DeFi: Finance Without Banks

A Primer

BSc Blockchain, Crypto Economy & NFTs
Digital Finance Program

Follow Maya as she discovers the world of Decentralized Finance for the first time.

What you will learn:

What DeFi is and why it exists
Self-custody, TVL, and composability
How a DeFi transaction works end-to-end
What can go wrong – and how to stay safe

Spring Semester 2026

Contents

1 How to Use This Primer

This primer is designed as a self-study companion. You do not need any prior crypto or programming knowledge—only an open mind and willingness to look up unfamiliar terms.

Suggested reading path:

1. Read sections 1–4 in order. They establish the story and core concepts.
2. Skim sections 5–6 to see real-world context and risks.
3. Work through the practice problems (section 9) slowly, one at a time.
4. Check your answers in the Solutions appendix.
5. Return to any concept that is not clear. Repetition is fine.

Reading time: Roughly 2–3 hours for the main content, plus 1–2 hours for exercises.

A note on boxes: This primer uses colored boxes to organize content:

- **Blue story boxes** follow Maya's journey.
- **Purple definition boxes** give formal definitions.
- **Green example boxes** work through numerical problems.
- **Orange history boxes** describe real-world events.
- **Red warning and misconception boxes** flag important caveats.
- **Blue "Explain Like I'm 5" boxes** give simple analogies.
- **Purple cryptoeconomics boxes** apply the course's 6-question framework.

If you skip the theory but read only the boxes, you will still learn the key ideas. If you read everything carefully, you will understand DeFi well enough to use it (cautiously) with your own money.

2 Meet Maya

Maya's Story

Maya is a third-year BSc Finance student in Zurich. She has studied banking, portfolio theory, and corporate finance. One Friday night at 2:17 AM, her roommate Lea sends her CHF 200 using a phone app. The money arrives in eight seconds.

"Wait," Maya asks the next morning. "What bank processed that at 2 AM?"

Lea grins. "No bank. I used a DeFi protocol. It runs on code, not bankers."

Maya is skeptical. She studied the fractional-reserve system for three semesters. The idea that financial services can run without banks, without opening hours, without anyone's permission—it sounds too good to be true. She decides to investigate.

This primer follows Maya's investigation. By the end, you will understand what DeFi is, how it works, what it promises, and what it risks.

3 The Story: Maya Tries the Old Way

Maya's Story

Maya's aunt in Brazil needs CHF 5,000 urgently—a medical bill. Maya walks to her bank on Monday morning. The teller explains: international wire, 3–5 business days, CHF 45 fee, and the exchange rate includes a 2.5% markup. Total cost: roughly CHF 170. Delivery: Thursday at the earliest.
Maya remembers Lea's 8-second transfer. She opens her laptop.

Maya has stumbled onto the core **problem** that DeFi tries to solve: traditional finance depends on intermediaries (banks, brokers, clearinghouses) that add cost, delay, and exclusion.

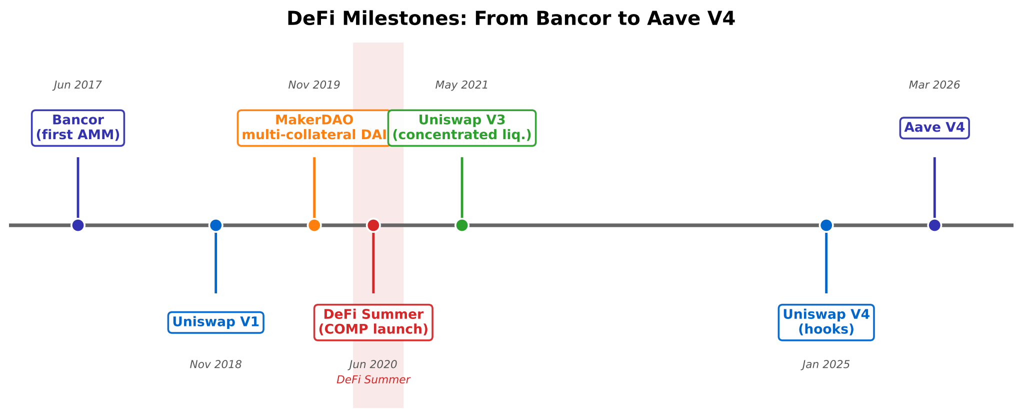
Definition: Decentralized Finance (DeFi)

Decentralized Finance (DeFi) is an umbrella term for financial services—lending, borrowing, trading, insurance—built on public blockchains using smart contracts instead of traditional intermediaries. DeFi protocols are typically open-source, permissionless, and composable.

