DeFi Failures

When Code Meets Greed

BSc Blockchain, Crypto Economy & NFTs

Digital Finance Program

Follow Aisha as she reconstructs the 2022 crypto crash for her thesis.

What you will learn:

Five categories of DeFi failure
The Terra/UST collapse day by day
How contagion turned one failure into a $70B+ disaster
MEV, flash loan attacks, and the human factor

Spring Semester 2026

Contents

1 Meet Aisha

Aisha's Story

Aisha is a final-year BSc Finance student in London. In November 2022, she watched FTX collapse in real time on Twitter. The headline read: "Crypto Winter Claims $60B+." Her professor suggested she write her thesis on the 2022 crypto crash.
"But where do I start?" Aisha asks. "Was it one event or many? Was it a technology failure or a human failure?"
"Both," her professor says. "And that is what makes it interesting."

Aisha's thesis question: *Was the 2022 crypto crash a cascade of technical failures, economic design flaws, or fraud—and how did they interact?*

2 The Story: Mapping the Crash

Aisha's Story

Aisha draws a timeline on her whiteboard. She marks six events in 2022:
1. **May 7–13:** Terra/UST collapse ($45B destroyed).
2. **June 13:** Celsius freezes withdrawals ($12B locked).
3. **June 17:** Three Arrows Capital defaults ($3.5B).
4. **July 6:** Voyager Digital files for bankruptcy.
5. **Nov 2:** CoinDesk publishes Alameda Research balance sheet.
6. **Nov 11:** FTX files for bankruptcy ($8B+ customer funds missing).

"It is a domino chain," Aisha realizes. "Each collapse exposed the next."

Definition: Death Spiral

A **death spiral** is a positive feedback loop in which selling an asset causes further selling. In crypto: a price drop triggers liquidations, which dump more assets, which cause further price drops. Once started, the loop is very difficult to stop.

Explain Like I'm 5

A death spiral is like a stampede for the exit. The first few people run. Their running scares others. Soon everyone is running, and the doorway is too small. The crowd crushes itself.

Definition: Contagion

Contagion is the spread of financial distress from one entity to others through shared exposures (loans, deposits, trading positions). In 2022, Terra's collapse triggered a chain of failures because many firms had lent to, borrowed from, or invested in each other.

Explain Like I'm 5

Financial dominoes. Push one over, and it knocks down the next, which knocks down the next. The dominoes were standing too close together because everyone was lending to everyone.

Definition: Systemic Risk

Systemic risk is the risk that the failure of one participant or protocol causes the failure of the entire system. In traditional finance, this is why "too big to fail" bailouts exist. In DeFi, there are no bailouts.

3 Key Concepts: Five Failure Categories

Aisha's Story

Aisha categorizes every major DeFi failure she finds into five types. She discovers that most failures combine multiple categories.

3.1 Framework: Why Failures Cluster

Before listing categories, Aisha observes a pattern in her research: failures rarely occur in isolation. Multiple failures happen simultaneously, and each amplifies the others.

Definition: Correlated Failure

Correlated failure occurs when multiple seemingly independent systems fail at the same time because they share hidden dependencies. In DeFi, hidden dependencies include:

- Shared oracles (if Chainlink goes down, many protocols suffer).
- Shared stablecoins (if USDC depegs, all protocols using USDC collateral suffer).
- Shared liquidity pools (if Curve's 3pool breaks, many stablecoin swaps suffer).
- Shared narratives (if a "safe yield" narrative breaks, capital flees multiple protocols simultaneously).
- Shared custody (if a key signer of a bridge or exchange is compromised, many assets are exposed).

Traditional finance has regulators and circuit breakers to contain correlated failures. DeFi, without them, is inherently more fragile during crises.

Explain Like I'm 5

Imagine a row of houses sharing one water pipe. Everyone thinks they have independent plumbing until the pipe bursts. Then all the houses flood at the same time. DeFi has many shared pipes—oracles, stablecoins, bridges—that most users do not even know about.

3.2 Category 1: Design Flaws

Definition: Economic Design Flaw

A protocol whose core mechanism is mathematically or economically unsound. The failure is inevitable given the right conditions—it is a *when*, not an *if*.

Worked Example: Terra/UST

UST was an algorithmic stablecoin backed by LUNA through a mint/burn mechanism. Anchor Protocol offered 20% APY on UST deposits, funded by reserves that were shrinking. The design relied on continuous inflows to sustain unsustainable yields—a structure that, in traditional finance, would be called a Ponzi-adjacent scheme.

3.3 Category 2: Smart Contract Exploits

Definition: Smart Contract Exploit

A vulnerability in protocol code that allows an attacker to drain funds, manipulate state, or bypass intended logic. Exploits can target reentrancy, flash loan interactions, access control, or mathematical precision errors.

