Side:
Enable large-scale attacks with zero capital
Attack Pattern:

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

Major Flash Loan Attacks



Oracle manipulation is most common attack vector

Attack Example: Oracle Manipulation

Vulnerability:
Protocol uses single DEX 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

Defense Mechanisms

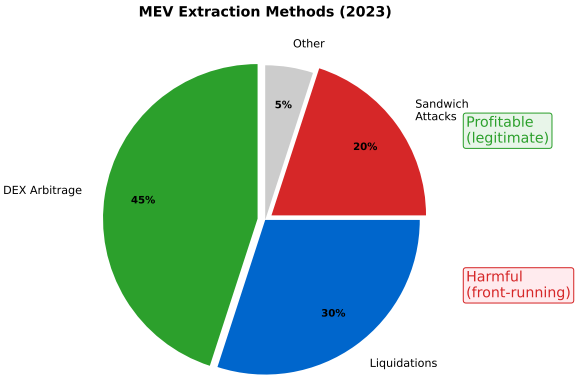
Oracle Protection:

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

Protocol Protection:

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

MEV and Flash Loans



Flash loans amplify both legitimate arbitrage and harmful MEV extraction

MEV Extraction Techniques

MEV: Maximal Extractable Value
Profit from transaction ordering
Techniques:

- **Front-running**: 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

Economic Impact

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

(c) Joerg Osterrieder 2025

Flash Loans and Regulation

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

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

Summary

Flash Loans:

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

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?

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 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.