Why DeFi Needs Blockchain: Trust, Cost, and Disintermediation

Digital Finance Intensive: Day 5B

Prof. Dr. Joerg Osterrieder

Digital Finance – Intensive Course

The question every student asks after Day 5A: could DeFi run on a regular database? The answer is no – and understanding why is the key to understanding DeFi's value proposition.

Three Puzzles You Cannot Solve With a Database

Puzzle 1: In 2000 nobody would rent a bedroom to a stranger. In 2024 there are 7 million Airbnb listings. What changed?

Puzzle 2: Someone borrowed $1 billion with no collateral and repaid it in 12 seconds. Is this fraud, magic, or a new financial instrument?

Puzzle 3: On 15 September 2008 banks stopped lending to each other overnight. Was it the math or the trust that failed?

All three puzzles have the same answer: the cost of trust. And DeFi's answer to that cost is programmable trust – which requires a blockchain.

We will work through each puzzle, then formalize the theory. By the end you will be able to predict when blockchain reduces trust costs and when it does not.

These three puzzles – Airbnb, flash loans, and Lehman – all turn on the same economic concept: the cost of verifying and enforcing agreements between parties who do not trust each other.

Airbnb: Would You Let a Stranger Sleep in Your Home?

The year 2000:

- Someone calls and asks to rent your spare room for a week
- You do not know them. You have never met them.
- They offer cash upfront.
- **Most people say no.**

The year 2024:

- 7 million Airbnb listings in 220 countries
- 1.5 billion guest arrivals since founding
- Hosts earn $1B+ annually
- **The answer is now often yes.**

2000: What you feared

Stranger damages your property.
Stranger steals your belongings.
You have no recourse.
Nobody to call.

2024: What Airbnb changed

Reviews: 250M+ peer assessments.
ID verification for every guest.
$3M host damage protection.
24/7 support line.

The world did not become safer between 2000 and 2024. The infrastructure for verifying trust became cheaper and more accessible. That is the economic story.

Airbnb: What Makes You Trust a Stranger?

Discussion (2 minutes): You are listing your apartment on Airbnb for the first time. Name three things the platform does that make you comfortable accepting a booking from someone you have never met.

Your list:

1.

2.

3.

What the economics says:

Each item on your list is a **verification cost** that Airbnb reduced.

Without Airbnb absorbing that cost, you would bear it yourself (or refuse the booking).

Airbnb's entire business model is the monetisation of reduced verification cost.

This exercise maps directly to Ronald Coase (1937): intermediaries exist because they reduce transaction costs at scale. Airbnb is a trust intermediary, not a property platform.

Airbnb's Hidden Trust Infrastructure

What Airbnb built to make strangers trust strangers:

1. **Identity verification:** government ID checks for all users
2. **Reputation system:** 250M+ two-way reviews (host rates guest, guest rates host)
3. **Payment escrow:** money held until 24h after check-in; Airbnb releases it to host
4. **Insurance:** $3M AirCover for hosts; $1M liability protection
5. **24/7 dispute resolution:** human support team as enforcement backstop

Who pays for all of this?

- Airbnb charges **3% host service fee + 14% guest service fee**
- On a $100/night booking: Airbnb earns $17
- That $17 IS the price of the trust infrastructure

The punchline:
You are not paying for the bedroom.
You are paying for the **verification** that the bedroom is safe and the **enforcement** that your money will be returned if it is not.

Airbnb's 2023 revenue: $9.9B. Almost all of it is verification and enforcement cost that guests and hosts were willing to pay to trade with strangers. Trust has a market price.

Decomposing a $100 Airbnb Night

Search cost

How did you find the listing? Airbnb's search + ranking algorithm.
Reduces search from days to minutes.

Verification cost

ID check, review system, Superhost badge.
Converts unknown stranger into rated entity.

Enforcement cost

Escrow, AirCover, dispute team.
Converts promise to pay into guaranteed payment.

The question: What if we could encode verification and enforcement into software instead of into Airbnb's staff and insurance contracts?

