Decentralised Finance (DeFi)

ECOM215: Blockchain Economics and Digital Assets

Dr Daniele Bianchi

Queen Mary, University of London

Semester B, 2025/2026

Today's Agenda

What is DeFi?

Automated Market Makers (AMMs)

Lending Protocols

Oracles: The Data Problem

DeFi Risks and Failures

Summary and Next Steps

What is DeFi?

The DeFi Vision

Decentralised Finance (DeFi)

Financial services—lending, borrowing, trading, insurance—built on smart contracts instead of traditional intermediaries.

Traditional finance: Banks, brokers, and exchanges sit between you and financial services. They custody assets, match orders, assess credit, and take fees.

DeFi: Smart contracts perform these functions. Code replaces institutions (see Week 3).

Key properties:

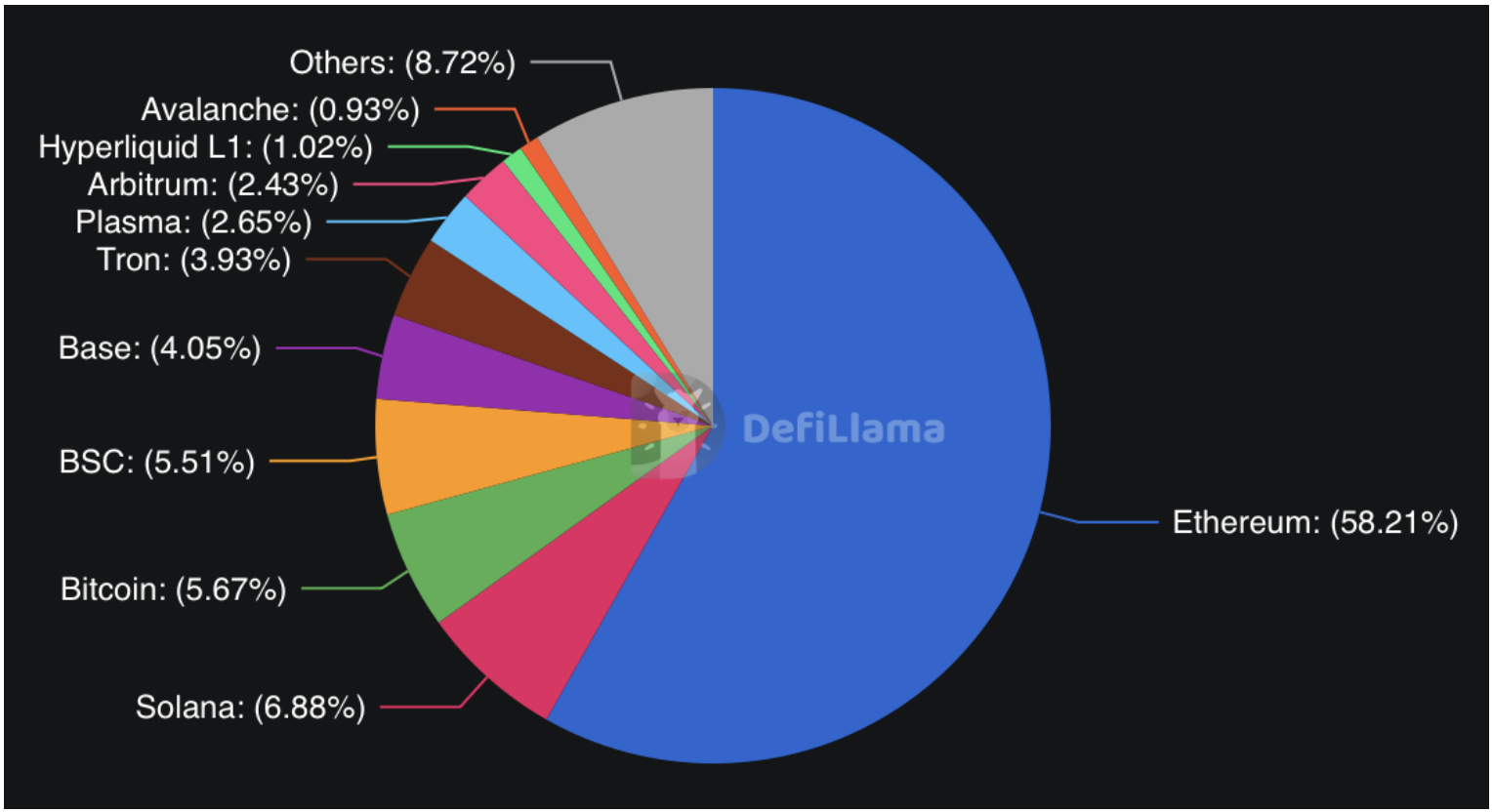
- **Permissionless**: Anyone with a wallet can "plug-in"
- **Non-custodial**: Users retain control of their assets
- **Transparent**: All transactions are publicly visible (e.g., etherscan.io)
- **Composable**: Protocols can be combined like building blocks

DeFi by the Numbers

Total Value Locked (TVL): how much capital is deposited in DeFi protocols—the standard metric for DeFi adoption.

Perspective: Global banking assets exceed $180 *trillion*. DeFi remains tiny, but is growing.

DeFi by the Numbers



Perspective: Ethereum holds ≈60% of total DeFi TVL. Other chains (Solana, BNB Chain) account for ≈20% combined, while Layer 2s (Arbitrum, Optimism) hold a growing share.

"Money Legos": Composability

DeFi protocols can interact with each other, creating complex financial products from simple building blocks.

