When DeFi Breaks: Crashes, Hacks & Lessons

Terra/Luna and the 2022 Meltdown

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

Learning Objectives

By the end of this lecture, you will be able to:

1. **Describe** the Terra/UST death spiral step by step [Understand]
2. **Explain** how contagion spread through CeFi and DeFi in 2022 [Understand]
3. **Classify** the 5 main DeFi failure categories [Analyze]
4. **Evaluate** whether a protocol is safe using a risk checklist [Evaluate]

No math required. Main slides use only plain English and pictures.
Technical formulas are in the Appendix for those who want them.

Bloom's levels covered: Understand, Analyze, Evaluate. The Appendix adds Apply.

What You Need to Know Before This Lecture

Wallet
A digital keychain that stores your private keys and lets you send and receive tokens.

Stablecoin
A token designed to stay at a fixed price, usually one dollar.

Token
A digital asset on a blockchain. Can represent money, ownership, or a vote.

Collateral
An asset you lock up as security for a loan. If you do not repay, you lose it.

Smart Contract
A self-executing program on the blockchain. Once deployed, it runs exactly as written.

Liquidity Pool
A pot of tokens locked in a smart contract that enables trading without a middleman.

Key terms from Decks 1–4. If any of these are unfamiliar, review the earlier lectures first.

The Problem

May 2022

40 billion dollars vanished
in 5 days.

How?

Could it happen again?

The Terra/Luna collapse was the largest single failure in crypto history. This lecture explains exactly what happened.

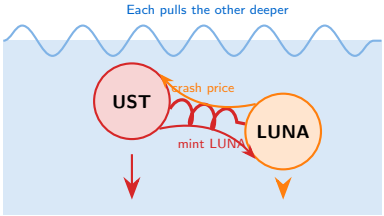
The Drowning Analogy

UST and LUNA were like **two drowning people pulling each other under**.

The deadly loop:

1. UST loses its dollar peg
2. LUNA is minted to restore it
3. More LUNA means lower LUNA price
4. Lower LUNA means less backing for UST

Result: Both drown together.



Reflexive feedback loop: once it starts, it is almost impossible to stop.

This is called a reflexive feedback loop. Once it starts, it accelerates — each step makes the next step worse.

Terra Before the Crash

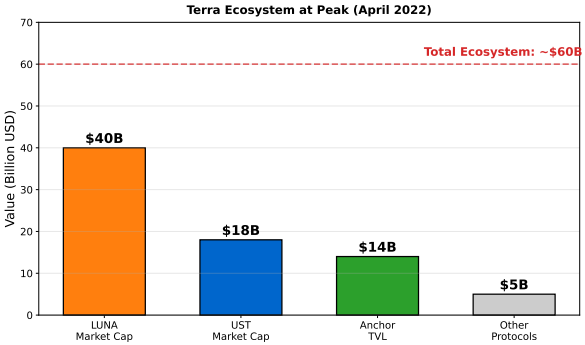
The Terra ecosystem looked impressive on paper:

UST: 18 billion dollar algorithmic stablecoin

Anchor: 20% APY on UST deposits

The problem: 14 billion in deposits vs only 1.5 billion in borrows

The math did not work. Anchor was paying out far more than it earned.



20% yield with almost no borrowers. Terra injected $470M on Feb 18, 2022 to keep Anchor running.

Anchor: The 20% Trap

Anchor offered **20% interest** on UST deposits.
Where did the yield come from?

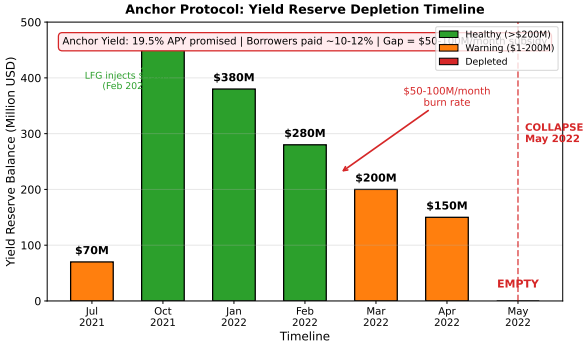
Not from borrowers

Only $1.5B in borrows could not fund $14B in deposit interest.

From Terra's treasury

Terra subsidized it: $470M injected Feb 2022. A one-way money drain.

When the treasury ran out, the music stopped.

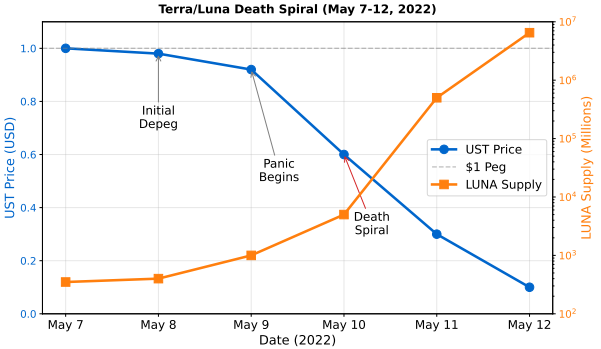


If yield does not come from real economic activity, it comes from new deposits. That is a Ponzi dynamic.