A smart contract could: hold the payment in escrow automatically, release it based on GPS check-in confirmation, refund it if the listing does not match the description. No Airbnb needed.

The 17% Airbnb fee is the trust tax. It exists because verification and enforcement are expensive. The promise of programmable trust: make this tax approach zero for specific transaction types.

From Airbnb to Programmable Trust: The Bridge

Airbnb's model: intermediary-based trust

- Trust exists because Airbnb holds the money and enforces the rules
- Remove Airbnb and the trust evaporates
- The 17% fee is permanent overhead – the cost of the intermediary

The programmable trust alternative:

- Smart contract holds escrow automatically
- Release triggered by verifiable on-chain event (GPS proof, IoT sensor)
- Reputation score is a cryptographic proof (on-chain history), not a star rating
- Cost: one gas fee (currently \$0.50–5), not 17%

Trust Architecture Comparison

Airbnb model:
User → Airbnb (trust this) → Counterparty
Cost: 17% of transaction

Programmable trust model:
User → Smart contract (code is rules) → Counterparty
Cost: gas fee only

The constraint:
Works for **digital assets only**.
"Did the guest actually check in?" still requires an oracle or human.

The same trust logic that powers Airbnb powers DeFi – except DeFi replaces the intermediary with code. The limitation: the real world still needs oracles. The promise: for purely digital assets, the trust tax can approach zero.

A $1 Billion Loan: No Collateral, Repaid in 12 Seconds

This Actually Happened

In February 2020, a trader borrowed **$10 million from Aave** with no collateral, used it to buy and sell tokens across three different exchanges in a single operation, returned the $10 million, and kept a **$350,000 profit** – all within a single Ethereum transaction (13 seconds).

Traditional finance lens:

This is impossible. No collateral = no loan. No credit history = no loan. 13-second repayment does not exist in banking.

DeFi lens:

This is a *flash loan*: a loan that exists for exactly one transaction. If repayment fails, the entire transaction is reversed – as if it never happened.

Flash loans have processed billions of dollars in volume across DeFi protocols. They are simultaneously the most elegant DeFi instrument and the most common vector for DeFi exploits.

Flash Loan: Crime, Exploit, or Legitimate Innovation?

Discussion (2 minutes): A trader borrows $10M with no collateral and repays it 13 seconds later. Is this:

A: Money laundering

The complexity hides illicit funds.

B: Regulatory exploit

Bypasses lending rules that exist for good reason.

C: Legitimate instrument

Efficient arbitrage, benefits markets.

D: Tech curiosity

Clever code with no lasting use case.

Note: Flash loans have also been used to attack DeFi protocols for hundreds of millions in losses. The same instrument that enables arbitrage enables exploitation.

Your answer reveals your prior about DeFi. Most regulatory frameworks have no category for flash loans: they are not loans (no credit risk), not securities (no ownership transfer), and not payments (no net transfer of funds).

Flash Loans: Atomic Transactions Make This Possible

What "atomic" means:

An atomic transaction is **all-or-nothing**. Either every step succeeds and the transaction is recorded, or any step fails and the entire transaction is reversed – as if it never happened.

The flash loan mechanism:

1. Borrow $10M from Aave
2. Execute arbitrage trades (3 exchanges)
3. Repay $10M + 0.09% fee to Aave
4. Keep the profit

If step 3 fails (not enough to repay), steps 1 and 2 are reversed. Aave never lost a dollar and the borrower never received the funds.

Atomicity is a database concept (ACID transactions). Ethereum extends it to multi-party financial operations across smart contracts – enabling financial logic that is impossible in systems where steps settle independently.

Flash Loans: Only Programmable Trust Enables This

Why traditional finance cannot do this:

- Traditional loans settle in 1–3 days; repayment is enforced by courts over weeks
- No court can reverse a loan retroactively if the borrower fails to repay in 13 seconds
- Without repayment guarantee, the lender cannot release funds without collateral
- Conclusion: **flash loans require the blockchain's guarantee of atomic execution**

Legitimate uses of flash loans:

- **Arbitrage:** profit from price differences across DEXes in one transaction
- **Collateral swap:** replace your Aave collateral without closing the position
- **Liquidations:** fund a liquidation bot without pre-existing capital
- **Self-liquidation:** close your own undercollateralised position cleanly

The punchline:

Flash loans demonstrate that blockchain is not just a "decentralised database." It is a **programmable trust machine** that enables financial operations structurally impossible in any architecture where enforcement happens after the fact.