Example: A single transaction might:

1. Swap ETH for USDC on Uniswap
2. Deposit USDC into Aave as collateral
3. Borrow DAI against that collateral
4. Deposit DAI into a yield aggregator

All of this happens atomically—either everything succeeds or nothing does.

Benefits: Innovation, capital efficiency, user choice
Risks: Failures cascade. 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.

DeFi vs Traditional Finance: Key Differences

	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 is strictly better—they involve different trade-offs. DeFi offers access and transparency; traditional finance offers protections and recourse.

Automated Market Makers (AMMs)

The Problem AMMs Solve

Traditional exchanges use order books:

- Buyers post bids, sellers post asks
- Market makers provide liquidity by quoting both sides
- Orders match when prices meet

Problem for DeFi: Order books are expensive on-chain. Every order placement, cancellation, and modification costs gas fees. Professional market makers need speed that blockchains cannot provide.

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

Automated Market Maker

A smart contract that holds reserves of two (or more) tokens and allows anyone to trade against those reserves at a price determined by an algorithm.

How Uniswap Works: The Constant Product Formula

Uniswap (launched 2018) pioneered the **constant product** AMM:

$$x \cdot y = k$$

Where:

- x = quantity of Token A in the pool
- y = quantity of Token B in the pool
- k = constant (the "invariant")

The rule: After any trade, the product $x \cdot y$ must remain equal to k.

Example: A pool has 100 ETH and 200,000 USDC.

- $k = 100 \times 200{,}000 = 20{,}000{,}000$
- Implied price: 200,000 / 100 = 2,000 USDC per ETH

Trading Against the Pool

Example: You want to buy 1 ETH from the pool.

Starting state: 100 ETH, 200,000 USDC

- Constant product: $k = 100 \times 200{,}000 = 20{,}000{,}000$
- Current price: $\frac{200{,}000}{100} = 2{,}000$ USDC per ETH

After you remove 1 ETH: Pool has 99 ETH. How much USDC must remain?

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

Your cost: The pool had 200,000 USDC, now needs 202,020.20 USDC.

$$\text{You pay: } 202{,}020.20 - 200{,}000 = \mathbf{2{,}020.20 \ \ USDC}$$

Effective price: $\frac{2{,}020.20}{1} = 2{,}020.20$ USDC per ETH

You paid 20.20 USDC *more* than the initial price of 2,000. This premium is **slippage**—the cost of moving the pool's reserves.

Why Does Slippage Occur?

The constant product rule means larger trades get worse prices.

Example: What if you want to buy 10 ETH instead of 1?

Pool after trade: $100 - 10 = 90$ ETH remain.

$$90 \times y = 20{,}000{,}000 \implies y = \frac{20{,}000{,}000}{90} = 222{,}222.22 \text{ USDC}$$

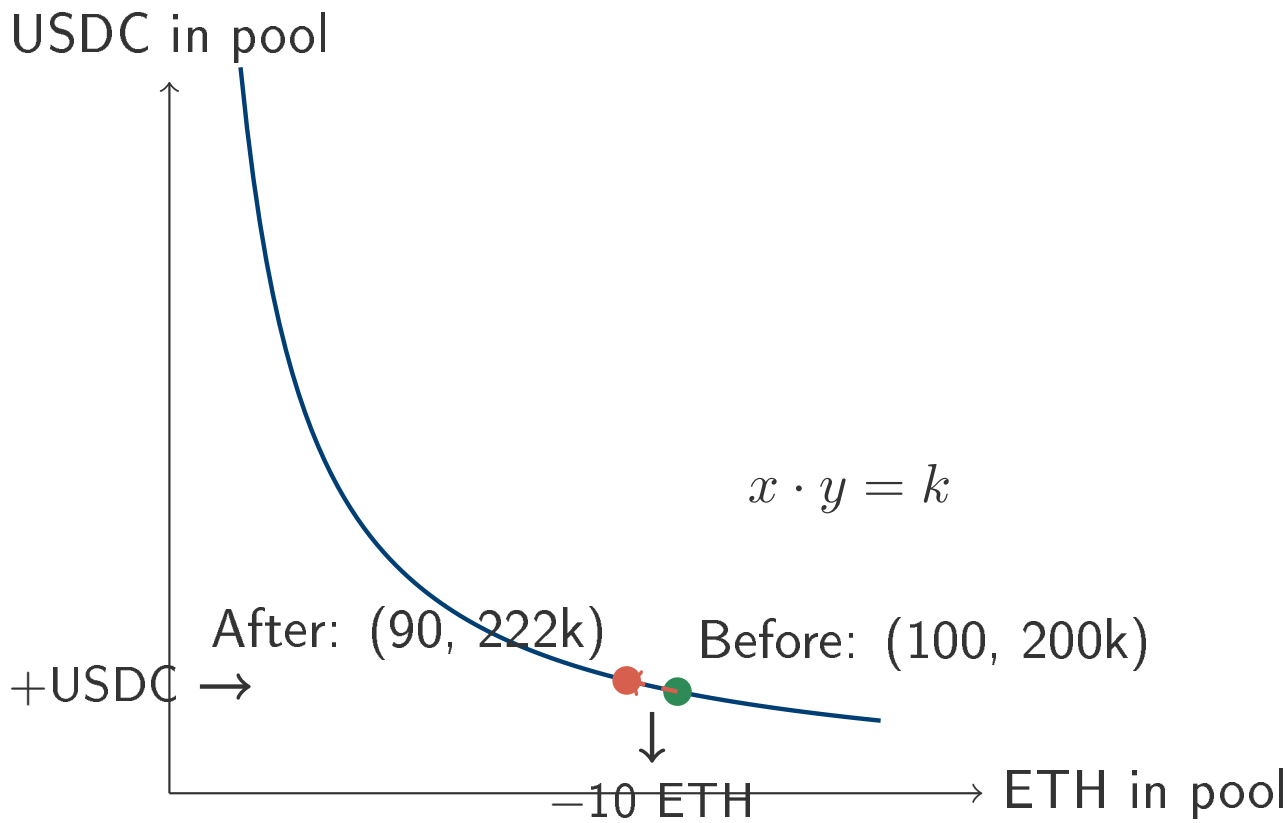
Your cost: $222{,}222.22 - 200{,}000 = 22{,}222.22$ USDC for 10 ETH.

