L33: Introduction to DeFi

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

Banks Hate This Trick

[COMIC: Banks hate this trick]

Placeholder for comic showing traditional bank gatekeeping vs. open DeFi access

The Setup

- Traditional finance: permission required
- Banks as gatekeepers
- Geographic and identity restrictions

The Punchline

- DeFi: permissionless access
- Smart contracts replace bankers
- Anyone with internet can participate

What if finance worked without asking permission?

Learning Objectives

- Define Decentralized Finance (DeFi) and its core principles
- Interpret Total Value Locked (TVL) as a key DeFi metric
- Explore the DeFi technology stack
- Analyze composability and its implications
- Compare DeFi to Traditional Finance (TradFi)

Building on L32: Lab: Tokenomics Analysis

The Problem: What is decentralized finance?

The Challenge
Traditional financial systems exclude 1.4 billion unbanked adults worldwide, charge high fees for basic services, and require trust in intermediaries. Can we create financial services that are accessible to anyone with internet access, operate 24/7 without banks, and execute automatically without human intervention?

Why It Matters

- Traditional finance excludes billions due to KYC/AML requirements and geographic restrictions
- Centralized intermediaries charge high fees and introduce counterparty risk (FTX, Celsius collapses 2022)
- MakerDAO (2017) pioneered decentralized stablecoins; Compound (2018) introduced money markets; DeFi Summer (2020) saw explosive growth to $15B TVL

What We Need

- Trustless verification mechanism
- Financial services operating without intermediaries
- Programmable money that executes automatically
- Protocols that can compose like building blocks

The Cryptoeconomics Question
Coordinating without trusted intermediaries

Today's lesson: How DeFi addresses financial inclusion through blockchain-based protocols

What Is DeFi and Why Does It Matter?

Definition: Decentralized Finance (DeFi) refers to financial services built on blockchain networks, operating without traditional intermediaries.

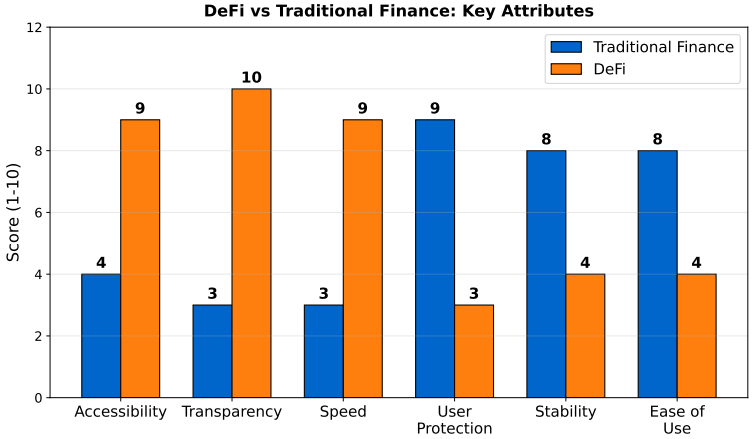
Core Principles:

- **Permissionless:** Anyone can access without approval
- **Transparent:** All transactions visible on blockchain
- **Non-custodial:** Users control their own assets
- **Composable:** Protocols integrate seamlessly (money legos)
- **Programmable:** Smart contracts automate execution

Vision: Recreate traditional financial system with greater accessibility, transparency, and efficiency.

→ *Problem: What is decentralized finance? — What is DeFi? DeFi's core principles directly answer "what is decentralized finance" – finance without banks.*

How Does DeFi Compare to Traditional Finance?



DeFi excels in accessibility and transparency; TradFi offers stability and user protection

What Are the Key Differences Between DeFi and TradFi?

