

L38: Stablecoin Mechanisms

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

Why Put a Dollar On Blockchain?

[COMIC: Dollar but on blockchain]

Placeholder for comic showing confused person asking "Why do we need a dollar on blockchain?" while another shows instant global transfers, 24/7 availability, and programmable money

Stablecoins solve the "I can't buy coffee with BTC" problem

The Setup

- Crypto is too volatile for payments
- BTC: \$69k to \$15k in one year
- Can't price coffee in something that moves 10%/day

The Punchline

- Stablecoins: crypto stability
- Dollar value, blockchain speed
- Best of both worlds

- Classify different stablecoin mechanism types (fiat-backed, crypto-backed, algorithmic)
- Analyze fiat-backed stablecoins (USDC, USDT)
- Explore crypto-backed stablecoins (DAI, MakerDAO)
- Evaluate algorithmic stablecoins and their failure modes
- Compare stablecoin trade-offs (decentralization, stability, efficiency)

Building on L37: Lending Protocols

The Problem: How do we create stable value on-chain?

The Challenge

Cryptocurrencies are highly volatile (BTC: \$69k to \$15k in 2022). DeFi needs price-stable assets for payments, lending, and savings, but blockchain systems lack native connection to fiat currencies.

Why It Matters

- Volatility makes crypto unusable for everyday payments and savings
- Historical example: Tether (2014), DAI (2017), algorithmic failures (Terra/Luna 2022)

What We Need

- System design principles
- Price stability mechanism resistant to market shocks and attacks

The Cryptoeconomics Question

Creating systems with desired properties

Today's lesson: How Stablecoin Mechanisms addresses this challenge

What Are Stablecoins and Why Do We Need Them?

Definition: A cryptocurrency designed to maintain a stable value relative to \$1 USD.

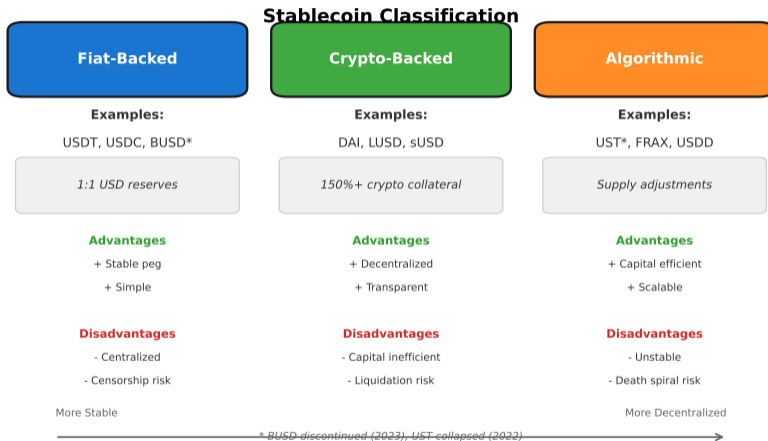
Why Stablecoins?

- Price stability (avoid crypto volatility)
- Medium of exchange, store of value
- DeFi building block (lending, trading, yield)
- Fast, cheap cross-border payments

Total Market Cap: \$310B (Dec 2025), up from \$140B in Dec 2024

Stablecoins maintain \$1 value on-chain, enabling saving and trading without crypto volatility.

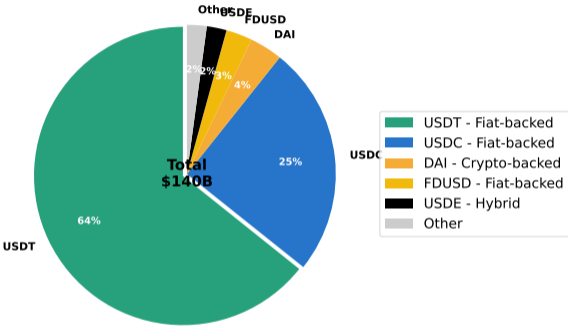
What Types of Stablecoins Exist?



Three main types: fiat-backed (stable, centralized), crypto-backed (decentralized, inefficient), algorithmic (scalable, risky)

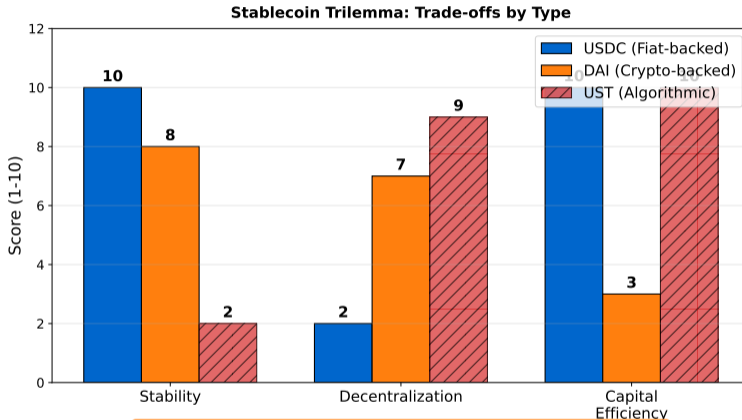
Which Stablecoins Dominate the Market?