Effective price: $\frac{22{,}222.22}{10} = 2{,}222.22$ USDC per ETH

Trade Size	Effective Price	Slippage
1 ETH	2,020.20	+1.01%
10 ETH	2,222.22	+11.1%

This is how the AMM automatically adjusts prices to reflect demand.

Visualising the Constant Product Curve



When you buy ETH (move left on x-axis), you add USDC (move up on y-axis) to stay on the curve.

Key property: The curve never touches the axes—you can never fully drain one token. As reserves approach zero, price approaches infinity.

Liquidity Providers (LPs)

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

Example: A pool has 100 ETH + 200,000 USDC (worth $400,000 at current prices). You want to add liquidity.

Rule: You must deposit both tokens in the current pool ratio.

- Current ratio: $\frac{200{,}000}{100} = 2{,}000$ USDC per ETH
- To deposit 1 ETH, you must also deposit 2,000 USDC

Your ownership share:

$$\text{Share} = \frac{\text{Your deposit}}{\text{Total pool after deposit}} = \frac{1 \text{ ETH}}{101 \text{ ETH}} \approx 0.99\%$$

You receive: LP tokens representing your 0.99% claim on the pool.

How LPs earn: Traders pay a fee (typically 0.3%) on each swap. Fees stay in the pool, increasing its value. Your LP tokens entitle you to your share of the growing pool.

LP Returns: An Example

Setup: You own 1% of a pool. Pool starts with 100 ETH + 200,000 USDC.

Your position value (at ETH = \$2,000):

$$1\% \times (100 \times \$2{,}000 + \$200{,}000) = 1\% \times \$400{,}000 = \$4{,}000$$

Trading activity: Over one month, \$10 million in volume passes through the pool at a 0.3% fee.

$$\text{Total fees collected} = \$10{,}000{,}000 \times 0.003 = \$30{,}000$$

Your share of fees: $\$30{,}000 \times 1\% = \$300$

Annualised return (if this rate continues):

$$\text{APR} = \frac{\$300 \times 12}{\$4{,}000} = 90\%$$

Sounds great—but there's a catch: While you earned fees, the pool composition changed as traders swapped. If prices moved, your position may have **underperformed** simply holding. This is **impermanent loss**.

Impermanent Loss: Setup

Scenario: You provide liquidity when ETH = 2,000 USDC.

Your initial deposit:

- 1 ETH + 2,000 USDC = \$4,000 total value
- You own some share of the pool (exact % doesn't matter for this calculation)

Later: ETH price rises to 4,000 USDC (doubles).

Question: What is your LP position worth now?

Key insight: Arbitrageurs will trade against the pool until the pool price matches the external market price. This *rebalances* the pool composition.

The pool must satisfy two conditions simultaneously:

1. Constant product: $x \cdot y = k$ (unchanged)
2. Market price: $\frac{y}{x} = 4{,}000$ (new external price)

Impermanent Loss: The Rebalancing Calculation

Finding the new pool composition:

Let the pool have x ETH and y USDC after rebalancing.

$$x \cdot y = k = 1 \times 2{,}000 = 2{,}000 \qquad \text{(constant product)}$$

$$\frac{y}{x} = 4{,}000 \qquad \text{(new market price)}$$

From the second equation: $y = 4{,}000 \cdot x$

Substitute into the first equation:

$$x \cdot (4{,}000 \cdot x) = 2{,}000 \implies x^2 = \frac{2{,}000}{4{,}000} = 0.5 \implies x = \sqrt{0.5} \approx \mathbf{0.707 \ \ ETH}$$

And therefore:

$$y = 4{,}000 \times 0.707 = \mathbf{2{,}828 \ \ USDC}$$

What happened? Arbitrageurs bought ETH from the pool (cheap relative to market), removing ETH and adding USDC until prices equalised.

Impermanent Loss: The Cost

Your LP position after rebalancing:

- 0.707 ETH @ \$4,000 = \$2,828
- 2,828 USDC = \$2,828
- **Total**: \$5,656

If you had just held the original tokens:

