

L33: Introduction to DeFi

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

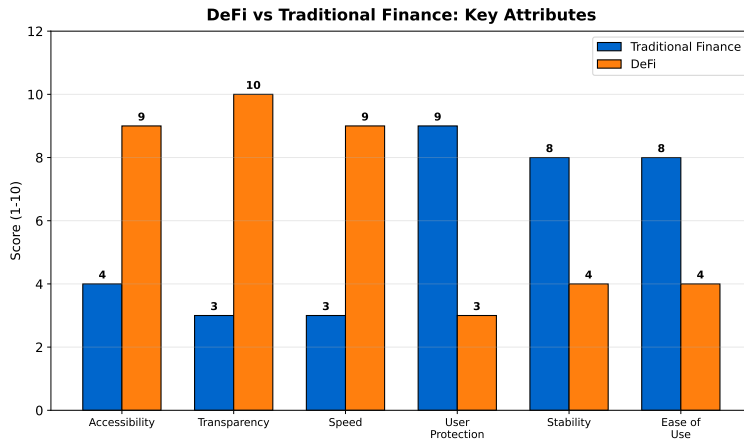
- Define Decentralized Finance (DeFi) and its core principles
- Understand Total Value Locked (TVL) as a key metric
- Explore the DeFi technology stack
- Analyze composability and its implications
- Compare DeFi to Traditional Finance (TradFi)

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.



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

Traditional Finance (TradFi)

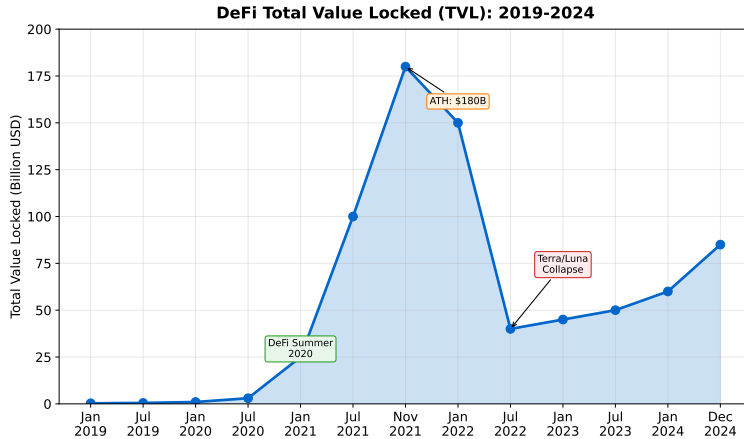
- Centralized intermediaries (banks)
- KYC/AML requirements
- Business hours, slow settlements
- Geographic restrictions
- High barriers to entry

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.

The Rise of DeFi: TVL History



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

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 (Late 2024):

- Total DeFi TVL: \$85 billion (recovered from 2022 lows)
- Ethereum: 55% of TVL
- Layer 2s (Arbitrum, Base): 12% combined

TVL Calculation Example

Hypothetical Lending Protocol:

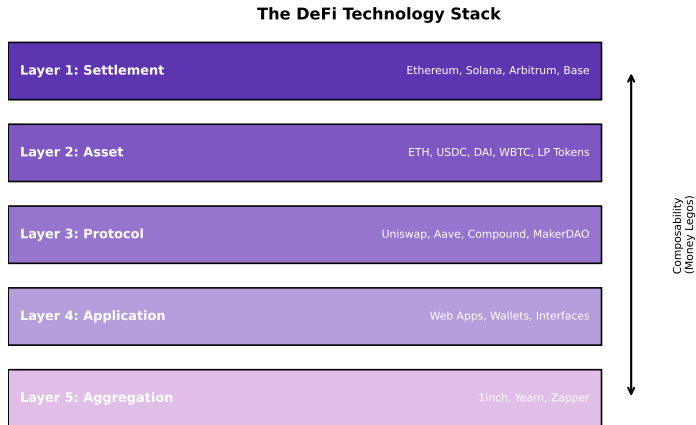
Deposits:

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

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.



