Generic gmUSD Whitepaper V1.0

By Anthony Leutenegger, Carlos Juarez and Ivan Fartunov

1. Abstract

gmUSD is a fully collateralised synthetic dollar issued on Ethereum mainnet and represented on connected networks. The initial collateral set consists of USDC, USDT and USDS, each held in its vault under fixed hard caps. gmUSD mints are price-based at the oracle value of the deposited asset and gmUSD value of $1. Redemptions pay the redemption value (RV) per gmUSD, where *RV = min(basket_value / supply, 1.00)*. A collateral buffer maintains RV = $1. All accounting and settlement occur on the canonical chain; bridged balances on other networks reflect canonical supply. Collateral is allocated to whitelisted Ethereum strategies (i.e. Morpho, Aave, Sky). Realised yield mints new fully-backed gmUSD on Ethereum and is bridged pro rata to connected networks. gmUSD offers blockchain networks a single USD-denominated quote asset, which enhances capital efficiency, reduces fragmentation, and alleviates the incentive burden, while leveraging otherwise idle assets to generate real yield.

2. Problem Statement

Stablecoin supply on L1 and L2 networks is split across multiple contract variants: native USDC and bridged USDC.e, USDT, DAI, etc. Each carries independent risk and liquidity, forcing rollups to maintain separate pools, oracle feeds, and lending parameters. This creates three systemic inefficiencies:

- Capital dilution - Depth is thinly spread. A $1 million swap between “stable” tokens on most L2 DEXs can slip 20-40 bp during off-peak hours.

- Budget drain - To offset this, rollups spend heavily on incentives, often eight-figure token grants per year, yet spreads and slippage persist.
- Yield isolation - TVL on L2s cannot natively access L1 yield streams. Networks rely solely on emissions rather than real earnings to fund their liquidity budgets.

The result is a persistent drain on capital efficiency and an inflated subsidy burden for L2 ecosystems, while composability across the stack suffers and user execution deteriorates.

A stable, yield-bearing synthetic dollar that consolidates collateral and behaves consistently across all rollups is therefore critical. It allows networks to collapse fragmented pairs into a single quote asset (a quote asset is the second asset in a trading pair, used as a consistent denomination), reduce reliance on subsidies, and integrate real yield into their incentive mix.

3. Design Principles and Architecture

3.1 Invariants

The following properties must always hold, regardless of collateral composition or market conditions:

- **Redemption integrity** — Every gmUSD is fully backed; redemptions always pay the current RV (≤ $1), either in the requested asset or via routed/pro-rata payout (implemented on the UI).
- **No over-par issuance** — Deposits are valued at min(p, $1), ensuring the system never issues more than 1 unit of gmUSD per 1 unit of accepted collateral.
- **Bounded exposure** — Vault hard caps limit the blast radius of any single collateral's failure.
- **Single source of truth** — All supply and accounting occur on Ethereum L1; rollups hold mirrored balances only.

These invariants anchor the economic design and frame the risk model described in later sections.

3.2 Canonical Chain and OFT Mirroring

All gmUSD supply operations—mint, redeem, collateral allocation, oracle checks—execute exclusively on Ethereum mainnet (the "canonical chain"). Every other connected network only holds a representation minted via arbitrary message passing through the chain designated bridge.

- **Lock-and-mint:** Canonical tokens are locked on L1 and bridged representations minted on L2.
- **Burn-and-unlock:** L2 balances are burned to release canonical tokens. This ensures global supply coherence: non-canonical chains cannot inflate supply or alter collateral.

3.3 Collateral Vaults

Collateral is held in isolated ERC-4626 vaults, one for each collateral asset (initially USDC, USDT, and USDS). Collateral in each vault is deposited into whitelisted mainnet strategies (Morpho, Aave, Sky):

- Each vault has a hard cap, expressed as % of the total collateral value.
- Deposits that would breach a cap are rejected; redemptions are preferentially serviced over-cap vaults until they return within limits.
- Vaults do not transfer assets among themselves outside controlled rebalancing.
- Hard caps enforce diversification and limit the impact of a collateral de-peg.

