DeFi Failures | **When DeFi Breaks: Crashes, Hacks & Lessons** | **Standalone**

Pillar: Risk | *Complete before class*

What You Should Already Know

Stablecoin – A crypto token designed to maintain a stable price, usually $1.00 | **Peg** – The target price a stablecoin tries to maintain | **Algorithmic** – A stablecoin that uses code (not reserves) to manage supply and maintain its peg | **Collateral** – An asset pledged as security for a loan | **Liquidity pool** – Tokens locked in a smart contract for others to trade against

Key Terms Preview **Death spiral** (Self-reinforcing collapse loop) | **Contagion** (One failure triggering others) | **Smart contract exploit** (Bug in code that attackers drain) | **Bridge hack** (Attack on cross-chain token transfer contracts) | **Oracle manipulation** (Feeding wrong prices to smart contracts) | **MEV** (Profit from reordering transactions in a block) | **Flash loan attack** (Borrow, exploit, repay in one transaction)

The Problem

An investment platform offers 20% annual yield on your stablecoin deposits. "Guaranteed." Your friend invested their savings. Six months later, everything is gone. How do you analyze what went wrong?

If code is law and transactions are irreversible, what happens when the code fails or the economics collapse?

In 2022 alone, the crypto industry lost over $62B to failures, hacks, and fraud. Understanding how things break is as important as understanding how they work.

Warm-Up

Name one company or bank that collapsed in your lifetime. What caused it? Who lost money?

Your answer: _____

Discovery Questions

Q1. An investment offers 20% annual yield, guaranteed. What questions should you ask before depositing your savings?

Hint: Where does the yield come from? Is it sustainable? What is the track record?

Your answer: _____

Q2. UST and LUNA were designed so that burning LUNA creates UST (and vice versa). If UST loses its $1 peg, what happens to LUNA? And then what happens to UST?

Hint: Draw a feedback loop.

Your answer: _____

Q3. Celsius, Three Arrows Capital, Voyager, and FTX all collapsed within 6 months of Terra. How could one failure cause others?

Hint: Who lent to whom? What happens when your debtor goes bankrupt?

Your answer: _____

Q4. A hacker exploits a smart contract bug and steals $200M. The code is immutable. What are the options?

Hint: Can code be "un-hacked"? Who decides?

Your answer: _____

Cryptoeconomics Challenge

The 2022 cascade destroyed $62B+ in value. Traditional finance has FDIC insurance, lender of last resort, and circuit breakers. Design ONE mechanism that DeFi could adopt without sacrificing decentralization.

After-Class Reflection

After the lecture, list 3 warning signs that a DeFi protocol might be unsustainable. Would you have spotted Anchor's 20% APY as a red flag before the collapse?

Solutions

Complete answers to all discovery questions.

Warm-Up Answer

Examples: Lehman Brothers (2008), SVB (2023), FTX (2022). Common pattern: excessive risk-taking, insufficient reserves, and interconnected exposures that turned one failure into many. In each case, depositors/customers lost money because the entity's liabilities exceeded its assets. The parallel to DeFi is direct.

Answers

Q1: Key questions: (1) Where does the yield come from? (Real borrowing demand, or token emissions?) (2) Is it sustainable? (Anchor had \$14B deposits but only \$1.5B in borrows – the math did not work.) (3) Has the protocol been audited? (4) What happens in a market crash? (5) Is there insurance? "If you cannot identify the source of yield, YOU are the yield." Anchor's 20% APY was subsidized by Terra's treasury and collapsed when reserves ran out.

Q2: Death spiral: UST falls below \$1 → holders burn UST to mint LUNA (arbitrage) → massive LUNA minting crashes LUNA price → LUNA's falling price destroys confidence in UST's backing → more UST selling → more LUNA minting → repeat. This is a positive feedback loop with no natural floor. On May 7, UST was \$0.985. By May 13, UST was \$0.02 and LUNA was worthless. \$45B destroyed in 6 days.

Q3: Contagion through interconnected balance sheets: Celsius had UST exposure and froze \$4.7B in withdrawals. Three Arrows Capital (3AC) had positions in Terra and borrowed from Celsius; it collapsed with \$3.5B in claims. Voyager had lent \$670M to 3AC. FTX/Alameda had exposure across all of these. Each entity's collapse revealed the next one's hidden risk. The lesson: counterparty risk does not disappear just because you use blockchain.

Q4: Options after a hack: (1) Negotiate with the hacker (Euler Finance recovered \$197M this way). (2) Fork the protocol to reverse the hack (Ethereum did this after the 2016 DAO hack – controversial). (3) Use insurance protocols (Nexus Mutual) if coverage exists. (4) Accept the loss – "code is law" means immutability applies to bugs too. (5) Law enforcement (Lazarus Group from the \$1.5B Bybit hack faces international sanctions). Most often, the funds are gone permanently.

Cryptoeconomics Answer

One decentralized mechanism: **on-chain circuit breakers**. Smart contracts could include automatic pause triggers – e.g., if TVL drops more than 20% in 24 hours, withdrawals are rate-limited (not frozen) to prevent bank-run dynamics. This preserves decentralization (the rule is in code, not a human decision) while adding resilience. Additional options: decentralized insurance pools (protocol-level mutual funds), mandatory reserve ratios enforced by smart contracts, or time-delayed large withdrawals. The key constraint: any mechanism must be automated and transparent, not reliant on a central authority.