#9 Stablecoins: Fiat-Backed vs Crypto-Backed

Lecture Notes for CS190N: Blockchain Technologies and Security October 29, 2025

Stablecoins underpin DeFi by supplying a stable unit of account and medium of exchange that enables everyday transactions, lending, and trading. Their designs fall into three families with distinct trade-offs: fiat-backed (e.g., USDC) offer high price stability and operational simplicity but rely on centralized issuers and banking rails; crypto-backed (e.g., DAI) provide on-chain transparency and censorship resistance yet are capital-inefficient and sensitive to market and technical stress; algorithmic approaches promise fully on-chain stability but have proved fragile without strong collateral or circuit breakers. In practice, DeFi uses a mix and allows seamless conversion among major stablecoins, so builders choose according to whether they prefer regulatory and banking exposure or crypto-volatility and protocol risk. The ecosystem is converging toward hybrids: fiat-backed issuers improve reserve transparency and legal safeguards, while crypto-backed protocols incorporate real-world assets (such as short-term Treasuries) to strengthen the peg. No stablecoin is risk-free—the nature of the backing determines whether users bear banking, market/technical, or confidence risk. Overall, stablecoins deliver the "right kind of money" for programmable finance, but progress will continue to balance stability, decentralization, and security as designs evolve.

1 WHY DEFI NEEDS STABLECOINS

- Decentralized Finance (DeFi) is built on the promise of open, programmable money, but most crypto assets are notoriously volatile. Imagine trying to build a house with a measuring tape that stretches and shrinks unpredictably; that's what building financial applications on pure crypto (like ETH or BTC) is like. This is where **stablecoins** enter the scene as the steady **"unit of account"** and **medium of exchange** that DeFi desperately needs.
- **Stable value anchor:** Crypto assets (e.g. BTC, ETH) are highly volatile. Stablecoins provide a reliable "unit of account" so prices and loans aren't constantly changing.
- **Safe haven:** Traders and investors park funds in stablecoins to avoid market crashes, similar to moving into cash during turbulence.
- **Foundation of DeFi:** Most crypto trading volume is in stablecoins (around 2/3 of on-chain transactions, ~80% of exchange trading). They enable lending, borrowing, and exchange activities by acting as "crypto-dollars." Without them, decentralized markets would lack a stable base and would be hard to build on.

2 TWO MAIN MODELS: FIAT-BACKED VS CRYPTO-BACKED

- **Fiat-Backed Stablecoins:** Each token is backed by real-world currency (usually USD) held in reserve by a central issuer. Think of it like a fully-funded bank: for every 1 USDC or USDT token, there is (in theory) $1 in a bank account or equivalent. Examples include USDC (Circle) and USDT (Tether). The issuer manages reserves and honors redemptions, while arbitrage keeps the market price near $1.
- **Crypto-Backed Stablecoins:** These use cryptocurrency as collateral and operate entirely on-chain via smart contracts. Users lock up volatile crypto (e.g. ETH) into a protocol (like a crypto mortgage) and mint stablecoins against it. For safety, they over-collateralize: e.g. $150 of ETH for $100 of stablecoin (DAI). If collateral value falls too much, the system automatically liquidates it to repay the loan. This model (MakerDAO's DAI) relies on decentralized code and market incentives to maintain the peg.

3 HOW FIAT-BACKED STABLECOINS WORK (USDC EXAMPLE)

- **Reserves and Issuance:** USDC tokens are issued by a central company (Circle). For each USDC minted, $1 worth of dollar assets (cash or short-term Treasuries) is held in reserve. Reserves are audited regularly to prove backing.
- **Peg Maintenance:**
  - If USDC trades below $1 (say $0.99), arbitrageurs buy the cheap USDC and redeem it 1:1 for real USD from Circle, profiting $0.01, this pushes the price back up.
  - If USDC ever trades above $1 (rare), authorized participants can deposit $1 and get 1 USDC to sell, increasing supply and pushing the price down.
- **Advantages:** Stable price (close to $1), simplicity, high liquidity, and wide acceptance. Regulated issuance and transparency (audits, legal structures) give users confidence. USDC has remained very stable even through crypto market crashes, acting as a dependable "digital dollar."
- **Vulnerabilities:** Centralization and counterparty risk. USDC holders must trust the issuing company, its banks, and auditors. Examples: in March 2023, fears about Circle's bank (SVB) led USDC to briefly drop to ~$0.88. Such events show fiat-backed coins can face "bank-run" panic if reserve confidence falters. Also, issuers can censor transactions or freeze coins under legal pressure (USDC's smart contract allows blacklisting), meaning regulatory events can directly impact these stablecoins.