The risk:

Flash loans are also the primary vector for DeFi exploits. An attacker borrows $100M, manipulates a price oracle within the same transaction, profits from the manipulation, repays the loan. Total risk capital required: one gas fee.

Aave v3 earned over $100M in flash loan fees. The fee is 0.09% per transaction – comparable to a wire transfer fee, but the loan is uncollateralised and settled in 13 seconds.

What Flash Loans Reveal About DeFi Design

Property 1: Composability

Flash loans work because Aave, Uniswap, and Curve are all smart contracts that can call each other within a single transaction. This "money lego" composability is unique to blockchain.

Property 2: Credible neutrality

The flash loan contract does not care who the borrower is. It executes identically for a hedge fund and a student with a laptop. No gatekeeping.

Property 3: Code as enforcement

No legal contract, no KYC, no credit bureau. The code enforces repayment mechanically. This is the programmable trust that makes flash loans possible.

Next: what does this architecture look like when applied to a standard $500,000 loan?

Composability, credible neutrality, and code-as-enforcement are the three core architectural properties that DeFi inherits from blockchain. Remove any one and you have a startup with crypto branding, not DeFi.

Lehman Brothers: 15 September 2008, 6:01 AM

The timeline:

- **6:01 AM:** Lehman Brothers files for Chapter 11 bankruptcy – the largest in US history
- **By 9 AM:** Interbank overnight lending market freezes. Banks will not lend to each other.
- **By noon:** The Reserve Primary Fund "breaks the buck" (NAV falls below \$1.00) – a money market fund has never done this
- **By evening:** The US Treasury and Federal Reserve are designing emergency interventions

Scale of Lehman at failure:
\$600 billion in assets, 25,000 employees, 158 years of history, operations in 40+ countries.

What Froze in 2008

Overnight repo markets: Banks stopped lending to each other

Commercial paper: Companies could not roll short-term debt

Interbank FX swaps: Cross-border credit lines cut

Money markets: Retail investors fleeing

\$2 trillion in frozen credit markets within 48h

Lehman's balance sheet losses were large but not catastrophic relative to the financial system. What collapsed was not the math – it was the trust network that connected every bank to every other bank.

Lehman: Was It the Math or the Trust That Failed?

Discussion (2 minutes): Lehman had $600B in assets. The actual losses were large but the US economy had absorbed similar losses before. Why did this bankruptcy freeze $2 trillion in credit markets overnight?

Hypothesis A: The math failed

Lehman's losses were so large that every institution with Lehman exposure was actually insolvent. The freeze was rational.

Hypothesis B: The trust failed

Nobody knew which banks held Lehman exposure. Even banks that were fine stopped lending because they could not verify who was safe. Fear of the unknown froze the market.

Evidence: The Federal Reserve's subsequent interventions did not change the math (losses were real). They changed the trust (the Fed guaranteed liquidity). The market unfroze when trust was restored.

Ben Bernanke (Nobel Prize 2022) later wrote that the financial crisis was primarily a "financial panic" – a self-fulfilling collapse of trust – amplified by real losses, not caused by them.

Counterparty Risk: The Hidden Cost of Interbank Trust

What is counterparty risk?

The risk that the entity on the other side of your agreement cannot honour it when the time comes.