Worked Example: Hack Losses by Year

Year	Total Losses	Notable Event
2020	$0.2B	Harvest Finance ($34M)
2021	$1.3B	Poly Network ($611M)
2022	$3.8B	Ronin ($625M), Wormhole ($326M)
2023	$1.7B	Euler ($197M), Mixin ($200M)
2024	$2.2B	WazirX ($234M)
2025	$3.41B	Bybit ($1.5B)

3.4 Anatomy of a Smart Contract Exploit

Definition: Reentrancy Attack

A **reentrancy attack** exploits a contract that calls an external function before updating its own state. The external function can call back into the original contract, tricking it into repeating a withdrawal multiple times before the balance is debited.

Worked Example: Simplified Reentrancy

Vulnerable contract logic:
1. Check user's balance.
2. Send the funds to user.
3. Update user's balance to zero.

If step 2 calls a user-controlled contract, that contract can re-enter step 1 *before* step 3 runs. The balance is still the original amount, so the contract sends again. Loop until the vault is empty.

Fix: Update state *before* external calls (the Checks-Effects-Interactions pattern). Historical example: The DAO hack (2016) drained $60M of ETH using reentrancy, leading to the Ethereum hard fork that created ETH and ETC.

3.5 Category 3: Oracle Attacks

Definition: Oracle Manipulation

An attack that profits by feeding incorrect price data to a DeFi protocol, typically by manipulating the price of a thinly traded token on a DEX, then borrowing against the inflated collateral value.

3.6 Category 4: Fraud and Mismanagement

Definition: CeFi Fraud

Centralized entities (exchanges, lenders) that commingle customer funds, fabricate financial statements, or operate without proper risk management. FTX, Celsius, and Voyager all fell into this category.

3.7 Category 4b: The Human Element

Definition: Social Engineering

Social engineering attacks exploit human psychology rather than code. Phishing, fake airdrops, impersonation of team members, and manipulation of multi-sig signers have become increasingly common as pure code exploits grow harder.

Worked Example: The Bybit UI Attack

In the February 2025 Bybit hack, the attackers did not break the multi-sig cryptography. Instead:

1. They compromised the web interface used by Bybit signers.
2. When a signer opened a legitimate-looking transaction to review, the UI *displayed* the correct details but *signed* a malicious transaction underneath.
3. Three signers approved before the fraud was detected.
4. Result: $1.5B transferred to attacker-controlled addresses.

The cryptographic signatures were genuine. The attack targeted the trust between the human signer and the software they were using.

3.8 Category 5: MEV Extraction

Definition: Maximal Extractable Value (MEV)

MEV is the profit a block producer (or searcher) can extract by reordering, inserting, or censoring transactions within a block. Common MEV strategies include front-running (seeing a pending trade and trading ahead of it), sandwich attacks (front-run + back-run around a victim's trade), and just-in-time (JIT) liquidity.

Explain Like I'm 5

Someone cuts in line at the grocery store, buys all the bread, and sells it to you at a markup—all in the time between you deciding to buy bread and actually reaching the register. That is MEV. Total MEV extracted since 2020 exceeds $3B.

Self-Assessment Checkpoint

Can you name all five failure categories with one example each? Can you explain the difference between a design flaw (Category 1) and a smart contract exploit (Category 2)? If yes, continue.

4 How It Works: The Mechanics of Failure

Aisha's Story

Aisha decides her thesis needs quantitative depth. She models the Terra collapse and the Anchor sustainability gap.

4.1 The UST/LUNA Mint-Burn Mechanism

Formula: UST Peg Mechanism (Simplified)

If UST > $1:

$$\text{Burn \$1 of LUNA} \rightarrow \text{Mint 1 UST}$$

Increases UST supply, pushing price down toward $1.

If UST < $1:

$$\text{Burn 1 UST} \rightarrow \text{Mint \$1 of LUNA}$$

Decreases UST supply, pushing price up toward $1.

Problem: When UST < $1 during a panic, mass redemptions create massive LUNA supply, crashing LUNA's price. As LUNA falls, each redemption mints *more* LUNA per UST. This is the death spiral.

4.2 The Anchor Sustainability Gap

Formula: Anchor Protocol Yield Gap

$$\text{Annual cost} = \text{UST deposits} \times \text{APY} = \$14\text{B} \times 20\% = \$2.8\text{B/year}$$

$$\text{Annual income} = \text{Borrows} \times \text{Borrow rate} \approx \$1.5\text{B} \times 10\% = \$150\text{M/year}$$

$$\text{Gap} = \$2.8\text{B} - \$150\text{M} = \$2.65\text{B/year}$$

The gap was funded by a "yield reserve" that was shrinking by $200M+ per month. At that rate, the reserve would have been depleted by mid-2022 even without the depeg.

