Blockchain Economics and Digital Assets

Lecture 4: Decentralised Finance (DeFi)

Dr Daniele Bianchi

Queen Mary, University of London

Semester B, 2025/2026

Contents

Overview

The previous lectures introduced blockchain infrastructure: how blocks are created, how consensus is reached, and how smart contracts execute code. This lecture examines what has been built on top of that infrastructure: **Decentralised Finance**, or DeFi.

DeFi aims to recreate traditional financial services—lending, borrowing, trading, insurance—using smart contracts instead of banks and brokers. The vision is compelling: permissionless access, transparent operations, and 24/7 availability without intermediaries extracting rents. By early 2024, over $80 billion was locked in DeFi protocols.

But DeFi also carries substantial risks. Smart contract bugs can drain millions instantly. Economic design flaws can trigger cascading failures. The Terra/Luna collapse in May 2022 destroyed approximately $60 billion and demonstrated how "decentralised" systems can fail catastrophically.

This lecture covers the core DeFi primitives: Automated Market Makers (how trading works without order books), lending protocols (how borrowing works without credit checks), and oracles (how smart contracts access real-world data). We conclude with an examination of DeFi risks and failures, including flash loan attacks and the Terra/Luna case study.

1 What is DeFi?

1.1 The DeFi Vision

> **Decentralised Finance (DeFi)** refers to financial services—lending, borrowing, trading, insurance—built on smart contracts instead of traditional intermediaries.

In traditional finance, banks, brokers, and exchanges sit between you and financial services. They custody assets, match orders, assess credit, and extract fees. In DeFi, smart contracts perform these functions. Code replaces institutions.

The key properties that distinguish DeFi from traditional finance are as follows. First, DeFi is **permissionless**: anyone with a wallet can participate without identity verification or approval. Second, it is **non-custodial**: users retain control of their assets rather than depositing them with an institution. Third, DeFi is **transparent**: all transactions and smart contract code are publicly visible on the blockchain. Fourth, DeFi is **composable**: protocols can interact with each other, creating complex financial products from simple building blocks.

1.2 DeFi by the Numbers

The standard metric for DeFi adoption is **Total Value Locked** (TVL)—the amount of capital deposited in DeFi protocols. TVL peaked at approximately $180 billion in late 2021 during the crypto bull market, collapsed to around $40 billion during the 2022 bear market, and has recovered to approximately $80–100 billion by early 2024.

For perspective, global banking assets exceed $180 *trillion*. DeFi remains a tiny fraction of the global financial system, though it has grown from essentially zero in 2019.

Ethereum dominates DeFi, holding approximately 60% of total TVL. Layer 2 solutions (Arbitrum, Optimism) are gaining share as users seek lower transaction costs. Other chains (Solana, BNB Chain) collectively hold about 20% of TVL.

1.3 Composability: Money Legos

One of DeFi's distinctive features is **composability**—protocols can interact with each other seamlessly. A single transaction might swap ETH for USDC on Uniswap, deposit USDC into Aave as collateral, borrow DAI against that collateral, and deposit DAI into a yield aggregator. All of this happens atomically: either everything succeeds or nothing does.

This composability enables rapid innovation and capital efficiency. Developers can build new financial products by combining existing protocols rather than building from scratch.

However, composability also creates systemic risk. Failures can cascade across protocols. A bug in one protocol can affect all protocols that depend on it. This interconnectedness is both DeFi's greatest strength and its greatest vulnerability.

1.4 DeFi vs Traditional Finance

	Traditional Finance	**DeFi**
Access	Permissioned (KYC)	Permissionless
Custody	Institutions hold assets	Users hold assets
Operating hours	Business hours	24/7/365
Settlement	T+2 days (typical)	Minutes
Transparency	Opaque	Fully public
Recourse	Legal system	Code is law
Regulation	Extensive	Minimal/unclear
Insurance	FDIC, etc.	Limited/none
Reversibility	Possible	Generally not

Neither system is strictly better—they involve different trade-offs. DeFi offers access and transparency; traditional finance offers consumer protections and legal recourse. The appropriate choice depends on the user's circumstances and risk tolerance.