Day by Day: The Collapse

Date	Event	UST
May 7	375M UST withdrawn from Anchor	$0.985
May 8	LFG pledges $750M BTC defense	$0.98
May 9	Death spiral begins	$0.35
May 13	Blockchain halted	$0.02

LUNA went from $80 to $0.0001.
Supply: 350M to 6.5 **trillion** tokens.



In 5 days, $40 billion in value was destroyed. LUNA went from $80 to $0.0001.

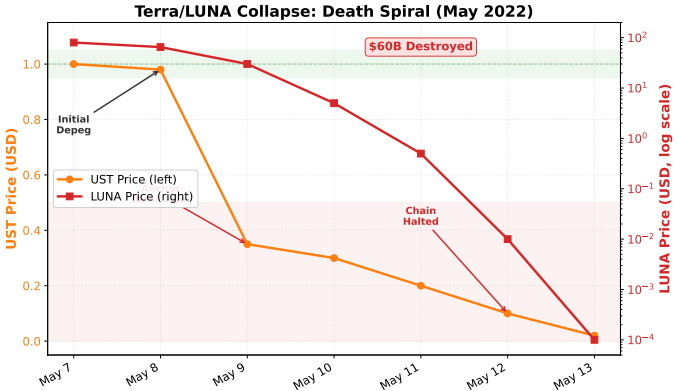
Terra/Luna: The Collapse Visualized

What a $40 billion collapse looks like:

- LUNA price: $80 → $0.0001
- UST price: $1.00 → $0.02
- LUNA supply: 350M → 6.5 trillion
- Market cap lost: **$45B+**

Five days. That is how long it took.

The fastest destruction of value in crypto history.



Zoom-out view: the whole Terra ecosystem, wiped out in a week.

The Death Spiral Explained

The 4-step cycle that destroyed Terra:

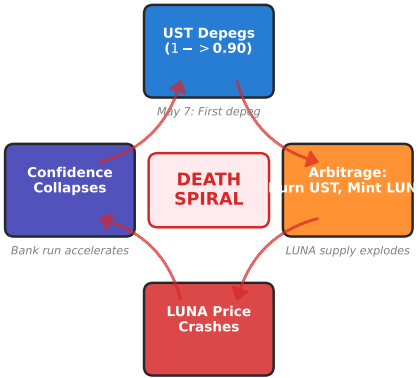
Step 1: UST loses its dollar peg

Step 2: Arbitrageurs mint LUNA to redeem UST at face value

Step 3: LUNA supply explodes (350M to 6.5 trillion)

Step 4: LUNA crashes, making UST even less backed. Repeat.

Terra/Luna Death Spiral Mechanics



May 7-12, 2022: UST $1.00 -> $0.01 | LUNA 350M -> 6.5T tokens | $40B+ lost

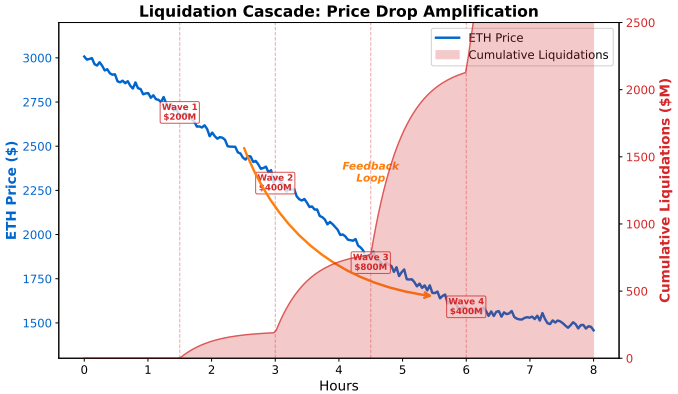
LUNA supply went from 350 million to 6.5 TRILLION tokens in 5 days. Each step made the next step worse.

Liquidation Cascades: When Collateral Dies

Death spirals happen in lending too.

When prices drop fast, loans get liquidated. Liquidators dump the collateral on the market — pushing prices down further — triggering more liquidations.

- **Black Thursday (Mar 2020)** — MakerDAO lost $8.3M to zero-bid auctions
- **Luna (May 2022)** — same pattern, bigger scale



Any reflexive system — algo stablecoins, leveraged lending — can cascade. That is what "systemic risk" means in DeFi.

