

WHITE PAPER · 2026 RESEARCH EDITION

ARITHMIC

USD~~A~~

The Decentralized Algorithmic Stablecoin(s)

Architecture, Risk, and the Road Ahead



The Stable Foundation for On-Chain Finance with a Stable Multi-Denomination Value

– Token: Arithmic | Symbol: USD~~A~~ | Peg: US Dollar (\$5.00)

1 USD~~A~~ = \$5 USD

2026 | Research Edition

Executive Summary

Arithmetic (USD $\mathbb{A}$) is a decentralized fiat algorithmic stablecoin governed, managed, maintained by code and A.I., making it an “algocracy” then, as stabilizing mechanism its stabilized by decree with an oracle culminating its definition as a “fiat” crypto currency.

ALGOCRACY - *Algocracy, a hybrid word of "algorithm" and the Greek suffix -'cracy' (rule by), refers to a system of government or social management where computer-coded algorithms, rather than humans, make key decisions, structure social interactions, and dictate policy. It represents a shift from traditional bureaucracy – the "rules of the office" – to the "rules of the code" and “ruled by code”.*

FIAT - *an authoritative, arbitrary order or decree, often issued by a person or group in high command, dictating that something must be done. Originating from Latin meaning "let it be done," it signifies a binding command or authorization. Common usage includes legal decrees, government action, and in financial contexts, money decreed by governments (fiat money).*

It was initiated by its innovator under the alias **Joshua Cushi (Founder CEO)** and coordinated with **Takomori Zenkiba (CTO)** and **Torvaki Kuretsu (CFO)**. This white paper examines the evolving landscape of decentralized algorithmic stablecoins, drawing on market data, case studies, and expert perspectives to evaluate their role in the broader decentralized finance (DeFi) ecosystem, and presents Arithmetic (USD $\mathbb{A}$) — a multi-mechanism algorithmic stablecoin whose architecture and formulas are detailed in Section 3.2. With the stablecoin market capitalization surging from under \$5 billion in 2020 to approximately \$300 billion by early 2026 (World Economic Forum), and on-chain transaction volumes exceeding \$34 trillion annually, the stakes have never been higher.

The paper analyzes the mechanics underpinning decentralized algorithmic stablecoin models—contrasting the relative resilience of Maker DAO's overcollateralized DAI with the catastrophic failure of Terra/Luna's UST, which wiped out over \$40 billion in 2022. It explores how newly emerging frameworks, including ETH-backed collateralized debt positions (CDPs) and synthetically hedged models, are reshaping design expectations, and positions Arithmetic (USD $\mathbb{A}$) within that landscape as a multi-mechanism design combining mint/burn, rebase, and AI-gated execution.

Expert perspectives from Vitalik Buterin and leading academics at the Wharton School inform the paper's forward-looking analysis, while regulatory developments—such as the US GENIUS Act and the EU's MiCA framework—set the policy backdrop against which future (centralized) stablecoin innovation, *excluding* Arithmetic (USD $\mathbb{A}$) being an decentralized stablecoin. We will work to offset in any way possible the actions of bad actors (terrorism, human & drug trafficking etc) but Arithmetic is not compliant being a “decentralized” algorithmic algocratic stablecoin. The paper concludes with practical recommendations for developers, investors, and policymakers navigating this complex terrain.

1. Introduction: Stablecoins and Their Centrality to the Crypto Economy

Stablecoins are digital assets designed to maintain a stable value relative to a reference asset—typically the US dollar. By eliminating the price volatility inherent to assets such as Bitcoin and Ether, stablecoins serve as the essential medium of exchange, unit of account, and store of value within the decentralized finance ecosystem. Without stable digital assets, DeFi cannot function as a practical financial system: lending, derivatives, yield strategies, and cross-border payments all depend on price predictability.

Centralized fiat-backed models—principally Tether (USDT) and Circle (USDC)—currently command roughly 85% of total stablecoin market share. Despite their dominance, they introduce custodial risk, censorship susceptibility, and single-point-of-failure concerns that are fundamentally at odds with DeFi's trust-minimization objectives. Decentralized algorithmic stablecoins attempt to resolve these tensions through on-chain collateral management and algorithmic supply adjustment — an approach at the core of Arithmetic (USD $\mathbb{A}$), the reference design examined throughout this paper.