Traditional Finance (TradFi)

- Centralized intermediaries (banks)
- KYC/AML requirements
- Business hours, slow settlements
- Geographic restrictions
- High barriers to entry

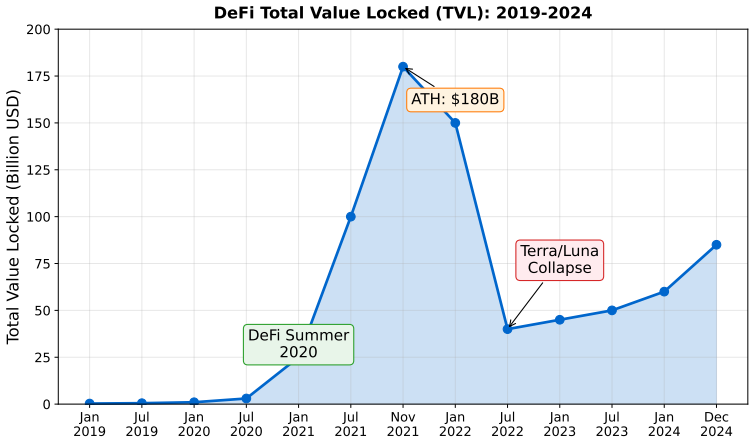
Decentralized Finance (DeFi)

- Smart contracts (no intermediaries)
- Pseudonymous (wallet addresses)
- 24/7 operation, instant settlement
- Global access
- Low barriers (internet + wallet)

Trade-off: DeFi offers accessibility and transparency but carries smart contract risks and regulatory uncertainty.

Compare the approaches shown above

How Has DeFi TVL Evolved Over Time?



DeFi Summer 2020 marked explosive growth; 2022 bear market saw major correction

What Does Total Value Locked (TVL) Measure?

Definition: The total amount of assets deposited in DeFi protocols, measured in USD.

What TVL Measures:

- Capital deployed across lending, DEXs, staking, derivatives
- Proxy for DeFi adoption and trust
- Indicator of liquidity depth

Current State (January 2026):

- Total DeFi TVL: $180 billion (recovered past December 2024 peak of $140B, led by Ethereum + L2s)
- Ethereum: 38% of TVL ($69B); Base L2 at 43% of L2 market share
- Top protocols: Aave ($34B), Lido ($26B), EigenLayer ($13B)

→ Problem: What is decentralized finance? — Total Value Locked (TVL) TVL measures how much money people trust in DeFi – higher TVL = more confidence that decentralized finance works.

How Is TVL Calculated?

Hypothetical Lending Protocol:

Deposits:

- 1,000 ETH at \$2,000/ETH = \$2,000,000
- 500,000 USDC at \$1/USDC = \$500,000
- 10 BTC at \$40,000/BTC = \$400,000

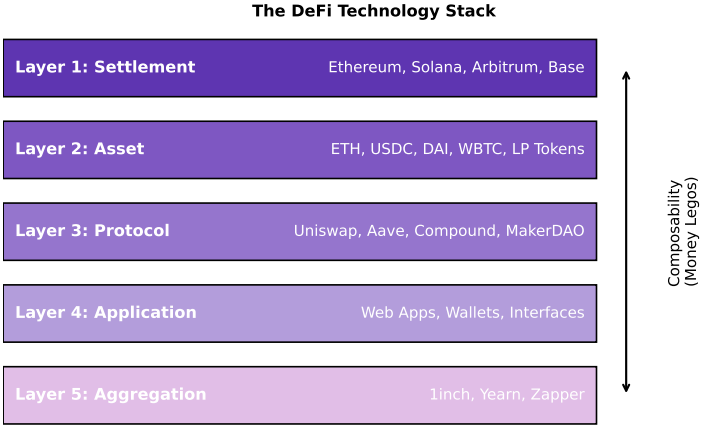
Total TVL:

$$\text{TVL} = \$2{,}000{,}000 + \$500{,}000 + \$400{,}000 = \$2{,}900{,}000$$

Note: TVL fluctuates with crypto prices; double-counting can inflate numbers.

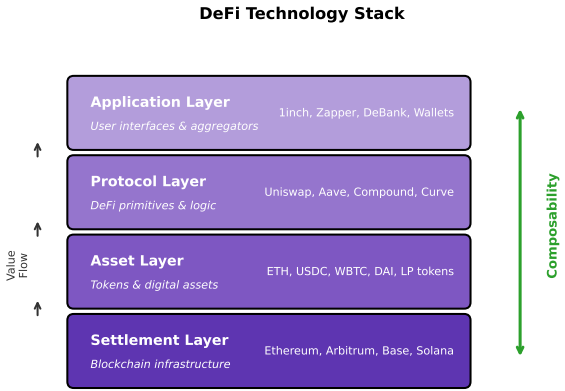
Key point: Hypothetical Lending Protocol

What Are the Layers of the DeFi Technology Stack?