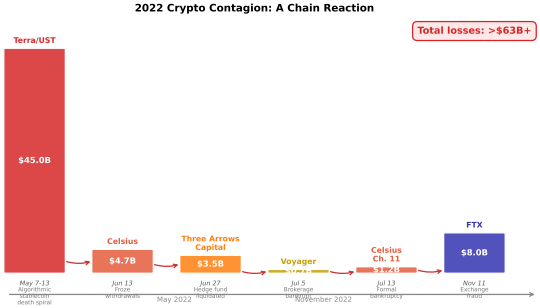
The Domino Effect

Terra did not collapse alone. It pulled down a chain of companies that were secretly connected through loans and investments.

The chain reaction:

- Three Arrows Capital invested in Terra
- Celsius and Voyager lent to Three Arrows
- FTX/Alameda lent to everyone

Hidden leverage amplified every failure.

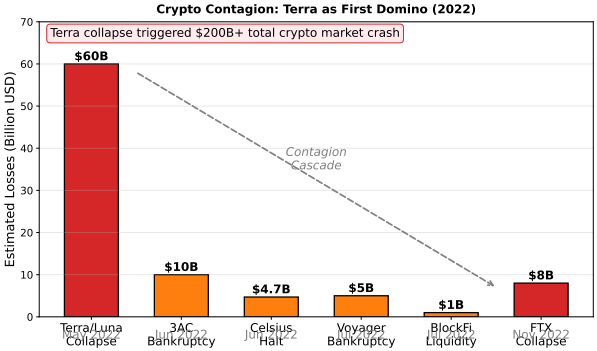


Total 2022 losses: $70B+ across the cascade from Terra to FTX. Interconnected leverage was the common thread.

The 2022 Cascade

Date	Event	Lost
May 7–13	Terra/UST collapse	$45B
Jun 13	Celsius freezes withdrawals	$4.7B
Jun 27	Three Arrows Capital	$3.5B
Jul 5	Voyager Digital	$670M
Jul 13	Celsius Chapter 11	$1.2B
Nov 11	FTX bankruptcy	$8B

Total: over 70 billion dollars destroyed in 6 months.

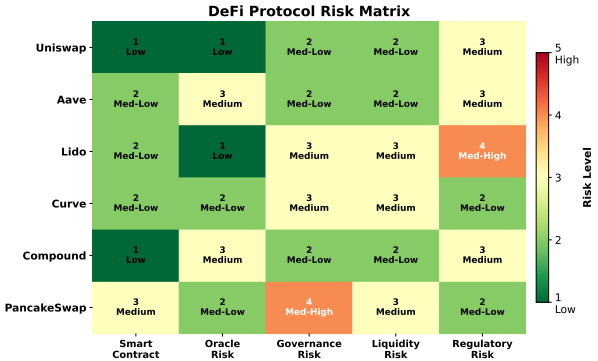


Each failure revealed the next. Interconnected leverage was the common thread.

Five Ways DeFi Breaks

Category	Example	Lost
Algo stablecoin	Terra/UST	$45B
Smart contract	Euler Finance	$197M
Bridge hack	Ronin Bridge	$625M
Oracle attack	Mango Markets	$117M
CeFi counterparty	FTX	$8B

Knowing the categories helps you evaluate risk before using a protocol.



Five categories, five different attack surfaces. A protocol can be vulnerable to more than one.

Category 1: Smart Contract Exploits

Bugs in code. Smart contracts are public — anyone can read them, including hackers.

Euler Finance (Mar 2023)

$197M drained via flash loan exploit. One unprotected function (`donateToReserves`).

Outcome: Attacker returned all funds after negotiation.

Smart contract code is public. Anyone can read it — including hackers. See Appendix A2 for the full attack.

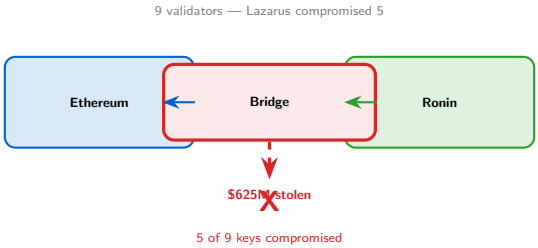
Category 2: Bridge Hacks

Bridges connect blockchains. They hold large amounts of locked tokens — making them high-value targets.

Ronin Bridge

March 23, 2022: North Korea's Lazarus Group stole $625M by compromising 5 of 9 validator keys.

The hack went **undetected for 6 days**. Nobody noticed $625M was missing.