Composability allows protocols to build on each other like “money legos”

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)

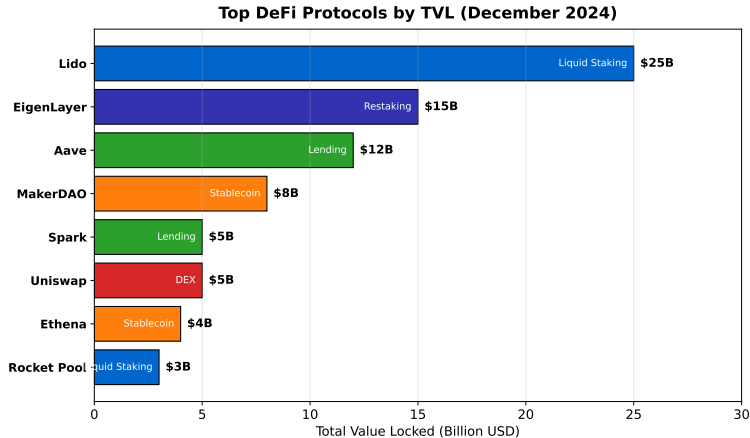
4. Derivatives

- Futures, options, synthetic assets (dYdX, GMX)

5. Yield Aggregators

- Automated yield optimization (Yearn Finance)

Top DeFi Protocols by TVL



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

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

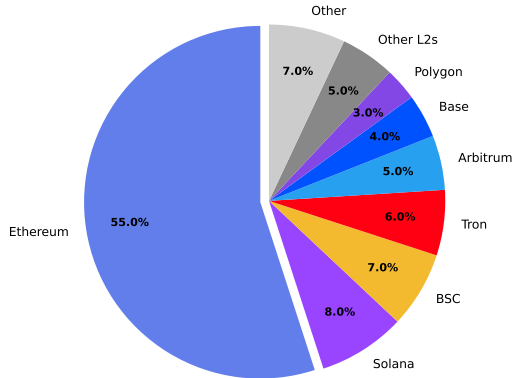
Example Workflow:

- 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

Benefits: Capital efficiency, innovation from combinations

Risks: Complexity increases attack surface, protocol failure can cascade

DeFi TVL Distribution by Blockchain (Dec 2024)



Ethereum maintains dominance; Layer 2s growing share rapidly

Ethereum dominates; L2s growing rapidly

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

Common Vulnerabilities:

- Reentrancy attacks (famous: DAO hack 2016)
- Oracle 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

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).

Permissionless Access:

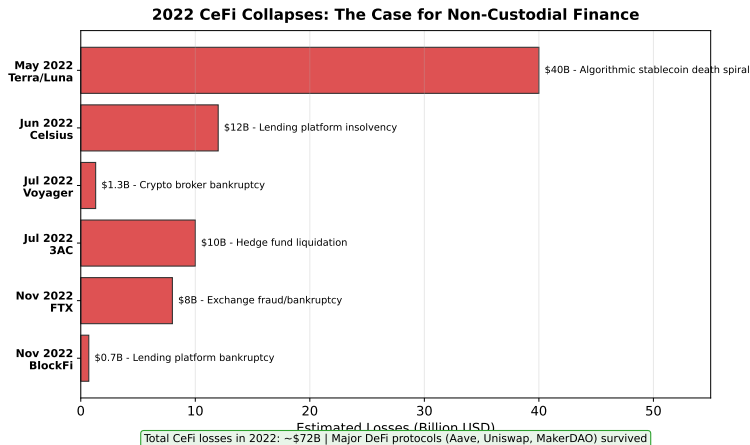
- No identity verification, no geographic restrictions
- Only need: internet connection + crypto wallet
- Benefits: Financial inclusion, censorship resistance

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.

2022 CeFi Collapses: The Case for DeFi



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

Centralized Crypto Platforms: Coinbase, Binance, BlockFi, Celsius

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.

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:

- \$15B+ TVL in EigenLayer by late 2024
- Liquid Restaking Tokens (LRTs): eETH, rsETH, ezETH
- Criticism: Added systemic risk, complexity

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 Takeaways:

- DeFi recreates financial services on blockchain: permissionless, transparent, non-custodial
- TVL measures capital deployed (\$85B in late 2024)
- Composability enables innovation but increases complexity
- Smart contract risk and oracle manipulation are key concerns
- Restaking (EigenLayer) emerged as major 2024 innovation
- Ethereum dominates but L2s capturing increasing share

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

- 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?