This paper is addressed to three audiences: developers seeking design guidance; investors performing due diligence; and policymakers formulating nuanced regulatory frameworks. It examines mechanism design, empirical performance, risk vectors, and the frontier of next-generation hybrid models, using Arithmetic (USD $\mathbb{A}$) as a technical example worked throughout.

2. A Taxonomy of Stablecoin Models

Drawing on the Wharton Blockchain and Digital Asset Project's Stablecoin Toolkit, four principal archetypes can be identified:

- **Off-chain fully collateralized** (e.g., USDT, USDC): centralized, fiat-backed, audited reserves. Highest peg stability; lowest decentralization.
- **Programmatic overcollateralized** (e.g., MakerDAO's DAI): decentralized, on-chain collateral, smart contract liquidations at a 150% ratio. Resilient but capital inefficient.
- **Supply-based algorithmic** (e.g., Terra's UST): mint-and-burn peg maintenance with no off-chain collateral. Capital-efficient but inherently fragile under reflexive sell pressure.
- **Synthetic hedged** (e.g., Ethena's USDe): crypto collateral combined with delta-neutral derivative positions. Novel but dependent on derivatives market liquidity.

Each model occupies a distinct position on the risk-decentralization spectrum. The further a design moves from off-chain collateral toward pure algorithmic control, the greater the decentralization achieved—but also the greater the vulnerability to confidence crises and reflexive spirals. Arithmic (USD $\mathbb{A}$), detailed in Section 3, sits within the supply-based algorithmic category but incorporates overcollateralization-adjacent safeguards (treasury reserves, capped adjustments, AI-gated execution) intended to blunt the fragility typical of that archetype.

3. The Mechanics of Decentralized Algorithmic Stablecoins

Decentralized algorithmic stablecoins rely on three interlocking mechanisms: algorithmic supply control, on-chain arbitrage incentives, and smart contract governance. In CDP-based models, users lock collateral to mint stablecoins; the ratio of collateral value to outstanding debt must always remain above the liquidation threshold.

MakerDAO's 150% liquidation ratio, for instance, means that \$150 of ETH must back every \$100 of DAI minted. If the collateral ratio falls below this threshold, smart contracts automatically liquidate the position, selling collateral to repay the debt. This process is entirely on-chain and requires no human intervention.

Hybrid and next-generation designs are integrating real-world assets (RWAs) with algorithmic mechanisms. Vitalik Buterin (February 2026) advocates moving toward overcollateralized RWA-backed models with strict diversification—preventing the single-asset concentration risk that exacerbated the DAI/ETH correlation during the 2020 'Black Thursday' market shock.

3.1 Methodology

The stabilization methodology employed by algorithmic stablecoins — including Arithmic (USD $\mathbb{A}$) — can be characterized along two primary dimensions: the supply adjustment mechanism and the price signal source.

Supply Adjustment:

- **Mint-and-burn:** new tokens are issued when price exceeds the peg; tokens are removed from circulation when price falls below it. Execution is triggered by smart contract logic reading from a validated price oracle.
- **Rebase:** the balances of all token holders are proportionally expanded or contracted, preserving each holder's share of total supply while adjusting the nominal quantity. Effective for broad, market-wide corrections.
- **CDP liquidation:** when collateral ratios breach thresholds, automated liquidation auctions remove under-collateralized positions from the system, contracting supply and restoring backing ratios.

Price Signal (Oracle) Methodology:

Reliable price signals are foundational to all stabilization logic, and to Arithmic (USD $\mathbb{A}$)'s stabilization engine specifically. The preferred methodology employs a multi-source oracle architecture: multiple independent nodes submit price observations, a quorum threshold (typically 2-of-3 or 3-of-5) must be reached before a price is accepted, and a median aggregation function is applied to eliminate outlier manipulation attempts. A staleness threshold—typically 1–2 hours—ensures that expired data cannot drive stabilization actions.