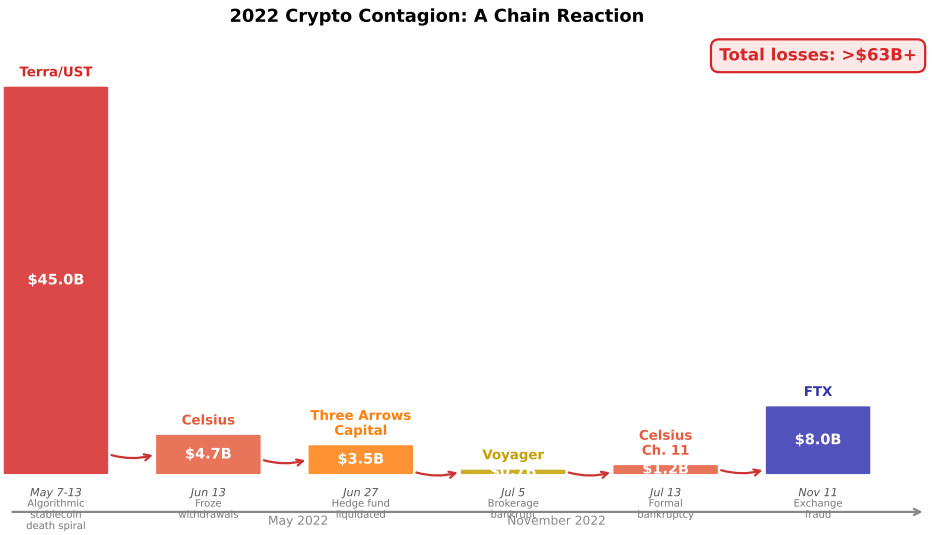
Worked Example: Flash Loan Attack (Euler Finance)

March 13, 2023. The attacker exploited Euler's "donate" function:

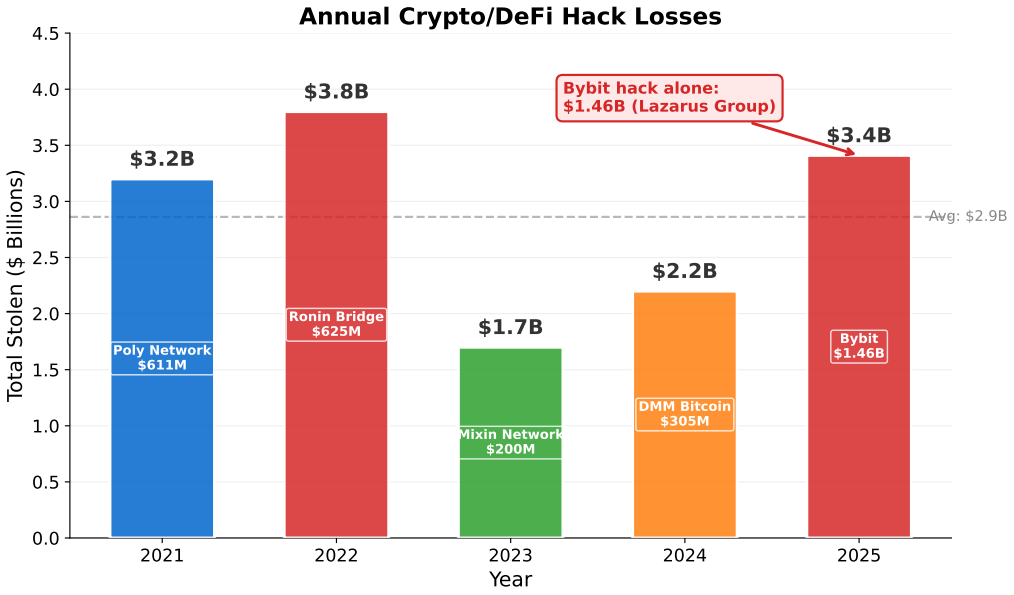
1. Borrow $30M via Aave flash loan.
2. Deposit into Euler, then use Euler's leverage to multiply the position.
3. "Donate" the leveraged tokens back to the protocol, creating artificial bad debt.
4. The protocol's accounting now shows a shortfall; the attacker exploits the resulting liquidation logic to extract $197M.
5. Repay the $30M flash loan. Profit: $167M.

The entire attack happened in a single transaction. Euler was audited six times.

2022 Contagion Chain



Crypto Hack Losses by Year



Key Takeaway

The 2022 crash was not one failure but a cascade: a design flaw (Terra) triggered contagion through interconnected CeFi lenders (Celsius, 3AC, Voyager), which culminated in the exposure of outright fraud (FTX). Technology, economics, and human dishonesty all played a role.

4.3 The Do Kwon Case

Definition: Do Kwon Legal Timeline

Do Kwon, the co-founder of Terraform Labs and architect of UST/LUNA, faced criminal charges in multiple jurisdictions:

- **May 2022:** Terra collapses; Do Kwon initially remains in South Korea.

- **Sep 2022:** South Korean authorities issue arrest warrant; Kwon flees.
- **Mar 2023:** Arrested in Montenegro using falsified travel documents.
- **Feb 2024:** US SEC wins civil fraud case against Terraform Labs.
- **Dec 2024:** Extradited to the US for criminal trial.
- **2025–2026:** Criminal trial ongoing. Charges include fraud, conspiracy, and market manipulation.

Kwon insisted throughout that Terra's collapse was "a market failure, not a fraud." Prosecutors argue he knew the design was unsustainable.

4.4 The FTX Aftermath

Definition: FTX Bankruptcy

FTX, once valued at $32B, collapsed on November 11, 2022. The root cause: Alameda Research, FTX's sister trading firm, had borrowed $8B+ of customer funds from FTX without authorization. When customers tried to withdraw en masse, the funds were gone.