Explain Like I'm 5

DeFi is like a row of vending machines for money. They are open 24 hours a day, 7 days a week. No cashier needed. You put tokens in, the machine follows its programmed rules, and you get what you asked for. Nobody can refuse to serve you.

The DeFi Timeline – Key Milestones



3.1 The Coordination Problem

Before diving into mechanisms, it helps to see the problem DeFi is trying to solve in its most abstract form.

Definition: Coordination Problem (Finance Edition)

Finance is fundamentally about moving resources across time and space between strangers. This requires some mechanism for trusting that:

- The other party has the funds they claim to have.
- They will deliver when they say they will.
- The records of who owns what are accurate and persistent.

- Disputes will be resolved fairly.

Traditional finance solves this with **institutions**: banks, brokers, clearinghouses, regulators, courts. DeFi solves it with **code**: smart contracts, public ledgers, cryptographic proofs.

Explain Like I'm 5

Think of a group of kids who want to trade baseball cards but cannot agree on rules. Option A: they hire a trusted adult to hold the cards and verify every swap. Option B: they build a vending machine that takes one card and gives another according to fixed rules. Option A is traditional finance. Option B is DeFi.

3.2 Why does DeFi exist?

Traditional finance has three structural limitations:

1. **Exclusion.** Roughly 1.4 billion adults worldwide have no bank account. Even those who do face geographic and bureaucratic barriers.
2. **Cost.** The average international remittance fee is 6.2% (World Bank, 2024). A simple stock trade passes through broker, exchange, clearinghouse, and custodian—each taking a cut.
3. **Speed.** Cross-border wires take 1–5 business days. Settlement of securities takes T+1 or T+2 days.

DeFi replaces intermediaries with code. A smart contract enforces the rules automatically: no approval queue, no opening hours, no minimum balance.

3.3 What DeFi is *not*

Before going further, it is worth clarifying what DeFi is *not*:

- DeFi is not Bitcoin. Bitcoin is a single-purpose protocol focused on peer-to-peer digital cash. DeFi is a broad category of financial applications, mostly built on Ethereum and other smart-contract platforms.
- DeFi is not anonymous. All transactions are public on-chain. Addresses are pseudonymous, but chain analytics firms can often link addresses to real identities.
- DeFi is not insured. There is no FDIC, no deposit guarantee, no regulator you can call. If a protocol is hacked or a smart contract has a bug, your funds may be unrecoverable.
- DeFi is not (yet) scalable for everyone. Ethereum L1 processes 15–30 transactions per second globally. Layer 2 solutions and alternative chains are addressing this, but DeFi cannot yet serve billions of users on L1 alone.

Maya makes a note: "Understand what a thing is not before you trust it with your money."

4 Key Concepts

4.1 Self-Custody

Definition: Self-Custody

Self-custody means that the user holds their own private keys and therefore has sole control over their assets. No bank or exchange can freeze, seize, or move the funds without the user's cryptographic signature.

Explain Like I'm 5

Your keys = your money. It is like carrying cash in your own wallet instead of leaving it at the bank. Nobody can lock you out—but if you lose the wallet, nobody can help you get it back.

Worked Example: Self-Custody vs. Custodial

Feature	Self-Custody	Custodial (Bank/Exchange)
Who holds the keys?	You	The institution
Can funds be frozen?	No (except protocol-level)	Yes (compliance, court order)
Recovery if keys lost?	None (unless social recovery)	Contact support
24/7 access?	Yes	Depends on platform

4.2 Total Value Locked (TVL)

Definition: Total Value Locked (TVL)

TVL measures the total USD value of crypto assets deposited into a DeFi protocol's smart contracts. It is the most common metric for gauging the size and adoption of DeFi.

Worked Example: Reading TVL

As of early 2026, approximate TVL figures for major protocols:

Protocol	TVL (USD)
Aave (lending)	\$57B
Lido (staking)	\$35B
Uniswap (DEX)	\$4B+
Curve (DEX)	\$2.2B
Total DeFi ecosystem	**\$130–140B**

TVL fluctuates with token prices. A 20% drop in ETH price would reduce Aave's TVL significantly even if no user withdraws.

4.3 Composability

Definition: Composability

Composability means that DeFi protocols can be combined like building blocks. The output of one protocol can be the input of another, because they all share the same blockchain and token standards. This property is often called "Money Legos."

Explain Like I'm 5

Imagine every toy in your box is the same brand of building block. Any piece snaps onto any other piece. In DeFi, you can borrow on Aave, swap the borrowed tokens on Uniswap, and deposit the result into a yield farm—all in one transaction.

4.4 Permissionless Access

Definition: Permissionless

A system is **permissionless** if anyone can use it without approval, identity verification, or minimum balance requirements. The only requirement is a blockchain wallet and enough tokens to pay transaction fees.

