Stablecoins & CBDCs: A Quantitative Deep Dive

Standalone Technical Lecture

Prof. Dr. Joerg Osterrieder

University Lecture Series

March 5, 2026

Lecture Roadmap

Learning Objectives

- Understand peg mechanisms and collateral models
- Analyse fiat-backed and crypto-backed designs
- Evaluate algorithmic stablecoin risks and failures
- Compare CBDC architectures and policy implications
- Apply quantitative risk metrics to stablecoin portfolios

Prerequisites

- Blockchain fundamentals (Lessons 1–2)
- Smart contract basics (Lessons 3–4)
- DeFi protocols overview (Lesson 5)
- Basic monetary economics

Durat

90 minutes — 5 sections — ˜55 frames — Prerequisite: Lessons 1–4

Table of Contents

Navig

through 5 sections covering stablecoin fundamentals to CBDCs and regulation

Learning Objectives

By the end of this lecture, you will be able to:

1. **Classify** stablecoins by collateral type (fiat-backed, crypto-backed, algorithmic)
2. **Analyze** peg mechanisms and the conditions under which de-peg events occur
3. **Explain** the Terra/LUNA death spiral and lessons for algorithmic stablecoin design
4. **Compare** CBDC architectures (wholesale vs. retail, account vs. token-based)
5. **Evaluate** the regulatory landscape and systemic risks of stablecoins in DeFi

Bloom

taxonomy levels: Remember → Understand → Apply → Analyze → Evaluate → Create

Section 1: Stablecoin Fundamentals

Understanding price-stable digital assets and their role in the crypto ecosystem

What You Will Learn

- Why price stability matters in digital asset markets
- Core peg mechanisms: redemption, collateral, algorithms
- Taxonomy of stablecoin types and design trade-offs
- Market landscape: size, concentration, daily volumes
- Historical de-peg events and systemic risk

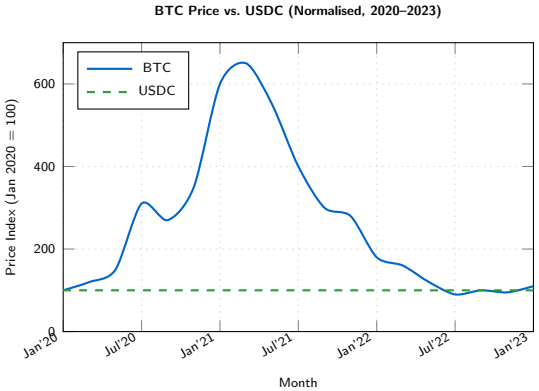
Frames in This Section

1 of 5 — Frames 4–14 — Foundational concepts before technical deep dives

The Volatility Problem

Why Volatility Breaks Money

- **Store of value:** BTC lost 80% in 2018, 75% in 2022 — unusable savings
- **Unit of account:** Prices denominated in BTC change daily; merchants cannot plan
- **Medium of exchange:** A $5 coffee may cost 0.00008 BTC today and 0.00012 BTC tomorrow
- **Annualised volatility:** BTC ≈70–80%; USD <1%; EUR ≈7%
- **Consequence:** DeFi protocols need a stable unit for loans, collateral, and settlement



Key Insight

Stablecoins decouple blockchain utility from crypto market volatility, enabling predictable financial applications.

BTC

annualised volatility source: CoinMetrics 2023 — USDC maintains $1 peg within ±0.1% under normal conditions

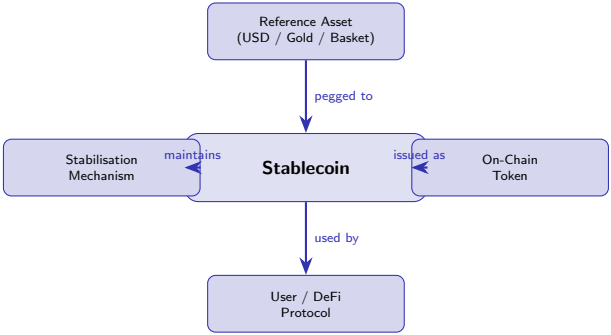
What is a Stablecoin?

Definition

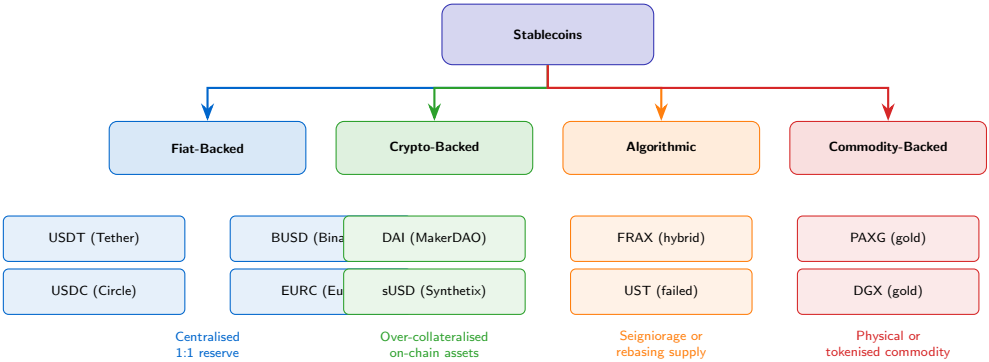
A **stablecoin** is a cryptographic token designed to maintain a stable value relative to a reference asset (peg), typically a fiat currency (USD, EUR), a commodity (gold), or a basket of assets.

Core Properties

- **Price stability:** Minimise deviation from peg ($|\Delta p| < \epsilon$)
- **Redeemability:** Holders can exchange tokens for underlying value
- **Scalability:** Supply adjusts to demand without destabilising peg
- **Decentralisation (optional):** Some designs avoid single issuer
- **Transparency:** Reserve composition verifiable by holders

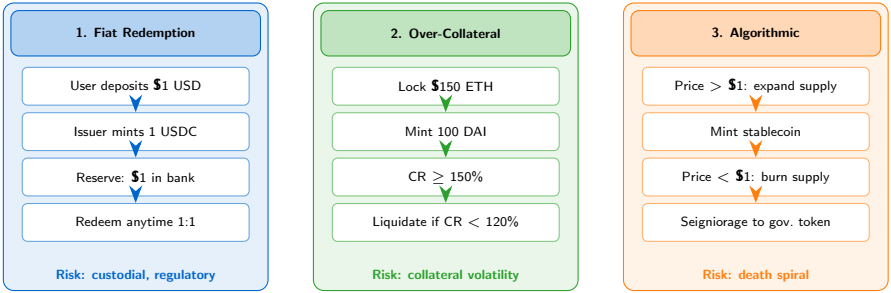


Stablecoin Taxonomy



Four primary design categories — Fiat-backed dominates with >85% market share — Each category presents distinct risk–trust trade-offs

Peg Mechanism Overview



Colla

ratio (CR) = collateral value / stablecoin value — Algorithmic designs depend on reflexive demand assumptions

Stablecoin Market Landscape

Metric	Value (2023)
Total market cap	$130B+
USDT share	~65%
USDC share	~20%
DAI share	~4%
Daily volume	$50B+
Active stablecoins	200+
Blockchains supported	50+ chains
Largest issuer reserve	T-bills & cash
YoY growth (2021–22)	+350%

Market Significance

- Stablecoins now exceed **10% of total crypto market cap**
- USDT daily volume rivals Visa on peak days
- Critical settlement layer for CEX and DEX trading
- Primary vehicle for DeFi liquidity provision
- Tether reserves include US Treasury bills, making it a significant holder

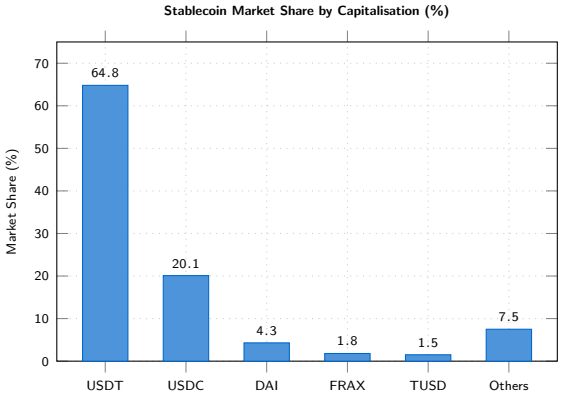
Concentration Risk

Top 2 stablecoins (USDT + USDC) control >85% of market. Systemic failure of either would cascade across all of DeFi and centralised exchanges.

