

# L33: Introduction to DeFi

## Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

# Learning Objectives

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

# What is DeFi?

**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.

## Traditional Finance (TradFi)

- Centralized intermediaries (banks)
- KYC/AML requirements
- Business hours, slow settlements
- Geographic restrictions
- Opaque processes
- Custodial (bank holds assets)
- High barriers to entry

## Decentralized Finance (DeFi)

- Smart contracts (no intermediaries)
- Pseudonymous (wallet addresses)
- 24/7 operation, instant settlement
- Global access
- Transparent on-chain data
- Non-custodial (user controls keys)
- Low barriers (internet + wallet)

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

# The Rise of DeFi

## Historical Timeline:

- **2015:** Ethereum launches, enabling smart contracts
- **2017:** MakerDAO creates DAI stablecoin
- **2018:** Uniswap V1 introduces AMM model
- **2019:** Compound launches money markets
- **2020:** DeFi Summer - explosive TVL growth (yield farming)
- **2021:** Peak TVL reaches \$180B+
- **2022:** Bear market, TVL drops to \$40B
- **2024:** Recovery to \$50-60B range

**Key Insight:** DeFi cycles with broader crypto market but maintains core innovation.

# Total Value Locked (TVL)

**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 (December 2024):

- Total DeFi TVL: \$50-55 billion
- Ethereum: 55% of TVL
- Binance Smart Chain: 10%
- Solana, Avalanche, Polygon: 5-8% each

## Top Protocols by TVL:

- ① Lido (liquid staking): \$20B
- ② MakerDAO (stablecoin): \$5B
- ③ Aave (lending): \$4B
- ④ Uniswap (DEX): \$3.5B

# TVL Calculation Example

## 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 issue: same assets deposited multiple times
- True TVL vs. inflated TVL (some trackers adjust for this)

# The DeFi Stack (Layers)

## Layer 1: Settlement Layer

- Base blockchain (Ethereum, Solana, etc.)
- Consensus and transaction finality

## Layer 2: Asset Layer

- Native tokens (ETH, BTC) and stablecoins (USDC, DAI)

## Layer 3: Protocol Layer

- Smart contracts for DeFi services (Uniswap, Aave, Compound)

## Layer 4: Application Layer

- User interfaces (web apps, wallets)

## Layer 5: Aggregation Layer

- Meta-protocols (1inch, Yearn) that route across multiple protocols

## 1. Decentralized Exchanges (DEXs)

- Token swapping without intermediaries
- Examples: Uniswap, SushiSwap, Curve

## 2. Lending & Borrowing

- Earn interest on deposits, borrow against collateral
- Examples: Aave, Compound, MakerDAO

## 3. Stablecoins

- Price-stable cryptocurrencies
- Examples: USDC (fiat-backed), DAI (crypto-backed)

## 4. Derivatives

- Futures, options, synthetic assets
- Examples: dYdX, Synthetix, GMX

## 5. Yield Aggregators

- Automated yield optimization
- Examples: Yearn Finance, Beefy

# Composability: Money Legos

**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
- ⑤ Stake Curve LP tokens in Convex for boosted rewards

## Benefits:

- Capital efficiency (same asset used multiple times)
- Innovation (new strategies emerge from combinations)
- User choice (pick best yields across protocols)

## Risks:

- Complexity increases attack surface
- One protocol failure can cascade

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

## Common Vulnerabilities:

- Reentrancy attacks (famous: DAO hack 2016)
- Integer overflow/underflow
- Oracle manipulation
- Front-running and MEV exploitation
- Access control failures

## Mitigation:

- Professional audits (Trail of Bits, OpenZeppelin, etc.)
- Bug bounties (incentivize white-hat hackers)
- Formal verification (mathematical proofs of correctness)
- Time-locks and multi-sig governance

**Reality:** Billions lost to hacks/exploits, but security improving over time.

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

**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 data providers aggregated (Chainlink)
- **On-chain:** Data derived from blockchain state (Uniswap TWAP)

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

**Example Attack:** Manipulate price oracle, borrow max, liquidate yourself profitably.

# Permissionless Access

## What it means:

- No identity verification required
- No geographic restrictions
- No credit checks or approval process
- Only need: internet connection + crypto wallet