Stablecoin Market Share (Dec 2024)



USDT dominates (59%, \$142B); USDC 24% (\$52B); fiat-backed = 90%+ of market

What Trade-offs Do Stablecoins Face?



No stablecoin achieves all three perfectly; each type makes trade-offs

Each type sacrifices one property; no perfect stablecoin exists

How Do Fiat-Backed Stablecoins Work?

Mechanism: 1 stablecoin backed by \$1 in bank account.

How It Works:

- 1 User deposits \$100 fiat to issuer
- 2 Issuer mints 100 tokens, holds reserves
- 3 User can redeem 100 tokens for \$100 anytime

Examples:

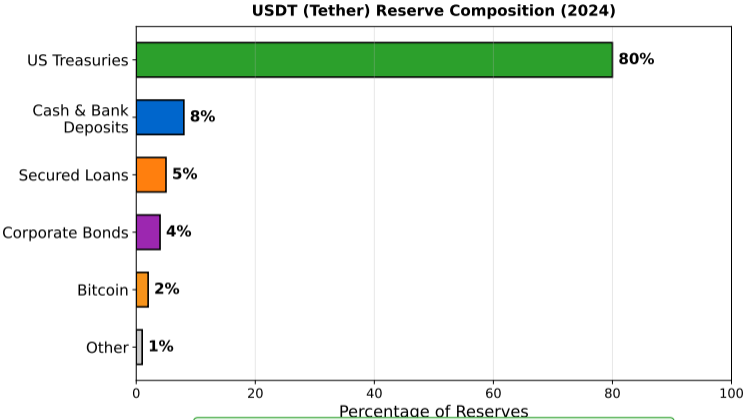
- **USDC:** Fully backed by cash + T-bills, monthly attestations
- **USDT:** Mixed reserves, largest but less transparent

Advantages: Strong peg, capital efficient, easy to understand

Disadvantages: Centralized, censorship risk, counterparty risk

Fiat-backed = 1 token backed by \$1 in bank. Trade-off: trusting a centralized issuer.

What Backs Tether (USDT)?



Tether has shifted heavily to US Treasuries after 2022 criticism

Tether has shifted to 80%+ US Treasuries after 2022 criticism

What Are the Risks of Fiat-Backed Stablecoins?

Centralization: Issuer can freeze addresses (OFAC compliance)

Counterparty Risk: Trust issuer to maintain reserves

Black Swan Example: SVB Collapse (March 2023)

- Circle had \$3.3B deposited at Silicon Valley Bank
- Bank failure caused USDC to depeg to \$0.87
- Recovered after Fed guarantee on deposits

Lesson: Even “safe” fiat-backed stablecoins have counterparty risk.

Key point: Centralization

How Do Crypto-Backed Stablecoins Maintain Their Peg?

Mechanism: Backed by crypto collateral (overcollateralized – deposit more value than borrowed, e.g., \$150 for \$100).

How It Works:

- 1 User deposits \$150 ETH as collateral
- 2 Protocol mints \$100 DAI (150% collateralization)
- 3 If ETH drops, position liquidated to protect peg

Example: DAI (MakerDAO)

- Largest decentralized stablecoin (\$5B)
- Backed by ETH, WBTC, USDC, RWAs
- Governed by MKR token holders

Advantages: Decentralized, transparent, censorship-resistant

Key point: Mechanism

Recall Our Problem

How do we create stable value on-chain?

What We've Learned So Far

- Three stablecoin types: fiat-backed (USDC), crypto-backed (DAI), algorithmic (failed UST)
- The stablecoin trilemma: no design achieves stability + decentralization + capital efficiency
- Different mechanisms = different trade-offs. Fiat-backed is stable but centralized.

Still to Address

- Algorithmic stablecoins: why most have failed (death spiral risk)
- Is true decentralization compatible with price stability?