Data:

CoinGecko, DefiLlama Q3 2023 — USDT issued by Tether Ltd (BVI) — USDC issued by Circle (US-regulated)

Stablecoin Market Share Chart



Key Observations

- **USDT dominance:** 64.8% despite repeated audit controversies
- **USDC growth:** Regulatory clarity driving institutional adoption
- **DAI resilience:** Survived 2022 crypto winter via over-collateralisation
- **FRAX hybrid:** Partial algorithmic design reduced risk vs. pure-algo
- **Long tail:** 200+ stablecoins share remaining 7.5%

Herfindahl–Hirschman Index

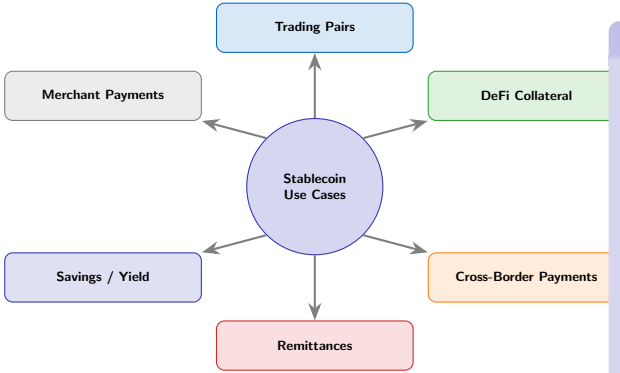
$\text{HHI} = \sum_i s_i^2 \approx 0.648^2 + 0.201^2 + \ldots \approx 0.465$

Very high concentration (HHI $>$ 0.25 = highly concentrated)

Sourc

CoinGecko November 2023 — HHI $>$ 0.25 indicates highly concentrated market — TUSD = TrueUSD

Stablecoin Use Cases



Use Case Details

- **Trading pairs:** BTC/USDT is the most-traded pair globally; avoids fiat withdrawal
- **DeFi collateral:** Aave, Compound accept USDC as highest-quality collateral
- **Cross-border:** Stellar USDC settles in 5s vs. 2–5 days SWIFT
- **Remittances:** MoneyGram–Stellar partnership; fees $<1\%$ vs. Western Union 5–8%
- **Savings/yield:** Anchor Protocol offered 20% APY (unsustainably; collapsed 2022)
- **Merchant:** Shopify, PayPal, Stripe now support USDC settlement

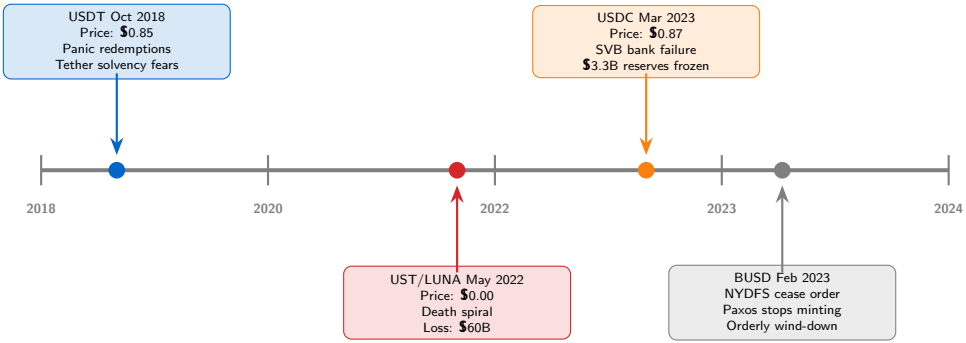
Emerging Use: CBDCs

Central banks are building their own stablecoins; retail CBDC pilots running in 130+ countries

Stabl

processed $7.4T in on-chain volume in 2022 (Visa processed $14T globally) — Fastest-growing payment rail in emerging markets

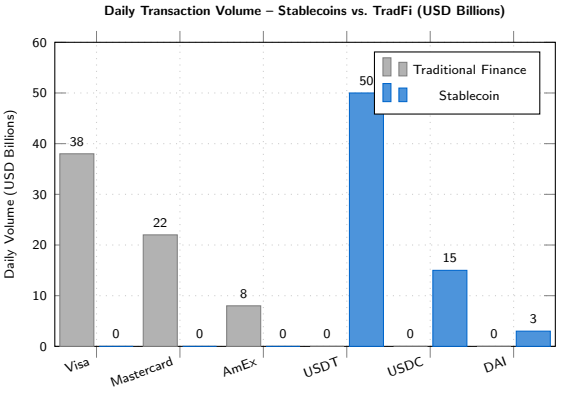
De-Peg Events Timeline



UST/

collapse (May 2022) is the largest stablecoin failure in history — USDC SVB de-peg recovered within 48 hours after US Treasury intervention

Transaction Volume vs. Traditional Finance



Volume Analysis

- **USDT surpasses Visa:** On peak days, USDT processes >$50B vs. Visa's $38B average
- **Settlement finality:** Stablecoin transfers settle in seconds; Visa settles in 1–3 days
- **Cost:** USDT transfer on Tron: $0.001; Visa merchant fee: 1.5–3.5%
- **Geography:** Stablecoins dominant in EM (Turkey, Argentina, Vietnam)

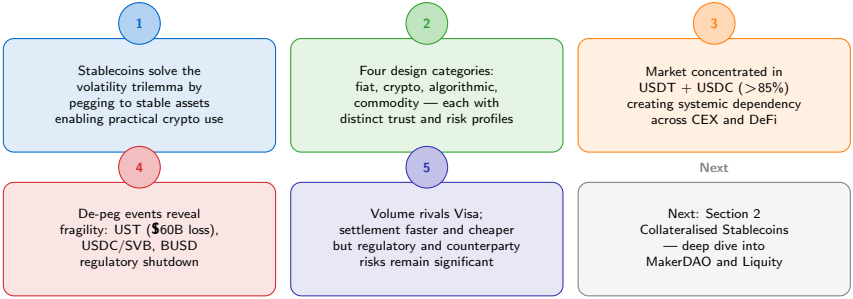
Settlement Efficiency

System	Settlement	Cost
Visa	1–3 days	1.5–3.5%
SWIFT	2–5 days	$15–50 flat
USDC (Eth)	12 sec	$0.50–2
USDC (Sol)	0.4 sec	$0.001

USD

volume: CoinMarketCap 2023 — Visa daily volume: Visa Inc. Annual Report 2023 — Stablecoin costs vary with network congestion

Section 1 Summary



Secti

1 complete — 5 key takeaways — Proceed to Section 2: Collateralised Stablecoins for technical deep dive into CDP mechanisms

Section 2: Collateralized Stablecoins

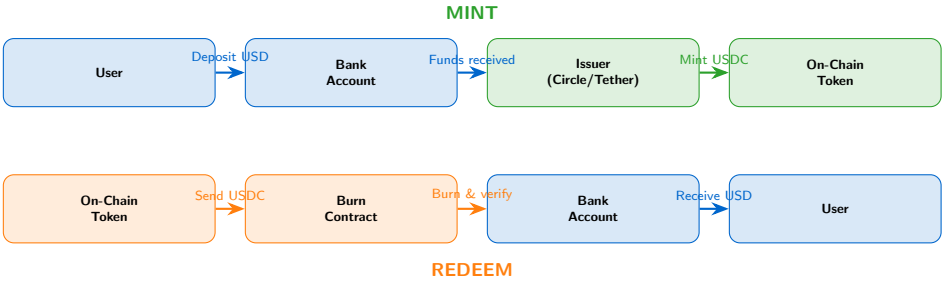
Fiat-backed and crypto-backed approaches to maintaining price stability

What You Will Learn

- How fiat-backed stablecoins mint and redeem tokens
- USDT and USDC: architecture, reserves, and controversies
- Crypto-backed designs and over-collateralisation rationale
- MakerDAO / DAI: vaults, liquidation, multi-collateral
- Commodity-backed stablecoins (PAXG, XAUT)