- 1 ETH @ \$4,000 = \$4,000
- 2,000 USDC = \$2,000
- **Total**: \$6,000

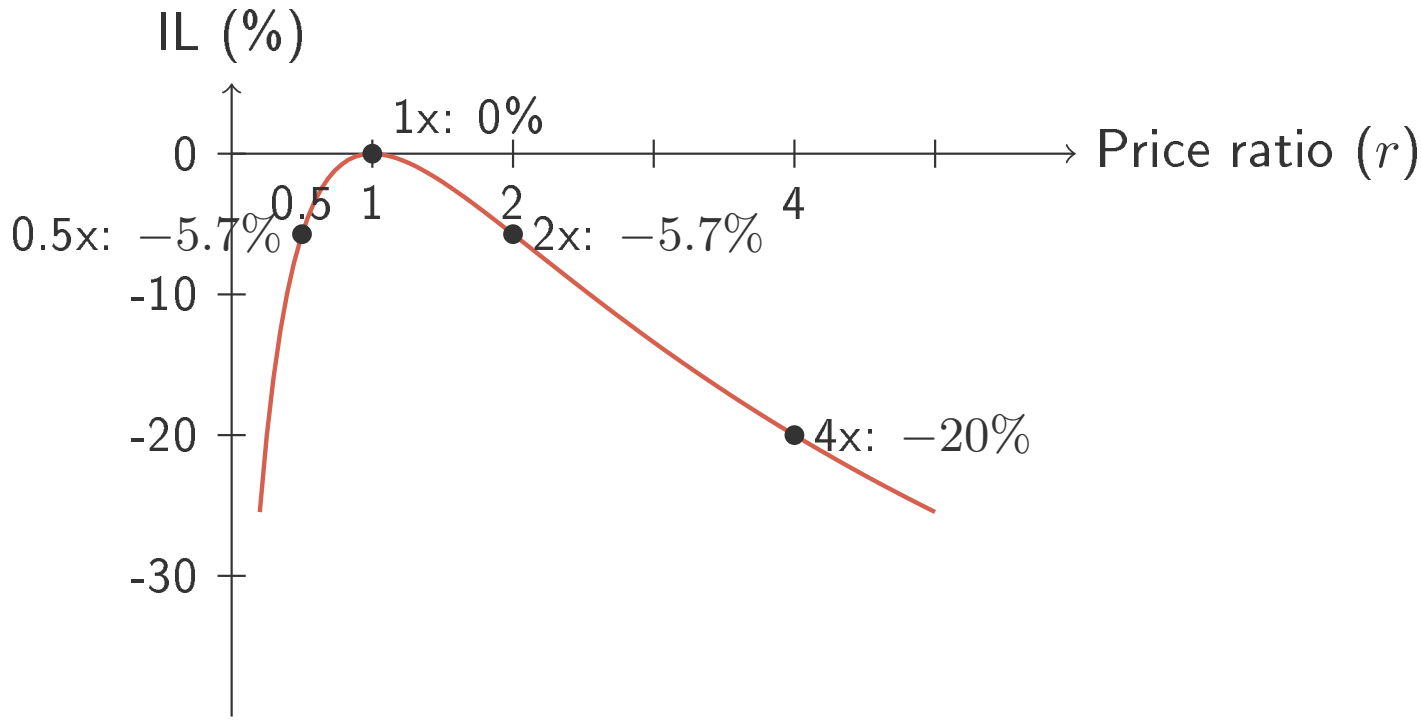
Impermanent loss:

$$\$6{,}000 - \$5{,}656 = \mathbf{\$344} \quad (5.7\% \text{ of hold value})$$

Why "impermanent"? If ETH returns to \$2,000, the pool rebalances back to 1 ETH + 2,000 USDC, and the loss disappears.

But: If you withdraw while prices have diverged, the loss becomes *permanent*. LPs must earn enough fees to compensate for this risk.