Worked Example: Who can use DeFi?

- A farmer in rural Kenya with a smartphone and $5 in crypto.
- A hedge fund deploying $50M into a lending protocol.
- A 16-year-old student experimenting with token swaps.

All three see the same interface, the same rules, the same fees. No credit check. No KYC.

4.5 The DeFi Stack

Definition: DeFi Stack

DeFi is built in **four layers**, each depending on the one below:

1. **Settlement layer** – the base blockchain (Ethereum, Solana, etc.)
2. **Asset layer** – tokens (ETH, USDC, DAI) and token standards (ERC-20, ERC-721)
3. **Protocol layer** – smart contracts for lending, trading, derivatives
4. **Application layer** – user-facing interfaces (dApps, wallets, aggregators)

4.6 CeFi vs. DeFi

Worked Example: Five-Dimension Comparison

Dimension	CeFi	DeFi
Custody	Institution	User (self-custody)
Access	KYC required	Permissionless
Transparency	Opaque (trust us)	Open-source, on-chain
Speed	Hours to days	Seconds to minutes
Regulation	Licensed, insured	Mostly unregulated

Self-Assessment Checkpoint

Can you explain the difference between self-custody and custodial in one sentence? Can you name three protocols and their TVL? If yes, continue. If not, re-read Section 3.

5 How It Works: A DeFi Transaction Step by Step

Maya's Story

Maya decides to try DeFi herself. She has 0.5 ETH in a MetaMask wallet. She wants to swap 0.1 ETH for USDC on Uniswap. Here is what happens.

1. **Connect wallet.** Maya visits `app.uniswap.org` and clicks "Connect Wallet." MetaMask pops up asking her to approve the connection. No username, no password—just her Ethereum address.

2. **Select tokens.** She selects ETH as the input token and USDC as the output. The interface shows a quote: 0.1 ETH ≈ 200 USDC (at $2,000/ETH), minus a 0.30% trading fee of $0.60.
3. **Approve and sign.** Maya clicks "Swap." MetaMask shows the transaction details: gas fee ≈ $1.50, receiving ≈ 199.40 USDC. She signs with her private key.
4. **On-chain execution.** The transaction is broadcast to the Ethereum network. A validator includes it in the next block (∼12 seconds). The Uniswap smart contract:
   - Takes 0.1 ETH from Maya's address.
   - Calculates the output using the constant-product formula.
   - Sends 199.40 USDC to Maya's address.
   - Adds Maya's ETH to the liquidity pool.
5. **Confirmation.** Within 15 seconds, Maya sees 199.40 USDC in her wallet. The entire process took less time than ordering coffee.

Important Caveat

Gas fees are unpredictable. During network congestion, the same swap could cost $20–$50 in gas. Failed transactions still consume gas. Always check the gas estimate before confirming.

Important Caveat

Phishing sites replicate DeFi interfaces pixel-for-pixel. Always verify the URL. Bookmark trusted sites. Never enter your seed phrase into a website.

Key Takeaway

A DeFi transaction has no bank, no broker, and no approval process. You connect a wallet, sign a transaction, and the smart contract executes the logic in seconds. The trade-off: you are fully responsible for your own security.

5.1 Anatomy of a Wallet

Definition: Non-Custodial Wallet

A **non-custodial wallet** is a software or hardware tool that stores your **private keys** locally. The wallet does not hold your funds—it holds the keys that prove ownership of funds recorded on the blockchain. Popular examples: MetaMask (browser), Rabby (browser), Ledger and Trezor (hardware).

Worked Example: Wallet Anatomy

A typical Ethereum wallet has three linked components:
- **Seed phrase (12 or 24 words).** The root secret. Anyone with these words controls all derived keys. Must be stored offline, ideally in two physically separate locations.
- **Private key (256 bits).** Derived from the seed phrase. Used to sign transactions.
- **Public address (∼42 characters, hex).** Derived from the private key. Shared publicly to receive funds.

Losing the seed phrase = permanent loss of all derived keys and funds.

5.2 Gas, Fees, and Layer 2

Definition: Gas Fee

Gas is the unit measuring computational work on Ethereum. Each opcode (transfer, swap, contract call) consumes a fixed amount of gas. The **gas fee** is the ETH paid to validators for including and executing your transaction: fee = gas used × gas price.