4 HOW CRYPTO-BACKED STABLECOINS WORK (DAI EXAMPLE)

- **Vaults and Collateral:** To get DAI, a user locks crypto (e.g. ETH, or other approved tokens) into a MakerDAO Vault. This is like a crypto collateralized loan. If you lock $150 of ETH, you can mint up to $100 DAI. The extra collateral acts as a safety cushion.
- **Over-Collateralization:** The system requires more collateral than the value of DAI minted (often 150% or higher). This means even if crypto prices drop, there should still be enough value to back the DAI.
- **Liquidation Mechanism:** If the collateral's value falls and the collateralization ratio drops below a minimum threshold, the protocol automatically liquidates the collateral: it sells your ETH for DAI to cover the debt. This protects the system by ensuring no DAI is under-backed. Think of it like a bank foreclosing on a house if its value falls too much.
- **Peg Maintenance:** There is no centralized redemption for USD. Instead, DAI's price is maintained by market incentives and protocol tools:
  - If DAI > $1 (high demand), borrowers can mint (create) more DAI by depositing collateral, or use the **Peg Stability Module (PSM)** (swap USDC for DAI) to increase DAI supply, which brings the price down.
  - If DAI < $1, people can buy DAI cheaply and repay their loans (burning DAI), or use PSM to swap DAI for USDC, reducing DAI supply and raising its price.
- **Peg Stability Module (PSM):** MakerDAO governance can adjust fees or limits to help this balancing act. The PSM specifically lets anyone swap 1 USDC for 1 DAI and vice versa at a fixed rate, acting like a vending machine that stabilizes the price.
- **Advantages:** DAI is decentralized and transparent. All collateral and debt are on-chain (anyone can verify the reserves). There's no single issuer who can seize or freeze DAI, only the protocol's rules apply. This censorship-resistance and trust-minimized nature makes it attractive for users who want to avoid central control. DAI also composes with other DeFi "legos": you can, for example, use ETH to mint DAI, then lend out that DAI or trade it, all without leaving crypto.

- **Vulnerabilities:** Complexity and dependence on crypto markets. DAI requires many moving parts (smart contracts, oracles, auctions, governance). It's less capital-efficient since lots of crypto must be locked up. In extreme crashes, its mechanism can be stressed, e.g., in March 2020, a sudden ETH price crash led to some DAI vaults being underwater and required emergency measures (like issuing new MKR tokens to cover losses). Fast crashes risk that liquidations can't catch up, briefly straining the peg. Also, ironically, DAI today holds a significant amount of USDC (via the PSM) as part of its "backing," which introduces some centralization risk.

5 USDC VS DAI: A DIRECT COMPARISON

- **Issuance & Backing:**
  - **USDC:** Issued by Circle (centralized). Backed 1:1 by off-chain US dollars/treasuries. Users trust Circle's reserves.
  - **DAI:** Issued by MakerDAO (decentralized protocol). Backed by on-chain crypto collateral (ETH, etc.) and some USDC via the PSM. Users trust the protocol code and collateral, not a company.
- **Peg Mechanism:**
  - **USDC:** Peg held by 1:1 redemption, large holders can redeem any amount of USDC for $1 each from Circle, so market price stays at $1 via arbitrage.
  - **DAI:** Peg maintained by economic incentives. If DAI > $1, borrowers mint more DAI or use PSM (swap USDC->DAI) to increase supply. If DAI < $1, people repay DAI loans or swap DAI->USDC in PSM to shrink supply. There's no direct fiat redemption, so it relies on active arbitrage and governance tools (stability fees, savings rate, etc.).
- **Transparency & Trust:**
  - **USDC:** Reserves are off-chain. Circle publishes attestations, but users must trust auditors and regulators. No public ledger showing all reserves in real time.
  - **DAI:** All collateral is on-chain. Anyone can view Maker's vaults and total collateral at any time. Trust comes from open-source code and over-collateralization, not legal promises.
- **Centralization vs Decentralization:**
  - **USDC:** Centralized. A company and its banks hold real dollars. The issuer can freeze transactions on legal grounds. This has happened (e.g. blocking sanctioned addresses).
  - **DAI:** Decentralized in ideal form. No single party can arbitrarily freeze DAI in normal operation (just smart-contract rules). However, because DAI uses the PSM with USDC, MakerDAO has amassed large USDC holdings, so in practice a portion of DAI's backing depends on centralized assets. Maker sets limits on how much USDC it uses to mitigate this.
- **Behavior in Market Crises:**
  - **USDC:** Generally holds $1 very well in crypto crashes (its backing is outside crypto). However, it's vulnerable to real-world banking issues: e.g. March 2023, when Silicon Valley Bank failed, some USDC reserves were temporarily at risk, causing USDC to drop to ~$0.88 briefly. Regulatory or banking trouble can thus momentarily break the peg until resolved.
  - **DAI:** Experiences stress if collateral values drop. In a crash, DAI might spike above $1 as borrowers rush to repay loans (buying DAI to close positions) or if liquidations suck up DAI supply. MakerDAO can adjust parameters (like lowering borrowing costs or using the PSM) to respond. During the 2023 USDC scare, DAI dipped (to about