Composability allows protocols to build on each other like "money legos"

How Do the DeFi Stack Layers Interact?



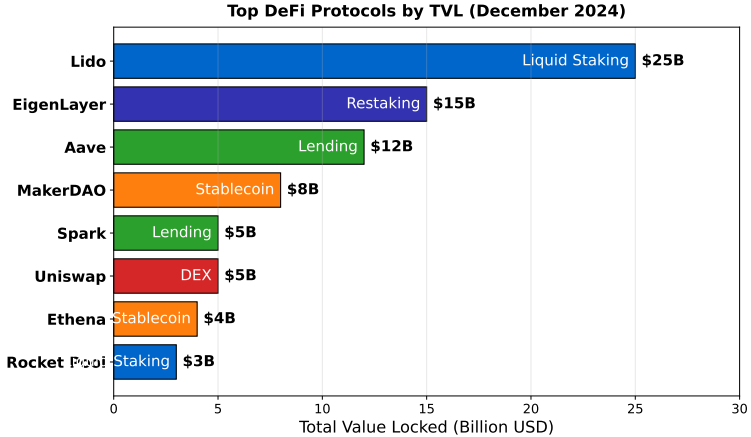
Each layer builds on the one below; value flows up through the stack

What Are the Core DeFi Building Blocks?

1. **Decentralized Exchanges (DEXs)**
   - Token swapping without intermediaries (Uniswap, Curve)
2. **Lending & Borrowing**
   - Earn interest on deposits, borrow against collateral (Aave, Compound)
3. **Stablecoins**
   - Price-stable cryptocurrencies (USDC, DAI)
4. **Derivatives**
   - Futures, options, synthetic assets (dYdX, GMX)
5. **Yield Aggregators**
   - Automated yield optimization (Yearn Finance)

Key point: 1. Decentralized Exchanges (DEXs)

Which Protocols Lead DeFi by TVL?



Liquid staking (Lido) and restaking (EigenLayer) dominate; lending and DEXs follow

Problem Check-In: DeFi Introduction

Recall Our Problem

What is decentralized finance?

What We've Learned So Far

- DeFi replaces banks with smart contracts (self-executing code on blockchain)
- TVL (Total Value Locked) measures trust: $180B deposited in DeFi protocols
- Together they show DeFi is real and growing – billions trusted to code, not banks

Still to Address

- Risks: smart contract bugs, oracle attacks, regulatory uncertainty
- Can DeFi scale to mainstream adoption without sacrificing decentralization?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "What is decentralized finance?"?

How Do DeFi Protocols Build on Each Other?

Definition: DeFi protocols can interact seamlessly, allowing complex strategies by combining simple primitives.

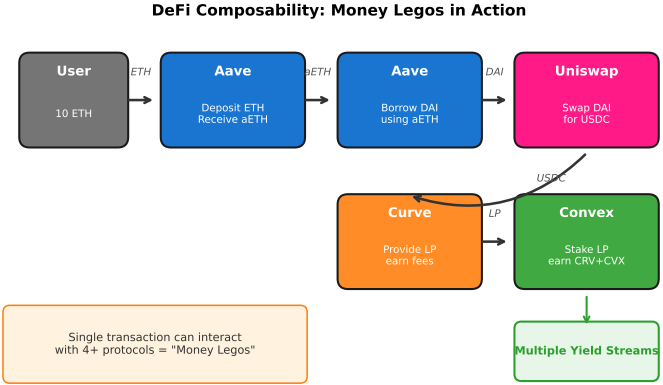
Example Workflow:

1. Deposit ETH in Aave, receive aETH (interest-bearing token)
2. Use aETH as collateral to borrow DAI
3. Swap DAI for USDC on Uniswap
4. Deposit USDC in Curve for yield farming (depositing crypto into DeFi protocols to earn interest or rewards)