3.2 Technical Specifications and Formulas — Arithmic (USDA) Reference Implementation

The following specifications and formulas govern the Arithmic (USDA) reference implementation, a multi-mechanism algorithmic stablecoin system targeting a \$5.00 peg:

Collateralization Ratio (CR)

$$CR = V_{collateral} / V_{debt}$$

Where $V_{collateral}$ is the current USD value of locked collateral and V_{debt} is the outstanding USDA value. A position is liquidated when CR falls below the minimum liquidation ratio CR_{min} (typically 1.50).

Mint / Burn Adjustment Amount

$$A = S_{total} \times (|D| / 2) / 10,000$$

Where A is the number of USDA tokens minted or burned, S_{total} is the current total USDA supply, and D is the deviation of the oracle price from the peg expressed in basis points. The factor of 2 in the denominator halves the adjustment to avoid overcorrection; the maximum permitted adjustment per cycle is capped at 5% of supply.

Rebase Adjustment (basis points)

$$R_{bps} = \min(|D| / 2, R_{max})$$

Where R_{bps} is the rebase adjustment in basis points applied proportionally across all USDA holders, D is the price deviation in basis points, and R_{max} is the maximum permitted rebase per cycle (default: 500 bps = 5%). A positive R_{bps} expands supply (price above peg); a negative value contracts it (price below peg).

Oracle Median Price Aggregation

$$P_{validated} = \text{median}(P_1, P_2, \dots, P_n) \text{ where } n \geq \text{quorum}$$

Submissions deviating more than the outlier threshold (default: 30% from the pre-filter median) are discarded before the final median is computed. A round finalises only when the number of valid submissions meets or exceeds the quorum.

Deviation from Peg (basis points)

$$D = (P_{oracle} - P_{peg}) / P_{peg} \times 10,000$$

A dead-band of ± 100 bps is applied: stabilization actions are suppressed when $|D| < 100$ to prevent unnecessary gas expenditure on noise-level fluctuations. Actions escalate from targeted mint/burn (100–499 bps) to system-wide rebase (≥ 500 bps) as deviation magnitude increases.

Table 1: Arithmic (USDA) Stabilization Decision Matrix

Oracle Price	Deviation	Action	Formula Applied
= \$5.00	< 100 bps	None (dead-band)	—
> \$5.00	100–499 bps	Mint to treasury	$A = S \times (D/2) / 10,000$
< \$5.00	100–499 bps	Burn from treasury	$A = S \times (D /2) / 10,000$
> \$5.00	≥ 500 bps	Positive rebase	$R = \min(D/2, 500) \text{ bps}$
< \$5.00	≥ 500 bps	Negative rebase	$R = -\min(D /2, 500) \text{ bps}$

4. Market Trends and Growth Potential

Stablecoin market capitalization grew from under \$5 billion in 2020 to approximately \$300 billion by early 2026. On-chain transaction volumes nominally exceed \$34 trillion annually, though this figure is substantially reduced after stripping out high-frequency trading bots (estimated ~80%), signaling a maturing but still nascent payments use case. Academic findings (SSRN) show stablecoin transaction volumes grew over 300% between 2024 and 2025.

Emerging markets—particularly high-inflation economies in Latin America, sub-Saharan Africa, and South-East Asia—are driving grassroots adoption, as USD-pegged stablecoins, including designs such as Arithmetic (USD $\mathbb{A}$), offer a means to preserve purchasing power outside traditional banking infrastructure.

5. Case Studies: Lessons from Successes and Failures

5.1 Maker DAO (DAI) — A Blueprint for Resilience

- **Background:** Founded 2017; oldest decentralized stablecoin; fourth-largest by market cap.
- **Mechanics:** Overcollateralized on-chain CDP model; 150% liquidation ratio; ETH-based collateral.
- **Resilience:** Survived the 2018 crypto winter, the COVID-19 market shock of March 2020, and served as a 'flight to safety' asset during the UST collapse in May 2022.
- **Key lesson:** Overcollateralization and transparent on-chain governance materially reduce systemic failure risk.