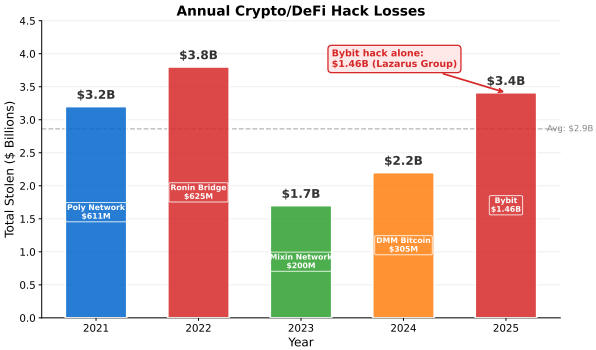


Bridges are DeFi's weakest link. They hold large amounts of locked tokens and often rely on a small set of validators.

Hack Losses by Year

Year	Stolen	Largest
2021	$3.2B	Poly Network $611M
2022	$3.8B	Ronin $625M
2023	$1.7B	Euler $197M
2024	$2.2B	DMM Bitcoin $305M
2025	**$3.41B**	**Bybit $1.5B**

2025 was the worst year. Bybit ($1.5B, Feb 21, 2025) was the single largest hack ever. Attributed to North Korea's Lazarus Group.



2025 was the worst year: $3.41B stolen. Bybit ($1.5B) was the single largest hack in crypto history.

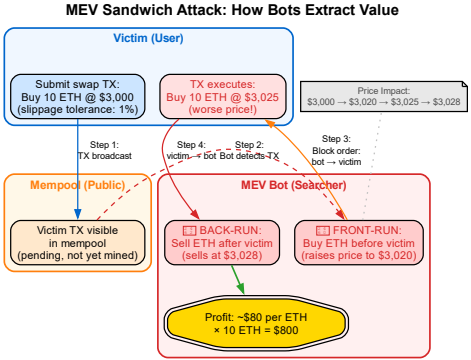
MEV: The Invisible Tax

MEV = Maximal Extractable Value. Invisible middlemen reorder your transactions to profit at your expense.

The sandwich attack:

1. You submit a big swap
2. A bot buys before you (front-run)
3. Your trade executes at a worse price
4. The bot sells after you (back-run)

Sandwich attacks: $289.76M in 2025 alone. Cumulative since 2020: over 7.2 billion dollars. Annual: 3 billion dollars or more.



MEV is a design flaw, not a bug. Every user of Ethereum pays this invisible tax. See Appendix A3 for a worked example.

Do Kwon: Legal Aftermath

Terra founder **Do Kwon** faces criminal charges across multiple jurisdictions.

Timeline:

- **May 2022:** Terra collapses
- **Sep 2022:** South Korea issues arrest warrant
- **Mar 2023:** Arrested in Montenegro
- **Dec 2024:** Extradited to the United States
- **2026:** Trial ongoing — fraud and market manipulation charges

Who is pursuing charges?

SEC (US): Securities fraud

DOJ (US): Wire fraud, market manipulation

South Korea: Capital markets violations

Montenegro: Document forgery

The legal consequences are still playing out **4 years** after the collapse.

Do Kwon's case will set precedent for crypto founder liability. Building a flawed protocol can lead to prison.

Lessons Learned

Lesson 1

If yield seems too high, ask where it comes from. Anchor's 20% was subsidized, not earned.

Lesson 2

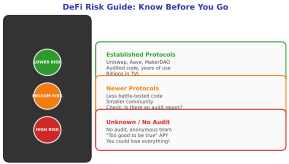
Algorithmic pegs can break. No amount of clever math can override a bank run.

Lesson 3

CeFi counterparty risk is real. FTX looked safe until it was not.

Lesson 4

Diversification matters. Never put everything in one protocol or one ecosystem.



The 2022 cascade taught the entire industry. Surviving protocols are now stronger because of it.

Your DeFi Safety Checklist

✓ Is the code audited?

Look for audits by Trail of Bits, OpenZeppelin, or Consensys Diligence.

✓ How decentralized are the validators?

More validators = harder to attack. Ronin had only 9.

✓ Is TVL growing or shrinking?

Shrinking TVL can signal loss of confidence. Check defillama.com.

✓ Is there a bug bounty?

Top protocols offer millions for found vulnerabilities. No bounty = red flag.

✓ Where does yield come from?

Real yield = fees from users. Fake yield = emissions or treasury subsidies.

Rule of thumb: If you cannot answer these 5 questions, do not deposit your money.

Use this checklist before depositing into ANY protocol. Five minutes of research can save thousands of dollars.

Try It Yourself

Step 1: Explore rekt.news

The searchable database of every major crypto hack. Look up: Ronin Bridge, Euler Finance, Terra/UST.

Step 2: Check DefiLlama hacks

Visit `defillama.com/hacks` for live statistics on all DeFi exploits with amounts and categories.

Step 3: Evaluate a protocol

Pick any DeFi protocol on DefiLlama. Apply the 5-question safety checklist from the previous slide.