Benefits: Capital efficiency, innovation from combinations
Risks: Complexity increases attack surface, protocol failure can cascade

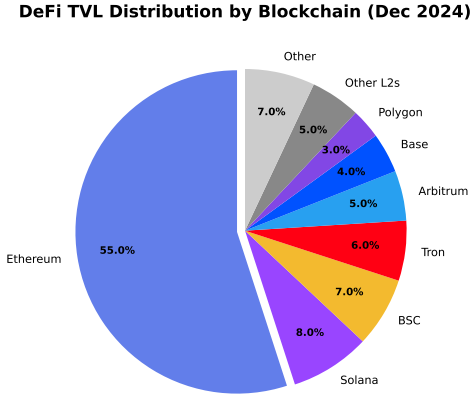
→ Problem: What is decentralized finance? — Composability: Money Legos Composability ("money legos") makes DeFi powerful – protocols stack like building blocks.

How Does Composability Work in Practice?



A single user can chain multiple protocols in one transaction for yield optimization

Which Blockchains Dominate DeFi TVL?



Ethereum maintains dominance; Layer 2s growing share rapidly

Ethereum dominates; L2s growing rapidly

What Can Go Wrong with Smart Contracts?

Definition: Bugs, exploits, or design flaws in smart contract code.

Common Vulnerabilities:

- Reentrancy attacks (famous: DAO hack 2016)
- Oracle (external data feed) manipulation
- Front-running and MEV exploitation
- Access control failures

Mitigation:

- Professional audits (Trail of Bits, OpenZeppelin)
- Bug bounties, formal verification
- Time-locks and multi-sig governance

Key point: Definition

How Do Smart Contracts Get External Data?

Challenge: Smart contracts can't natively access off-chain data (e.g., ETH price).

Solution: Oracles

- Third-party services that feed external data on-chain
- Example: Chainlink (decentralized oracle network)

Oracle Types:

- **Centralized:** Single trusted source (fast but risky)
- **Decentralized:** Multiple providers aggregated (Chainlink)
- **On-chain:** Data derived from blockchain state (Uniswap TWAP)

Risk: Oracle manipulation can drain DeFi protocols (flash loan attacks).

Key point: Challenge

What Makes DeFi Permissionless?

Permissionless Access:

- No identity verification, no geographic restrictions
- Only need: internet connection + crypto wallet
- Benefits: Financial inclusion, censorship resistance

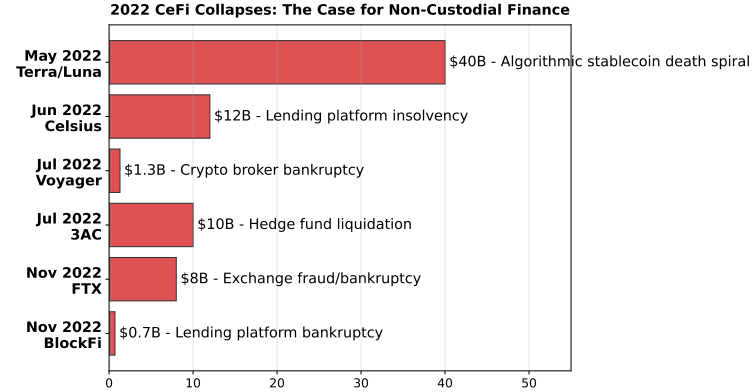
Non-Custodial Finance:

- You hold private keys, smart contract holds funds during interaction
- No third party can freeze or seize
- **Positive:** True ownership, no counterparty risk
- **Negative:** No recovery if you lose keys

Mantra: Not your keys, not your coins.

→ *Problem: What is decentralized finance? — Permissionless and Non-Custodial Permissionless access means anyone with internet can use DeFi – removing gatekeepers entirely.*

What Did the 2022 CeFi Collapses Reveal?



CeFi custodial risk exposed; DeFi protocols like Aave and Uniswap operated normally

How Does DeFi Compare to CeFi Platforms?