Frames in This Section

Fiat-Backed Stablecoins: How They Work



1:1 reserve required — Centralised issuer — KYC/AML required for mint/redeem — On-chain transfer permissionless

Fiat-backed stablecoins hold USD (or equivalents) in custody — Mint/redeem typically requires $100k+ minimums — Secondary market provides retail access

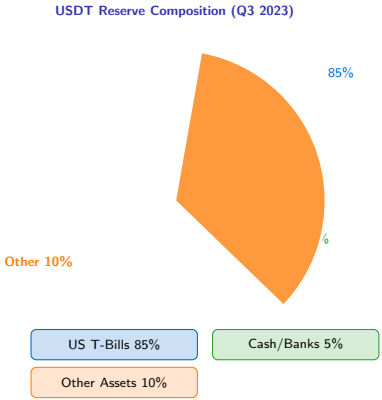
USDT (Tether) Deep Dive

Key Facts

- **Launch:** 2014 (originally "Realcoin")
- **Issuer:** Tether Limited (British Virgin Islands)
- **Supply:** $83B+ (largest stablecoin, 2023)
- **Chains:** Ethereum, Tron, Solana, BSC, Polygon
- **Tron share:** ≈50% of USDT volume
- **Reserve attestations:** Quarterly (not full audits)

Controversy

2019 NYAG investigation: Tether used reserves to cover $850M Bitfinex shortfall. Settled for $18.5M. Raised questions about full reserve backing.



USDT dominates stablecoin volume — Tether Q3 2023 attestation: BDO Italia — Full audit never published — Key systemic risk due to market size

USDC (Circle) Deep Dive

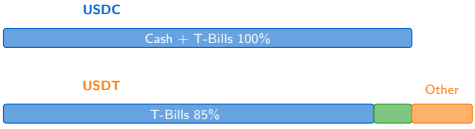
Key Facts

- **Launch:** 2018 (Circle + Coinbase consortium)
- **Issuer:** Circle Internet Financial (Boston, MA)
- **Supply:** $25B+ (2023, down from $56B peak)
- **Reserves:** 100% cash + short-term US Treasuries
- **Attestations:** Monthly by Deloitte
- **Regulation:** NY BitLicense; EU MiCA compliant path

Transparency Advantage

- Monthly reserve attestations (public)
- Segregated reserve account at regulated banks
- SVB incident (Mar 2023): $3.3B exposed, brief de-peg to $0.87
- Recovered within 48h after FDIC guarantee announcement

Reserve Quality: USDC vs. USDT



Attestation Frequency

USDC: Monthly (Deloitte)
USDT: Quarterly (BDO Italia)

Full independent audit: Neither

USDC lost market share after SVB (Mar 2023) and Binance halted BUSD (Feb 2023) — Circle files S-1 for IPO 2024 — MiCA compliance path established