Step 4: Compare

Compare Aave (established, audited) with a random new protocol. Which scores higher on the checklist?

Studying past failures is the best way to evaluate future risk. These are free, public resources anyone can use.

Key Takeaways

1. Death Spiral

Terra's reflexive feedback loop destroyed $45 billion. UST and LUNA pulled each other down.

2. Contagion

2022 total losses: $70 billion or more, from Terra to Celsius to Three Arrows to FTX.

3. Five Categories

Algo stablecoin, smart contract exploit, bridge hack, oracle manipulation, CeFi counterparty.

4. The Key Question

Always ask: where does the yield come from? If you cannot answer, do not invest.

DeFi is powerful but not safe by default.
Understanding risk is the real skill.

DeFi is powerful but not safe by default. Understanding risk is the real skill.

Quick Quiz (1–5)

Q1. What was Terra's UST?
A) A fiat-backed stablecoin B) An algorithmic stablecoin pegged to $1 C) A governance token D) A wrapped Bitcoin

Quick Quiz (1–5)

Q1. What was Terra's UST?
A) A fiat-backed stablecoin B) An algorithmic stablecoin pegged to $1 C) A governance token D) A wrapped Bitcoin
Answer: B – UST used a mint/burn mechanism with LUNA to maintain its peg, with no fiat reserves.

Q2. What caused UST's death spiral?
A) Reflexive feedback: UST depeg caused LUNA minting, crashing LUNA, further depegging UST
B) A government ban C) An exchange hack D) A bug in the code

Quick Quiz (1–5)

Q1. What was Terra's UST?
A) A fiat-backed stablecoin B) An algorithmic stablecoin pegged to $1 C) A governance token D) A wrapped Bitcoin
Answer: B – UST used a mint/burn mechanism with LUNA to maintain its peg, with no fiat reserves.

Q2. What caused UST's death spiral?
A) Reflexive feedback: UST depeg caused LUNA minting, crashing LUNA, further depegging UST
B) A government ban C) An exchange hack D) A bug in the code
Answer: A – Each step made the next step worse. Minting LUNA to restore UST crashed LUNA's price.

Q3. What was Anchor's fatal flaw?
A) Too few users B) High gas fees C) Bad user interface D) 20% yield with almost no borrowers

Quick Quiz (1–5)

Q1. What was Terra's UST?
A) A fiat-backed stablecoin B) An algorithmic stablecoin pegged to $1 C) A governance token D) A wrapped Bitcoin
Answer: B – UST used a mint/burn mechanism with LUNA to maintain its peg, with no fiat reserves.

Q2. What caused UST's death spiral?
A) Reflexive feedback: UST depeg caused LUNA minting, crashing LUNA, further depegging UST
B) A government ban C) An exchange hack D) A bug in the code
Answer: A – Each step made the next step worse. Minting LUNA to restore UST crashed LUNA's price.

Q3. What was Anchor's fatal flaw?
A) Too few users B) High gas fees C) Bad user interface D) 20% yield with almost no borrowers
Answer: D – $14B in deposits earning 20%, but only $1.5B in borrows. Terra subsidized the gap.

Q4. How much was lost in the Terra collapse?
A) $1 billion B) $10 billion C) Approximately 45 billion dollars D) $100 billion

Quick Quiz (1–5)

Q1. What was Terra's UST?
A) A fiat-backed stablecoin B) An algorithmic stablecoin pegged to $1 C) A governance token D) A wrapped Bitcoin
Answer: B – UST used a mint/burn mechanism with LUNA to maintain its peg, with no fiat reserves.

Q2. What caused UST's death spiral?
A) Reflexive feedback: UST depeg caused LUNA minting, crashing LUNA, further depegging UST
B) A government ban C) An exchange hack D) A bug in the code
Answer: A – Each step made the next step worse. Minting LUNA to restore UST crashed LUNA's price.

Q3. What was Anchor's fatal flaw?
A) Too few users B) High gas fees C) Bad user interface D) 20% yield with almost no borrowers
Answer: D – $14B in deposits earning 20%, but only $1.5B in borrows. Terra subsidized the gap.

Q4. How much was lost in the Terra collapse?
A) $1 billion B) $10 billion C) Approximately 45 billion dollars D) $100 billion
Answer: C – Direct losses from UST and LUNA were approximately $45 billion.

Q5. Which was the largest single hack in crypto history?
A) Ronin Bridge ($625M) B) Bybit ($1.5B, 2025, Lazarus Group) C) Poly Network ($611M) D) Mt. Gox ($460M)

Quick Quiz (1–5)

Q1. What was Terra's UST?
A) A fiat-backed stablecoin B) An algorithmic stablecoin pegged to $1 C) A governance token D) A wrapped Bitcoin
Answer: B – UST used a mint/burn mechanism with LUNA to maintain its peg, with no fiat reserves.