Centralized Crypto Platforms: Coinbase, Binance, BlockFi (collapsed 2022), Celsius (collapsed 2022)

CeFi Advantages

- User-friendly interfaces
- Customer support
- Fiat on/off ramps

CeFi Risks

- Custodial (platform holds assets)
- Counterparty risk (FTX collapse)
- Can freeze accounts

2022 Lesson: Multiple CeFi platforms collapsed (Celsius, FTX), highlighting custodial risk. DeFi protocols survived.

Compare the approaches shown above

What Is Restaking and Why Does It Matter?

What is Restaking?

- Reusing staked ETH to secure additional networks/services
- Introduced by EigenLayer (major growth 2024)

How It Works:

1. Stake ETH with Ethereum validators (earn 3-4% APY)
2. Opt-in to restaking via EigenLayer
3. Earn extra yield from securing additional services (AVS)

Impact:

- EigenLayer peaked at $19B (June 2024), now $12.6B (December 2025)
- Liquid Restaking Tokens (LRTs): eETH, rsETH, ezETH
- Criticism: Added systemic risk, complexity

Key point: What is Restaking?

Where Is DeFi Heading Next?

Emerging Trends:

- **Real-World Assets (RWA):** Tokenizing bonds, real estate
- **Undercollateralized Lending:** Credit scoring on-chain
- **Cross-Chain DeFi:** Seamless interaction across blockchains
- **Institutional Adoption:** Banks exploring DeFi rails
- **Regulation:** Clearer frameworks emerging (MiCA in EU)

Long-Term Vision:

- DeFi as backend infrastructure for TradFi
- 24/7 settlement for global finance
- Financial inclusion for billions

Key point: Emerging Trends

Problem Solved? DeFi Introduction

The Original Problem

What is decentralized finance?

How DeFi Solves It

- Smart contracts replace banks and brokers, enabling permissionless access without KYC/AML requirements
- Composability allows protocols to build on each other (Aave $\rightarrow$ Uniswap $\rightarrow$ Curve), creating capital-efficient strategies
- 24/7 operation with instant settlement removes geographic restrictions and business hours

Remaining Limitations

- Smart contract risk: Code bugs and exploits (DAO hack 2016, \$60M loss)
- Oracle dependence: External data manipulation can drain protocols (flash loan attacks)
- Regulatory uncertainty: Unclear legal frameworks for decentralized protocols

Open Questions

- Can DeFi achieve mainstream adoption without sacrificing decentralization?
- How to balance regulatory compliance with permissionless access?

DeFi enables financial services without intermediaries but introduces new technical and regulatory risks

Cryptoeconomics

The Economics of DeFi Introduction

Incentive Structure

- Coordinating without trusted intermediaries
- Participants verify rather than trust
- Users gain trustlessness, pay in complexity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users gain trustlessness, pay in complexity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: DeFi Introduction

Alternatives Considered

1. **Chosen Design:** Permissioned vs permissionless
2. **Alternative:** Traditional trusted third parties

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: DeFi Introduction

Critical Failure Mode

- **What breaks:** Sybil attacks, eclipse attacks
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Composability Risk Stack

[COMIC: Composability risk stack]

Placeholder for comic showing "money legos" stacked precariously, with one piece failing and whole tower collapsing

The Reality Check

- Composability = power + risk
- Each protocol layer adds vulnerability
- One failure can cascade through stack

Warning Signs

- Complex yield strategies
- Multiple protocol dependencies
- "Too good to be true" returns

Money legos are powerful – until one piece fails and the whole tower falls

Summary

Summary: Key Takeaways

Key Takeaways:

- DeFi recreates financial services on blockchain: permissionless, transparent, non-custodial
- TVL measures capital deployed ($180B in January 2026, recovered past the $140B December 2024 peak)
- Composability enables innovation but increases complexity
- Smart contract risk and oracle manipulation are key concerns
- Restaking (EigenLayer) emerged as major 2024 innovation (peaked $19B)
- Ethereum dominates (38%) of multichain TVL; Base L2 leads Layer 2 ecosystem (43% share)

Next Lecture: AMM Mechanics - How automated market makers work.