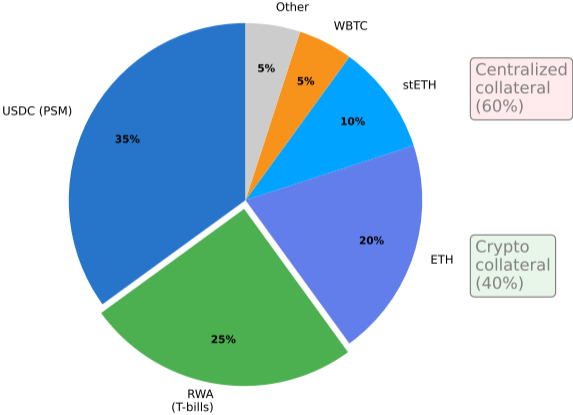
Think About

- 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 "How do we create stable value on-chain?"?

What Assets Back DAI?

DAI Collateral Composition (Dec 2024)



DAI's collateral mix reveals the trilemma: adding USDC improves stability but reduces decentralization.

How Does DAI Maintain Its Peg?

1. Arbitrage

- DAI \downarrow \$1: Mint DAI, sell for profit
- DAI \uparrow \$1: Buy DAI, repay vault for profit

2. Stability Fee (Interest Rate)

- High fee: Reduces supply (repayments)
- Low fee: Increases supply (more minting)

3. Peg Stability Module (PSM)

- Swap USDC for DAI 1:1 (backstop for large depegs)

Trade-off: PSM improves stability but increases centralization.

Key point: 1. Arbitrage

How Do Different Stability Mechanisms Compare?

How Stablecoins Maintain Their Peg



Capital Efficiency = Value of stablecoin / Value of backing required

Each mechanism trades off between stability, decentralization, and capital efficiency

How Do Algorithmic Stablecoins Work?

Mechanism: Maintain peg through supply adjustments (no/minimal collateral).

How It Works (Theoretically):

- Price \downarrow \$1: Increase supply (mint, sell)
- Price \uparrow \$1: Decrease supply (buy, burn)

Examples:

- **Terra UST:** Failed spectacularly (May 2022)
- **FRAX:** Hybrid (partially collateralized)

Theoretical Advantage: Capital efficient, decentralized, scalable

Reality: Most pure algorithmic stablecoins have failed (death spirals).

Key point: Mechanism

Mint-and-Burn Stabilization (Terra-style)

```
function stabilize(stablecoin_price):  
  if stablecoin_price > $1.00:  
    // Above peg: increase supply  
    mint_stablecoin(excess_demand)  
    burn_governance_token(equivalent_value)  
  if stablecoin_price < $1.00:  
    // Below peg: decrease supply  
    burn_stablecoin(excess_supply)  
    mint_governance_token(equivalent_value)  
    // DANGER: governance token dilution  
    // If confidence drops, death spiral begins
```

Key Insight: The mint-and-burn loop works *only while confidence holds*. When the governance token loses value, minting more cannot restore the peg – each mint dilutes further, accelerating collapse.

Terra/Luna's \$40B collapse in May 2022 demonstrated exactly this death spiral in practice

Why Do Algorithmic Stablecoins Keep Failing?

Death Spiral Scenario:

(Death spiral = self-reinforcing collapse where falling prices trigger more selling)

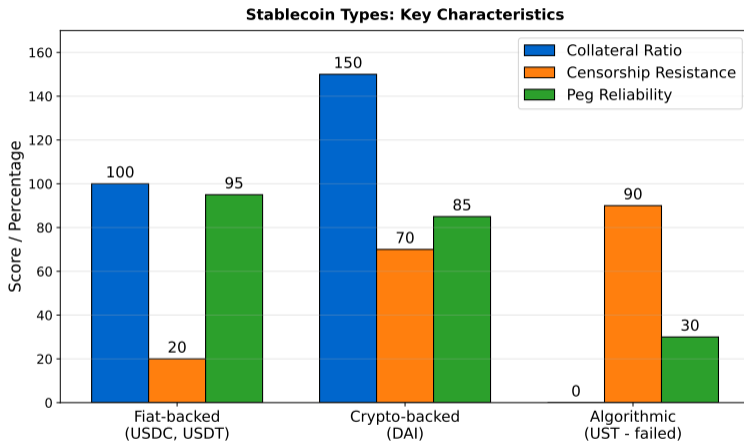
- 1 Stablecoin depegs below \$1
- 2 Protocol mints sister token to incentivize buying
- 3 Sister token crashes from dilution
- 4 Loss of confidence accelerates selling
- 5 Spiral to zero, total collapse

Root Cause: No intrinsic backing or demand floor.

Lesson: Algorithmic stability relies entirely on confidence. Once lost, irrecoverable.

Death spirals explain algo failures: no backing means confidence loss triggers collapse.

How Do the Three Stablecoin Types Compare?