Worked Example: Gas Fee Breakdown

A simple ETH transfer uses 21,000 gas. A Uniswap swap uses roughly 150,000–200,000 gas. At a gas price of 20 gwei (20×10^{-9} ETH) and ETH = $2,000:

Action	Gas	Cost (ETH)	Cost (USD)
ETH transfer	21,000	0.00042	$0.84
ERC-20 transfer	65,000	0.00130	$2.60
Uniswap swap	180,000	0.00360	$7.20
Mint an NFT	250,000	0.00500	$10.00

During congestion, gas prices can spike to 200+ gwei, multiplying these costs by 10x.

Definition: Layer 2 (L2)

A **Layer 2** is a separate chain that processes transactions off the main Ethereum chain (L1) and periodically posts compressed proofs back to L1. Users get L1's security guarantees at a fraction of the cost. Examples: Arbitrum, Optimism, Base, zkSync.

Worked Example: L1 vs. L2 Cost

The same Uniswap swap on different networks:

- **Ethereum L1:** $5–$50 depending on congestion.
- **Arbitrum (L2):** $0.05–$0.50.
- **Base (L2):** $0.01–$0.10.

L2s enable DeFi for users who cannot afford L1 fees. Trade-off: funds must be "bridged" between L1 and L2, which adds complexity and (on optimistic rollups) a 7-day withdrawal delay.

6 Real-World Cases

Historical Case Study: The Road to DeFi (2009–2020)

DeFi did not appear overnight. It was built on a decade of experimentation:

- **2009:** Bitcoin launches. First permissionless digital money.
- **2014:** Vitalik Buterin proposes Ethereum: Bitcoin plus programmable smart contracts.
- **2015:** Ethereum mainnet launches. First general-purpose smart contract platform.
- **2017:** MakerDAO launches DAI, the first major decentralized stablecoin.
- **2018:** Uniswap V1 deployed. Compound V1 launches permissionless lending.
- **2019:** "DeFi" becomes a term of art. Total TVL crosses $1B for the first time.
- **2020:** DeFi Summer. TVL explodes. The space becomes mainstream-crypto-famous.

Each step built on the previous one. Composability made DeFi possible—without a shared platform like Ethereum, these protocols could never interact.

Historical Case Study: DeFi Summer 2020

In June 2020, Compound launched its governance token COMP and distributed it to users who lent or borrowed on the protocol. This was the first major "liquidity mining" program. The result:

- DeFi TVL jumped from $1B to $10B in three months.
- Dozens of protocols launched their own tokens and yield-farming programs.
- Gas fees on Ethereum reached $50–$100 per transaction.
- The term "DeFi Summer" entered the crypto vocabulary.

DeFi Summer proved that token incentives could bootstrap liquidity rapidly—but it also attracted speculators chasing unsustainable yields.

Historical Case Study: Uniswap Reaches $1 Trillion Cumulative Volume

In early 2025, Uniswap crossed $1 trillion in all-time trading volume. For context, the New York Stock Exchange processes roughly $25 trillion per year. Key facts:

- Uniswap launched in November 2018 with a single developer (Hayden Adams).
- V3 (May 2021) introduced concentrated liquidity, improving capital efficiency 4,000x.
- V4 (January 30, 2025) added "hooks"—custom plugins for pools.
- The protocol has processed more volume than many national stock exchanges.

Worked Example: DeFi by the Numbers (Early 2026)

Metric	Value
Total DeFi users (unique wallets)	27.7M+
Total Value Locked	$130–140B
Stablecoin total market cap	$311B
Largest DeFi protocol (Aave) TVL	$57B
Largest DEX (Uniswap) monthly volume	$60B+

6.1 The DeFi Protocol Landscape

Definition: DeFi Verticals

DeFi is typically divided into several **verticals**—categories of protocols that serve distinct financial functions:

- **DEXs (Decentralized Exchanges)** – Uniswap, Curve, Balancer. Swap tokens without an intermediary.
- **Lending** – Aave, Compound, Morpho. Deposit collateral, borrow assets.
- **Stablecoins** – DAI/USDS, USDC, USDT. Tokens pegged to fiat currencies.
- **Derivatives** – dYdX, GMX, Synthetix. Perpetual futures, synthetic assets.
- **Liquid Staking** – Lido, Rocket Pool. Stake ETH while retaining a tradable receipt token.
- **Yield Aggregators** – Yearn, Beefy. Auto-compound returns across protocols.
- **Insurance** – Nexus Mutual, InsurAce. Coverage against smart contract risk.

Worked Example: Maya Explores Each Vertical

Maya decides to interact with one protocol per vertical with very small amounts ($20 each) to learn hands-on:

1. DEX: swap 0.01 ETH for USDC on Uniswap.

2. Lending: deposit 0.01 ETH as collateral on Aave, borrow 5 USDC.
3. Stablecoin: hold 10 USDC in her wallet.
4. Liquid staking: stake 0.005 ETH via Lido, receive stETH.
5. Yield aggregator: deposit 5 USDC into a Yearn vault.