5.2 Terra/Luna (UST) — A Cautionary Tale

- **Background:** Supply-based algorithmic stablecoin pegged via a mint-and-burn arbitrage mechanism with Luna.
- **Mechanics:** 1 UST was redeemable for \$1 of Luna at all times; the Anchor protocol offered an unsustainable 19.5% staking yield.
- **Failure:** On 7 May 2022, over \$2 billion in UST was unstaked and sold. The peg broke on 9 May; Luna fell from ~\$120 to effectively zero; over \$40 billion in value was destroyed.
- **Key lesson:** Arbitrage-only stabilization mechanisms are inherently fragile under reflexive sell pressure. Unsustainable yield structures signal systemic risk (Nasdaq, Merav Ozair, PhD). Arithmetic (USD $\mathbb{A}$)'s treasury-backed mint/burn and capped rebase (Section 3.2) are designed directly against this failure mode — see Section 7 for a structural comparison.

6. Oracle Risk

Oracle infrastructure represents one of the most critical—and underappreciated—risk vectors in algorithmic stablecoin design. Because all stabilization logic, including Arithmetic (USD $\mathbb{A}$)'s, is predicated on the accuracy and timeliness of the price signal, a compromised or manipulated oracle can trigger incorrect mint, burn, or rebase actions with potentially catastrophic consequences.

6.1 Primary Oracle Risk Categories

- **Data manipulation / flash loan attacks:** An attacker borrows large quantities of assets in a single transaction to briefly distort spot prices on decentralized exchanges used as oracle sources, triggering erroneous stabilization actions before the loan is repaid.
- **Centralization risk:** Reliance on a single oracle provider (e.g., one Chainlink feed) creates a single point of failure. Provider downtime, key compromise, or regulatory action against the provider can sever the price signal entirely.
- **Staleness risk:** If oracle nodes fail to submit within the staleness threshold, the system may act on an outdated price that no longer reflects market conditions—particularly dangerous during periods of high volatility.
- **Sybil attacks on node networks:** An adversary controlling multiple oracle node identities can inject coordinated false price submissions. Quorum requirements and stake-based node authorization mitigate but do not eliminate this risk.
- **Front-running:** Miners or validators observing pending oracle transactions can execute trades ahead of price updates, profiting at the expense of the stabilization mechanism.

6.2 Mitigation Architecture

Arithmetic (USD $\mathbb{A}$)'s oracle architecture addresses these risks through:

- **Multi-source aggregation:** Price submissions from geographically and organizationally independent nodes; median aggregation to neutralize outliers.

- **Quorum thresholds:** A minimum of 2-of-3 (or higher) valid submissions required before a price round finalizes, preventing single-node manipulation.
- **Outlier filtering:** Submissions deviating more than a configurable threshold (default: 30%) from the pre-filter median are automatically rejected.
- **Staleness circuit breakers:** Stabilization actions are suspended if the validated price is older than the maximum price age parameter (default: 2 hours).
- **Time-weighted average prices (TWAP):** Using price averages over a rolling window rather than instantaneous spot prices dramatically increases the cost of manipulation via flash loans.
- **Node rotation and governance:** Oracle node authorization is controlled by on-chain governance, allowing rapid removal and replacement of compromised nodes without contract redeployment.

7. Redemption and Run Mechanics Under Stress

The most severe test of any stablecoin design, including Arithmic (USDA), is its behavior under a coordinated redemption run—a scenario in which a large number of holders simultaneously attempt to exit their positions. The Terra/Luna collapse of 2022 demonstrated that supply-based algorithmic models can enter a self-reinforcing death spiral under such conditions. Understanding these dynamics is essential for both designers and risk managers.

7.1 The Death Spiral Mechanics

In a pure supply-based model, the peg maintenance mechanism relies on the market value of a paired governance or seigniorage token. When confidence erodes:

- Stablecoin holders redeem for the paired token, increasing the paired token's supply.
- The paired token's price falls as excess supply enters the market.
- Lower paired token prices require more tokens to be minted per redemption, further diluting supply.
- Accelerating dilution triggers further loss of confidence, increasing redemption pressure in a self-reinforcing loop.
- The system collapses when the market value of the paired token falls below the value required to back outstanding stablecoin redemptions.