Reserve Composition: Smart Contract Interface

Listing 1: Stablecoin Interface

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

interface IStablecoin {
    function mint(address to, uint256 amount)
        external;
    function burn(address from, uint256 amount)
        external;
    function totalSupply()
        external view returns (uint256);
    function reserveBalance()
        external view returns (uint256);
    function collateralRatio()
        external view returns (uint256);
}
```

Interface Explanation

- **mint**: Creates new tokens when USD deposited; restricted to issuer
- **burn**: Destroys tokens on redemption; releases equivalent USD
- **totalSupply**: Circulating token count; must equal reserve for 1:1 peg
- **reserveBalance**: Off-chain verified reserve value in USD (18 decimals)
- **collateralRatio**: $\frac{\text{reserveBalance}}{\text{totalSupply}} \times 100$ — should be ≥ 100

Key Insight

Fiat-backed issuers publish `totalSupply` on-chain but `reserveBalance` is off-chain attested. The gap between on-chain and off-chain is the core trust assumption.

USDC

contract: 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48 (Ethereum) — Solidity interface pattern — Collateral ratio audit: off-chain attestation required

Crypto-Backed Stablecoins: Overview

	Fiat-Backed		Crypto-Backed
Collateral	USD / bank deposit	Collateral	ETH, WBTC, stETH, RWA
Ratio	1:1 (100% collateral)	Ratio	150%+ (over-collateral)
Custody	Centralised (bank)	Custody	Decentralised (smart contract)
Censor Risk	High (issuer can freeze)	Censor Risk	Low (protocol-controlled)

Pros:
Capital efficient
Simple to understand
Tight peg

Cons:
Counterparty risk
Regulatory exposure
Censorship possible

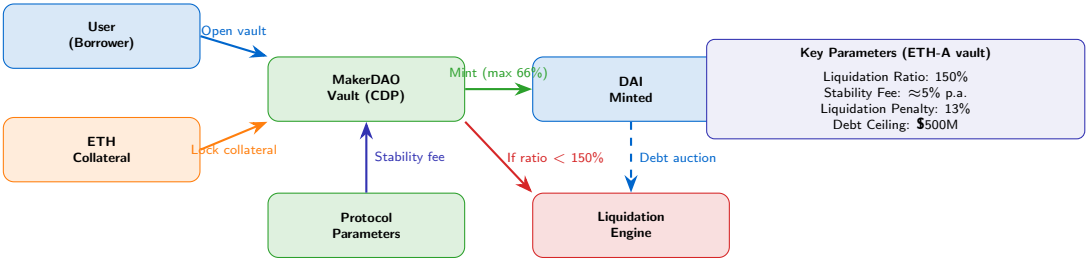
Pros:
Permissionless
Transparent on-chain
No bank dependency

Cons:
Capital inefficient
Liquidation risk
Complex governance

Crypt

backed stablecoins: DAI ($5B+), sUSD, LUSD — Over-collateralisation absorbs crypto price volatility — CDP = Collateralised Debt Position

MakerDAO and DAI

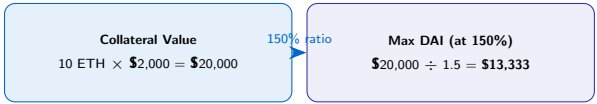


Make

launched 2017 — DAI peg maintained via stability fee adjustments and PSM — MKR holders govern protocol parameters — $8B+ TVL peak 2022

Over-Collateralisation Mechanics

Worked Example: 10 ETH at $2,000 per ETH



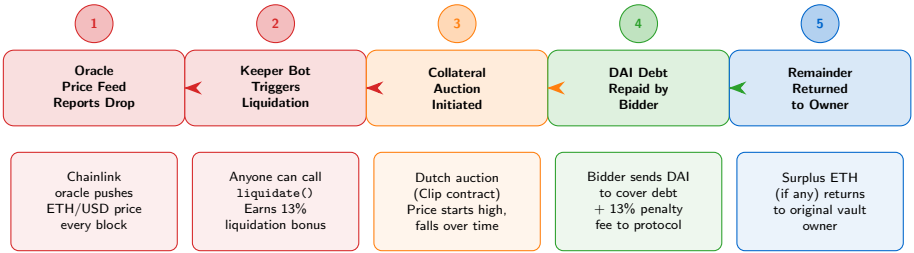
Scenario: ETH drops from $2,000 to $1,400

New collateral value: $10 \times \$1{,}400 = \$14{,}000$ New ratio: $\$14{,}000 \div \$13{,}333 = 105\%$ **Liquidation triggered at 150% — vault undercollateralised**

$$\text{Collateral Ratio} = \frac{\text{Collateral Value (USD)}}{\text{DAI Debt}} \times 100\% \qquad \text{Liquidation if CR} < \text{Liquidation Ratio}$$

Over-collateralisation buffers against crypto volatility — ETH 30-day volatility ≈60% annualised — 150% ratio provides ≈33% price drop buffer before liquidation

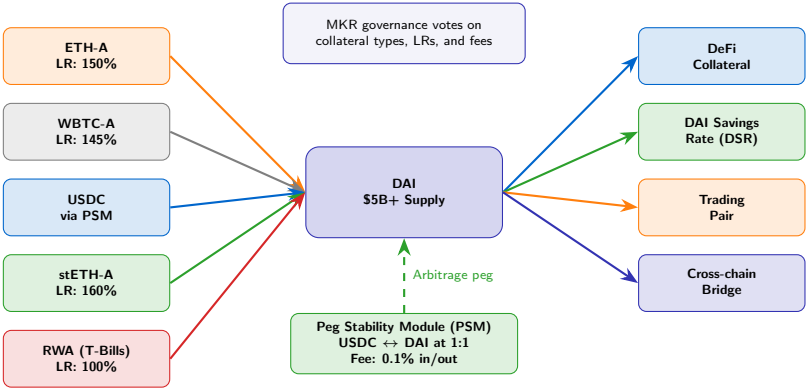
Liquidation Process



Make

liquidations: $240M+ in March 2020 “Black Thursday” — Keeper network monitors ≈50,000 vaults — Clip auction system introduced in MCD upgrade 2021

Multi-Collateral DAI



MCD launched Nov 2019 — PSM introduced 2020 for USDC 1:1 swap — RWA (real-world assets) added 2022 – Monetalis Clydesdale holds US Treasuries — DSR: 5% (2023)

Commodity-Backed Stablecoins

PAX Gold (PAXG)

- **Issuer:** Paxos Trust Company (NYDFS regulated)
- **Backing:** 1 PAXG = 1 troy ounce of LBMA gold
- **Storage:** Brinks vaults, London
- **Redemption:** Physical gold or cash (min. 430 oz)
- **Supply:** ≈250,000 oz ($500M+ at $2,000/oz)
- **Attestation:** Monthly by WithumSmith+Brown

Tether Gold (XAUT)

- **Issuer:** Tether (British Virgin Islands)
- **Backing:** 1 XAUT = 1 troy ounce of fine gold
- **Storage:** Swiss vaults (undisclosed locations)
- **Attestation:** Quarterly (same as USDT)
- **Supply:** ≈246,000 oz

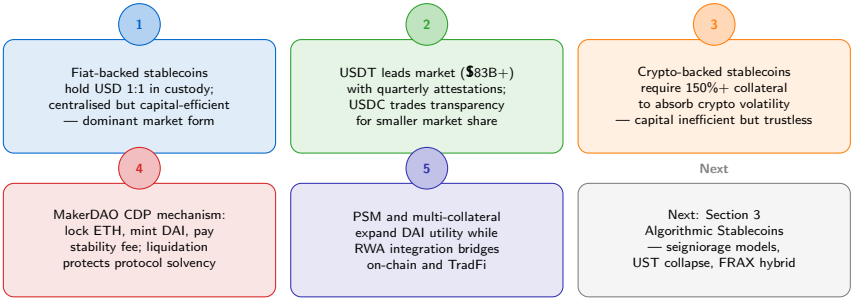
Comparison: PAXG vs. XAUT

Feature	PAXG	XAUT
Regulator	NYDFS	BVI (offshore)
Audit	Monthly	Quarterly
Chains	ETH, Solana	ETH, Tron
Redeem	Physical gold	Physical gold
Fee	0.02% tx	0.25% tx

Use Case:
Gold exposure without storage risk
Inflation hedge on-chain
DeFi collateral (Aave, Compound)

Gold-backed stablecoins: $1B+ combined market cap — PAXG price tracks LBMA spot gold — Volatility ≈15% annualised (vs. 70%+ for BTC) — Not ideal for DeFi collateral due to price moves

Section 2 Summary



Secti

2 complete — 5 key takeaways — Proceed to Section 3: Algorithmic Stablecoins for seigniorage models and the UST failure post-mortem

Section 3: Algorithmic Stablecoins

Achieving price stability through smart contract mechanisms without full collateral

What You Will Learn

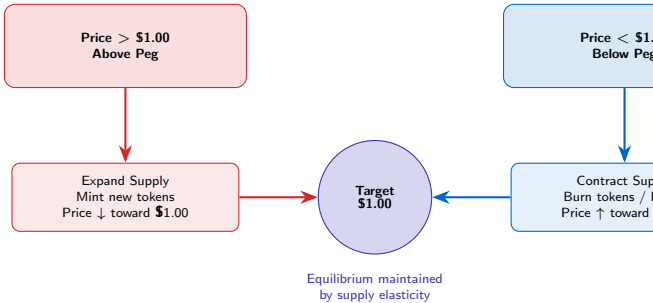
- How algorithmic peg mechanisms work without collateral
- Rebasing and seigniorage models compared
- Terra/LUNA architecture and the May 2022 collapse
- Why most algorithmic stablecoins fail
- Hybrid approaches: Frax fractional-algorithmic design
- The stablecoin trilemma: stability, efficiency, decentralisation

Frames in This Section

Algorithmic Stablecoin Concept

Core Idea

- **No collateral required:** Peg maintained purely through supply control
- **Above $1.00:** Protocol expands supply — more coins, price falls
- **Below $1.00:** Protocol contracts supply — fewer coins, price rises
- **Incentive:** Arbitrageurs profit by exploiting deviations
- **Risk:** Mechanism depends on market confidence; no backstop



Key Insight

Algorithmic stablecoins replace collateral with game theory: if everyone believes the peg holds, it holds. When belief breaks, no assets exist to restore it.

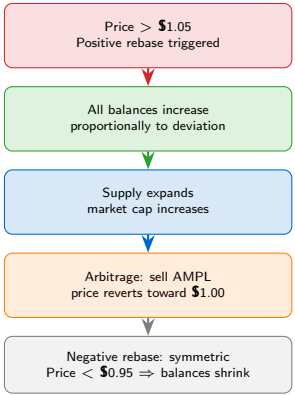
Algor

stablecoins: Basis, Empty Set Dollar, Ampleforth, Terra/UST — Combined peak market cap >$60B (May 2022) — All major designs have failed or required collateral backstop

Rebasing Mechanism: Ampleforth (AMPL)

How Rebasing Works

- **Elastic supply:** All AMPL balances adjust simultaneously every 24h
- **Positive rebase:** Price $>$ \$1.05 — every wallet balance increases proportionally
- **Negative rebase:** Price $<$ \$0.95 — every wallet balance decreases proportionally
- **No rebase zone:** \$0.95–\$1.05 — supply unchanged
- **Key property:** Your % share of total supply never changes



Example: 10,000 AMPL at \$1.10

Rebase factor $= \frac{1.10-1.00}{0.10} \times 0.10 = +10\%$

New balance: $10{,}000 \times 1.10 = 11{,}000$ AMPL

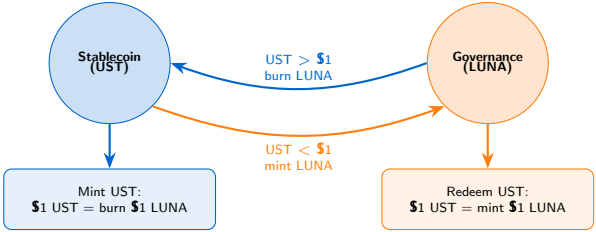
Price target: supply ↑ pushes price ↓ to \$1.00

AMP launched 2019 — Peak market cap \$800M (Jul 2020) — Rebasing does not guarantee price stability — supply elasticity shifts purchasing power not price — AMPL remains live but niche

Seigniorage Model: Two-Token Design

Seigniorage Mechanics

- **Two tokens:** Stablecoin (pegged) + Governance/seigniorage token (volatile)
- **Expansion:** When stablecoin $>$ \$1, mint new stablecoins and distribute to governance holders
- **Contraction:** When stablecoin $<$ \$1, sell bonds/coupons to absorb supply
- **Arbitrage loop:** Burn 1 governance token to mint \$1 of stablecoin; or redeem \$1 stablecoin for \$1 governance token
- **Stability assumption:** Governance token must retain value to back the peg



Arbitrage profit drives both tokens toward equilibrium — in theory

Fatal Flaw

If governance token price collapses, the mint/burn arbitrage loop becomes unprofitable, destroying the peg mechanism entirely.

Seign

models: Basis (shutdown 2018), Terra/LUNA (collapsed 2022), Olympus DAO (fragile) — Two-token design popular 2020–2022 — All major implementations ultimately failed

Terra/LUNA Architecture

Listing 2: Simplified Terra Swap Logic

```
// Simplified Terra swap logic
contract TerraSwap {
    uint256 public ustSupply;
    uint256 public lunaPrice;