- **CEO:** Sam Bankman-Fried (SBF).
- **Customer funds missing:** $8B+.
- **Sentence (Mar 2024):** 25 years in federal prison.
- **Recovery:** Surprisingly, by 2024, customers were being repaid nearly in full (at 2022 dollar values) due to the appreciation of assets held by the bankruptcy estate.

Worked Example: FTX vs. Terra Comparison

Factor	Terra	FTX
Category	Design flaw (Cat. 1)	Fraud (Cat. 4)
Value destroyed	$45B+	$8B+ direct, $30B+ total
Root cause	Unsustainable yield	Misappropriation
Blockchain involved?	Yes (Terra chain)	No (centralized exchange)
Recovery prospects	None (tokens worthless)	Nearly full (assets recovered)

The key insight: FTX was a CeFi failure with a crypto veneer. The blockchain was not the problem; the *absence* of blockchain-level transparency was.

4.5 The Insurance Gap

Definition: DeFi Insurance

DeFi insurance protocols (Nexus Mutual, InsurAce, Unslashed) offer coverage against smart contract exploits, stablecoin depegs, and other risks. Coverage is typically capped, and claims require governance approval.

Worked Example: Insurance Economics

An Aave depositor buys smart contract coverage for 1 year on $10,000 of deposits.

- Premium: 2% annually = $200.
- Effective yield after insurance: base APY minus 2%.
- Coverage: full value of deposits if Aave is exploited.

If more than 2% of users bought insurance across DeFi, the total premium pool would dwarf actual losses—but adoption is low (<1% of TVL is insured). DeFi users systematically under-insure.

4.6 Lessons for the Next Cycle

Worked Example: Warning Signs Checklist

From Aisha's thesis research, here is a checklist of 10 warning signs that a DeFi platform may be headed for failure:

1. Unsustainable yields (above the risk-free rate by 5+ percentage points with no clear source).
2. Anonymous or unaccountable team.
3. Rapid TVL growth without proportional product usage.
4. Unaudited or shallowly audited smart contracts.
5. Heavy reliance on a single dependency (oracle, bridge, stablecoin).
6. Lock-up periods that prevent withdrawals during stress.
7. Commingling of customer funds with treasury or trading operations.
8. Governance controlled by a small number of addresses.
9. Opaque reserve composition.
10. Exponential growth in token supply or obligations without matching revenue.

A platform with 3+ of these signs should be treated with extreme caution.

5 Real-World Cases

Historical Case Study: Terra Collapse – Day by Day

Date	Event
May 7	Large UST sell on Curve (allegedly $285M). UST depegs slightly to $0.985.
May 8	Luna Foundation Guard (LFG) deploys $1.5B in Bitcoin reserves to defend peg. UST recovers briefly.
May 9	UST falls to $0.90. Anchor deposits plunge from $14B to $11B in hours. Panic withdrawals begin.
May 10	UST at $0.60. LUNA falls 50%. Death spiral accelerating. Do Kwon tweets "Deploying more capital."
May 11	UST at $0.30. LUNA collapses from $30 to $1. Terraform Labs halts the blockchain twice to prevent governance attacks.
May 12	UST at $0.10. LUNA below $0.01. Anchor APY drops to 2%. The yield that attracted $14B is gone.
May 13	UST effectively worthless. Total value destroyed: ~$45B. Largest algorithmic stablecoin failure in history.

Historical Case Study: 2022 Contagion Chain

The Terra collapse exposed interconnected risk:

1. **Three Arrows Capital (3AC)** – Held large LUNA/UST positions. Lost $3.5B+. Defaulted on loans from Celsius, Voyager, and BlockFi.
2. **Celsius Network** – Froze $12B in customer withdrawals (Jun 13). Had lent to 3AC and held illiquid stETH positions. Filed bankruptcy Jul 13.
3. **Voyager Digital** – $650M exposure to 3AC. Filed bankruptcy Jul 6.
4. **BlockFi** – Significant 3AC exposure. FTX "rescued" it with a $400M credit facility (later revealed as predatory). Filed bankruptcy Nov 28.
5. **FTX / Alameda Research** – Alameda had large exposure to the crisis. Used FTX customer funds ($8B+) to cover losses. Collapsed Nov 11.

6. **Genesis Trading** – Lent to 3AC and Alameda. Filed bankruptcy Jan 2023. $3B in claims. Combined estimated losses: $70B+.

Historical Case Study: Bybit Hack (February 21, 2025)

The largest single crypto hack in history:
- $1.5B stolen from Bybit's cold wallet infrastructure.
- Attributed to the Lazarus Group (North Korean state-sponsored hackers).
- The attack exploited the multi-signature signing process by compromising the UI displayed to signers—they approved a malicious transaction while seeing a legitimate one.
- Bybit covered losses from reserves and did not freeze withdrawals.

Historical Case Study: Ronin Bridge (March 23, 2022)

- $625M stolen from the Ronin Bridge (Axie Infinity's sidechain).
- The bridge was secured by 9 validators; the attacker compromised 5 (majority).
- 4 validators were controlled by Sky Mavis (centralization risk).
- The hack went undetected for 6 days.
- Also attributed to the Lazarus Group.

