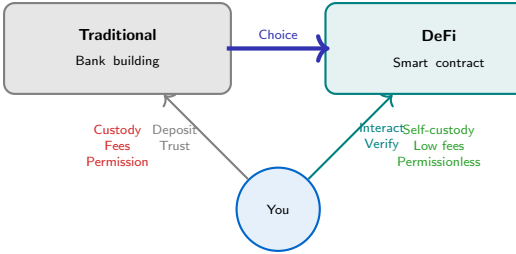
What if you could get a loan, earn interest, and trade assets – all without a bank?

Traditional finance requires intermediaries:

- Banks hold your deposits and lend them out
- Exchanges custody your assets and match trades
- Payment processors facilitate transactions
- Each intermediary takes a fee and controls access

Decentralized finance is different:

- Smart contracts replace banks and exchanges
- You control your assets in your own wallet
- Trading, lending, and payments happen peer-to-peer
- No permission needed, no identity checks



The promise: A financial system with no gatekeepers.
The risk: Every traditional risk reappears without safety nets.

Key Insight

DeFi recreates every financial service without intermediaries. But removing banks also removes deposit insurance, customer support, and legal recourse.

You can build an entire financial system on smart contracts. But should you?

The Bank With No Manager

Person 1: "I think there is a bug in the smart contract."
Person 2: "Great! Just call customer service and ask them to fix it."
Person 1: "There is no customer service."
Person 2: "Then call the manager."
Person 1: "There is no manager. Just code."

DeFi replaces bankers with smart contracts – but who do you call when the code has a bug?

Why This Matters

Decentralization means no human can fix mistakes. Code is the only authority.

Have you ever earned interest on savings and wondered where that yield actually comes from?

What are the main building blocks of the DeFi ecosystem?

Core DeFi primitives:

- **Decentralized exchanges:** Trade tokens without intermediaries
- **Lending protocols:** Borrow and lend crypto assets
- **Stablecoins:** Price stability in a volatile ecosystem
- **Derivatives:** Leverage, hedging, and speculation
- **Yield aggregators:** Automate profit-seeking strategies
- **Insurance protocols:** Hedge against smart contract failures

Primitive	Function
DEX	Swap tokens
Lending	Earn yield, borrow
Stablecoin	Unit of account
Derivatives	Leverage, hedge
Yield farm	Maximize returns
Insurance	Risk mitigation

Key insight: Composability is DeFi's superpower. Each protocol builds on others, creating exponential complexity and risk.

What makes DeFi composable:

- Every protocol is open and permissionless
- Protocols can call other protocols in a single transaction
- This creates "money legos" that stack infinitely
- Example: Deposit in lending protocol, use receipt token as collateral elsewhere

Key Insight

DeFi protocols are like Lego blocks: they snap together in infinite combinations. This creates innovation and fragility in equal measure.

Composability allows rapid innovation but also creates cascading failure risks when one protocol breaks.

How does an automated market maker execute a trade without an order book?

Traditional exchanges use order books:

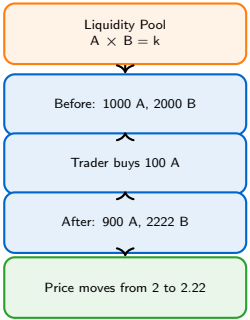
- Buyers place bids, sellers place asks
- Exchange matches orders at overlapping prices
- Requires market makers to provide liquidity

AMMs use a constant product formula:

- Pool holds reserves of two tokens
- Invariant: reserve A times reserve B equals constant
- Price emerges from the ratio of reserves
- Trades shift reserves, changing the ratio

Example: Pool with 1000 units A and 2000 units B.

- Constant = 2 million
- Current price: 2 B per A
- Trader buys 100 A: pool now has 900 A
- New B reserve: 2 million divided by 900 = 2222 B
- Trader pays: 222 B for 100 A (effective price 2.22 B per A)



Key property: Larger trades move the price more. The pool never runs out – it just gets expensive.

Key Insight

AMMs replace order books with algorithmic pricing. The constant product formula ensures liquidity at all price levels but introduces slippage.

How do centralized exchange and DeFi protocol architectures differ?

Centralized exchange architecture:

- Users deposit funds into exchange wallets
- Exchange stores private keys in hot and cold wallets
- Order matching engine runs on private servers
- Trades settle in the exchange database
- Withdrawals require exchange approval

DEX architecture:

- Users keep funds in their own wallets
- Smart contract holds pooled liquidity
- Trades execute atomically on-chain
- Settlement is instant and verifiable
- No withdrawal approval needed

Trade-offs:

- CEX: Fast, cheap, but custody risk
- DEX: Self-custody, but high gas costs and front-running risk

Property	CEX	DEX
Custody	Exchange	User
Matching	Order book	AMM
Settlement	Database	Blockchain
Speed	Instant	Seconds
Cost	Low	High
Risk	Counterparty	Smart contract

Key insight: CEXs optimize for speed and cost. DEXs optimize for trustlessness and transparency.

Key Insight

Centralized exchanges are fast and cheap but require trust. DEXs eliminate trust but introduce new costs and risks.