Total interaction cost: ~\$15–\$30 in gas on Ethereum L1, or ~\$1–\$3 on Arbitrum. Maya's conclusion: "Learning by doing is cheap on L2, expensive on L1."

6.2 How DeFi Measures Itself

Definition: Key DeFi Metrics

Beyond TVL, analysts track several other metrics:

- **24h Volume** – Total trading volume in the last 24 hours.
- **Revenue** – Fees actually earned by the protocol.
- **Active users** – Unique addresses interacting with the protocol.
- **Fee/TVL ratio** – How efficiently the protocol generates fees from locked capital.
- **Price-to-Sales (P/S)** – Token market cap divided by annual revenue (analog of traditional equity P/S).

Worked Example: Comparing Two Protocols

Metric	Protocol A	Protocol B
TVL	\$5B	\$500M
Annual revenue	\$50M	\$40M
Fee/TVL ratio	1.0%	8.0%
Token market cap	\$2B	\$300M
P/S ratio	40	7.5

Protocol B has 10x less TVL but nearly the same revenue—it is more capital-efficient. Its P/S ratio of 7.5 suggests the token may be undervalued relative to A's P/S of 40.

7 What Can Go Wrong

Maya's Story

Maya is impressed but cautious. "If there is no bank to call when something goes wrong," she thinks, "what exactly *can* go wrong?"

She makes a list of every failure she has heard about, then classifies each by type. The list is long, and the categories overlap.

Important Caveat

Smart contract risk. DeFi protocols are only as secure as their code. Bugs, exploits, and logic errors have caused billions in losses. In 2024 alone, crypto hacks cost \$2.2B (Chainalysis). Even audited protocols have been exploited (Euler Finance, \$197M, March 2023).

Common Misconception: "DeFi is completely safe because it runs on the blockchain"

The blockchain itself is secure (extremely expensive to attack), but the *smart contracts* deployed on it can have bugs. A flawed contract is like a flawed vending machine: the building is solid, but the machine gives wrong change. Security audits reduce risk but cannot eliminate it.

Common Misconception: "DeFi makes banks obsolete"

DeFi excels at specific functions: permissionless trading, transparent lending, and global transfers. But it lacks consumer protection, insurance (FDIC), fiat on-ramps, and regulatory clarity. For most people, traditional banks remain essential. DeFi and CeFi are converging, not replacing each other.

Key Takeaway

DeFi eliminates some risks (censorship, single points of failure) but introduces new ones (smart contract bugs, user error, scams). "Be your own bank" also means "be your own security department."

7.1 A Five-Risk Framework

Definition: The Five DeFi Risks

Maya groups DeFi risks into five categories:
1. **Smart contract risk** – bugs in protocol code.
2. **Economic risk** – unsustainable yields, cascading liquidations, stablecoin depegs.
3. **Oracle risk** – manipulated or delayed price feeds.
4. **Governance risk** – malicious proposals, vote-buying, protocol parameter changes.
5. **User risk** – lost keys, phishing, wallet approvals granted to malicious contracts.

Worked Example: Risk-Mitigation Matrix

Risk	Mitigation
Smart contract	Use audited, battle-tested protocols. Diversify.
Economic	Understand yield sources. Avoid above-market APYs.
Oracle	Prefer protocols using Chainlink or TWAP oracles.
Governance	Check proposal history. Avoid protocols with single-admin keys.
User	Hardware wallet. Revoke unused approvals. Bookmark trusted URLs.

7.2 User Error: The Largest Hidden Risk

Important Caveat

A 2023 study estimated that **20% of all Bitcoin supply is permanently lost** due to forgotten passwords, discarded hard drives, and lost keys. DeFi users face the same risks—plus the additional risks of approving malicious contract interactions. User error is silent: it does not make headlines, but it is the single largest source of crypto loss.

Worked Example: Common User Errors

1. **Sending to wrong chain.** Maya bridges USDC from Ethereum to Polygon but pastes an Optimism address. Funds are lost unless the recipient controls the same address on Polygon.
2. **Signing infinite approvals.** Approving "unlimited spending" is the default on many dApps. If that dApp is later exploited, the attacker can drain all approved tokens.
3. **Seed phrase in cloud storage.** A seed phrase in iCloud, Google Drive, or a password manager that syncs to the cloud is as secure as the cloud password—which is probably less secure than the seed phrase warrants.
4. **Clicking phishing links.** Fake DeFi interfaces advertised on search engines or social media can drain wallets in seconds once the user signs a malicious transaction.