Impermanent Loss: The General Pattern

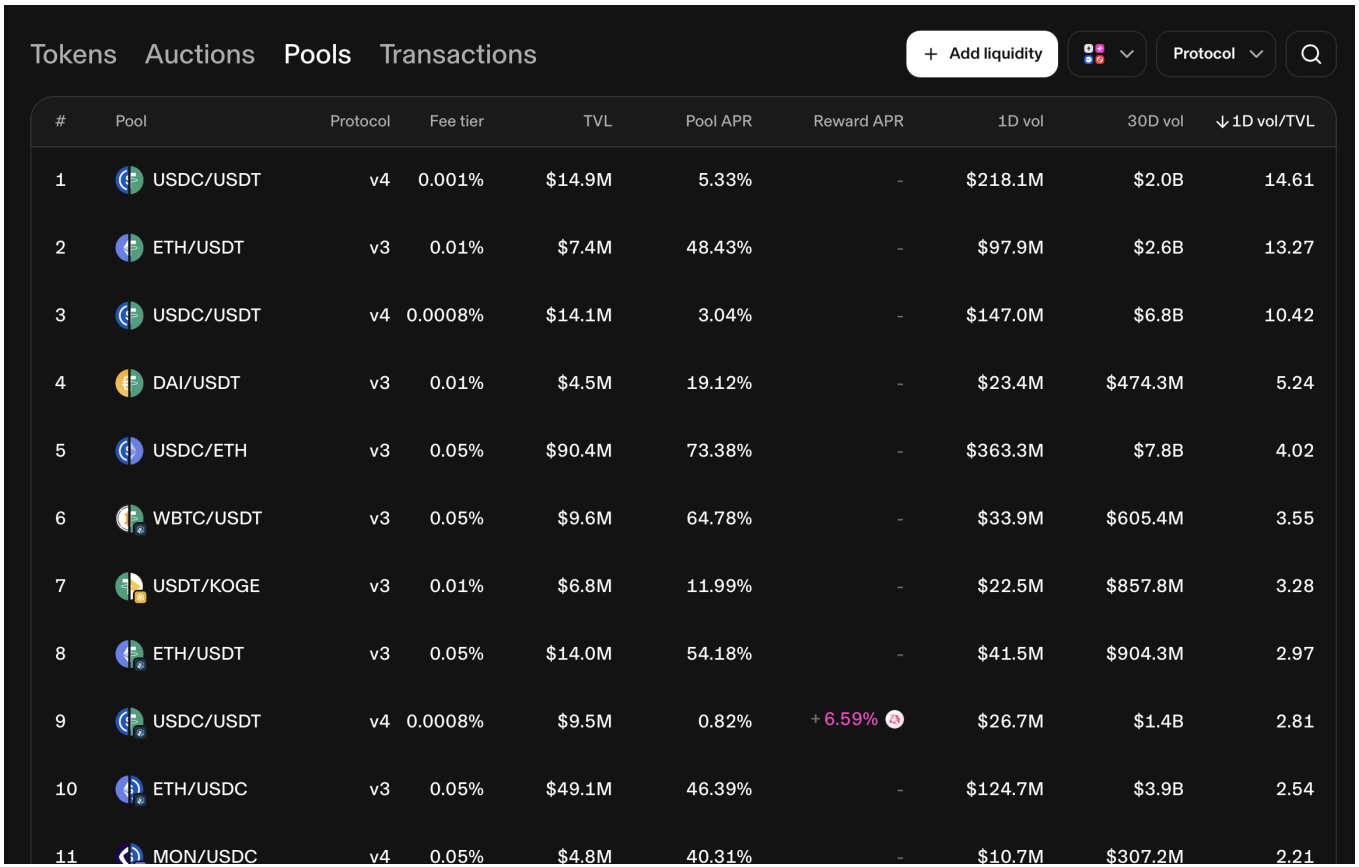


Key observations:

- IL depends on price *divergence*, not direction (2x up = 0.5x down)
- IL accelerates with larger price moves
- At 5x price change: IL $\approx 25\%$. At 10x: IL $\approx 42\%$.

Implication: LPs in volatile pairs (e.g., ETH/USDC) face higher IL than stable pairs (e.g., USDC/USDT). This explains APR differences across pools.

Interpreting LP Yields: A Real Example



#	Pool	Protocol	Fee tier	TVL	Pool APR	Reward APR	1D vol	30D vol	↓1D vol/TVL
1	USDC/USDT	v4	0.001%	$14.9M	5.33%	-	$218.1M	$2.0B	14.61
2	ETH/USDT	v3	0.01%	$7.4M	48.43%	-	$97.9M	$2.6B	13.27
3	USDC/USDT	v4	0.0008%	$14.1M	3.04%	-	$147.0M	$6.8B	10.42
4	DAI/USDT	v3	0.01%	$4.5M	19.12%	-	$23.4M	$474.3M	5.24
5	USDC/ETH	v3	0.05%	$90.4M	73.38%	-	$363.3M	$7.8B	4.02
6	WBTC/USDT	v3	0.05%	$9.6M	64.78%	-	$33.9M	$605.4M	3.55
7	USDT/KOGE	v3	0.01%	$6.8M	11.99%	-	$22.5M	$857.8M	3.28
8	ETH/USDT	v3	0.05%	$14.0M	54.18%	-	$41.5M	$904.3M	2.97
9	USDC/USDT	v4	0.0008%	$9.5M	0.82%	+6.59%	$26.7M	$1.4B	2.81
10	ETH/USDC	v3	0.05%	$49.1M	46.39%	-	$124.7M	$3.9B	2.54
11	MON/USDC	v4	0.05%	$4.8M	40.31%	-	$10.7M	$307.2M	2.21

Source: Uniswap pool data, sorted by 1-day volume/TVL ratio (February 2026).

Interpreting LP Yields: A Real Example

Key columns:

- **Fee tier**: What LPs earn per swap (0.0008% to 0.05%)
- **TVL**: Total capital deposited by LPs
- **Pool APR**: Annualised fee income relative to TVL
- **1D vol/TVL**: Daily trading volume as multiple of pool size

The fee income formula:

$$\text{Pool APR} \approx \text{Fee Tier} \times \frac{\text{Volume}}{\text{TVL}} \times 365$$

Compare three pools:

Pool	Fee	Vol/TVL	APR	Why?
USDC/USDT	0.001%	14.61	5.3%	High turnover, minimal IL risk
ETH/USDT	0.01%	13.27	48.4%	Similar turnover, **IL risk**
USDC/ETH	0.05%	4.02	73.4%	Lower turnover, higher fee + IL

Lesson: High APR compensates for impermanent loss risk—not free money.