Q2. What caused UST's death spiral?
A) Reflexive feedback: UST depeg caused LUNA minting, crashing LUNA, further depegging UST
B) A government ban C) An exchange hack D) A bug in the code
Answer: A – Each step made the next step worse. Minting LUNA to restore UST crashed LUNA's price.

Q3. What was Anchor's fatal flaw?
A) Too few users B) High gas fees C) Bad user interface D) 20% yield with almost no borrowers
Answer: D – $14B in deposits earning 20%, but only $1.5B in borrows. Terra subsidized the gap.

Q4. How much was lost in the Terra collapse?
A) $1 billion B) $10 billion C) Approximately 45 billion dollars D) $100 billion
Answer: C – Direct losses from UST and LUNA were approximately $45 billion.

Q5. Which was the largest single hack in crypto history?
A) Ronin Bridge ($625M) B) Bybit ($1.5B, 2025, Lazarus Group) C) Poly Network ($611M) D) Mt. Gox ($460M)
Answer: B – Bybit lost $1.5B on February 21, 2025. Attributed to North Korea's Lazarus Group.

Quick Quiz (6–10)

Q6. What is a bridge hack?
A) Stealing locked tokens from a cross-chain bridge B) Attacking a network router
C) Exploiting a stablecoin D) Manipulating an oracle

Quick Quiz (6–10)

Q6. What is a bridge hack?
A) Stealing locked tokens from a cross-chain bridge B) Attacking a network router
C) Exploiting a stablecoin D) Manipulating an oracle
Answer: A – Bridges hold large pools of locked tokens, making them high-value targets.

Q7. Total stolen from DeFi hacks in 2025?
A) $500 million B) $1.7 billion C) $2.2 billion D) $3.41 billion

Quick Quiz (6–10)

Q6. What is a bridge hack?
A) Stealing locked tokens from a cross-chain bridge B) Attacking a network router
C) Exploiting a stablecoin D) Manipulating an oracle
Answer: A – Bridges hold large pools of locked tokens, making them high-value targets.

Q7. Total stolen from DeFi hacks in 2025?
A) $500 million B) $1.7 billion C) $2.2 billion D) $3.41 billion
Answer: D – 2025 saw $3.41 billion stolen, the worst year on record.

Q8. What is MEV?
A) A type of stablecoin B) A consensus mechanism
C) Value extracted by reordering transactions in a block D) A governance attack

Quick Quiz (6–10)

Q6. What is a bridge hack?
A) Stealing locked tokens from a cross-chain bridge B) Attacking a network router
C) Exploiting a stablecoin D) Manipulating an oracle
Answer: A – Bridges hold large pools of locked tokens, making them high-value targets.

Q7. Total stolen from DeFi hacks in 2025?
A) $500 million B) $1.7 billion C) $2.2 billion D) $3.41 billion
Answer: D – 2025 saw $3.41 billion stolen, the worst year on record.

Q8. What is MEV?
A) A type of stablecoin B) A consensus mechanism
C) Value extracted by reordering transactions in a block D) A governance attack
Answer: C – MEV bots front-run and back-run user trades to extract profit. Over $3B annually.

Q9. Which entity collapsed AFTER Terra but BEFORE FTX?
A) Coinbase B) Three Arrows Capital (June 2022) C) Binance D) MakerDAO

Quick Quiz (6–10)

Q6. What is a bridge hack?
A) Stealing locked tokens from a cross-chain bridge B) Attacking a network router
C) Exploiting a stablecoin D) Manipulating an oracle
Answer: A – Bridges hold large pools of locked tokens, making them high-value targets.

Q7. Total stolen from DeFi hacks in 2025?
A) $500 million B) $1.7 billion C) $2.2 billion D) $3.41 billion
Answer: D – 2025 saw $3.41 billion stolen, the worst year on record.

Q8. What is MEV?
A) A type of stablecoin B) A consensus mechanism
C) Value extracted by reordering transactions in a block D) A governance attack
Answer: C – MEV bots front-run and back-run user trades to extract profit. Over $3B annually.

Q9. Which entity collapsed AFTER Terra but BEFORE FTX?
A) Coinbase B) Three Arrows Capital (June 2022) C) Binance D) MakerDAO
Answer: B – Three Arrows Capital collapsed in June 2022, five months before FTX in November.

Q10. Best question to ask before using a DeFi protocol?
A) "Where does the yield come from?" B) "What is the token price?"
C) "How many Twitter followers?" D) "Is the logo nice?"

Quick Quiz (6–10)

Q6. What is a bridge hack?
A) Stealing locked tokens from a cross-chain bridge B) Attacking a network router
C) Exploiting a stablecoin D) Manipulating an oracle
Answer: A – Bridges hold large pools of locked tokens, making them high-value targets.