    // Mint UST by burning LUNA
    function mintUST(uint256 lunaAmount)
        external {
        uint256 ustAmount = lunaAmount
            * lunaPrice / 1e18;
        ustSupply += ustAmount;
        // burn lunaAmount from sender
    }

    // Redeem UST for LUNA
    function redeemUST(uint256 ustAmount)
        external {
        uint256 lunaAmount = ustAmount
            * 1e18 / lunaPrice;
        ustSupply -= ustAmount;
        // mint lunaAmount to sender
    }
}
```

Arbitrage Mechanism

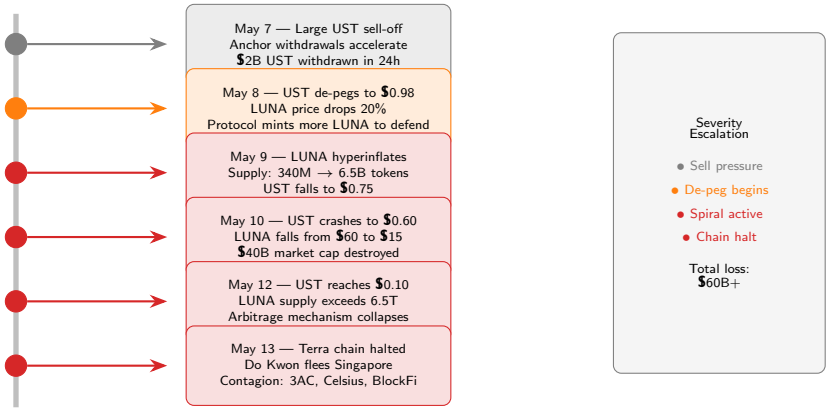
- **UST > $1:** Burn $1 of LUNA, receive 1 UST; sell UST for >$1; pocket profit
- **UST < $1:** Buy 1 UST for <$1; burn UST, receive $1 LUNA; pocket spread
- **lunaPrice oracle:** Updated by Terra validators; manipulation risk
- **ustSupply:** Unbounded growth possible if LUNA price rises fast
- **Critical path:** Arbitrage only works if LUNA has positive market value

Design Vulnerability

When LUNA price falls rapidly, arbitrageurs must receive ever-increasing LUNA quantities per UST redeemed — hyperinflating LUNA supply and accelerating price collapse.

Terra blockchain: Cosmos SDK, native LUNA token — UST peak supply: $18.7B (May 2022) — Mint/burn module: terra/market — Oracle manipulation resistance: weighted median from 30+ validators

Terra/LUNA Collapse Timeline: May 2022

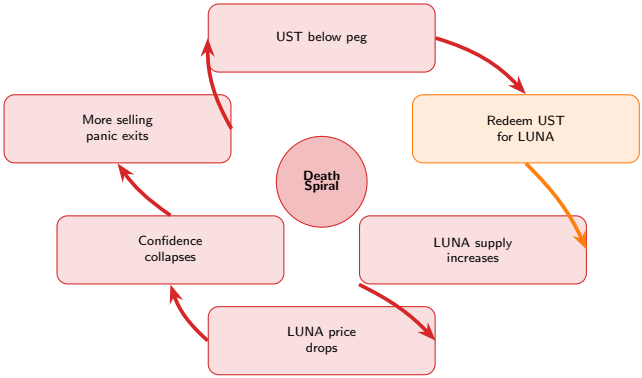


Total value destroyed: $60B+ — LUNA: $119 peak (Apr 5) to $0.0002 (May 13) — UST: $18.7B supply to $0 — Do Kwon indicted by US DOJ (2023) — Largest crypto collapse in history

Death Spiral Mechanics

Why Spirals Are Inevitable

- **Reflexivity:** Falling LUNA price makes UST defence more expensive
- **Dilution:** Each UST redeemed mints more LUNA, diluting existing holders
- **Confidence:** Rational actors exit before others, accelerating collapse
- **No floor:** Unlike crypto-backed, no collateral to liquidate for recovery
- **Bank run dynamics:** Game theory favours early exit for all participants



Nash Equilibrium

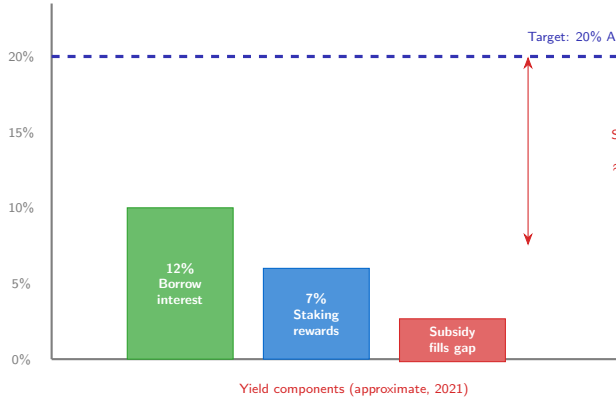
Once confidence wavers, the dominant strategy for every holder is to exit immediately. This creates a self-fulfilling prophecy that guarantees collapse.

Death spiral: positive feedback loop where each step amplifies the next — First described in context of currency attacks (Soros/GBP 1992) — Applies to any undercollateralised peg system — No known algorithmic fix

Anchor Protocol and the 20% APY Problem

How Anchor Offered ≈20% APY

- **Mechanism:** Deposit UST, receive aUST bearing yield
- **Collateral:** Borrowers deposit bLUNA/bETH (staked assets) as collateral
- **Yield source 1:** Borrower interest payments (variable, ≈12%)
- **Yield source 2:** Staking rewards from bLUNA/bETH collateral (≈6-8%)
- **Yield source 3:** Luna Foundation Guard (LFG) subsidised shortfall from reserves
- **Reality:** Subsidies burned through $450M reserve in 3 months



Yield components (approximate, 2021)

Warning Signal

Anchor paid depositors more than borrowers paid in interest. The $450M reserve was a time-limited subsidy, not sustainable yield.

Protocol: $14B TVL at peak (Mar 2022) — LFG reserve: $450M depleted in <90 days — 20% APY attracted 72% of all UST supply — Unsustainable yield primary driver of UST demand and subsequent collapse

Lessons from Algorithmic Stablecoin Failures

Name	Mechanism	Peak Cap	Failure Mode	Date
Basis Cash	Seigniorage bonds/shares	$150M	Bond demand collapsed	Jan 2021
Empty Set Dollar	Rebase + coupons	$200M	Coupon death spiral	Feb 2021
Iron Finance	Fractional algorithmic	$2B	Bank run TITAN $\rightarrow$ $0	Jun 2021
UST (Terra)	Mint/burn LUNA arb	$18.7B	Death spiral 60B lost	May 2022

Common Pattern: All designs assume stable demand for governance tokens or bonds during contraction. When confidence fails, contraction mechanism becomes inoperable — no collateral exists to restore peg.

Failed

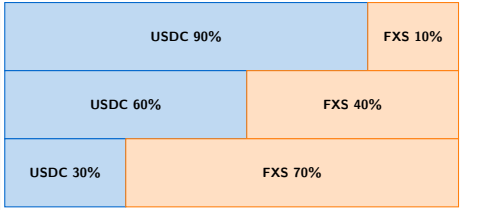
algorithmic stablecoins: 100% failure rate for pure designs — Combined losses: >$70B — Iron Finance: Mark Cuban investor — Pattern: works in bull markets, fails catastrophically in downturns

Fractional-Algorithmic Approach: Frax

Frax Hybrid Design

- **Two tokens:** FRAX (stablecoin) + FXS (Frax Shares, governance)
- **Collateral ratio (CR):** Adjustable 0–100%; starts at 100% USDC
- **Expansion:** If FRAX $>$ \$1, CR decreases (less collateral needed)
- **Contraction:** If FRAX $<$ \$1, CR increases (more collateral required)
- **Mint:** Deposit \$CR of USDC + burn \$(1-CR) of FXS to receive 1 FRAX
- **Redeem:** Burn 1 FRAX, receive \$CR of USDC + \$(1-CR) of FXS

Frax Collateral Ratio (CR) Examples



FXS: captures seigniorage revenue
Governance over CR adjustments and treasury

FRAX remained stable through UST collapse (May 2022)