6 What Can Go Wrong

Aisha's Story

Aisha develops a red-flag checklist for her thesis. She wants to identify warning signs that a protocol or platform is at risk of failure.

Important Caveat

"20% APY Guaranteed" is a red flag. If a protocol offers yields far above market rates without a clear, sustainable source of income, the yield is coming from new deposits (Ponzi dynamics) or from a reserve that is being depleted. Anchor's 20% was the most expensive red flag in DeFi history: $45B.

Common Misconception: "Audited protocols cannot be hacked"

Euler Finance was audited six times by reputable firms before losing $197M. An audit checks code at a specific point in time, against known vulnerability patterns. It cannot catch all logic errors, novel attack vectors, or economic exploits. Audits reduce risk; they do not eliminate it.

Common Misconception: "DeFi failures only affect crypto users"

The 2022 contagion chain involved centralized lenders (Celsius, BlockFi, Voyager) that had millions of retail customers—many of whom did not understand they were exposed to DeFi risk. FTX's collapse affected mainstream investors, sports sponsorships, and political donations. Crypto risk leaks into the real economy.

Key Takeaway

The five failure categories are not mutually exclusive. The 2022 crash combined design flaws (Terra), smart contract risk (bridges), fraud (FTX), and contagion (interconnected lending). A robust thesis on DeFi failures must analyze all five layers.

7 The Cryptoeconomics Lens

Before applying the six questions, Aisha reflects on a broader question: *what separates a bold experiment from a catastrophic failure?*

Definition: The Permissionless Paradox

DeFi's greatest strength—anyone can build and deploy anything—is also its greatest weakness. The same permissionlessness that enables innovation also enables:

- Launching a protocol with no audit.
- Offering yields that are mathematically unsustainable.
- Recreating financial primitives (leverage, derivatives) without the risk-management tooling developed over centuries of traditional finance.
- Operating without any jurisdiction that can enforce consumer protection.

Aisha's thesis argues that the 2022 crash was not just a series of failures—it was the inevitable result of scaling permissionless innovation faster than the safety infrastructure could keep up. The question is not whether DeFi will have another crash, but whether the next crash will be contained or catastrophic.

Explain Like I'm 5

Imagine if anyone could open a bank with no license, no deposit insurance, and no inspections. Some of these banks would be amazing innovations. Some would be frauds. Many would be well-intentioned but poorly designed. Customers would have no way to tell them apart. That is DeFi today, with only the veneer of smart contract transparency as a safety net.

Cryptoeconomics Lens

Apply the six cryptoeconomics questions to DeFi failures:

1. **PROBLEM:** DeFi promises permissionless finance, but permissionless systems are also permissionless for attackers, scammers, and poorly designed protocols. The coordination problem is: how do you allow innovation while preventing catastrophic failures?
2. **INCENTIVES:** Attackers are incentivized by the profit from exploits (MEV: $3B+, hacks: $3.41B in 2025 alone). Auditors are incentivized by reputation, not by the size of losses they prevent. Users are incentivized by yield and often ignore risk. The incentive structure systematically underprices risk.
3. **BENEFITS / COSTS:** Benefits accrue to users (access), developers (token rewards), and the ecosystem (innovation). Costs are borne disproportionately by retail users who lack the sophistication to assess protocol risk. The 2022 crash destroyed $70B+ in value, much of it retail savings.
4. **FAILURE MODE:** Cascading failure. Terra → 3AC → Celsius/Voyager → FTX. Each entity's collapse created obligations that the next entity could not meet. The "composability" that makes DeFi powerful also makes it fragile: interconnection amplifies shocks.
5. **DESIGN:** Insurance protocols (Nexus Mutual), formal verification, multi-sig governance,

time-locks, bug bounties. Each is a partial defense. No design eliminates all five failure categories simultaneously.

6. **ALTERNATIVES:** Regulated DeFi (MiCA), proof-of-reserves attestations, on-chain circuit breakers, and mandatory insurance could reduce systemic risk. The challenge: these mechanisms often reduce permissionlessness, reintroducing the centralization DeFi was built to avoid.

8 Deep Dive: Rebuilding Trust After Each Crisis

Aisha realizes her thesis needs not just a description of failures but an analysis of how the ecosystem responded. She writes a chapter on recovery and reform.

8.1 Response 1: Proof of Reserves

Definition: Proof of Reserves (PoR)

Proof of Reserves is a cryptographic attestation that a custodian (exchange, stablecoin issuer) holds at least as much of an asset as it claims to owe customers. After FTX, PoR became standard practice for reputable centralized exchanges.

Worked Example: How PoR Works

1. The exchange publishes a list of its on-chain addresses holding customer funds.
2. Customer balances are committed to a Merkle tree whose root is published.
3. Any customer can verify their balance is included via a Merkle proof.
4. An auditor compares the sum of all leaves in the Merkle tree to the sum of on-chain holdings.
5. If total holdings $\geq$ total liabilities, the proof is valid.