8 The Cryptoeconomics Lens

Maya's Story

Maya steps back from the technical details and asks herself six fundamental questions about DeFi as a system.

Before applying the six-question framework, Maya pauses on a subtler question: *who controls DeFi if no single entity does?*

Definition: Decentralization as a Spectrum

"Decentralized" is not binary. DeFi protocols sit on a spectrum:

- **Admin-key decentralized:** A multi-sig controls critical functions. The team can upgrade or pause at will. Most new protocols are here.
- **Time-locked governance:** Changes require a delay, giving users time to exit. Aave and Compound use this model.
- **Token-holder governance:** All changes require a token vote. More decentralized but vulnerable to vote-buying and governance attacks.
- **Immutable:** The contract cannot be upgraded. Maximum decentralization, minimum flexibility. Uniswap V2 is a famous example.

The point on the spectrum is a choice with trade-offs. More decentralization means less agility but more censorship resistance and user sovereignty.

Cryptoeconomics Lens

Apply the six cryptoeconomics questions to DeFi:

1. **PROBLEM:** What coordination problem does DeFi solve?
   → Financial services require trust in intermediaries. DeFi replaces institutional trust with cryptographic verification and smart contract logic.

2. **INCENTIVES:** Why do participants behave correctly?
   → Liquidity providers earn fees. Borrowers post collateral (skin in the game). Governance token holders vote for protocol health because their tokens lose value if the protocol fails.
3. **BENEFITS / COSTS:** Who pays and who gains?
   → Users gain 24/7 access and lower fees. They pay in gas costs, complexity, and risk. LPs earn fees but bear impermanent loss. Developers build open-source for token rewards.
4. **FAILURE MODE:** What breaks it?
   → Smart contract exploits, oracle manipulation, governance attacks, liquidity crises, and regulatory bans. DeFi Summer 2020 showed that unsustainable yield incentives attract capital that flees at the first sign of trouble.
5. **DESIGN:** What alternatives exist?
   → AMMs vs. order books, over-collateralized vs. algorithmic stablecoins, on-chain vs. off-chain governance. Each design choice trades off efficiency, security, and decentralization.
6. **ALTERNATIVES:** How could it be improved?
   → Account abstraction for usability, intent-based trading for MEV reduction, Layer 2 scaling for lower fees, and regulatory sandboxes for institutional adoption.

9 Deep Dive: Four Canonical DeFi Interactions

Before the practice problems, Maya walks through four canonical DeFi interactions in detail. These four patterns appear in almost every DeFi session.

9.1 Interaction 1: Swap Tokens on a DEX

Worked Example: Swap ETH to USDC on Uniswap

Goal: Convert 0.5 ETH to USDC with minimum slippage.
Steps:
1. Connect wallet (MetaMask) to `app.uniswap.org`.
2. Select "ETH" as input, "USDC" as output.
3. Enter 0.5 in the amount field. The interface shows the expected output: ∼994 USDC after the 0.30% fee.
4. Set slippage tolerance (e.g., 0.5%). This is the maximum price movement you accept.
5. Click "Swap." MetaMask pops up showing: ETH sent, USDC received, estimated gas.
6. Confirm the transaction. Wait ∼15 seconds for confirmation.
7. USDC appears in your wallet.

Key risks: Front-running (MEV bots may sandwich the trade), network congestion (gas spikes), phishing (always verify the URL before connecting).

9.2 Interaction 2: Deposit Collateral and Borrow

Worked Example: Borrow USDC Against ETH on Aave

Goal: Keep ETH exposure while obtaining stablecoins for short-term expenses.
Steps:
1. Connect wallet to `app.aave.com`.
2. Click "Supply" next to ETH. Enter 2 ETH. Approve and confirm.
3. After deposit, click "Borrow" next to USDC. The interface shows max borrow (∼3,000 USDC at 75% LTV).
4. Enter a conservative amount ($2,000). The interface shows your new health factor.

5. Confirm. USDC appears in your wallet. Interest starts accruing immediately.
Monitoring: Set up alerts for HF thresholds. Most DeFi dashboards (DeBank, Zapper) can monitor position health and notify you.

9.3 Interaction 3: Provide Liquidity

Worked Example: Add Liquidity to a Uniswap V3 Pool

Goal: Earn trading fees on an ETH/USDC pool.
Steps:
1. Connect wallet to Uniswap V3.
2. Click "Pool" → "New Position."
3. Select ETH and USDC, choose the 0.05% fee tier (standard for ETH/USDC).
4. Set a price range: e.g., $1,800–$2,200 if current price is $2,000.
5. Deposit equal value of ETH and USDC (proportions vary with range).
6. Confirm. Your position earns fees whenever ETH trades within the range.