Fiat-backed wins on reliability; crypto-backed best censorship resistance

How Do Specific Stablecoins Compare?

Type	Example	Backing	Decent.	Efficient
Fiat-backed	USDC	USD (1:1)	No	Yes
Fiat-backed	USDT	Mixed	No	Yes
Crypto-backed	DAI	ETH+USDC	Partial	No
Algorithmic	UST	None	Yes	Yes
Hybrid	FRAX	USDC+FXS	Partial	Partial

Key Insight: No stablecoin achieves all three properties (trilemma).

Compare the approaches shown above

How Is Stablecoin Regulation Evolving?

US:

- SEC scrutiny (some stablecoins may be securities)
- Bank-like regulation proposed (reserve requirements)

EU (MiCA):

- Stablecoin issuers need authorization
- Reserve and redemption requirements
- Significant stablecoins face additional rules

Impact (Dec 2024):

- BUSD shut down (Feb 2023, regulatory pressure)
- MiCA full effect: USDT delisted from EU exchanges (Coinbase, Kraken EU)
- Circle USDC MiCA-compliant (EMI license July 2024)
- Increasing compliance costs favor large, regulated players

Key point: US

The Original Problem

How do we create stable value on-chain?

How Stablecoin Mechanisms Solves It

- Fiat-backed (USDC, USDT): Simple 1:1 reserves – strong peg but centralized
- Crypto-collateralized (DAI): Overcollateralization + arbitrage + PSM – decentralized but capital inefficient
- Algorithmic: Supply adjustments – capital efficient but unstable (most failed)

Remaining Limitations

- Centralization risk: Fiat-backed requires trust in issuer; DAI increasingly uses USDC
- Depeg events: SVB collapse (USDC), death spirals (Terra/Luna)
- Regulatory pressure: MiCA compliance, USDT delistings

Open Questions

- Is fully decentralized stable value achievable without centralized collateral?
- Risk: Regulatory crackdown on unregulated stablecoins, confidence crises

Stablecoin Mechanisms partially solves “create stable value on-chain” but introduces new trade-offs

Incentive Structure

- Creating systems with desired properties
- Mechanism design for target behaviors
- Complexity vs simplicity

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?

Complexity vs simplicity

Design Principle

Attack Cost $>$ Potential Gain

Design Space

Alternatives Considered

- 1 Architecture patterns, upgrade mechanisms
- 2 Alternative design patterns

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.

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **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?

[COMIC: Reserve transparency issues]

Placeholder for comic showing user asking “Is my stablecoin really backed 1:1?” while issuer nervously hides a pie chart showing commercial paper, loans, and “other”

“Fully backed” means different things to different issuers

The Trust Problem

- Fiat-backed = trust the issuer
- “Trust us, the money is there”
- Attestation is not an audit

Historical Examples

- USDT reserve composition debates
- USDC SVB depeg (\$0.87)
- Counterparty risk is real

Key Takeaways:

- Stablecoins maintain \$1 peg; \$310B market cap (Dec 2025)
- Fiat-backed (USDC, USDT): Stable but centralized
- Crypto-backed (DAI): Decentralized but capital inefficient
- Algorithmic: Capital efficient but unstable (most failed)
- Stablecoin trilemma: Can't have stability + decentralization + efficiency
- DAI's centralization debate: USDC backing vs. pure crypto
- Regulation increasing (MiCA, US proposals)

Next Lecture: Terra/Luna Case Study.

Next Lesson: L39 – Terra/Luna Case Study

Key point: Key Takeaways

Reflection

- ① Why do algorithmic stablecoins tend to fail during market stress?
- ② How does the PSM help DAI maintain its peg? What's the trade-off?
- ③ Would you trust a stablecoin backed by 80% US Treasuries?
- ④ How might stablecoin regulation impact DeFi?
- ⑤ Is perfect decentralization compatible with price stability?

Key point: Questions for Reflection

Quiz Questions (1–5)

Q1. What is the primary purpose of a stablecoin?

- A) To maximize returns
- B) To maintain a stable value relative to \$1 USD
- C) To replace Bitcoin
- D) To eliminate transaction fees

Answer: B – Stablecoins are designed to maintain price stability, avoiding crypto volatility.

Q2. What was the approximate total stablecoin market cap in December 2025?

- A) \$50B
- B) \$150B
- C) \$310B
- D) \$500B

Answer: C – The market cap reached \$310B (USDT \$187B, USDC \$77B), up from \$140B in Dec 2024.

Q3. Which stablecoin has the largest market share?