In 2008, counterparty risk cascaded:

- Bank A has a repo agreement with Bank B: lend $100M overnight
- Bank A suddenly fears Bank B has Lehman exposure
- Bank A does not know how much. Bank B cannot credibly prove zero exposure.
- Bank A refuses to roll the repo.
- Bank B now has a liquidity crisis – even if its books are sound

The verification failure:

In traditional finance:

- Balance sheets are private
- Exposures are disclosed quarterly, not in real time
- No bank could prove to another bank in real time that it was solvent

What DeFi offers:

- All positions on Aave are publicly visible in real time
- Collateral ratios are on-chain and auditable by anyone
- Liquidations happen automatically before insolvency
- No equivalent of "Lehman uncertainty" is possible

The interbank market froze because nobody could verify counterparty solvency in real time. DeFi's radical transparency – every position visible on-chain – eliminates this specific failure mode.

Blockchain Replaces Counterparty Risk with Code Risk

In a DeFi lending protocol (e.g. Aave):

- You can see every position in real time on the blockchain
- Liquidation bots enforce solvency before positions become undercollateralised
- There is no counterparty who can secretly accumulate bad exposure
- Settlement is final in 13 seconds, not 2–5 days

The Lehman scenario on Aave:
If ETH price falls 30%, all undercollateralised positions are automatically liquidated. The protocol remains solvent. No interbank panic. No opaque balance sheets.

The punchline:

Blockchain does not eliminate risk. It changes the **nature** of the risk:

Traditional finance risk:
Counterparty default + contagion uncertainty

DeFi risk:
Smart contract bugs + oracle manipulation + governance attacks

The trade:
Visible, auditable code risk *vs.* invisible, opaque counterparty risk

"Code is law" means smart contract bugs are also law. The 2016 DAO hack exploited a recursive call bug to drain $60M. The risk is different from Lehman's risk – not absent.

Three Hooks, One Lesson

Airbnb:
Trust tax = 17%.
Blockchain alternative: smart escrow reduces to gas fee.
Limit: oracle problem for real-world events.

Flash Loan:
Impossible in TradFi.
Only atomic blockchain execution makes uncollateralised lending safe.
Same mechanism enables exploits.

Lehman:
Counterparty risk froze markets.
DeFi's on-chain transparency eliminates opaque exposure.
Code risk replaces counterparty risk.

Common thread: all three cases turn on the cost of verifying and enforcing financial agreements. Blockchain reduces both – for specific use cases, under specific conditions.

Now: we formalise the theory, then walk through Aave step-by-step.

The three hooks (Airbnb, flash loans, Lehman) are three different manifestations of the same Transaction Cost Economics problem: verification and enforcement of agreements between untrusting parties.

Learning Objectives

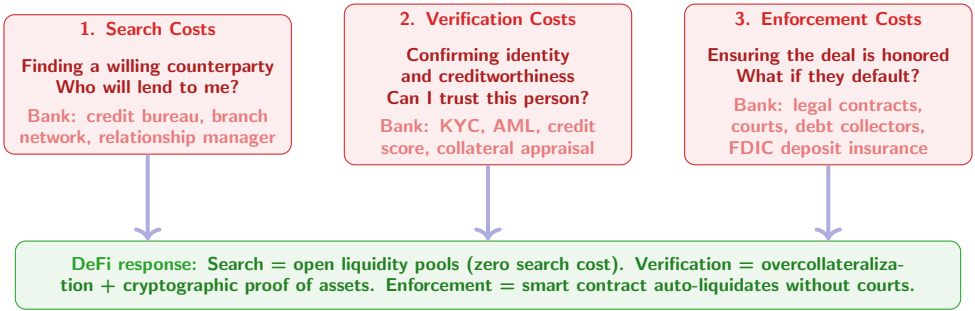
After working through the three puzzles, here is the toolkit this lecture delivers:

1. **Define** the three categories of transaction costs and give financial examples of each [Understand]
2. **Explain** why removing trust costs requires a specific technical architecture (blockchain) [Apply]
3. **Map** every step of a traditional bank loan to its DeFi equivalent in Aave [Apply]
4. **Describe** how token incentives align behavior without institutional authority [Analyze]
5. **Evaluate** when blockchain does *not* reduce transaction costs net of its own overhead [Evaluate]

The thread: Day 5A showed *who gets paid*. Day 5B explains *why the architecture makes that possible*.