2 Automated Market Makers (AMMs)

2.1 The Problem AMMs Solve

Traditional exchanges use **order books**. Buyers post bids specifying the price they are willing to pay; sellers post asks specifying the price they want to receive. When a bid matches an ask, a trade executes. Professional market makers provide liquidity by continuously quoting both buy and sell prices.

Order books work poorly on blockchains for two reasons. First, every order placement, modification, and cancellation costs gas fees, making the rapid order updates characteristic of traditional markets prohibitively expensive. Second, professional market makers require the speed that blockchains cannot provide—block times of seconds are far too slow for high-frequency strategies.

The AMM solution replaces the order book with a mathematical formula that automatically determines prices based on supply and demand in the pool.

2.2 The Constant Product Formula

Uniswap, launched in 2018, pioneered the **constant product** AMM. The core mechanism is remarkably simple:

$$x \cdot y = k \tag{1}$$

where x is the quantity of Token A in the pool, y is the quantity of Token B in the pool, and k is a constant (the "invariant").

The rule is that after any trade, the product $x \cdot y$ must remain equal to k.

Consider a pool containing 100 ETH and 200,000 USDC. The constant is $k = 100 \times 200{,}000 = 20{,}000{,}000$. The implied price is $200{,}000/100 = 2{,}000$ USDC per ETH.

2.3 Trading Against the Pool

Suppose you want to buy 1 ETH from this pool. After you remove 1 ETH, the pool has 99 ETH. To maintain the constant k:

$$99 \times y = 20{,}000{,}000 \implies y = 202{,}020.20 \text{ USDC}$$

You must add $202{,}020.20 - 200{,}000 = 2{,}020.20$ USDC.

Notice that you paid 2,020.20 USDC for 1 ETH—more than the initial "price" of 2,000 USDC. This difference is **slippage**. Larger trades cause more slippage because they move the reserves further along the curve. This is how the AMM automatically adjusts prices to reflect demand: buying a token raises its price; selling lowers it.

The constant product curve is a hyperbola that never touches the axes. You can never drain the pool completely because as reserves of one token approach zero, its price approaches infinity.

2.4 Liquidity Providers

Where do pool reserves come from? Anyone can deposit tokens and become a **liquidity provider** (LP).

Consider the pool with 100 ETH and 200,000 USDC. If you deposit 1 ETH and 2,000 USDC, you now own 1% of the pool. You receive LP tokens representing this share. When traders swap through the pool, they pay a fee (typically 0.3% on Uniswap). These fees remain in the pool, so total reserves grow. Your 1% share is now worth more than what you deposited.

To withdraw, you burn your LP tokens and reclaim your proportional share of the pool. If fees have accumulated, you receive back more than you put in.

The trade-off for LPs is straightforward: they earn trading fees but face **impermanent loss**.

2.5 Impermanent Loss

Impermanent loss occurs when the price ratio of pooled tokens changes from when you deposited. The pool automatically rebalances through arbitrage, and this rebalancing can leave you worse off than simply holding the tokens.

Consider providing liquidity when ETH trades at 2,000 USDC. You deposit 1 ETH and 2,000 USDC, worth $4,000 total. Later, ETH rises to 4,000 USDC.

If you had simply held your original tokens, you would have 1 ETH @ $4,000 plus 2,000 USDC, totalling $6,000.

But your LP position has been rebalanced by arbitrageurs. Due to the constant product formula, your position is now approximately 0.707 ETH and 2,828 USDC, worth $5,656.

The **impermanent loss** is \$6,000 − \$5,656 = \$344, or 5.7%.

The loss is called "impermanent" because if prices return to the original ratio, the loss disappears. But if you withdraw when prices have diverged, the loss becomes permanent. LPs must earn enough fees to compensate for this risk.