3.4 Collateral Manager

Steakhouse Financial will serve as a designated collateral manager to oversee the allocation of collateral across whitelisted L1 strategies (e.g., Morpho, Aave, Sky in v1) with limited authority:

- Can allocate or withdraw across strategies and harvest rewards.
- Can trigger rebalancing (see section 3.5)
- Can change the security buffer percentage and trigger overflow of the generated yield (see section 5.2)
- **Cannot** modify vault caps, add new strategies, or alter minting and redemption rules.

For more detailed role information, see Section 8.

3.5 Rebalancing Framework

When vault utilisation approaches its hard cap, the Collateral Manager rebalances collateral through onchain swaps.

- If any vault exceeds 95% of its hard cap, the manager may initiate a swap.
- Over-represented collateral is swapped for under-represented collateral via pre-approved deep-liquidity DEX pools (e.g., Curve stableswap).
- Swaps are executed at prevailing pool prices with tolerance-bounded slippage.

In v1, the collateral manager multisig executes swaps; future releases may automate trigger, routing and execution.

This approach simplifies operations compared to sealed-bid auctions, while still ensuring that vault composition remains inside configured target weights.

4. Peg Stability Mechanism

Peg stability is a core function of gmUSD. The protocol ensures that each gmUSD is always redeemable for value equal to the collateral basket.

4.1 Definitions

- **a_gmUSD** — circulating supply of gmUSD
- **bValue** — basket value = Σ ($amount_i \times price_i$), using oracle prices
- **RV (Redemption Value)** = min(bValue / a_gmUSD, 1.00)

4.2 Redemption Value (RV)

- Redemptions always return RV per gmUSD, never exceeding $1.
- RV falls below $1 only if bValue < a_gmUSD.
- The redeemed asset (i.e. USDC, USDT, USDS) is priced as max (p, $1)
- Users may request a payout in a specific collateral asset; if direct vault liquidity is insufficient, the request is routed through designated liquidity (e.g., stableswap). Routing is handled on the UI side and is not part of the protocol.
- This ensures the redemption value is invariant, even if the payout form varies.

4.3 Mint Valuation

- Deposits are valued at min(p, $1), where p = oracle price of the deposited asset.
- Minted gmUSD = deposit amount × min(p, $1).
- Over-peg deposits (p > 1): valued at $1 to block premium extraction.
- Under-peg deposits (p < 1): mint fewer gmUSD; if the asset re-pegs, the system retains a minting surplus that strengthens the collateral buffer.

4.4 Transparency and Monitoring (introduced only in v1.1)

The protocol publishes in real time:

- gmUSD total supply
- Total backing value by collateral type
- Redemption Value (RV)
- Collateral buffer percentage
- Oracle health: freshness/heartbeat status and Chainlink↔TWAP divergence

These signals enable users and integrators to independently verify the health of the peg.

4.5 v1 Design Assumptions

The v1 design assumes collateral assets (USDC, USDT, USDS) are stablecoins with low depeg probability and a high likelihood of re-pegging after volatility.

- Temporary deviations: Small, short-lived under-pegs are absorbed by the collateral buffer; as long as basket value ≥ supply, RV remains $1.
- Stress conditions: If the basket value falls below the supply, the RV decreases proportionally. As redeemed assets are valued at max(p,$1), redemption of under-peg assets is disincentivised, protecting the protocol.
- Persistent failure: If a stablecoin fails to re-peg, the RV reflects the loss directly. gmUSD remains backed by the remaining basket; market price may trade below $1 until collateral values recover.

This assumption narrows v1's scope: the mechanism is designed for volatility and temporary depegs, not permanent collateral collapse.

Generic

5. Yield and Distribution

gmUSD consolidates collateral and channels value back into the system. Value first flows into peg stability mechanisms, with surplus being released as gmUSD yield.

5.1 Sources of Value Flow

- **Strategy yield** — rewards harvested from whitelisted L1 strategies (Morpho, Aave, Sky in v1).
- **Minting/redemption surplus** — created when under-peg deposits mint fewer gmUSD than face value, with recovery accruing to the vaults. Also created when users redeem over-peg assets from the collateral basket

In V1, harvests and distribution checks occur weekly, striking a balance between gas efficiency and timely delivery.