Understanding the trust architecture of DeFi also explains its limits: the cases where blockchain adds costs without reducing them.

Transaction Cost Economics: The Three Costs That Banks Charge For



Ronald Coase (1937) argued that firms exist to reduce transaction costs. Blockchain reduces verification and enforcement costs to near zero for specific transaction types – but adds new costs (gas, oracle risk, smart contract bugs).

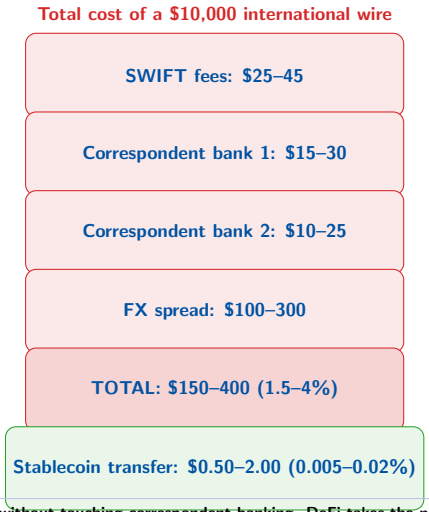
The Trust Tax: What Intermediaries Actually Cost

In a traditional bank loan:

- **Origination fee:** 0.5–1% of loan value (search + admin)
- **Interest spread:** 3–5% above cost of funds (verification + risk)
- **Early repayment fee:** 1–2% (enforcement / contract lock-in)
- **Account maintenance:** €/$10–20/month (ongoing relationship)

In a cross-border wire transfer:

- **Correspondent banking chain:** 3–5 intermediary banks
- **Total fees:** typically 3–7% of transfer amount
- **Settlement time:** 1–5 business days (T+2 to T+5)
- **Root cause:** each bank does its own verification at each hop



Wise (formerly TransferWise) built a $12B business by arbitraging the FX spread alone – without touching correspondent banking. DeFi takes the next step by removing the intermediary chain entirely.

Why AWS Is Not Enough: The Control Problem

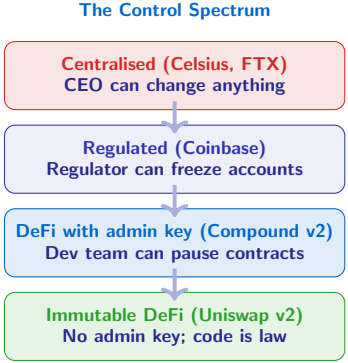
Scenario: You lend $10,000 USDC through a platform running on AWS.

Who controls the server?

- The platform company does
- They can: change interest rates, freeze withdrawals, modify loan terms, go bankrupt, be hacked, comply with a government seizure order

Historical evidence this matters:

- Celsius Network (2022): froze $4.7B in user assets; later declared bankruptcy
- FTX (2022): customer funds were moved to Alameda Research without users' knowledge
- Both were centralised platforms presenting as "DeFi-like"



"Not your keys, not your coins" is not a technical slogan. It is the core governance question: who controls the assets when the platform is under stress? The answer determines the system's trust architecture.

You Need $500K in 4 Hours: The Traditional Finance Gauntlet

Scenario: You own $800K in ETH. You need $500K in cash for a business deal that closes in 4 hours. What are your options?

Option A: Sell the ETH

Exchange order: instant.
Capital gains tax on the gain.
You lose your ETH position.
If ETH rises 20% next week, you missed it.

Cost: tax + opportunity

Option B: Bank loan

Application + credit check: 2–5 days.
Collateral appraisal (not crypto): weeks.
KYC and documentation.
Business purpose review.

Cost: time + origination fee + spread

Option C: Crypto-backed loan (CeFi)

Platform (e.g. BlockFi, Nexo): 24h.
Counterparty risk (remember Celsius).
Platform can change terms.

Cost: 8–15% APR + counterparty risk

This scenario is real. Crypto-wealthy individuals have been locked out of traditional credit markets because banks do not accept crypto as collateral. This is the exact gap that DeFi lending fills.