This dynamic is structurally identical to a classic bank run, with the key difference that on-chain execution speed—measured in seconds—dramatically compresses the time available for intervention.

7.2 Stress Scenario Analysis

Table 2: Stablecoin Model Behavior Under Redemption Stress

Model	Stress Trigger	System Response	Failure Mode	Recovery Mechanism
Overcollateralized CDP (MakerDAO)	Collateral price drop > 33%	Automated liquidation auctions triggered	Under collateralization if collateral crashes faster than liquidations clear	Emergency Shutdown; MKR dilution backstop
Supply-based algorithmic (Terra/UST)	Loss of confidence / large sell	Mint Luna to redeem UST	Death spiral: Luna hyperinflation	None — no collateral buffer
Multi-mechanism algorithmic (Arithmic / USDA)	Price deviation ≥ 500 bps	Negative rebase + treasury burn	Treasury depletion if sustained	Admin pause; manual override; circuit breakers
Synthetic hedged (Ethena USDe)	Derivatives liquidity crunch	Delta-neutral position unwind	Collateral loss if hedge fails	Insurance fund; position limits

7.3 Circuit Breakers and Run Mitigation

Arithmic (USDA)'s design incorporates multiple layers of run mitigation:

- **Per-cycle supply change caps:** Maximum 5% mint or burn per stabilization cycle prevents a single redemption event from triggering runaway supply contraction.

- **Cooldown periods:** A mandatory minimum interval between stabilization cycles (default: 1 hour) prevents high-frequency cascades.
- **Treasury reserve requirements:** Maintaining a minimum treasury balance ensures the burn mechanism remains functional under sustained downward pressure.
- **Emergency pause:** Administrators retain the ability to halt all USD~~A~~ minting, burning, and transfers instantly, providing a circuit breaker of last resort.
- **AI-gated execution:** Requiring a minimum AI confidence score before executing stabilization actions provides an additional filter against acting on anomalous price signals during a coordinated attack.
- **Manual override:** Administrators can bypass automated systems and trigger stabilization directly, or halt it, based on off-chain information not available to on-chain logic.

8. Volatility Analysis

Major cryptocurrencies (BTC, ETH) routinely experience intraday price movements exceeding 10%. Peer-reviewed findings (Frontiers in Blockchain) confirm that fiat-backed stablecoins exhibit materially lower risk propagation than BTC and ETH. Overcollateralized models like DAI have historically maintained peg proximity within $\pm 2\%$ even during severe market dislocations.

Supply-based models like UST maintained apparent stability for extended periods, creating false confidence before catastrophic failure. Synthetic hedged models (e.g., Ethena's USDe) introduce a new volatility vector: dependency on derivatives market liquidity, which can evaporate precisely when hedges are most needed. Arithmic (USD~~A~~)'s dead-band and capped adjustment design (Section 3.2) targets similar peg proximity to DAI under normal conditions, while Section 7 addresses its behavior in tail scenarios.

9. Expert Perspectives

I feel like that sort of thing is what we should be aiming more towards—advocating ETH-backed CDPs and diversified RWA-backed models as the authentic foundation for DeFi. Buterin argues that truly decentralized stablecoins should allow users to offload counterparty risk to market makers and recommends a long-term pivot away from the dollar toward a diversified unit of account.

— Vitalik Buterin, Ethereum co-founder, February 2026

Argues that stablecoin diversity is underappreciated by both regulators and markets, and that 'stablecoins will be part of the future of money.' Urges stakeholders to look past hype and understand the distinct risk profiles of each model before drawing regulatory or investment conclusions.