Limitation: PoR proves assets at a specific moment. It cannot prove liabilities (off-chain debt, hidden loans) or that funds will remain present tomorrow.

8.2 Response 2: Regulatory Frameworks

Definition: Major Post-2022 Regulations

- **MiCA (EU, Dec 2024).** Comprehensive crypto regulation covering stablecoins, exchanges, and token issuance.
- **UK FSMA 2023.** Extends financial services law to crypto assets.
- **Japan stablecoin framework (2023).** Only licensed banks and trust companies can issue stablecoins.
- **Singapore MAS Digital Payment Token rules.** Licensing and consumer protection requirements.
- **US state-by-state approach.** Wyoming crypto-friendly laws; New York BitLicense; federal legislation still pending as of 2026.

8.3 Response 3: DeFi Improvements

Worked Example: Protocol-Level Safety Upgrades

After the 2022 crash and subsequent hacks, many DeFi protocols adopted new safety measures:

- **Time-delayed governance.** 48-hour delay between proposal approval and execution, giving users time to exit if the change is malicious.
- **Multi-oracle feeds.** Aggregating Chainlink, Pyth, and TWAP oracles instead of relying on a single source.
- **Circuit breakers.** Automatic pausing when anomalous activity is detected.
- **Bug bounty programs.** White-hat rewards up to $10M for critical vulnerabilities (Immunefi platform).
- **Formal verification.** Mathematical proofs of correctness for critical functions.
- **Progressive decentralization.** Starting with admin controls, removing them gradually as the protocol matures.

8.4 Response 4: Market Maturity

Worked Example: Pre- vs. Post-Crash Behaviors

Behavior	Pre-2022	Post-2022
Typical DeFi yield expectations	20–100% APY	3–10% APY
Audit coverage for new protocols	Optional	Mandatory
Customer use of self-custody	Low	Much higher
Exchange Proof of Reserves	Rare	Standard
Insurance adoption	<1% TVL	Growing (~3% TVL)
Regulatory clarity	Minimal	Substantially improved

8.5 What Has Not Been Fixed

Important Caveat

Despite progress, several structural problems remain:

- **MEV extraction** continues at $3B+/year. Solutions (fair ordering, encrypted mempools) are experimental.
- **Cross-chain bridges** remain the single largest attack surface ($2B+ stolen cumulatively).
- **Oracle-based attacks** against smaller, less liquid assets happen regularly.
- **Retail user protection** remains weak. Self-custody is powerful but unforgiving.
- **CeFi opacity** persists in some jurisdictions. Not all exchanges publish PoR.

Aisha concludes her thesis with a chapter titled "What Cycle 2027 Might Look Like."

9 Practice Problems

Discovery Exercise 1

Anchor sustainability. Anchor has $14B in deposits at 20% APY and $1.5B in borrows at 10%. Calculate the annual yield gap. If the yield reserve has $500M remaining, how many months until depletion (assuming gap stays constant)?

Discovery Exercise 2

Terra timeline. On May 9, 2022, UST was at \$0.90 and LUNA at \$30. By May 12, UST was \$0.10 and LUNA below \$0.01. Calculate the percentage loss for someone who held (a) 10,000 UST, (b) 100 LUNA, and (c) both.

Discovery Exercise 3

Contagion modeling. If 3AC had \$3.5B in losses and its top three creditors each held 30%, 25%, and 15% of that exposure, calculate the direct loss for each creditor. What happens if Creditor 1 is also a depositor-facing platform with \$12B in customer funds?

Discovery Exercise 4

Flash loan economics. An attacker uses a \$30M flash loan (0.09% fee) to exploit a protocol for \$197M. Calculate the attacker's profit, the cost of the flash loan, and the return on "investment" (noting the investment is only the gas fee plus flash loan fee).

Discovery Exercise 5

MEV calculation. A sandwich attacker front-runs a \$50,000 swap on Uniswap. The front-run trade moves the price 0.3%, and the back-run captures the difference. Estimate the attacker's gross profit. If gas costs \$50, what is the net profit?

Discovery Exercise 6

Failure classification. Classify each event: (a) Ronin Bridge hack, (b) Terra/UST collapse, (c) FTX bankruptcy, (d) Mango Markets oracle attack, (e) Euler Finance exploit. Use the five-category framework.

Discovery Exercise 7

Audit limitations. Euler was audited six times before losing \$197M. List three reasons why audits fail to prevent exploits. Propose one additional safeguard that could have caught the Euler vulnerability.

Discovery Exercise 8

Red flag detection. Read the following description and identify all red flags: "NewToken Protocol offers 30% APY on stablecoin deposits. The team is anonymous. The smart contract is unaudited. The protocol launched last week and already has \$500M TVL. Withdrawals require a 7-day lock-up."

Discovery Exercise 9

Regulatory response. After the 2022 crash, the EU implemented MiCA (Dec 2024) and the US brought fraud charges against Do Kwon and Sam Bankman-Fried. Compare the two regulatory approaches. Which addresses which failure category?

Discovery Exercise 10

Thesis argument. In 200 words, argue whether the 2022 crash was primarily a failure of technology, economics, or human behavior. Support your position with at least three specific examples from this primer.