The Aave Option: Step by Step, $500K in 13 Minutes

Aave Loan: Step-by-Step Walkthrough

Step 1: Open Aave.com, connect MetaMask wallet. No account creation, no KYC, no application form.

Step 2: Deposit $750K ETH as collateral. Smart contract locks it. This takes 13 seconds on-chain.

Step 3: Borrow $500K USDC. Aave calculates your maximum borrow at 80% LTV ($600K max). Choose $500K.

Step 4: Receive $500K USDC in your wallet instantly. No wire transfer. No business hours.

Ongoing: Pay ~5–8% variable interest rate (algorithmic, adjusts with utilisation).

Risk: If ETH price falls below $625K ($500K / 80%), liquidation bots will sell your ETH automatically.

Close: Repay $500K USDC + accrued interest anytime. Retrieve your ETH.

Total elapsed time from wallet connection to $500K received: approximately 13 minutes.

No loan officer, no credit committee, no KYC, no waiting days. The entire loan process is encoded in the Aave smart contract. This is what "trustless lending" means in practice.

Aave vs Traditional Bank: The $500K Cost Comparison

Dimension	Traditional Bank Loan	Aave (DeFi)	Verdict
Time to funds	2–14 days	13 minutes	DeFi wins
KYC required	Yes (days of documentation)	No	DeFi wins
Collateral type	Real estate, receivables (not crypto)	ETH, USDC, WBTC (crypto only)	Split
Interest rate	6–12% fixed or variable	5–10% variable (algorithmic)	Comparable
Origination fee	0.5–2% of loan	Zero	DeFi wins
Liquidation risk	Months of process	Automatic at 80% LTV	TradFi wins
Who can use it	Credit-checked borrowers	Anyone with crypto collateral	Split
Recourse if fraud	Legal system available	No recourse	TradFi wins

Key insight: Aave wins on speed, cost, and access – for the specific case of **crypto-collateralised borrowing**. It cannot serve borrowers without existing assets.

Aave's killer insight: if you require 150% collateral, you do not need a credit check. The collateral IS the creditworthiness guarantee. DeFi lending is not inefficient – overcollateralisation is the design.

The Overcollateralisation Trade-off: Who Is Excluded?

What Aave enables:

- Anyone with ETH or USDC can borrow – no ID, no address, no bank account
- Instant, permissionless, global
- No credit history required

What Aave cannot do:

- Lend to someone who **does not already have assets**
- Underwrite based on **future income or reputation**
- Serve the **unbanked** who need credit precisely because they have no assets

The irony: DeFi is most accessible to those who need it *least* – people who already own crypto. Traditional microfinance (M-Pesa, Grameen Bank) does a better job reaching zero-asset borrowers.

Who can use DeFi lending?

YES: Has crypto assets
Lock $750K ETH, borrow $500K USDC

MAYBE: Has stablecoins
Supply USDC, earn 5–8% yield

NO: Has income but no assets
Traditional bank loan needed

EXCLUDED: Unbanked
No wallet, no assets = DeFi inaccessible

DeFi solves the trust problem for asset holders. It does not solve the access problem for the assetless. Financial inclusion requires both trust and access solutions – they are not the same thing.

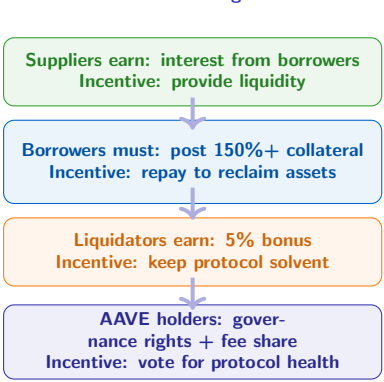
Mechanism Design: How Tokens Replace Institutional Authority

The coordination problem:
Traditional finance relies on *institutions* (banks, regulators, courts) to coordinate behavior. DeFi has no institutions. How does it prevent bad behavior?

Answer: Mechanism Design
Design the *rules of the game* so that rational self-interest produces the desired outcome – without any authority enforcing it.