Key Advantage vs. Pure Algorithmic

Collateral provides a floor. Even at 10% CR, \$0.10 of real assets backs each FRAX, limiting maximum downside unlike UST's zero-collateral model.

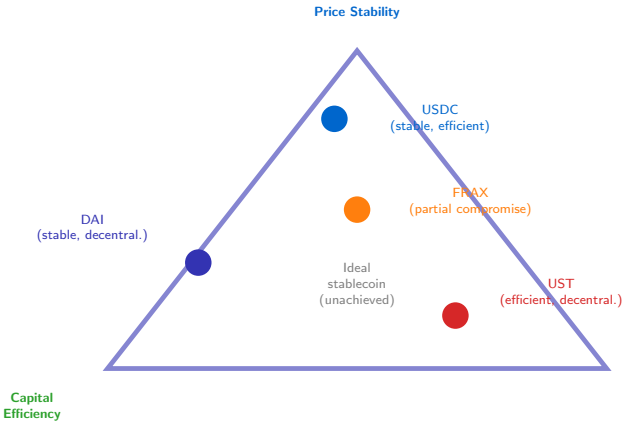
Frax

Finance launched Dec 2020 — Peak FRAX supply \$3B (2022) — CR dynamically adjusts via PID controller — FRAX maintained peg through UST collapse — FXS market cap: \$500M+ — Most robust algorithmic design to date

The Stablecoin Trilemma

Three Desiderata

- **Price Stability:** Peg holds under stress; low deviation; rapid recovery
- **Capital Efficiency:** Low collateral per $1 issued; scalable supply
- **Decentralisation:** No trusted custodian; censorship-resistant; permissionless
- **Trilemma:** Achieving all three simultaneously appears impossible
- **USDC:** Stable + efficient, but centralised (Circle can freeze)
- **DAI:** Stable + decentralised, but capital-inefficient (150%+ collateral)
- **UST:** Efficient + decentralised, but fatally unstable



Open Research Problem

No stablecoin has achieved all three properties. FRAX attempts the middle ground with adjustable CR, but retains partial centralisation via USDC collateral.

Section 3 Summary

1

Algorithmic stablecoins maintain peg via supply expansion/contraction without collateral backing

2

Rebasing (AMPL) adjusts all balances uniformly; seigniorage (UST) uses two-token mint/burn arb

3

Terra/LUNA collapsed May 2022: death spiral destroyed $60B in 6 days — largest crypto failure

4

Anchor's 20% APY was subsidised, not earned; unsustainable demand drove over-reliance on UST

5

Frax hybrid (fractional-algorithmic) survived UST collapse via partial USDC backing

Next

Next: Section 4 Central Bank Digital Currencies — state-issued digital money design

Secti

3 complete — 5 key takeaways — Algorithmic designs: 100% failure rate for pure models — Proceed to Section 4: CBDCs for state-issued digital currency architecture

Section 4: Central Bank Digital Currencies

Government-issued digital money: motivations, architectures, and global initiatives

What You Will Learn

- Why central banks are pursuing digital currencies
- Wholesale vs. retail CBDC distinctions
- Account-based vs. token-based architectures
- Global CBDC landscape: launched, piloting, researching
- Privacy considerations and design tradeoffs

Frames in This Section

Secti

4 of 5 — Frames 39–48 — 130+ countries exploring CBDCs as of 2024 — BIS: 93% of central banks engaged in CBDC work

What is a CBDC?

Definition

- **Central Bank Digital Currency:** A digital form of a country's sovereign currency, issued and backed by the central bank
- **Direct liability:** Unlike bank deposits, CBDCs are direct claims on the central bank (like digital cash)
- **Legal tender:** Designated as official means of payment by law
- **Programmable:** Can embed rules: expiry dates, spending categories, interest rates
- **Not cryptocurrency:** Centralised, permissioned, identity-linked

Instrument	Cash	Bank Deposit	Stablecoin	CBDC
Issuer	Central Bank	Commercial Bank	Private Entity	Central Bank
Form	Physical Notes	Electronic Record	Blockchain Token	Digital Record
Privacy	Full Anon.	Bank Knows	Varies	Govt. Controlled
Program.	None	Limited	Full (Smart Contracts)	Configurable by CB

Comparison: Four monetary instruments across four dimensions

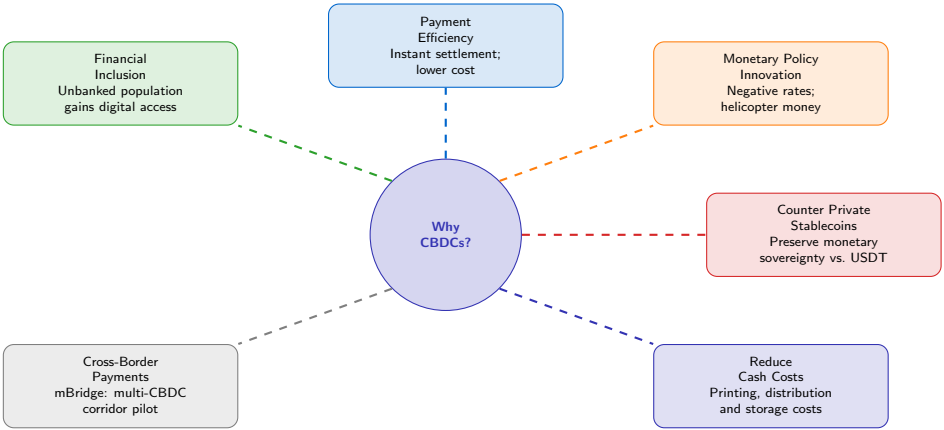
Key Distinction

A CBDC is *not* a stablecoin. It is issued by the state, carries no counterparty risk relative to the issuer, and may not use public blockchain infrastructure.

BIS

definition: CBDC is a digital form of CB money, different from existing reserves — IMF: 100+ countries in various stages of CBDC exploration — First live CBDC: Bahamas Sand Dollar, Oct 2020

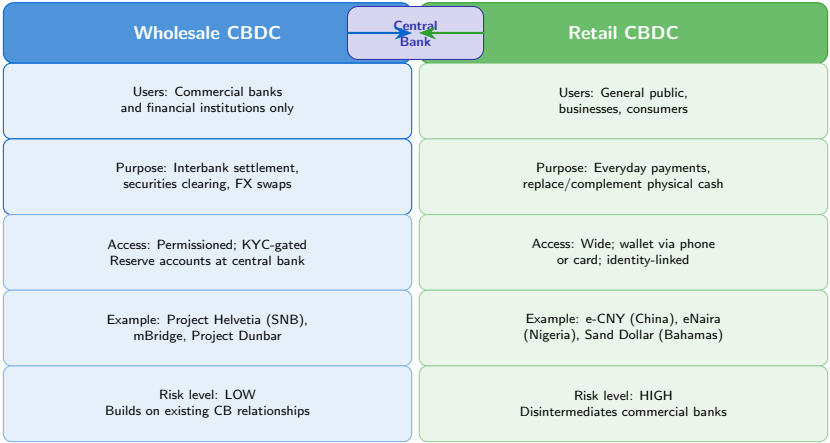
Why Are Central Banks Pursuing CBDCs?



BIS

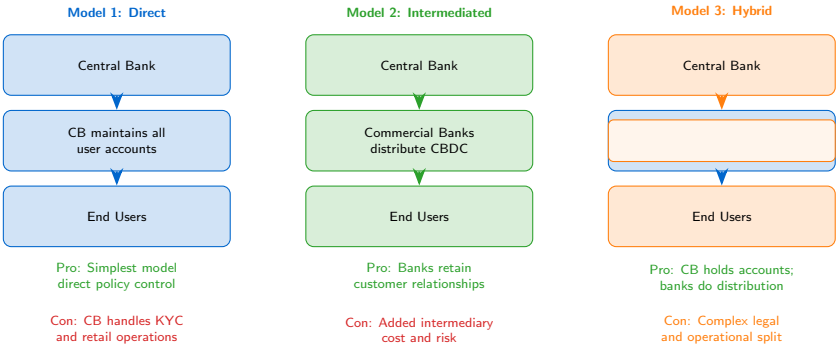
survey 2023: 93% of central banks exploring CBDCs — mBridge: BIS Innovation Hub multi-CBDC platform — Sweden Riksbank: e-Krona pilot since 2020; cash use $<10\%$ of transactions — ECB Digital Euro consultation: 6,500+ responses

Wholesale vs. Retail CBDC



Most early CBDCs are retail-focused — Wholesale CBDCs less disruptive to banking sector — mBridge: China, UAE, Thailand, HK multi-currency wholesale corridor — BIS: both types possible in parallel

CBDC Architecture Models



Most proposed retail CBDCs use Model 2 (intermediated) or Model 3 (hybrid) — e-CNY uses hybrid two-tier architecture

IMF:

60% of CBDC pilots use two-tier (intermediated) model — Digital Euro: hybrid model proposed — e-CNY: hybrid with PBOC at top, state banks distributing — Direct model: used in Eastern Caribbean (DCash)

Account-Based vs Token-Based

Listing 3: Account-Based CBDC Interface