Q7. Total stolen from DeFi hacks in 2025?
A) $500 million B) $1.7 billion C) $2.2 billion D) $3.41 billion
Answer: D – 2025 saw $3.41 billion stolen, the worst year on record.

Q8. What is MEV?
A) A type of stablecoin B) A consensus mechanism
C) Value extracted by reordering transactions in a block D) A governance attack
Answer: C – MEV bots front-run and back-run user trades to extract profit. Over $3B annually.

Q9. Which entity collapsed AFTER Terra but BEFORE FTX?
A) Coinbase B) Three Arrows Capital (June 2022) C) Binance D) MakerDAO
Answer: B – Three Arrows Capital collapsed in June 2022, five months before FTX in November.

Q10. Best question to ask before using a DeFi protocol?
A) "Where does the yield come from?" B) "What is the token price?"
C) "How many Twitter followers?" D) "Is the logo nice?"
Answer: A – Sustainable yield comes from real economic activity (fees, interest). If you cannot identify the source, stay away.

Appendix

Technical Deep Dives

The math and mechanics behind the failures

Click blue links in appendix slides to jump back to the main deck.

A1: UST Mint/Burn Mechanism

The algorithmic peg relied on a simple arbitrage mechanism:

Mint: Burn \$1 of LUNA $\rightarrow$ receive 1 UST

Burn: Burn 1 UST $\rightarrow$ receive \$1 of LUNA

A1: UST Mint/Burn Mechanism

The algorithmic peg relied on a simple arbitrage mechanism:

Mint: Burn \$1 of LUNA $\rightarrow$ receive 1 UST

Burn: Burn 1 UST $\rightarrow$ receive \$1 of LUNA

When UST $>$ \$1: Arbitrageurs burn LUNA to mint UST, sell UST for profit, increasing UST supply until price drops to \$1.

When UST $<$ \$1: Arbitrageurs buy cheap UST, burn it for \$1 of LUNA, sell LUNA for profit. This *should* reduce UST supply.

A1: UST Mint/Burn Mechanism

The algorithmic peg relied on a simple arbitrage mechanism:

Mint: Burn \$1 of LUNA $\rightarrow$ receive 1 UST

Burn: Burn 1 UST $\rightarrow$ receive \$1 of LUNA

When UST $>$ \$1: Arbitrageurs burn LUNA to mint UST, sell UST for profit, increasing UST supply until price drops to \$1.

When UST $<$ \$1: Arbitrageurs buy cheap UST, burn it for \$1 of LUNA, sell LUNA for profit. This *should* reduce UST supply.

The fatal flaw: When confidence collapses, *everyone* burns UST at once. LUNA supply explodes:

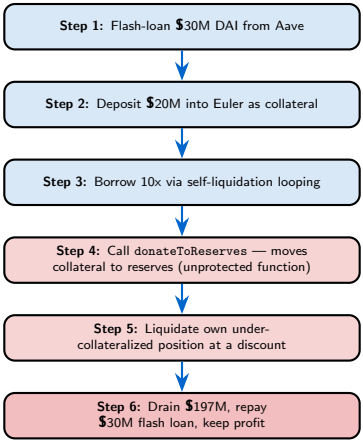
Date	LUNA Supply	LUNA Price
May 7	350 million	\$80.00
May 9	1.5 billion	\$4.00
May 11	70 billion	\$0.01
May 13	6.5 trillion	\$0.0001

← Back to main slide: The Death Spiral Explained

LFG deployed \$750M in BTC reserves as defense. Selling BTC further crashed the market, accelerating the spiral.

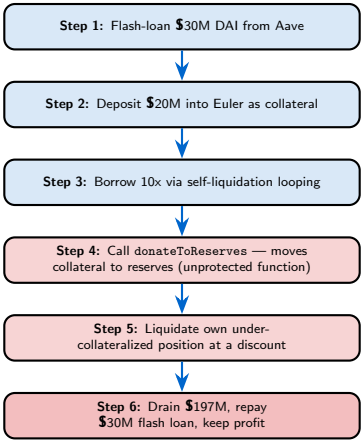
A2: Flash Loan Attack — Euler Finance Step-by-Step

March 13, 2023: $197M drained in a single transaction.



A2: Flash Loan Attack — Euler Finance Step-by-Step

March 13, 2023: $197M drained in a single transaction.



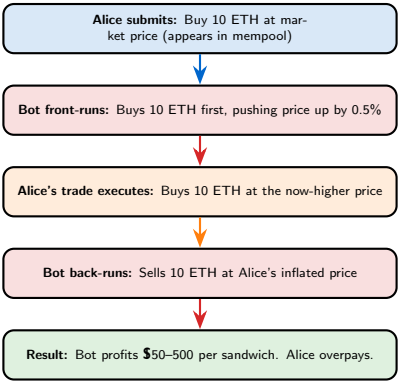
Outcome: After weeks of negotiation, the attacker returned all $197M. Euler resumed operations.