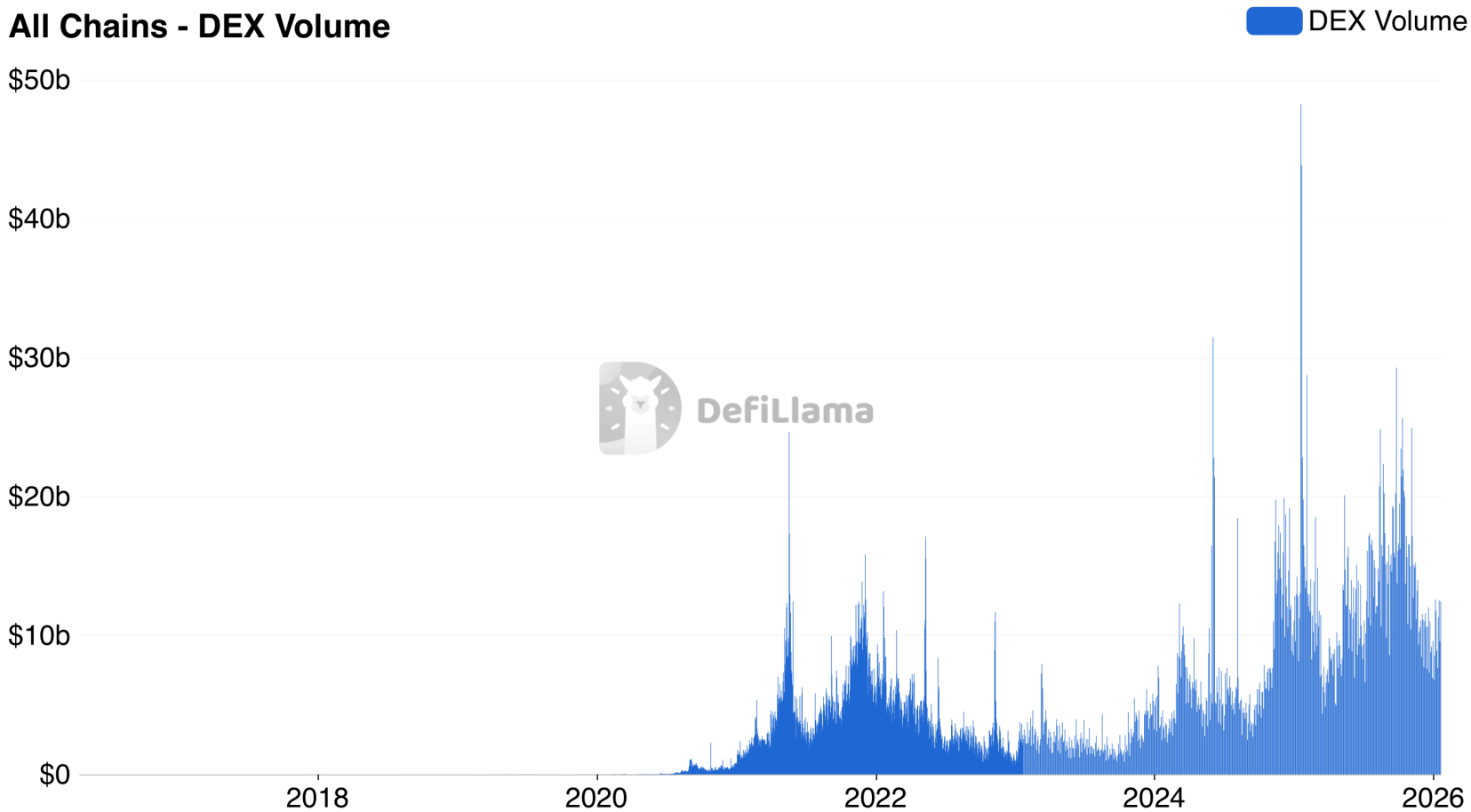
AMM Landscape

Uniswap remains dominant, but variations exist:

Protocol	Innovation
Uniswap v2	Basic constant product
Uniswap v3	Concentrated liquidity (LPs choose price ranges)
Curve	Optimised for stablecoin swaps (lower slippage)
Balancer	Multi-token pools with custom weights

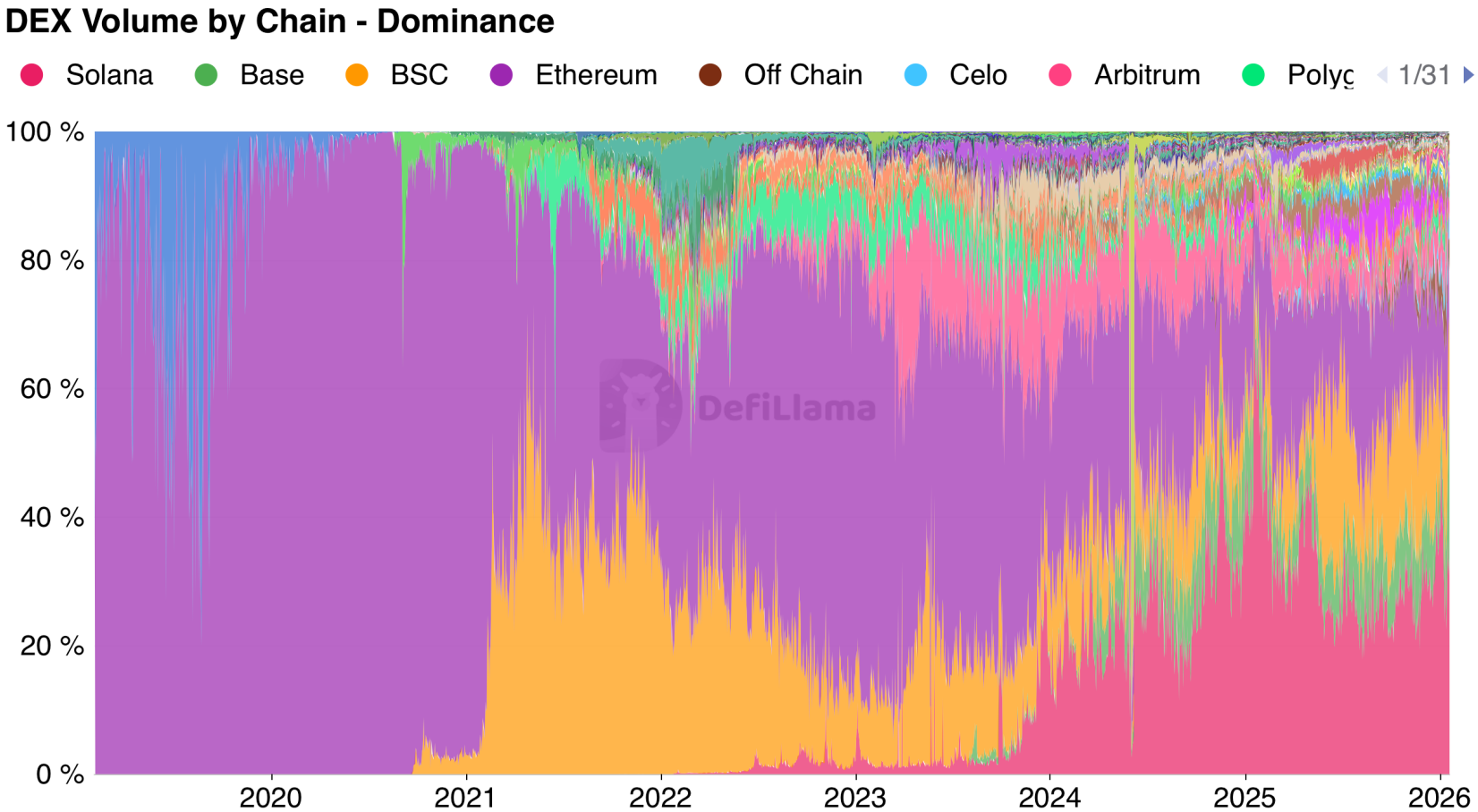
DEX vs CEX: Decentralised exchanges handle ≈15–20% of crypto spot trading volume. The majority still takes place on centralised exchanges (Binance, Coinbase).