In practice:

- Token **rewards** attract liquidity suppliers
- Token **slashing** penalizes malicious validators
- **Overcollateralization** makes default irrational
- **Governance tokens** align protocol stewards with protocol success



Leonid Hurwicz (Nobel Prize 2007) formalised mechanism design: "how do you construct rules so that self-interested participants produce collectively desirable outcomes?" Aave's smart contract is a mechanism design solution.

Aave Liquidity Mining: Bootstrapping a Protocol

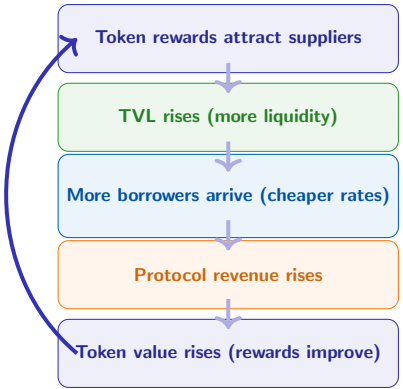
The cold-start problem:
A new lending protocol needs two things simultaneously: lenders who supply funds AND borrowers who want to borrow. Neither group shows up first.

Liquidity mining as a solution:

- Aave distributed **AAVE governance tokens** as rewards to early suppliers
- Effective APY = interest income + AAVE token value
- Example: 5% USDC interest + 15% AAVE rewards = 20% effective APY
- This attracted capital *before* organic demand existed

The risk of liquidity mining:
If AAVE token price falls, the reward APY collapses, capital leaves, creating a "DeFi bank run" dynamic.

The Liquidity Flywheel



Compound's yield farming summer (2020) demonstrated this flywheel: COMP token distribution drove TVL from $90M to $600M in 30 days. It also demonstrated the fragility: "mercenary capital" leaves when rewards are gone.

Uniswap LP Rewards: Passive Market-Making

Traditional market-making:

- Requires: Bloomberg terminal, risk capital, trading algorithms, licensed staff
- Accessible to: Goldman Sachs, Citadel, a few specialist HFT firms
- Barrier: regulatory licensing + millions in infrastructure

Uniswap LP (passive market-making):

- Requires: a crypto wallet and $1,000 in tokens
- Accessible to: anyone worldwide, 24/7
- Mechanism: deposit equal value of two tokens into a pool; earn 0.30% of every swap within your price range
- **The fee IS the market-making income**

Economic significance: Uniswap democratised market-making – a function previously reserved for billion-dollar institutions.

Uniswap LP: Who Benefits?

Small retail LPs
Earn proportional swap fees; no minimum deposit

Concentrated LPs (v3)
Earn higher fees by setting tight price ranges; requires active management

Protocol (UNI holders)
Currently earn $0 (fee switch off)

Traders
Benefit from deep, permissionless liquidity with no account required

Transaction Cost Economics applied to market-making: Uniswap reduced search costs (open pool), verification costs (no KYC), and enforcement costs (automatic settlement) to near zero for token swaps.

When Blockchain Wins vs When Crypto Twitter Loves It but the Math Fails

Cases where blockchain genuinely wins:

- **Cross-border stablecoin transfers:** multiple untrusting parties, no neutral intermediary, value is natively digital – all three conditions met
- **DeFi lending for crypto holders:** overcollateralised, instant, global, permissionless – trust cost is genuinely lower
- **Programmable settlement:** T+0 finalisation for tokenised assets removes Lehman-style uncertainty

The test: multiple untrusting parties + no neutral intermediary + value is digital

Cases crypto Twitter loves but the math does not support:

- **"Blockchain for supply chain":** the factory can lie at the IoT sensor. The blockchain records the lie faithfully. Garbage in, garbage out – now immutably.
- **Land registries in high-trust countries:** Sweden and Estonia have fully digital land registries on standard databases. Blockchain adds cost, no benefit.
- **Loyalty points within one company:** Starbucks Stars do not need a blockchain. There is one issuer, one ledger, one company. Use a SQL database.

Blockchain is not a magic trust-removal machine. It is a specific engineering trade-off: decentralised verification in exchange for higher cost, lower speed, and greater complexity. Choose it surgically.