Ongoing management: If ETH moves outside the range, the position stops earning fees and converts to 100% of the out-of-range token. You must decide whether to re-center the range (incurring gas + possible IL realization) or wait for price to return.

9.4 Interaction 4: Stake and Earn

Worked Example: Stake ETH via Lido

Goal: Earn ETH staking rewards without running a validator.
Steps:
1. Connect wallet to `stake.lido.fi`.
2. Enter the amount of ETH to stake.
3. Receive stETH 1:1. stETH is a liquid token you can trade or use as collateral.
4. Rewards accrue by the stETH balance growing daily (rebasing).
5. Unstake anytime by swapping stETH to ETH on Curve or Uniswap, or via Lido's native withdrawal queue.

APY: Typically 3–4% annually, depending on Ethereum network conditions. Lido charges a 10% fee on rewards.

10 Practice Problems

Discovery Exercise 1

Define DeFi. In two sentences, explain what DeFi is to someone who has never heard of blockchain.

Discovery Exercise 2

Self-custody trade-off. List two advantages and two disadvantages of self-custody compared to keeping funds on a centralized exchange like Coinbase.

Discovery Exercise 3

TVL calculation. A lending protocol has 50,000 ETH deposited at $2,000/ETH and 30M USDC. What is the protocol's TVL? If ETH drops to $1,500 (no withdrawals), what is the new TVL?

Discovery Exercise 4

Composability chain. Describe a three-step DeFi transaction that uses three different protocols (e.g., borrow on Protocol A, swap on Protocol B, deposit on Protocol C).

Discovery Exercise 5

CeFi vs. DeFi. For each scenario, state whether CeFi or DeFi is better suited and explain why: (a) sending $50 to a friend in the same country, (b) sending $10,000 abroad on a Sunday night, (c) a retiree managing savings.

Discovery Exercise 6

Gas fee analysis. Maya's swap costs $1.50 in gas on Ethereum L1. On Arbitrum (Layer 2), the same swap costs $0.05. Why is L2 cheaper? What trade-off does the user accept?

Discovery Exercise 7

DeFi Summer math. If DeFi TVL went from $1B to $10B in 3 months (June–September 2020), what is the compounded monthly growth rate? Express as a percentage.

Discovery Exercise 8

Smart contract risk. Explain why an "audited" protocol can still be hacked. Give one real example.

Discovery Exercise 9

Protocol comparison. Compare Aave (lending, $57B TVL) and Uniswap (DEX, $4B+ TVL). Why does the lending protocol have 14x more TVL than the trading protocol?

Discovery Exercise 10

Cryptoeconomics question. Using the six-question framework from Section 7, analyze a specific DeFi protocol of your choice. Answer all six questions in 2–3 sentences each.

11 Glossary

Airdrop
A free distribution of tokens to wallet addresses meeting certain criteria, often used to bootstrap a new protocol's community.

Approval
In ERC-20 tokens, a permission granted to a smart contract to spend tokens on the user's behalf. Infinite approvals are common but risky.

Bridge
A protocol that allows assets to move between different blockchains. Bridges have historically been the single largest source of hacks.

Composability
The property that DeFi protocols can be combined like Legos, each protocol's output usable as another's input.

DAO
Decentralized Autonomous Organization. A governance structure where token holders vote on protocol changes.

dApp
Decentralized application. A user interface to a smart contract protocol.

ERC-20
The Ethereum standard for fungible tokens. Most stablecoins and governance tokens follow ERC-20.

Gas
The unit of computational cost on Ethereum. Users pay gas fees to have their transactions processed.

Governance token
A token that grants voting rights in a protocol's DAO.

Gwei
One billionth of an ETH (10^{-9} ETH). The standard unit for gas prices.

Impermanent loss
The opportunity cost suffered by liquidity providers when token prices change relative to each other.

KYC
Know Your Customer. Identity verification processes used by centralized services.

LP token
A receipt token issued to liquidity providers representing their share of a pool.

MetaMask
The most popular non-custodial browser wallet for Ethereum and EVM-compatible chains.

Non-custodial
A wallet or service where the user holds their own private keys.

Permissionless
Accessible to anyone without approval, identity verification, or minimum requirements.

Private key
The cryptographic secret that proves ownership of funds at an address. Anyone holding the private key controls the funds.

Rug pull
A scam where the protocol team removes all liquidity and disappears, leaving token holders with worthless assets.

Seed phrase
A 12- or 24-word mnemonic that deterministically generates all keys in a wallet.

Self-custody
Holding your own private keys, without trusting a third party.

Smart contract
Code deployed on a blockchain that executes deterministically when called.

Stablecoin
A cryptocurrency designed to maintain a stable value relative to a fiat currency.