```
// Account-based CBDC model
interface IAccountCBDC {
    function balanceOf(address account)
        external view returns (uint256);
    function transfer(
        address to, uint256 amount
    ) external returns (bool);
    function freeze(address account)
        external; // regulatory
    function setSpendingLimit(
        address account, uint256 limit
    ) external;
}
```

Account-Based

- **Identity-linked:** Balance tied to verified identity; KYC enforced at account opening
- **Regulatory tools:** `freeze()` and `setSpendingLimit()` enable direct control
- **Traceability:** Full transaction history visible to issuer; AML-compliant
- **Offline:** Difficult; requires identity verification at every transfer

Design Choice Impact

Account-based: identity is primary — you prove who you are. Token-based: possession is primary — you prove you have the token. This determines privacy, offline capability, and programmability.

Token-Based

- **Possession-based:** Valid token = valid payment; like digital banknote
- **Privacy:** Bearer instrument; sender/receiver can be pseudonymous
- **Offline:** Possible via secure hardware element (TEE/SE chips)
- **Double-spend:** Requires cryptographic prevention (blind signatures, hardware)

Global CBDC Landscape

Launched	Pilot / Advanced	Research / Design	Cancelled
Nigeria eNaira (2021)	China e-CNY (140M+ users)	EU Digital Euro (ECB)	Ecuador Dinero Electrónico (2014–2018)
Bahamas Sand Dollar (2020)	India e-Rupee (since 2022)	United States FedNow (related)	Senegal eCFA (2016–2019)
Jamaica JAM-DEX (2022)	Sweden e-Krona (Riksbank)	United Kingdom Digital Pound (Britcoin)	
Eastern Caribbean DCash (2021)	South Korea Digital Won pilot	Canada Project Jasper	

Source: Atlantic Council CBDC Tracker 2024 — 130+ countries at various stages

Atlan

Council CBDC Tracker: 130 countries in some stage of CBDC — G7: all have active research programs — BIS mBridge: 26 observing members — eNaira adoption challenged by low uptake; only 0.5% of Nigerians used it by 2023

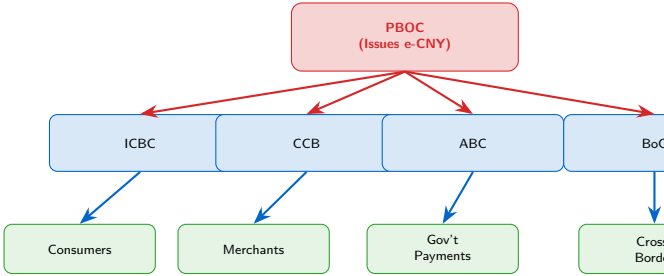
China's Digital Yuan: e-CNY

Key Facts

- **Issuer:** People's Bank of China (PBOC)
- **Launch:** Pilot since 2019; expanded to 26 cities
- **Users:** 260M+ registered wallets (2023)
- **Transactions:** $250B+ in pilot transactions
- **Technology:** Proprietary; not on public blockchain
- **Tiers:** Four wallet tiers by ID verification level
- **Anonymity:** Managed: PBOC sees all, but limited visibility for merchants

Strategic Objectives

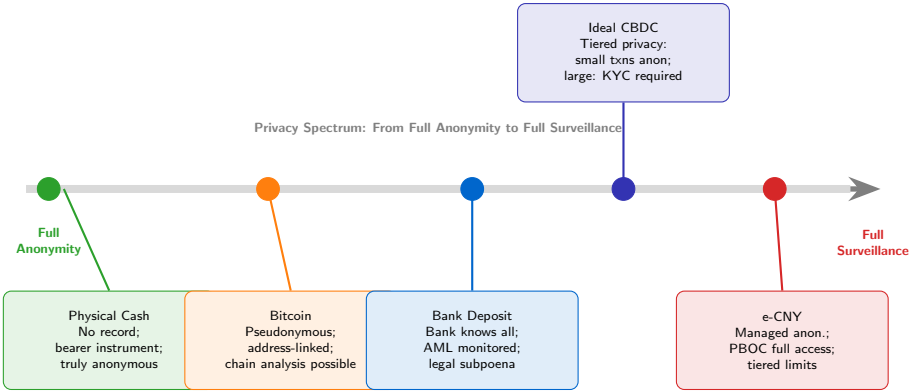
- Reduce dependence on USD in international trade
- Counter Alipay/WeChat Pay duopoly
- Enable programmable fiscal stimulus (expiry-dated vouchers)
- Lay groundwork for cross-border CNY



Two-tier hybrid architecture:
PBOC issues; state banks distribute

Offline NFC payments supported via hardware wallet

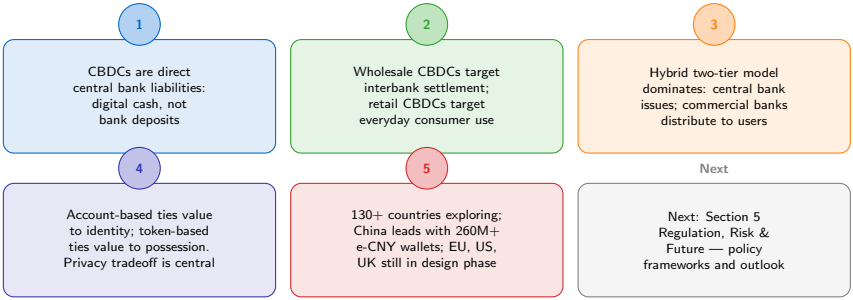
Privacy in CBDCs: A Spectrum



ECB

Digital Euro: privacy by design, offline payments without traceability for small amounts — BIS: tiered privacy model most likely for retail CBDCs — ZKP-based approaches (e.g., MIT Hamilton project) can provide privacy with AML compliance — Key tension: financial surveillance vs. civil liberties

Section 4 Summary



Secti

4 complete — 5 key takeaways — CBDCs: state response to private stablecoin growth — Proceed to Section 5: Regulation, Risk & Future

Section 5: Regulation, Risk & Future

Regulatory frameworks, systemic risks, and the future of programmable money

What You Will Learn

- Global regulatory frameworks for stablecoins
- Systemic risk categories and interdependencies
- Stablecoins as DeFi infrastructure components
- Cross-border payment revolution underway
- Future convergence of stablecoins and CBDCs

Frames in This Section

- Frame 50: Regulatory Landscape
- Frame 51: Systemic Risk Analysis
- Frame 52: Stablecoins in DeFi (Code)
- Frame 53: Cross-Border Payments
- Frame 54: Future of Programmable Money
- Frame 55: Key Takeaways

Secti

5 of 5 — Frames 49–55 — Regulation accelerating globally post-Terra/LUNA collapse — MiCA: world's first comprehensive crypto asset framework

Global Regulatory Landscape for Stablecoins

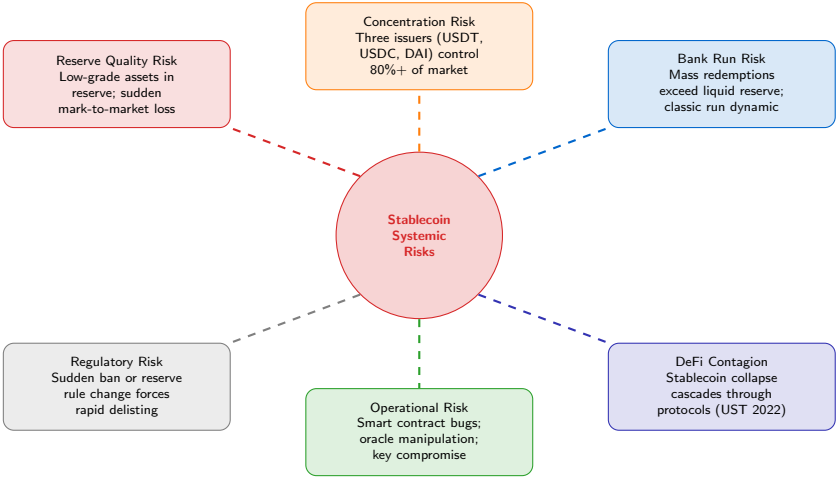
Jurisdiction	EU MiCA	US Proposals	Singapore MAS
Framework	Markets in Crypto Assets Regulation	Stablecoin TRUST Act / FIT21	Payment Services Act (PSA)
Status	In force June 2024	Proposed; not yet enacted	In force 2020; updated 2023
Reserve Req.	100% high-quality; monthly disclosure	1:1 USD or T-Bills required	Segregated client money; monthly audit
Issuer Rules	Must be licensed EU entity; capital req.	Fed-supervised depository only	MAS-licensed Major Payment Institution
Strictness	**HIGH** World's first comp. stablecoin law	**MEDIUM** Congressional deadlock ongoing	**HIGH** Sandbox with clear pathway

Japan PSA (2023): stablecoins must be issued by banks, trust cos., or fund transfer businesses

MiCA

Art. 17–49 cover ARTs and EMTs — USDC compliant with MiCA; Tether (USDT) not compliant as of mid-2024 — FSB: Cross-border regulatory coordination framework 2023 — G20: stablecoin regulation a priority since 2021

Systemic Risk Analysis



FSB

2022: stablecoins pose financial stability risk if systemically important — USDC March 2023: briefly de-pegged to $0.87 on SVB exposure ($3.3B reserves) — BIS: run risk structurally similar to money market funds — Tether: repeated opacity concerns; 2021 CFTC fine $41M

Listing 4: Stablecoin Lending Pool