AMM Landscape



Perspective: Trading volume on DEXs is a tiny fraction of, for example, equity markets (which are measured in trillions of dollars).

AMM Landscape



Perspective: Solana holds the relative majority of DEX volume; Ethereum is second (as of January 2026).

Lending Protocols

DeFi Lending: The Basics

Traditional lending requires credit checks because loans are *under*-collateralised—you borrow more than you put down.

DeFi lending is **over-collateralised**: You must deposit more value than you borrow.

Example (Aave):

- Deposit 10 ETH as collateral (worth $30,000)
- Borrow up to ≈75% in stablecoins: $22,500 USDC
- Pay interest on the borrowed amount
- Earn interest on your deposited collateral

Why would anyone do this?

- Get liquidity without selling (tax event, bullish on ETH)
- Leverage: Use borrowed funds to buy more ETH
- Yield farming: Deploy borrowed funds in other protocols

How Lending Protocols Work

Key participants:

- **Lenders**: Deposit assets into pools, earn interest
- **Borrowers**: Deposit collateral, borrow from pools, pay interest
- **Liquidators**: Monitor undercollateralised positions, liquidate for profit

Interest rates are set algorithmically based on **utilisation**:

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

- Low utilisation (lots of idle capital): Low rates to encourage borrowing
- High utilisation (capital scarce): High rates to attract deposits

This is supply and demand encoded in a smart contract.

The Health Factor and Liquidations

Health Factor: A measure of how safe your position is.

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

Example:

- Collateral: 10 ETH @ \$3,000 = \$30,000
- Liquidation threshold: 80%
- Borrowed: \$20,000 USDC
- Health Factor: $(30{,}000 \times 0.80)/20{,}000 = \mathbf{1.2}$

If ETH drops to \$2,500:

- Collateral: \$25,000
- Health Factor: $(25{,}000 \times 0.80)/20{,}000 = 1.0$

At Health Factor < 1: the position becomes **liquidatable**. Liquidators repay part of the debt and seize collateral at a discount (≈5–10%).

Liquidation Cascades

The danger: Liquidations can trigger more liquidations.

Scenario:

1. ETH price drops sharply
2. Many positions become undercollateralised
3. Liquidators seize and sell ETH collateral
4. This selling pressure pushes ETH price lower
5. More positions become undercollateralised
6. Repeat...

This is a **liquidation cascade**—a feedback loop that amplifies price drops.

Real example: On May 19, 2021, over $800 million was liquidated across DeFi in 24 hours during a market crash.

Major Lending Protocols

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

MakerDAO is special: Instead of borrowing existing tokens, you mint new DAI stablecoins against your collateral. This creates currency rather than lending it.

We'll explore stablecoins in depth in Topic 5.

Note: Despite being "decentralised," these protocols have governance tokens and upgrade mechanisms that introduce some centralisation.

Oracles: The Data Problem

Why DeFi Needs Oracles

Recall from Topic 3: Smart contracts can only access data on the blockchain.

But DeFi needs external data:

- **Lending**: What's the current price of ETH? (For liquidations)
- **Derivatives**: What's the S&P 500 level? (For settlement)
- **Insurance**: Did the flight get cancelled? (For payouts)

Oracle

A service that feeds external data to smart contracts.

The trust problem: The entire DeFi system can be "trustless," but if the oracle lies about prices, contracts execute on false data.

Oracles are a critical piece of infrastructure—and a major attack vector.

How Chainlink Works

Chainlink is the dominant oracle provider in DeFi.

Basic architecture:

1. Multiple independent node operators fetch data from off-chain sources
2. Each node signs and submits their answer on-chain
3. The protocol aggregates answers (typically median)
4. Smart contracts read the aggregated price

Security model:

- No single node can manipulate the price
- Nodes are incentivised with LINK tokens
- Nodes stake LINK that can be slashed for bad behaviour
- Reputation systems track node reliability

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

Oracle Attacks

If you can manipulate the oracle, you can drain the protocol.