TVL
Total Value Locked. The USD value of assets deposited in a protocol.

Wallet
Software or hardware that manages private keys and enables transaction signing.

Yield farming
Moving capital between protocols to maximize rewards, often by taking advantage of token incentive programs.

Solutions

Exercise 1. DeFi stands for Decentralized Finance—financial services like lending, trading, and insurance built on public blockchains using smart contracts instead of banks. Anyone with a crypto wallet can use DeFi without permission or identity verification.

Exercise 2. Advantages: (1) no third party can freeze your funds, (2) 24/7 access without institutional hours. Disadvantages: (1) if you lose your private key, funds are gone forever, (2) no customer support or fraud protection.

Exercise 3. Initial TVL = (50,000 × \$2,000) + \$30M = \$100M + \$30M = \$130M. After ETH drops to \$1,500: TVL = (50,000 × \$1,500) + \$30M = \$75M + \$30M = \$105M. TVL fell 19.2% even though no user withdrew—price change alone moves TVL.

Exercise 4. Example: (1) Deposit ETH as collateral on Aave and borrow USDC. (2) Swap USDC for DAI on Uniswap. (3) Deposit DAI into a Curve pool to earn trading fees. All three steps can execute in a single Ethereum transaction.

Exercise 5. (a) CeFi—instant mobile payment apps (Venmo, Revolut) are easier and cheaper for domestic transfers. (b) DeFi—no bank is open on Sunday night; a stablecoin transfer settles in seconds with a \$0.05–\$1.50 fee. (c) CeFi—a retiree benefits from deposit insurance (FDIC), customer support, and regulatory protection.

Exercise 6. L2s (like Arbitrum) batch many transactions and post a compressed proof to L1. This amortizes the L1 gas cost across hundreds of transactions. Trade-off: slightly weaker security guarantees (depends on L2's fraud/validity proof mechanism) and a withdrawal delay when bridging back to L1.

Exercise 7. Monthly growth rate r satisfies $1 \times (1+r)^3 = 10$, so $1 + r = 10^{1/3} \approx 2.154$, meaning $r \approx 115.4\%$ per month. Annualized, this is an absurd rate—which is why it was unsustainable.

Exercise 8. An audit checks the code at a specific point in time against known vulnerability patterns. It cannot catch all logic errors, economic exploits, or future attack vectors. Example: Euler Finance was audited multiple times but lost \$197M in March 2023 to a flash loan attack that exploited a logic flaw in its donation mechanism.

Exercise 9. Lending protocols lock collateral for the entire duration of a loan (weeks, months). DEXs hold liquidity but individual swaps are instantaneous—capital turns over rapidly. Aave's higher TVL reflects the long lock-up nature of collateralized lending vs. the transient nature of trading liquidity.

Exercise 10. Open-ended. A strong answer applies all six questions with specific details from the chosen protocol, identifies at least one failure mode with a historical example, and proposes a concrete improvement.

Further Reading

Introductory books and articles:

- Antonopoulos, A. M., & Wood, G. (2018). *Mastering Ethereum.* O'Reilly Media. Freely available on GitHub.
- Werner, S., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. (2022). "SoK: Decentralized Finance (DeFi)." *ACM AFT Conference.* A comprehensive academic survey.
- Harvey, C. R., Ramachandran, A., & Santoro, J. (2021). *DeFi and the Future of Finance.* Wiley. Written for finance professionals.

- Coase, R. H. (1937). "The Nature of the Firm." *Economica*. The original paper on why firms exist—directly relevant to the question of why decentralized protocols might replace them.

Data and analytics platforms:

- **DeFi Llama** (`defillama.com`) – TVL, yields, protocol statistics.
- **Dune Analytics** (`dune.com`) – User-created dashboards querying on-chain data.
- **CoinGecko** (`coingecko.com`) – Market caps, prices, trading volumes.
- **L2Beat** (`l2beat.com`) – Layer 2 comparison and statistics.

Tools to try (small amounts only):

- **MetaMask** – Browser wallet. Essential first step for any DeFi interaction.
- **Uniswap** – The archetypal DEX. Try a $5 swap on Base or Arbitrum L2.
- **Aave** – The archetypal lending protocol. Supply $10 of stablecoin to see the interface.
- **Zapper / DeBank** – Portfolio trackers that show all your DeFi positions in one dashboard.

Learn by doing:
The best way to understand DeFi is to use it—cautiously. Start with $10–$20 on a Layer 2 chain. Make a swap, supply to a lending protocol, unsupply. Observe the on-chain transaction. Read the transaction data on a block explorer. This hands-on experience teaches more than any textbook.