2.6 AMM Variations

Uniswap's constant product formula is not the only approach:

Protocol	Innovation
Uniswap v2	Basic constant product formula
Uniswap v3	Concentrated liquidity—LPs choose specific price ranges
Curve	Optimised for stablecoin swaps with lower slippage
Balancer	Multi-token pools with custom weight allocations

Curve is particularly important for stablecoin trading. Since stablecoins should trade near 1:1, Curve uses a modified formula that provides much lower slippage for trades near parity.

Decentralised exchanges (DEXs) using AMMs handle approximately 15–20% of crypto spot trading volume. The majority still occurs on centralised exchanges like Binance and Coinbase, which offer better prices and lower fees for most trades. Solana has recently gained significant DEX market share due to lower transaction costs.

3 Lending Protocols

3.1 Over-Collateralised Lending

Traditional lending requires credit checks because loans are typically *under*-collateralised—you borrow more than you put down (think of a mortgage where you put down 20% and borrow 80%).

DeFi lending works differently. Without identity or credit history, there is no way to pursue defaulting borrowers. The solution is **over-collateralisation**: you must deposit more value than you borrow.

On Aave, a typical lending protocol, you might deposit 10 ETH worth \$30,000 as collateral and borrow up to approximately 75% in stablecoins—\$22,500 USDC. You pay interest on the borrowed amount while simultaneously earning interest on your deposited collateral.

Why would anyone borrow if they must over-collateralise? Several reasons. First, you can access liquidity without selling your crypto holdings, avoiding a taxable event if you are bullish on ETH. Second, you can create leverage by using borrowed funds to buy more ETH. Third, you can deploy borrowed funds in other protocols for yield farming.

3.2 Interest Rate Mechanics

DeFi lending protocols set interest rates algorithmically based on **utilisation**:

$$\text{Utilisation} = \frac{\text{Total Borrowed}}{\text{Total Deposited}}$$

When utilisation is low (lots of idle capital), interest rates are low to encourage borrowing. When utilisation is high (capital is scarce), interest rates rise to attract more deposits and discourage borrowing. This is supply and demand encoded in a smart contract.

The three main participants in lending protocols are lenders (who deposit assets into pools and earn interest), borrowers (who deposit collateral and borrow from pools while paying interest), and liquidators (who monitor undercollateralised positions and liquidate them for profit).

3.3 Liquidations and the Health Factor

Lending protocols use a **Health Factor** to measure position safety:

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Borrowed Value}}$$

Consider a position with 10 ETH collateral at \$3,000 each (\$30,000 total), a liquidation threshold of 80%, and \$20,000 borrowed. The Health Factor is $(30{,}000 \times 0.80)/20{,}000 = 1.2$.

If ETH drops to \$2,500, collateral falls to \$25,000 and the Health Factor becomes $(25{,}000 \times 0.80)/20{,}000 = 1.0$.

When the Health Factor falls below 1, the position becomes **liquidatable**. Liquidators can repay part of the debt and seize collateral at a discount (typically 5–10%). This discount incentivises liquidators to monitor positions and act quickly, ensuring the protocol remains solvent.

3.4 Liquidation Cascades

Liquidations can trigger more liquidations in a dangerous feedback loop. When ETH price drops sharply, many positions become undercollateralised simultaneously. Liquidators seize and sell ETH collateral, and this selling pressure pushes ETH price even lower. More positions become undercollateralised, leading to more liquidations.

This is a **liquidation cascade**—a feedback loop that amplifies price drops. On May 19, 2021, over \$800 million was liquidated across DeFi in 24 hours during a market crash.

3.5 Major Lending Protocols

Protocol	TVL (2024)	Key Feature
Aave	∼\$10B	Multi-chain support, flash loans
Compound	∼\$2B	Pioneer protocol, simple design
MakerDAO	∼\$8B	Issues DAI stablecoin

MakerDAO is distinct: instead of borrowing existing tokens, users mint new DAI stablecoins against their collateral. This is currency creation rather than lending in the traditional sense. We examine stablecoins in detail in Topic 5.

4 Oracles: The Data Problem

4.1 Why DeFi Needs Oracles

Recall from Topic 3 that smart contracts can only access data on the blockchain. They cannot query external websites, APIs, or databases. But DeFi requires external data: lending protocols need current asset prices for liquidations, derivatives need reference prices for settlement, and insurance protocols need real-world event data for payouts.