10 Glossary of Failure-Related Terms

3AC (Three Arrows Capital)
A Singapore-based crypto hedge fund that collapsed in June 2022 after massive LUNA/UST losses.

Alameda Research
The trading firm sister to FTX, whose undisclosed losses led to FTX's collapse.

Anchor Protocol
Terra-based lending protocol offering 20% APY on UST; central to the Terra collapse.

Audit
A third-party review of smart contract code for vulnerabilities. Reduces risk but cannot eliminate it.

Bad debt
Debt that cannot be repaid because collateral is insufficient; must be absorbed by the protocol or users.

Bankman-Fried (SBF)
Sam Bankman-Fried, the founder of FTX. Convicted of fraud and sentenced to 25 years in March 2024.

BlockFi
A crypto lender that collapsed after 3AC exposure and FTX entanglement.

Bridge
A protocol allowing assets to move between blockchains. Historically the largest attack surface in DeFi.

Bybit
A centralized crypto exchange that suffered the largest hack in history ($1.5B, Feb 2025).

Celsius Network
A CeFi lender that froze $12B of customer deposits in June 2022 and later filed bankruptcy.

Chainalysis
A blockchain analytics company that tracks hack statistics and illicit flows.

Contagion
Financial distress spreading from one entity to others through shared exposures.

Cross-chain bridge
See "bridge."

Death spiral
A positive feedback loop where selling causes further selling until the asset is worthless.

Do Kwon
The co-founder of Terraform Labs, architect of UST/LUNA. Extradited to the US in December 2024.

Euler Finance
A DeFi lending protocol exploited for $197M in March 2023 via flash loan attack.

Exploit
An attack that abuses a vulnerability in smart contract code.

Flash loan
An uncollateralized single-transaction loan; often used as part of exploits.

Formal verification
Mathematical proof of correctness for smart contract functions.

FTX
A centralized exchange that collapsed in November 2022 after $8B+ of customer funds were found missing.

Front-running
Seeing a pending transaction and submitting another transaction to profit from it.

Genesis Trading
A crypto lender that filed bankruptcy in January 2023 due to 3AC and Alameda exposure.

Governance attack
An attack where an adversary gains enough voting power to pass malicious proposals.

Lazarus Group
North Korean state-sponsored hacking group responsible for Ronin, Bybit, and other major crypto thefts.

MEV
Maximal Extractable Value. Profit extracted by reordering, inserting, or censoring transactions.

Multi-sig
A wallet requiring multiple signatures to authorize transactions.

Nexus Mutual
A DeFi insurance protocol offering smart contract coverage.

Oracle
A service that provides off-chain data to smart contracts.

Oracle manipulation
An attack that feeds incorrect prices to a protocol to enable profitable exploits.

Proof of Reserves (PoR)
A cryptographic attestation that a custodian holds sufficient assets to cover liabilities.

Ponzi scheme
A fraud where returns to existing investors are paid from new investors' deposits rather than genuine income.

Reentrancy
An attack exploiting contracts that call external functions before updating state.

Ronin Bridge
A cross-chain bridge exploited for $625M in March 2022.

Rug pull
A scam where protocol operators remove all liquidity and disappear.

Sandwich attack
An MEV strategy that places trades before and after a target transaction to extract value.

Smart contract risk
The risk of loss due to bugs, exploits, or logic errors in protocol code.

Social engineering
Attacks exploiting human psychology rather than code.

Systemic risk
The risk that failure of one participant causes the failure of the entire system.

Terraform Labs
The company behind the Terra/UST/LUNA ecosystem, founded by Do Kwon.

Time-lock
A delay between governance proposal approval and execution, allowing users to exit if necessary.

TVL
Total Value Locked. Commonly used metric; dropped ∼77% during the 2022 crash.

UST
TerraUSD, the algorithmic stablecoin that collapsed in May 2022.

Voyager Digital
A CeFi lender that filed bankruptcy in July 2022 after 3AC exposure.

Solutions

Exercise 1. Annual cost = \$14B × 0.20 = \$2.8B. Annual income = \$1.5B × 0.10 = \$150M. Gap = \$2.8B − \$150M = \$2.65B/year, or ∼\$221M/month. Months until depletion: \$500M/\$221M ≈ 2.3 months. The yield reserve was a ticking clock.

Exercise 2. (a) 10,000 UST: was worth \$10,000 at par. At \$0.10: worth \$1,000. Loss: 90%. (b) 100 LUNA at \$30 = \$3,000. At \$0.01 = \$1. Loss: 99.97%. (c) Combined starting value: \$13,000. Ending: \$1,001. Loss: 92.3%.

Exercise 3. Creditor 1: 0.30 × \$3.5B = \$1.05B. Creditor 2: 0.25 × \$3.5B = \$875M. Creditor 3: 0.15 × \$3.5B = \$525M. If Creditor 1 holds \$12B in customer deposits and takes a \$1.05B hit, it may become insolvent (depending on reserves), freezing \$12B in customer funds—exactly what Celsius did.