$0.97) because the USDC in PSM was feared at risk. So DAI's stability can be indirectly affected by events in both crypto markets and stablecoin ecosystems.

- **Revenue Sources:**
  - **USDC:** The issuer earns interest on the cash/Treasuries backing USDC. That interest is profit or used to run the business (users don't directly share this yield).
  - **DAI:** MakerDAO (the protocol) earns stability fees (interest on DAI loans) and interest from on-chain holdings. Maker also invests some of its reserves (e.g. USDC from PSM) into real-world assets like U.S. Treasury bonds to earn yield for the DAO, which helps cover protocol costs or rewards.

6 MAKER'S PEG STABILITY MODULE (PSM) AND EVOLUTION

- **PSM Introduction (2020):** MakerDAO launched the Peg Stability Module to help keep DAI at $1 more smoothly. It allowed anyone to swap certain stablecoins (initially USDC) for DAI and vice versa at a fixed 1:1 rate, with very low fees. This acted like a direct vending machine to correct price deviations.
- **Effects:** The PSM greatly stabilized DAI's price when needed, as large volumes of USDC could flow in or out. However, it also meant MakerDAO accumulated billions in USDC reserves, making DAI partially dependent on a centralized asset (Circle's USDC). Over time, about 40% or more of DAI's backing came from USDC in the PSM.
- **Mitigations & Growth:** To manage this, MakerDAO set caps on the PSM and started diversifying how it handles these reserves. Rather than leaving USDC idle, Maker began investing some into short-term U.S. government securities (via custodians or partners) to earn yield and reduce single-counterparty risk. By mid-2023, MakerDAO had moved over $700M of USDC into U.S. Treasuries, a step in its "Endgame" plan to strengthen DAI with real-world asset backing while remaining decentralized. The goal is to balance DAI's stability with its decentralization ideals.

7 ALGORITHMIC STABLECOINS & THE COLLAPSE OF TERRAUSD (UST)

- **Design Principle:** Algorithmic stablecoins aim to maintain a $1 peg without full collateral, using code-based supply adjustments. TerraUSD (UST) was pegged via its sister token LUNA. The protocol allowed any user to swap $1 worth of LUNA for 1 UST, and vice versa, irrespective of market price.
- **Intended Mechanism:**
  - If UST > $1 (too expensive), users could burn $1 LUNA to mint 1 UST and sell it, increasing UST supply (pushing price down).
  - If UST < $1 (too cheap), users could buy 1 UST for e.g. $0.95, burn it and receive $1 worth of LUNA, effectively reducing UST supply (pushing price up).
- **What Happened (May 2022 Collapse):** The system worked while UST demand grew. But when confidence fell, UST started to depeg below $1. Large holders rushed to exit: they swapped their UST for LUNA to capture the dollar-equivalent value. To satisfy redemptions, the protocol minted enormous new LUNA, causing LUNA's price to crash (because supply exploded). As LUNA collapsed, the "$1 of LUNA" became worthless, eroding confidence further. UST holders fled completely, and UST lost most of its value. In a short time, UST and LUNA went from stable to near-zero.
- **Key Lesson:** Purely algorithmic stables (with little or no real collateral) are fragile. They rely entirely on market confidence and perpetual demand. In a crisis, there is no real asset to back the peg, so the system can't halt its collapse (no circuit breaker). UST's death spiral

showed that without substantial collateral or safeguards, an algorithmic stablecoin can implode like a modern bank run without a bailout.

- **Aftermath:** The collapse wiped out >$40 billion of value and undermined trust in algorithmic stablecoins. DeFi developers now treat such designs with caution. Some newer projects use hybrid approaches (partial collateral, dynamic adjustment, emergency pause mechanisms) to avoid a repeat of the UST scenario. The consensus is clear: algorithmic-only stablecoins must have very robust defenses or collateral to be viable long-term.