An **oracle** is a service that feeds external data to smart contracts.

The trust problem is fundamental. The entire DeFi system can be "trustless," but if the oracle provides false data, contracts execute on that false data. Oracles are critical infrastructure—and a major attack vector.

4.2 How Chainlink Works

Chainlink is the dominant oracle provider in DeFi. Its architecture distributes trust across multiple independent nodes. Multiple node operators fetch data from off-chain sources (exchanges, data providers). Each node signs and submits their answer on-chain. The protocol aggregates answers, typically taking the median. Smart contracts read the aggregated price.

The security model relies on decentralisation: no single node can manipulate the price. Nodes are incentivised with LINK tokens and must stake LINK that can be slashed for bad behaviour. Reputation systems track node reliability over time.

This is "decentralised" trust—you trust the network of oracles rather than any single data provider.

4.3 Oracle Attacks

If you can manipulate the oracle, you can drain the protocol. There are several attack vectors.

Spot price manipulation: If a protocol uses a single DEX as its price source, an attacker can temporarily manipulate that DEX's price, borrow or liquidate at the manipulated price, then return the market to normal.

Flash loan attacks: An attacker borrows millions with no collateral (we discuss flash loans below), uses the funds to manipulate prices, exploits a protocol at the bad prices, and repays the loan—all in one atomic transaction.

Mitigations include using time-weighted average prices (TWAP) that are harder to manipulate instantaneously, aggregating data from multiple oracle sources, and implementing circuit breakers that pause operations during extreme price movements.

4.4 The Oracle Landscape

Provider	Approach
Chainlink	Decentralised node network, most widely used
Uniswap TWAP	Time-weighted average from on-chain trades
Pyth	High-frequency data from trading firms
Band Protocol	Chainlink competitor with different chain focus

Open questions remain: How decentralised are "decentralised" oracles in practice? Who bears liability if oracle data is wrong? Can oracles scale to support high-frequency DeFi applications?

5 DeFi Risks and Failures

5.1 Categories of Risk

Risk Type	Examples
Smart contract	Bugs, exploits, reentrancy attacks
Economic design	Flawed incentives, death spirals
Oracle	Price manipulation, stale data
Governance	Malicious proposals, vote buying
Liquidity	Bank runs, liquidation cascades
Composability	Failures propagate across protocols
Regulatory	Legal uncertainty, enforcement actions

Over $3 billion was lost to DeFi exploits in 2022 alone. Unlike traditional finance, there is typically no insurance, no bailout, and no legal recourse.

5.2 Flash Loans

A **flash loan** is a loan that must be borrowed and repaid within the same transaction. No collateral is required.

The mechanics are as follows. You borrow $100 million from Aave with no collateral. You do something with the funds (arbitrage, liquidation, attack). You repay $100 million plus a small fee. If you cannot repay, the entire transaction reverts as if nothing happened.

Legitimate uses include arbitrage between exchanges, collateral swaps (replacing one type of collateral with another), and self-liquidation (unwinding your own position efficiently).

However, flash loans also enable attacks by giving anyone temporary access to massive capital. An attacker can manipulate prices on low-liquidity markets, exploit economic design flaws, or attack governance votes—all without putting up any capital.

Many major DeFi exploits have used flash loans as the funding mechanism. The innovation is double-edged: flash loans enable capital-efficient operations but also capital-efficient attacks.

5.3 Case Study: Terra/Luna Collapse (May 2022)

Terra was a blockchain with an algorithmic stablecoin called UST designed to maintain a $1 peg through arbitrage with a companion token, LUNA.

The mechanism: If UST traded above $1, anyone could mint UST by burning $1 worth of LUNA, increasing UST supply and pushing the price down. If UST traded below $1, anyone could burn UST to receive $1 worth of LUNA, decreasing UST supply and pushing the price up.

The sweetener: Anchor Protocol, built on Terra, paid 20% APY on UST deposits—an unsustainably high yield that attracted massive capital.