```
// Stablecoin lending pool
interface IStableLend {
    function deposit(
        address stablecoin, uint256 amt
    ) external returns (uint256 shares);
    function borrow(
        address stablecoin, uint256 amt
    ) external;
    function getAPY(address stablecoin)
        external view returns (uint256);
    function liquidate(
        address borrower
    ) external;
}
```

DeFi Role: Total Value Locked

- **Lending protocols:** USDC/DAI supplied as base assets; borrowers pledge ETH collateral
- **AMM pairs:** Uniswap, Curve pool stablecoin-stablecoin pairs (e.g., USDC/DAI); billions in daily volume
- **Yield farming:** Stablecoins deposited to earn protocol incentives; Anchor's 20% APY attracted $14B UST
- **Collateral:** DAI minted against ETH CDP; LUSD against ETH; stablecoin-as-output
- **TVL share:** Stablecoins represent ∼40–60% of DeFi TVL at peak

Protocol Dependency

Aave and Compound hold $5B+ in stablecoin liquidity. A single stablecoin failure propagates instantly: collateral liquidations trigger cascading margin calls across all protocols using that asset.

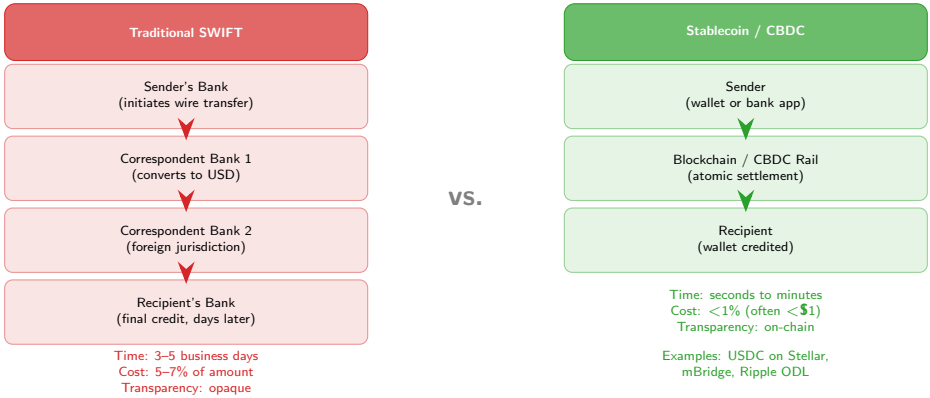
Key Risk: Composability

DeFi protocols compose atomically. A stablecoin depeg triggers simultaneous liquidations across Aave, MakerDAO, Curve, and Uniswap with no circuit breaker.

DeFi

TVL peak: $180B Nov 2021 — Curve 3pool (USDC/USDT/DAI): largest single stablecoin pool; $5B+ liquidity — Aave v3 supports 10+ stablecoins as collateral — Composability risk: no single point of control — systemic failures propagate instantly

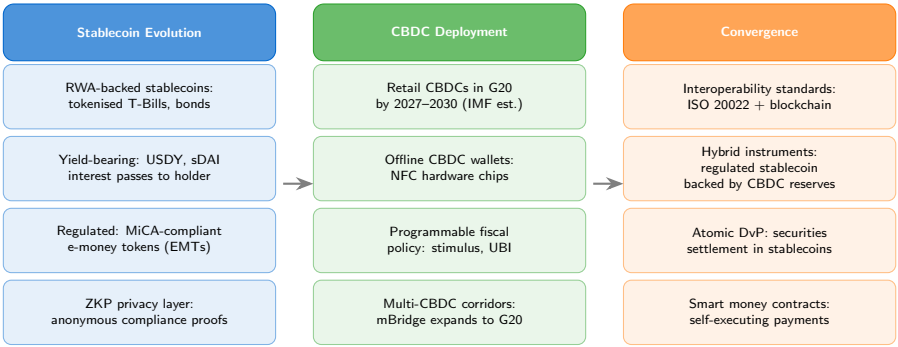
Cross-Border Payments Revolution



Global remittances: $860B/year (2023) — Average cost via SWIFT: 6.2% — Via stablecoin: <1% — Potential saving: $45B+ annually

World Bank: remittances exceeded $860B in 2023 — Stellar USDC: sub-second settlement, $0.00001 fee — mBridge: live multi-CBDC corridor since 2022 — Ripple ODL (On-Demand Liquidity): XRP bridge for cross-border USD settlement

The Future of Programmable Money

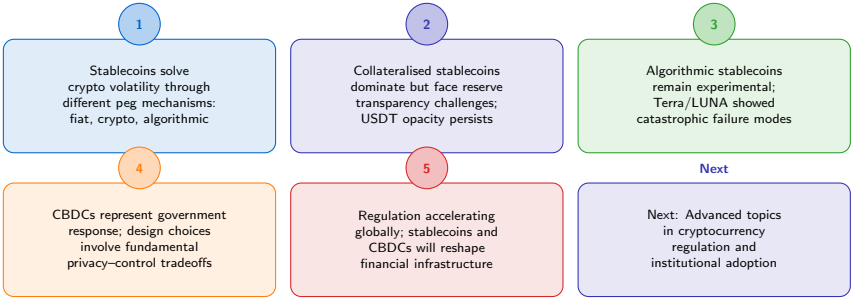


The distinction between public and private digital money will blur as interoperability standards mature

Black

BUIDL: tokenised T-Bill fund; $500M in 3 months — sDAI: MakerDAO savings rate; 5%+ yield — BIS Project Mariana: automated FX using AMMs and wCBDCs — ISO 20022: global financial messaging standard adopted by SWIFT by 2025

Key Takeaways and Course Summary



Lectu

complete: 55 frames — 5 sections — Key insight: digital money design is fundamentally about the trust triangle — issuer, user, regulator — Further reading: BIS Annual Economic Report 2023, FSB stablecoin framework, ECB Digital Euro reports