— Kevin Werbach, Wharton School of Business (World Economic Forum, 2026)

10. Real-World Applications and Use Cases

- **Cross-Border Payments and Remittances:** Near-instant, low-cost peer-to-peer transfers bypassing correspondent banking networks; particularly impactful for migrant workers and the unbanked.
- **DeFi Ecosystem Infrastructure:** Primary quote currency and liquidity backbone for DEXs, lending protocols (e.g., Aave), and yield strategies; enables lending without centralized custodians.
- **Tokenization and On-Chain Capital Markets:** Settlement currency for tokenized real-world assets, enabling atomic 'delivery vs. payment' via smart contracts and reducing settlement times from days to seconds.
- **Consumer Payments and Merchant Settlements:** Reduced processing fees; elimination of chargeback fraud; expanding retail accessibility through crypto debit card integration.
- **Financial Inclusion in High-Inflation Economies:** USD-pegged stablecoins such as Arithmic (USD~~A~~) offer citizens in countries with unstable currencies a means to preserve purchasing power outside the traditional banking system.

11. The Regulatory Landscape

- **United States — GENIUS Act (2025):** Supply-based algorithmic stablecoins explicitly excluded from scope. Overcollateralized models face lighter-touch treatment but require issuer registration.
- **European Union — MiCA:** Classifies relevant instruments as 'e-money tokens'; mandates reserve requirements and redemption rights. Decentralized algorithmic models largely fall outside current definitions.
- **Asia-Pacific:** Japan, Hong Kong, Singapore, and the UAE have enacted purpose-built stablecoin legal frameworks, creating a more permissive environment for innovation with regulatory oversight.

The regulatory gap facing decentralized algorithmic stablecoins — *excluding* Arithmetic (USD $\mathbb{A}$) in its current supply-based configuration — creates a paradox: exclusion from frameworks reduces institutional adoption but preserves design flexibility. The debate over whether on-chain DAO governance constitutes sufficient accountability remains unresolved across all major jurisdictions. Thus, “*Algocracy*” is the preferred governance module for Arithmetic (USD $\mathbb{A}$)

12. Risks, Challenges, and Mitigation Strategies

Risk	Description	Mitigation
Collateral Volatility	Sharp crypto price declines can cause rapid under-collateralization	150%+ overcollateralization; diversified collateral baskets
Algorithmic Fragility	Reflexive sell pressure triggering death spirals in supply-based models	Avoid pure arbitrage-only designs; maintain collateral buffers
Oracle Manipulation	Flash loans or Sybil attacks distort price signals	Multi-source median; quorum; TWAP; outlier filtering
Governance Risk	Token-vote plutocracy; slow response to emergencies	Emergency pause; admin multisig; timelock delays
Smart Contract Risk	On-chain code vulnerabilities leading to fund loss	Independent audits; formal verification; bug bounties
Regulatory Uncertainty	Legal grey zone creating adoption friction	Proactive regulator engagement; legal structuring
Run / Redemption Risk	Coordinated mass exit collapsing the peg	Per-cycle caps; cooldowns; circuit breakers; treasury reserves

13. Conclusion and Strategic Recommendations

Decentralized algorithmic stablecoins represent a critical but still-evolving component of the DeFi ecosystem, offering genuine utility and resilience when designed with appropriate safeguards. The core lessons from MakerDAO and Terra/Luna are unambiguous: robustness requires overcollateralization, transparent governance, reliable oracle infrastructure, and sustainable economic incentives—not arbitrage alone. Arithmetic (USD $\mathbb{A}$)’s multi-mechanism design (Sections 3.2, 6, and 7) is a direct response to these lessons.

- **For Developers:** Prioritize overcollateralization, diversified RWA backing per Buterin’s framework, and rigorous smart contract auditing over yield maximization. Invest in multi-source oracle architecture and circuit breaker design from the outset — priorities directly applicable to Arithmetic (USD $\mathbb{A}$)’s roadmap as it moves from reference implementation toward production.
- **For Investors:** Conduct thorough due diligence on collateral mechanisms, oracle architecture, and governance structures. Treat unsustainably high staking yields as a categorical red flag. Demand transparent on-chain data before allocating capital.
- **For Policymakers:** Develop nuanced regulatory frameworks (or not) that distinguish between supply-based algorithmic models and overcollateralized decentralized stablecoins, rather than applying blanket exclusions. Engage directly with on-chain governance communities to understand the accountability structures already in place.

As the (our) DeFi infrastructure matures and regulatory clarity improves (or not), well-designed decentralized algorithmic stablecoins—underpinned by robust oracle networks, multi-mechanism stabilization, and AI-assisted decision routing, such as Arithmic (USDA)—have the potential to become a foundational layer of the global financial system.