At the peak in April 2022, UST market cap was approximately $18 billion, LUNA market cap was approximately $40 billion, and LUNA traded around $80.

The death spiral unfolded over May 7–13, 2022. Large UST withdrawals from Anchor broke the peg slightly. Panic led to more UST selling. The UST-to-LUNA arbitrage massively inflated LUNA supply: from 350 million to 6.5 *trillion* tokens. LUNA price collapsed from $80 to $0.0001. Without valuable LUNA, UST had no backing. UST collapsed to $0.10.

Total losses: approximately $60 billion destroyed in one week.

5.4 Lessons from Terra/Luna

The fundamental problem was **circular backing**. UST was backed by LUNA, whose value depended on demand for UST. When confidence broke, both collapsed together.

Additional factors included unsustainable yields (20% APY attracted capital but was paid from dwindling reserves), no external collateral (nothing outside the system could absorb shocks), and a reflexive death spiral (the mechanism supposed to restore the peg instead accelerated collapse).

Broader lessons apply across DeFi. "Algorithmic" does not mean safe—it means the risks are encoded in code. High yields often signal high risk or unsustainable subsidies. Circular dependencies create fragility. Stablecoins need robust, external collateral.

Terra's collapse accelerated regulatory scrutiny of stablecoins worldwide.

5.5 The "Decentralisation Illusion"

DeFi markets itself as decentralised, but centralisation persists at many points.

Development teams are often small groups that control upgrades. Governance tokens are frequently concentrated among venture capitalists and founders. Most protocols depend on Chainlink for price feeds. Stablecoins like USDC can freeze addresses (and have done so). Most users access DeFi through centralised website frontends. Infrastructure providers like Infura and Alchemy handle most node traffic.

The implication is that DeFi has reduced some intermediaries but created new dependencies. "Trustless" is often aspirational rather than actual. This does not make DeFi useless, but claims should be evaluated critically.

5.6 Systemic Risk

Currently, DeFi remains largely isolated from traditional banking. Banks have minimal direct crypto exposure, and most DeFi users are crypto-native.

However, connections are growing. Bitcoin and Ethereum ETFs were approved in 2024. Banks are offering crypto custody. Stablecoins are backed by bank deposits and treasuries. Institutional DeFi participation is increasing.

Potential spillover channels include stablecoin runs stressing money markets, crypto crashes hitting institutional portfolios, and leverage in DeFi amplifying traditional market moves. Regulators are increasingly focused on these connections.

6 Summary and Looking Ahead

This lecture has covered the core primitives of DeFi. Key takeaways:

DeFi replaces intermediaries with smart contracts. It is permissionless, transparent, and composable—but also carries substantial risks without traditional consumer protections.

Automated Market Makers enable trading without order books. The constant product formula $x \cdot y = k$ determines prices algorithmically. Liquidity providers earn fees but face impermanent loss.

Lending protocols use over-collateralisation. Algorithmic interest rates respond to supply and demand. Liquidations enforce solvency but can cascade during market stress.

Oracles are critical infrastructure. Chainlink dominates the market. Price manipulation through oracles is a real and significant attack vector.

DeFi carries substantial risks. Smart contract bugs, economic design flaws, and the Terra/Luna collapse demonstrate the stakes. "Decentralisation" is often partial, and systemic connections to traditional finance are growing.

In the next lecture, we turn to stablecoins and central bank digital currencies—examining how digital money maintains stable value, the different mechanisms used, and what happens when those mechanisms fail.

Readings

Required:

- Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). *DeFi and the Future of Finance*. Wiley. Chapters 1–3. Accessible introduction to DeFi concepts.

Supplementary:

- Adams, H., Zinsmeister, N., & Robinson, D. (2020). "Uniswap v2 Core." Whitepaper. Technical specification of constant product AMM.
- Gudgeon, L., et al. (2020). "DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency." *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*.
- Aramonte, S., Huang, W., & Schrimpf, A. (2021). "DeFi Risks and the Decentralisation Illusion." *BIS Quarterly Review*, December.