## Benefits:

- Financial inclusion (unbanked populations)
- Censorship resistance
- Privacy (pseudonymous transactions)
- Fast onboarding

## Drawbacks:

- Money laundering concerns
- No consumer protections
- No recourse for errors/scams
- Regulatory uncertainty

## Traditional Finance:

- Bank holds your money
- You trust bank to not freeze accounts
- Bank can restrict access

## DeFi:

- You hold private keys
- Smart contract holds funds during interaction
- No third party can freeze or seize

## Implications:

- **Positive:** True ownership, no counterparty risk
- **Negative:** No recovery if you lose keys
- **Responsibility:** User must secure own assets

**Mantra:** Not your keys, not your coins.

# Transparency and Auditability

## All DeFi transactions are public:

- Every trade, deposit, borrow visible on-chain
- Wallet balances and positions are transparent
- Smart contract code is open-source (usually)

## Benefits:

- Anyone can audit protocol reserves
- Real-time risk monitoring
- Trust through verification, not authority

## Trade-offs:

- Privacy concerns (address linkage to identity)
- Front-running opportunities (MEV)
- Competitive intelligence (whales tracked)

**Tools:** Etherscan, Dune Analytics, DeBank for on-chain analysis.

## 1. High-Yield Savings

- Earn 3-10% APY on stablecoins (vs. ~1% in banks)

## 2. Borrowing without Credit Checks

- Collateralized loans (over-collateralized)

## 3. Cross-Border Payments

- Fast, cheap transfers without intermediaries

## 4. Trading 24/7

- DEXs never close, no geographic restrictions

## 5. Yield Farming

- Provide liquidity, earn fees + token rewards

## 6. Synthetic Assets

- Gain exposure to stocks, commodities on-chain

## 1. Scalability

- Ethereum congestion leads to high gas fees
- Layer 2s and alt-chains offer solutions

## 2. User Experience

- Complex interfaces, steep learning curve
- Risk of user error (wrong address, lost keys)

## 3. Regulatory Uncertainty

- Unclear legal status in many jurisdictions
- Potential for restrictive regulations

## 4. Security Risks

- Smart contract bugs, hacks, exploits
- No insurance (generally)

## 5. Centralization Concerns

- Some protocols have admin keys
- Governance token concentration

**Centralized Crypto Platforms:** Coinbase, Binance, BlockFi, Celsius

## CeFi Advantages

- User-friendly interfaces
- Customer support
- Insurance (sometimes)
- Fiat on/off ramps
- Higher yields (historically)

## CeFi Risks

- Custodial (platform holds assets)
- Counterparty risk (FTX, Celsius collapses)
- KYC requirements
- Geographic restrictions
- Can freeze accounts

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

# Major DeFi Protocols Overview

Protocol	Category	TVL (approx.)
Lido	Liquid Staking	\$20B
MakerDAO	Stablecoin & Lending	\$5B
Aave	Lending	\$4B
Uniswap	DEX	\$3.5B
Curve	Stablecoin DEX	\$2B
Compound	Lending	\$1.5B
Rocket Pool	Liquid Staking	\$1.2B
Convex	Yield Aggregator	\$1B

Note: TVL values fluctuate with market conditions (Dec 2024 estimates).

## Why Ethereum Leads:

- First-mover advantage (smart contracts since 2015)
- Largest developer ecosystem
- Most battle-tested protocols
- Highest liquidity and composability
- Strong network effects

## Challenges:

- High gas fees during congestion
- Slower finality than newer chains

## Competitors:

- **Binance Smart Chain:** Cheaper fees, more centralized
- **Solana:** Fast, low-cost, but less battle-tested
- **Avalanche, Polygon:** Ethereum-compatible, lower fees

## 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
- Programmable money and automated compliance

## Key Takeaways:

- DeFi recreates financial services on blockchain: permissionless, transparent, non-custodial
- TVL measures capital deployed ( \$50B currently)
- Composability enables innovation but increases complexity
- Smart contract risk and oracle manipulation are key concerns
- DeFi outperformed CeFi during 2022 crisis (decentralization mattered)
- Ethereum dominates but faces competition from faster, cheaper chains

**Next Lecture:** AMM Mechanics - How automated market makers work (Uniswap model).

## 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?