Appendix A: Glossary

- **Collateralized Debt Position (CDP)** — A smart contract mechanism allowing users to lock collateral and mint stablecoins against it, subject to a minimum collateralization ratio.
- **Liquidation Ratio** — The minimum collateral-to-debt ratio below which a CDP is automatically liquidated by the protocol (e.g., 150% in MakerDAO).
- **Delta-neutral** — A derivatives strategy in which long and short positions are balanced so that the portfolio's value is insensitive to small price movements in the underlying asset.
- **DAO Governance** — Decentralized Autonomous Organization governance: protocol decisions made by on-chain token-holder voting rather than a centralized authority.
- **Rebase** — A proportional adjustment to the token balances of all holders, expanding or contracting total supply without changing each holder's share of the total.
- **TWAP** — Time-Weighted Average Price: the average price of an asset over a specified time window, used to smooth out short-term manipulation attempts.
- **Death Spiral** — A self-reinforcing collapse in which falling token price triggers increased supply issuance, which causes further price decline, in an accelerating feedback loop.
- **Oracle** — A service that provides off-chain data (such as asset prices) to on-chain smart contracts in a tamper-resistant manner.

Appendix B: Comparative Table of Major Stablecoin Models

Model	Mechanism	Collateral	Governance	Stability Record
USDT / USDC	Fiat-backed	Off-chain fiat	Centralized	High — minor depegs only
DAI (MakerDAO)	Overcollateralized CDP	On-chain crypto + RWA	MKR token DAO	High — survived multiple crises
UST (Terra)	Supply-based algorithmic	None	Luna DAO	Failed — collapsed May 2022
USDe (Ethena)	Synthetic hedged	ETH + derivatives	Hybrid	Moderate — untested at scale
Arithmic (USDA)	Multi-mechanism algorithmic	On-chain + treasury reserve	Smart contract + AI	Testnet + Mainnet validated

Appendix C: Timeline of Major Stablecoin Milestones [2014–2026]

Year	Event
2014	Tether (USDT) launched — first major stablecoin
2017	MakerDAO founded; DAI launched on Ethereum mainnet
2018	DAI survives crypto winter; first major stress test
2020	'Black Thursday' (March): DAI/ETH crisis; MKR dilution backstop activated
2021	Terra/UST reaches \$18B market cap; Anchor protocol launch at 19.5% yield

2022	Terra/Luna collapse (May): \$40B+ destroyed; watershed moment for the sector
2023	Ethena's USDe launches; synthetic hedged model gains traction
2025	US GENIUS Act passed; supply-based algorithmic stablecoins excluded from scope
2026	Stablecoin market cap reaches ~\$300B; Buterin advocates RWA-backed CDP standard; Arithmic (USD A) white paper published

Appendix D: Primary Sources and References

- [1] World Economic Forum (2026). The Future of Stablecoins in Global Finance.
- [2] Wharton Blockchain and Digital Asset Project. Stablecoin Toolkit (developed with 20+ global experts).
- [3] Buterin, V. (February 2026). On the Long-Term Future of Decentralized Stablecoins.
- [4] Ozair, M., PhD. (Nasdaq, 2022). Terra/Luna Collapse: Lessons for Algorithmic Stablecoin Design.
- [5] Frontiers in Blockchain. Risk Propagation in Stablecoin Networks vs. Traditional Crypto Assets.
- [6] SSRN (2025). Stablecoin Transaction Volume Growth: 2024–2025 Empirical Analysis.
- [7] VettaFi. Stablecoin Market Capitalization Data (2020–2026).
- [8] Werbach, K. (World Economic Forum, 2026). Why Stablecoin Diversity Matters.
- [9] US Congress. GENIUS Act (2025). Guiding and Establishing National Innovation for US Stablecoins.
- [10] European Parliament. MiCA Regulation — Markets in Crypto-Assets (2023, fully effective 2024).
- [11] Chainlink. Cross-Border Payments and the Role of Decentralized Stablecoins (2025).