Next Lesson: L34 – AMM Mechanics

Key point: Key Takeaways

Questions for Reflection

1. How does TVL differ from traditional finance metrics like AUM?
2. Why is composability both a strength and a risk in DeFi?
3. What are the trade-offs between DeFi and CeFi for retail users?
4. How do oracles solve the external data problem, and what risks remain?
5. What regulatory challenges does DeFi face in the next 5 years?

Key point: Questions for Reflection

Quiz Questions (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries like banks.

Q2. Which of the following is NOT a core principle of DeFi?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their own assets with private keys.

Q3. What does TVL (Total Value Locked) measure?
A) Number of users B) Transaction volume C) Assets deposited in protocols D) Token prices
Answer: C – TVL is the total USD value of assets deposited across DeFi protocols.

Q4. As of January 2026, what is the approximate total DeFi TVL?
A) $50 billion B) $120 billion C) $180 billion D) $300 billion
Answer: C – DeFi TVL is $180B as of January 2026, having recovered past the 2024 peak of $140B.

Q5. Which blockchain dominates DeFi TVL?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: B – Ethereum holds the largest share (38%) of total DeFi TVL as of January 2026, followed by L2 ecosystems.

Quiz Questions (6–10)

Q6. What does "composability" mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows DeFi protocols to work together like "money legos."

Q7. Which protocol had the highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $31B TVL, followed by Lido ($26B).

Q8. What is the main risk of composability in DeFi?
A) Slower transactions B) Higher gas fees C) Cascading failures D) Reduced liquidity
Answer: C – Complex protocol interactions increase attack surface; one failure can cascade.

Q9. What is a reentrancy attack?
A) Exploiting oracle data B) Calling a function recursively before it completes C) Front-running trades D) Draining liquidity pools
Answer: B – Reentrancy exploits recursive calls (famous example: DAO hack 2016).

Q10. Which of the following is NOT a DeFi primitive?
A) Decentralized Exchanges B) Lending & Borrowing C) Custodial wallets D) Stablecoins
Answer: C – Custodial wallets are centralized; DeFi uses non-custodial wallets.

Quiz

Quiz Questions (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts on-chain.

Q12. Which oracle type is considered most decentralized?
A) Single trusted source B) Chainlink aggregated feeds C) Uniswap TWAP D) Exchange API
Answer: B – Chainlink uses multiple providers with aggregation for decentralization.

Q13. What does "permissionless" mean in DeFi?
A) No fees required B) No KYC/AML verification needed C) No smart contracts D) No token holdings
Answer: B – Anyone can access DeFi without identity verification or approval.

Q14. What happened during the 2022 CeFi collapses?
A) DeFi protocols failed B) Ethereum stopped working C) Centralized platforms froze assets D) Gas fees spiked
Answer: C – Celsius, FTX, and BlockFi collapsed, but DeFi protocols operated normally.

Q15. What is the main advantage of CeFi over DeFi?
A) Decentralization B) User-friendly interfaces C) Lower fees D) Smart contracts
Answer: B – CeFi offers better UX, customer support, and fiat on/off ramps.

Quiz Questions (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens D) Converting staked tokens
Answer: B – Restaking allows staked ETH to secure additional networks for extra yield.

Q17. What was EigenLayer's peak TVL in 2024?
A) $5 billion B) $12.6 billion C) $19 billion D) $31 billion
Answer: C – EigenLayer peaked at $19B in June 2024, now $12.6B (December 2025).

Q18. Which Layer 2 network has the largest share of L2 TVL?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads Layer 2 ecosystem with 43% market share as of December 2025.

Q19. What does "non-custodial" mean in DeFi?
A) No transaction fees B) Users hold their own private keys C) No smart contracts D) Centralized control
Answer: B – Non-custodial means users control assets; no third party holds keys.

Q20. What is a major emerging trend in DeFi's future?
A) Removing smart contracts B) Tokenizing Real-World Assets C) Eliminating oracles D) Centralized governance
Answer: B – RWA tokenization (bonds, real estate) is a growing DeFi trend.