- A) USDC
- B) DAI
- C) USDT
- D) BUSD

Answer: C – USDT (Tether) dominates with 59% market share (\$142B).

Q4. What does the stablecoin trilemma state?

- A) All stablecoins will fail
- B) Only 3 stablecoins can exist
- C) No stablecoin can achieve stability, decentralization, and efficiency
- D) Stablecoins need 3 types of collateral

Answer: C – Each stablecoin type sacrifices one of the three properties.

Q5. How does a fiat-backed stablecoin maintain its peg?

- A) Algorithmic supply adjustments
- B) 1:1 backing with USD reserves
- C) Overcollateralized crypto
- D) Community voting

Answer: B – Users deposit \$1 fiat, issuer mints 1 token backed by reserves.

Quiz Questions (6–10)

Q6. What is the main disadvantage of fiat-backed stablecoins?

- A) High volatility
- B) Centralization and counterparty risk
- C) Low liquidity
- D) No use case

Answer: B – They are centralized and require trust in the issuer to maintain reserves.

Q7. What caused USDC to depeg to \$0.87 in March 2023?

- A) Hacker attack
- B) Algorithmic failure
- C) Silicon Valley Bank collapse
- D) Regulatory ban

Answer: C – Circle had \$3.3B at SVB; recovered after Fed guarantee.

Q8. How does a crypto-backed stablecoin like DAI work?

- A) 1:1 fiat backing
- B) Overcollateralized with crypto assets
- C) No collateral
- D) Government bonds

Answer: B – Users deposit \$150 ETH to mint \$100 DAI (150% collateralization).

Q9. What is DAI's approximate market cap?

- A) \$1B
- B) \$5B
- C) \$50B
- D) \$100B

Answer: B – DAI is the largest decentralized stablecoin at \$5B.

Q10. What collateral types back DAI?

- A) Only ETH
- B) ETH, WBTC, USDC, RWAs
- C) Only USDC
- D) Gold and silver

Answer: B – DAI uses diversified collateral including crypto and real-world assets.

Quiz Questions (11–15)

Q11. What is the Peg Stability Module (PSM)?

- A) A voting mechanism
- B) 1:1 swap between USDC and DAI
- C) An insurance fund
- D) A liquidation bot

Answer: B – PSM allows swapping USDC for DAI 1:1, backstopping large depegs.

Q12. What is the trade-off of using the PSM in MakerDAO?

- A) Higher fees
- B) Lower liquidity
- C) Improved stability but increased centralization
- D) Faster transactions

Answer: C – PSM relies on USDC (centralized), reducing DAI's decentralization.

Q13. How do algorithmic stablecoins theoretically maintain their peg?

- A) Fiat reserves
- B) Supply adjustments (mint/burn)
- C) Overcollateralization
- D) Central bank intervention

Answer: B – They increase supply when price \downarrow \$1, decrease when price \uparrow \$1.

Q14. Which algorithmic stablecoin failed spectacularly in May 2022?

- A) USDC
- B) DAI
- C) Terra UST
- D) FRAX

Answer: C – Terra UST collapsed in a death spiral, losing its peg completely.

Q15. What is a “death spiral” in algorithmic stablecoins?

- A) Slow decline in price
- B) Depeg triggers sister token dilution, accelerating collapse
- C) Government shutdown
- D) Network congestion

Answer: B – Loss of confidence causes selling, sister token crashes, spiral to zero.

Quiz

Quiz Questions (16–20)

Q16. What is the root cause of algorithmic stablecoin failures?

- A) Poor marketing
- B) No intrinsic backing or demand floor
- C) High transaction fees
- D) Slow block times

Answer: B – They rely entirely on confidence; once lost, there's no recovery mechanism.

Q17. What percentage of Tether's (USDT) reserves are in US Treasuries?

- A) 20%
- B) 50%
- C) 80%+
- D) 0%

Answer: C – Tether shifted to 80%+ US Treasuries after 2022 criticism.

Q18. Which stablecoin was shut down in February 2023 due to regulatory pressure?

- A) USDT
- B) USDC
- C) DAI
- D) BUSD

Answer: D – BUSD was shut down following regulatory action.

Q19. Under EU MiCA regulation (Dec 2024), what happened to USDT?

- A) Approved for all EU exchanges
- B) Delisted from major EU exchanges
- C) Given special exemption
- D) Banned globally

Answer: B – USDT was delisted from EU exchanges like Coinbase and Kraken EU.

Q20. Which stablecoin became MiCA-compliant with an EMI license in July 2024?

- A) USDT
- B) DAI
- C) USDC
- D) FRAX

Answer: C – Circle's USDC obtained EMI license and became MiCA-compliant.