Attack types:

1. **Spot price manipulation**:
   - If a protocol uses a single DEX as its price source...
   - Attacker manipulates that DEX price temporarily
   - Borrows/liquidates at the manipulated price
   - Returns the market to normal
2. **Flash loan attacks** (more on this later):
   - Borrow millions with no collateral
   - Use funds to manipulate prices
   - Exploit protocol at bad prices
   - Repay loan, pocket profit—all in one transaction

Mitigation: Use time-weighted average prices (TWAP), multiple oracle sources, and circuit breakers.

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, different chain focus

Open questions:

- How decentralised are "decentralised" oracles really?
- Who bears liability if oracle data is wrong?
- Can oracles scale to support high-frequency DeFi?

Oracles remain one of the most critical—and most debated—pieces of DeFi infrastructure.

DeFi Risks and Failures

Categories of DeFi 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

Scale of losses: Over $3 billion was lost to DeFi exploits in 2022 alone.

Unlike traditional finance, there's usually no insurance, no bailout, and no recourse.

Flash Loans: A Double-Edged Sword

Flash Loan

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

How it works:

1. Borrow $100 million from Aave (no collateral)
2. Do something with the funds (arbitrage, liquidation, etc.)
3. Repay $100 million + small fee
4. If you can't repay, entire transaction reverts as if nothing happened

Legitimate uses: Arbitrage, collateral swaps, self-liquidation

Attack vector: Anyone can temporarily access massive capital to:

- Manipulate prices on low-liquidity markets
- Exploit economic design flaws
- Attack governance votes

Many major DeFi exploits have used flash loans as the funding mechanism.

Case Study: Terra/Luna Collapse (May 2022)

Figure: Exchange rate between UST and USD (as of January 2026).

Case Study: Terra/Luna Collapse (May 2022)

Background: Terra was a blockchain with an algorithmic stablecoin (UST) designed to maintain a \$1 peg through arbitrage with LUNA tokens.

The mechanism:

- UST $>$ \$1: Mint UST by burning LUNA (increases UST supply)
- UST $<$ \$1: Burn UST to mint LUNA (decreases UST supply)
- Anchor protocol paid 20% APY on UST deposits

The collapse:

1. Large UST withdrawals broke the peg slightly
2. Panic led to more UST selling
3. UST $\rightarrow$ LUNA arbitrage massively inflated LUNA supply
4. LUNA price collapsed (from \$80 to \$0.0001)
5. Without valuable LUNA, UST had no backing
6. Death spiral: $\approx$\$60 billion in value destroyed in days

Lessons from Terra/Luna

What went wrong:

- Circular backing: UST was backed by LUNA, whose value depended on UST demand
- Unsustainable yields: 20% APY attracted capital but was paid from reserves
- No external collateral: Nothing outside the system to absorb shocks
- Reflexive death spiral: The mechanism that was supposed to restore the peg instead accelerated collapse

Broader lessons:

- "Algorithmic" doesn't 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 collateral (Topic 5)

Terra's collapse accelerated regulatory scrutiny of stablecoins worldwide.

The "Decentralisation Illusion"

DeFi markets itself as decentralised, but centralisation persists:

Points of centralisation:

- **Development teams**: Small groups control upgrades
- **Governance tokens**: Often concentrated among VCs and founders
- **Oracles**: Most protocols depend on Chainlink
- **Stablecoins**: USDC can freeze addresses (and has)
- **Frontends**: Most users access DeFi through centralised websites
- **Infrastructure**: Infura, Alchemy handle most node traffic

Implication: DeFi has reduced some intermediaries but created new dependencies. "Trustless" is often aspirational rather than actual.

This doesn't make DeFi useless—but claims should be evaluated critically.

Systemic Risk: DeFi and Traditional Finance

Currently: DeFi is largely isolated from traditional banking.

- Banks have minimal direct crypto exposure
- Most DeFi users are crypto-native

Growing connections:

- Bitcoin and Ethereum ETFs (approved 2024)
- Banks offering crypto custody
- Stablecoins backed by bank deposits and treasuries
- Institutional DeFi participation increasing

Potential spillover channels:

- Stablecoin runs could stress money markets
- Crypto crashes could hit institutional portfolios
- Leverage in DeFi could amplify traditional market moves

Regulators are increasingly focused on these connections.

Summary and Next Steps

Key Takeaways

1. **DeFi replaces intermediaries with smart contracts**
   - Permissionless, transparent, composable—but also risky
2. **AMMs enable trading without order books**
   - Constant product formula: $x \cdot y = k$
   - LPs earn fees but face impermanent loss
3. **Lending is over-collateralised with algorithmic rates**
   - Liquidations enforce solvency but can cascade
4. **Oracles are critical infrastructure—and attack vectors**
   - Chainlink dominant; price manipulation is real
5. **DeFi carries substantial risks**
   - Smart contract bugs, economic design flaws, Terra collapse
   - "Decentralisation" is often partial

What's Next

Topic 5: Stablecoins and Central Bank Digital Currencies

- Types of stablecoins (fiat-backed, crypto-backed, algorithmic)
- How USDC, USDT, DAI work
- Stablecoin risks and regulation
- Central Bank Digital Currencies (CBDCs)
- The future of money

Preparation:

- Think about: What makes "stable" coins stable—and what can break that stability?
- Explore: Look at stablecoin market caps on CoinGecko—which are largest?

Questions?