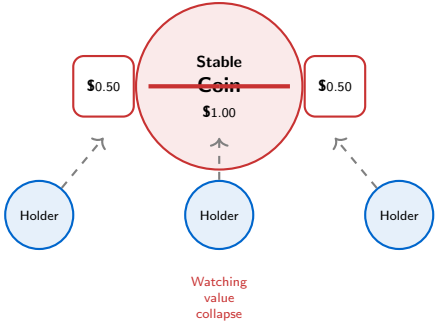
What happens when a stablecoin loses its peg?

Stablecoins promise price stability:

- Designed to maintain 1-to-1 value with a reference asset
- Critical for DeFi lending, trading, and payments
- Without a stable unit of account, DeFi cannot function

When the peg breaks:

- Holders panic and sell
- Selling pressure pushes price further from peg
- Redemption mechanisms fail under stress
- Spiral: more selling leads to more panic
- Permanent collapse: price goes to near-zero



Death spiral: Selling triggers more selling. Algorithmic stabilization fails. Holders lose everything.

Key Insight

Stablecoin de-pegs create self-reinforcing spirals. Algorithmic stabilization without reserves is fragile under stress.

A stablecoin that loses its peg can collapse to near-zero in days, destroying billions in value.

Where has DeFi total value locked grown and contracted, and what drove the swings?

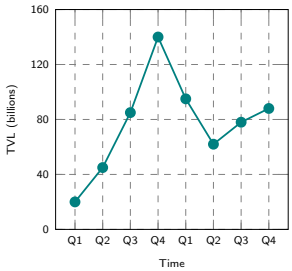
Total Value Locked (TVL) measures DeFi size:

- TVL = aggregate value of assets in DeFi protocols
- Primary metric for DeFi adoption and growth
- Reflects both capital inflows and asset price changes

Key drivers of TVL swings:

- **Bull markets:** Rising asset prices inflate TVL
- **Yield farming:** High APRs attract speculative capital
- **Bear markets:** Falling prices and withdrawals shrink TVL
- **Exploits:** Major hacks trigger capital flight
- **Regulation:** Regulatory uncertainty reduces deposits

Caveat: TVL can be inflated by recursive borrowing (same capital counted multiple times).



Pattern: TVL surges during bull markets and collapses during crashes. Yield incentives accelerate both booms and busts.

Key Insight

DeFi TVL is volatile and correlated with crypto asset prices. High yields attract speculative capital that flees during downturns.

TVL growth reflects both genuine adoption and speculative bubbles. Distinguishing the two is difficult.

Who captures value in DeFi and who bears the risk?

Value capture:

- **Liquidity providers:** Earn trading fees but face impermanent loss
- **Lenders:** Earn interest but risk protocol insolvency
- **Governance token holders:** Capture protocol revenue and control parameters
- **Developers:** Pre-mine tokens or earn protocol fees
- **Arbitrageurs:** Extract profit from price inefficiencies

Risk bearing:

- **Retail users:** Bear smart contract risk, impermanent loss, and liquidation risk
- **Borrowers:** Risk liquidation cascades during market crashes
- **Stablecoin holders:** Risk de-peg events
- **Governance participants:** Risk governance attacks and parameter manipulation

Actor	Value / Risk
LP	Fees / IL
Lender	Yield / Insolvency
Borrower	Leverage / Liquidation
Gov holder	Control / Governance attack
Retail	Access / All risks
Developer	Tokens / Reputation

Tension: Insiders (developers, large token holders) capture asymmetric value. Retail users bear asymmetric risk.

Key Insight

DeFi distributes value creation but also distributes risk. Retail users often bear the highest risk with the lowest information advantage.

DeFi democratizes access to financial services but does not democratize risk or information symmetry.

Four questions to evaluate any DeFi protocol before depositing funds

The DeFi Due Diligence Test:

Question 1: Where does the yield come from?

- Sustainable: trading fees, borrowing interest
- Unsustainable: token emissions, Ponzi mechanics

Question 2: Is the code audited and the audit public?

- Look for audits from reputable firms
- Check if critical issues were resolved

Question 3: What happens if the collateral price drops suddenly?

- Understand liquidation thresholds
- Assess cascade risk in market crashes

Question 4: Can governance change the rules after you deposit?

- Check if parameters are timelocked
- Assess concentration of governance tokens

Red Flag	Risk
Yield too high	Ponzi
No audit	Code bug
Single oracle	Manipulation
Team controls gov	Rug pull
Anonymous devs	Exit scam
New protocol	Untested

Green flags:

- Multiple audits
- Timelock on governance
- Battle-tested code
- Transparent yield source
- Decentralized oracle

Most DeFi losses come from predictable risks. The due diligence test filters out the most dangerous protocols.

Your Challenge

Evaluate Three Stablecoin Peg Mechanisms

Scenario: You have three stablecoin designs:

1. **Fiat reserve:** Each coin backed 1-to-1 by dollars in a bank account
2. **Crypto over-collateral:** Each coin backed by crypto worth 150 percent of its value
3. **Algorithmic:** Supply adjusts automatically based on demand, no reserves

Your task: Evaluate each design using the four questions from slide 9:

- Where does the yield come from?
- Is the mechanism transparent and auditable?
- What happens if the collateral price drops suddenly?
- Can governance change the rules after you deposit?

Hint: Consider trust assumptions, capital efficiency, and de-peg risks for each design.

Reflection

No stablecoin design is perfect. Each trades off decentralization, capital efficiency, and peg stability.

The best way to understand DeFi risks is to apply the due diligence test to real protocols.