Exercise 4. Flash loan fee: \$30M × 0.0009 = \$27,000. Gross exploit: \$197M. Net profit: \$197M − \$30M − \$27,000 − gas ≈ \$167M. ROI on the ∼\$27,050 "investment" (fee + gas): \$167M/\$27,050 ≈ 617,000%. This is why flash loan attacks are so attractive.

Exercise 5. Front-run moves price 0.3% on a \$50,000 swap. Price impact captured: \$50,000 × 0.003 = \$150. Gas cost: \$50. Net profit: \$100. Small per trade, but MEV bots execute thousands of such attacks daily.

Exercise 6. (a) Ronin: Category 2 (smart contract/bridge exploit) + Category 3 (validator compromise). (b) Terra: Category 1 (design flaw). (c) FTX: Category 4 (fraud and mismanagement). (d) Mango Markets: Category 3 (oracle manipulation). (e) Euler: Category 2 (smart contract exploit via flash loan).

Exercise 7. (1) Audits check code at a point in time; subsequent updates can introduce vulnerabilities. (2) Economic exploits (flash loan interactions) are hard to model statically. (3) Auditors have limited time and scope; novel attack vectors may not be in their checklist. Additional safeguard: formal verification (mathematical proof of correctness for critical functions) or time-delayed governance with monitoring bots that pause the protocol if anomalous withdrawals are detected.

Exercise 8. Red flags: (1) 30% APY with no clear source of yield. (2) Anonymous team—no accountability. (3) Unaudited contract—unknown vulnerabilities. (4) \$500M TVL in one week—possible wash trading or unsustainable incentives. (5) 7-day lock-up—prevents users from exiting during a crisis (similar to Celsius before its freeze). This profile matches multiple pre-failure patterns from 2022.

Exercise 9. MiCA (EU) is preventive regulation: licensing, reserve requirements, consumer disclosure. It addresses Category 1 (design flaws via reserve rules) and Category 4 (fraud via licensing). US approach is enforcement-focused: criminal charges against individuals (Do Kwon for fraud, SBF for wire fraud). It addresses Category 4 (fraud) after the fact. MiCA aims to prevent failures; the US approach aims to punish them. Neither directly addresses Category 2 (code exploits) or Category 5 (MEV).

Exercise 10. Open-ended. A strong argument identifies the interaction: technology (algorithmic stablecoin design), economics (unsustainable yields, interconnected lending), and human behavior (greed driving \$14B into 20% APY, fraud at FTX). The best answers argue that the crash was primarily an *economics* failure (mispriced risk, unsustainable incentive structures) enabled by technology (permissionless access, composability) and amplified by human behavior (fraud, panic selling).

Further Reading

Case study books and long-form journalism:

- Lewis, M. (2023). *Going Infinite: The Rise and Fall of a New Tycoon.* W.W. Norton. The FTX story, with intimate access to SBF.
- Faux, Z. (2023). *Number Go Up: Inside Crypto's Wild Rise and Staggering Fall.* Crown. Investigative reporting on the 2022 crash.
- Chayka, K. (2022). "The Fall of Crypto's Biggest Exchange." *The New Yorker.* FTX post-mortem.
- Various (2022). Bloomberg, CoinDesk, The Block coverage of the 2022 crash. Real-time reporting is a valuable primary source.

Academic analyses:

- Briola, A., Vidal-Tomás, D., Wang, Y., & Aste, T. (2022). "Anatomy of a Stablecoin's failure: The Terra-Luna case."
- Liu, J., Makarov, I., & Schoar, A. (2023). "Anatomy of a Run: The Terra Luna Crash."
- Zhou, L., Qin, K., Torres, C. F., Le, D. V., & Gervais, A. (2021). "High-Frequency Trading on Decentralized On-Chain Exchanges." MEV analysis.
- Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., ... & Juels, A. (2020). "Flash Boys 2.0." The original MEV paper.

Data sources for hack analysis:

- **Chainalysis Crypto Crime Report** – Annual report on hack and fraud statistics.
- **Rekt News** (`rekt.news`) – Detailed post-mortems of major DeFi exploits.
- **DeFiLlama Hacks** (`defillama.com/hacks`) – Chronological list of DeFi hacks with amounts.
- **Crystal Blockchain** – On-chain analytics for illicit flows.

Legal and regulatory primary sources:

- SEC vs. Terraform Labs (2023) – Court documents detailing alleged fraud.
- United States v. Samuel Bankman-Fried (2024) – Criminal trial transcripts.
- FTX Chapter 11 filings – Bankruptcy proceedings with creditor committee reports.
- US Commodity Futures Trading Commission enforcement actions.

Aisha's thesis conclusion:
Aisha's final thesis argues that the 2022 crypto crash was a **correlated failure**: a single catalyst (Terra) exposed latent risks in an interconnected financial system with no regulator, no deposit insurance, and no lender of last resort. The crash destroyed roughly $2 trillion in market value. The ecosystem has rebuilt with better safeguards—proof of reserves, MiCA, formal verification, insurance—but the fundamental tension remains: DeFi promises permissionless innovation, and permissionless innovation includes permission to fail catastrophically. Her thesis receives high honors and is published in a special issue on crypto market structure.