Smart Contracts: Code as Credible Commitment

Why credible commitment matters:
A promise is only valuable if it is *credibly binding*. Institutions provide credibility (courts, regulators). Smart contracts substitute *technical binding* for *institutional binding*.

Concrete example:

- A borrower promises to repay. On paper: courts enforce this.
- On Aave: collateral is automatically liquidated at 80% LTV. No promise needed – the code makes default mechanically impossible at that threshold.

The trade-off:
Smart contracts are credibly binding *in the direction of the code*. If the code has a bug, the bug is also credibly binding. "Code is law" is both the strength and the danger.

Credible Commitment: Two Architectures

Traditional: Promise + Institution
Contract → court enforcement
Lag: months to years; cost: legal fees

DeFi: Code + Network
Smart contract → auto-execution
Lag: 13 seconds; cost: gas fee ($0.50–5)

Shared risk: both fail when the underlying assumption breaks (court corruption vs. oracle manipulation)

Oliver Hart (Nobel Prize 2016) on incomplete contracts: real agreements cannot anticipate every contingency. Smart contracts encode only what is specified; reality often produces the unspecified case.

Everything We Said Assumes Rational Actors. Day 6 Breaks That Assumption.

DeFi's mechanism design works when actors are rational:

- Liquidation bots mechanically enforce solvency
- Token incentives align rational self-interest
- Flash loan repayment is guaranteed by code

DeFi is fragile under irrational or panicking actors:

- **Death spirals:** falling collateral prices trigger liquidations which further depress prices (Terra-LUNA, 2022)
- **Bank run dynamics:** everyone withdraws simultaneously; the protocol cannot serve all redemptions
- **Herding:** DeFi users follow each other on social media; a single influencer can trigger $1B in withdrawals

Day 6B: When Digital Finance Fails

Five real crisis cases.
For each: Canvas Q3 ("what can break this?") applied systematically.

You will find the same behavioral failure modes in every case – regardless of the technology.

The pattern: Rational mechanism design + irrational human behavior = crisis. See Day 6, lecture 2.

Terra-LUNA (May 2022): a death spiral took the protocol from $40B market cap to near zero in 72 hours. Mechanism design had not modelled the case where rational actors become rational panic-sellers simultaneously. Day 6 dissects this.

Summary: Why DeFi Needs Blockchain

1. Trust costs money

Search + verification + enforcement = 3–7% on every financial transaction

2. Blockchain eliminates specific costs

Cryptographic verification + smart contract enforcement = near-zero marginal cost

3. But adds new costs

Gas, oracle risk, smart contract bugs, key management. Net benefit is case-specific.

The economic prediction: Disintermediation occurs when blockchain trust costs are less than the intermediary margin. This is true for crypto-native assets. It is contested for real-world assets.

Mechanism Design aligns rational self-interest without authority. Behavioral Finance breaks this when panic is contagious. Canvas Q3 is always: "what human behavior does this mechanism fail to anticipate?"

DeFi needs blockchain for one reason: to make financial rules credibly neutral and permissionless. Any architecture where one party can change the rules is not DeFi – it is a startup with a crypto front end.

Activity 2: Kill the Middleman

Your assigned financial service: (see group card)

Task (60 minutes):

1. **Map every intermediary step** in the traditional version of your financial service
2. **Identify the transaction cost category** at each step (search / verification / enforcement)
3. **Propose a DeFi or blockchain alternative** that reduces each cost
4. **Answer the critical question:** when is removing this intermediary *harmful*?

Output: A 3-minute verbal walkthrough of your map

Assigned services: Cross-border wire transfer / Mortgage origination / Insurance claim settlement / Equity settlement (T+2)

Remember from Day 5A: Revenue follows intermediaries. If you remove the intermediary, the revenue model changes too.

The critical question is not "can we remove this intermediary?" but "should we, and what do we lose when we do?" Recourse, consumer protection, fraud recovery, and regulatory accountability can all disappear with the intermediary.