← Back to main slide: Smart Contract Exploits

The `donateToReserves` function lacked a check that the caller had sufficient collateral after donation. One missing line of code.

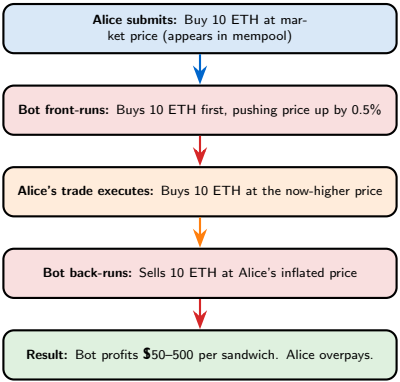
A3: MEV Sandwich Attack — Worked Example

Alice wants to buy 10 ETH on Uniswap.



A3: MEV Sandwich Attack — Worked Example

Alice wants to buy 10 ETH on Uniswap.



2025 MEV stats:

- Sandwich attacks: $289.76M extracted (51.56% of all MEV)
- Cumulative MEV since 2020: over $7.2 billion
- Annual MEV: over $3 billion

A4: Reentrancy Attack Pattern

The most famous smart contract vulnerability. Used in the 2016 DAO hack ($60M).

Vulnerable pattern (Solidity pseudocode):

```
function withdraw(amount) {
require(balances[msg.sender] >= amount);
// BUG: sends ETH BEFORE updating balance
msg.sender.call{value:  amount}("");
balances[msg.sender] -= amount;  // too late!
}
```

A4: Reentrancy Attack Pattern

The most famous smart contract vulnerability. Used in the 2016 DAO hack ($60M).

Vulnerable pattern (Solidity pseudocode):

```
function withdraw(amount) {
require(balances[msg.sender] >= amount);
// BUG: sends ETH BEFORE updating balance
msg.sender.call{value:  amount}("");
balances[msg.sender] -= amount;  // too late!
}
```

The attack: The attacker's contract has a `receive()` function that immediately calls `withdraw()` again — before the balance is updated. The loop drains all funds.

Fixed pattern (Checks-Effects-Interactions):

```
function withdraw(amount) {
require(balances[msg.sender] >= amount);
balances[msg.sender] -= amount;  // update FIRST
msg.sender.call{value:  amount}("");
}
```

← Back to main slide: Smart Contract Exploits

The Checks-Effects-Interactions pattern: (1) check conditions, (2) update state, (3) interact with external contracts. Always in this order.

A5: Do Kwon — Full Legal Timeline

Date	Event
May 7–13, 2022	Terra/UST collapses. $45B in losses.
Jun 2022	SEC opens investigation into Terraform Labs.
Sep 14, 2022	South Korean court issues arrest warrant for Do Kwon.
Sep 17, 2022	Interpol issues Red Notice. Do Kwon tweets "I am not on the run."
Mar 23, 2023	Arrested in Montenegro using a fake Costa Rican passport.
Jun 2023	Montenegro convicts Kwon of document forgery (4 months).
Feb 16, 2024	SEC wins $4.47B judgment against Terraform Labs.
Dec 31, 2024	Extradited from Montenegro to the United States.
Jan 2025	Pleads not guilty to 9 federal charges (fraud, conspiracy).
2026	Trial ongoing in US District Court, Southern District of New York.

← Back to main slide: Do Kwon Legal Aftermath

Terraform Labs settled with the SEC for $4.47B. Do Kwon personally faces up to 40+ years if convicted on all charges.

A6: Cryptoeconomics Lens — DeFi Failures

Question	DeFi Failures
1. Problem	Tail risk in open financial systems: how do you prevent cascading failures in permissionless, interconnected protocols?
2. Incentives	Misaligned: 20% yield attracted deposits without sustainable revenue. Anchor rewarded growth, not solvency.
3. Benefits/Costs	Benefits: permissionless innovation, composable building blocks. Costs: systemic risk, no lender of last resort, no deposit insurance.
4. Failure Mode	Reflexive feedback (Terra), hidden leverage (3AC/FTX), bridge vulnerabilities (Ronin), oracle manipulation (Mango).
5. Design	Circuit breakers, insurance funds, redundant oracles, gradual liquidation, time-delayed withdrawals.
6. Alternatives	Traditional risk management, DeFi insurance protocols (Nexus Mutual), regulatory frameworks (MiCA), proof of reserves.

← Back to main slide: Key Takeaways

These six questions are the "Cryptoeconomics Lens" — apply them to every blockchain topic you study.