5.2 Collateral Buffer and Shortfall Recovery

The buffer is the first-loss reserve, designed to keep RV = $1 under volatility. It is topped up by minting surplus and part of the strategy yield.

Flow priority:

1. Cover shortfall: If RV < 1, incoming yield is used to restore RV toward $1.
2. Fill buffer: If RV = 1 but buffer < 1% of supply, value flows into the buffer.
3. Release surplus: If the buffer is≥ 1%, the incremental value is released downstream (§5.3).

In v1, overflow release is manually managed; automation is planned for later versions.

5.3 Yield Mint and Distribution

Once the buffer is full, new yield mints additional gmUSD on Ethereum. The yield compounds in the collateral vault, so gmUSD remains fully backed at all times. Newly minted gmUSD is distributed to rollups and the protocol:

- Rollups: Minted gmUSD is bridged in proportion to each chain's share of outstanding supply to a destination address or contract determined by the chain
    - v1: snapshot at harvest.

    - v1.2: time-weighted balances (“liquidity-days”).
- Protocol: Receives a fixed fraction α of the distributed yield.

5.4 Transparency (introduced only in v1.1)

Onchain data exposes the value pipeline end-to-end:

- Harvest amounts per strategy
- Redemption fees collected (if any)
- Surplus accrual from under-peg deposits
- Newly minted gmUSD for yield
- Distribution shares by rollup

This enables integrators and users to independently verify value generation and routing.

6. Economic Parameters

This section defines the parameters that govern gmUSD’s economic behaviour. They determine how value is routed, how the buffer is maintained, and which levers can be adjusted in future versions.

Parameter	Default Value	Rationale
Buffer Target	1% of gmUSD supply	Absorbs routine volatility (≈3% one-asset drop in a 3-asset basket).
Treasury Share (α)	10% of yield above buffer	Secures protocol sustainability while passing the majority of yield to rollups.
Harvest Interval	7 days	Balances gas cost with timely yield delivery.
Vault Hard Caps	45–50% per asset	Limits exposure to a single collateral issuer.

Note: Parameter setting will evolve in later versions of the protocol (see Roadmap).

Generic

7. Risk Model

This section outlines the primary failure modes for gmUSD v1 and the corresponding controls in place to mitigate each one. The list is scoped to risks that can affect peg integrity or collateral solvency; commercial or regulatory risk is addressed elsewhere.

7.1 Smart-Contract Risk

Scope: Vault implementations (ERC-7575), mint/redeem state machine, rebalancing auction contracts, LayerZero OFT adapter.

Mitigations:

- Employing unit testing, integration testing, and simulation of edge cases before deployment to verify contract logic and catch bugs.
- Independent and regular code audits by external experts to discover and patch vulnerabilities
- Limiting who can trigger sensitive contract functions (principle of least privilege) via role-based access and well-defined permissioning
- Upgradable proxy and modular architecture to allow security patches and improvements post-deployment.
- Dependency on well-audited codebases such as OpenZeppelin

7.2 Oracle Dependency

- Primary feed: Chainlink USD price for each collateral asset.

7.3 Cross-chain Risk

Scope: LayerZero endpoint or relayer compromise could inflate the bridged supply.

Mitigations:

- Canonical chain is single source of truth; non-canonical chains can only mint if canonical tokens are locked.
- Daily supply coherence check: The script verifies bridged balances equal the locked amount and emits an alert on any mismatch.
- Rollups can choose in the integration to work with their native bridges instead, at the cost of faster messaging from LayerZero.

7.4 Collateral Risk

- Temporary depegs: Expected behaviour is recovery; buffer + RV redemption.
- Persistent failure: If a collateral does not re-peg, RV reflects the shortfall directly. Exposure bounded by vault hard caps.
- Design scope (v1): System is optimised for temporary depegs, not permanent issuer collapse (see section 4.6).

7.5 Strategy / Yield Risk

Scope: Insolvency or smart-contract failure in Morpho, Aave, or Sky.

Controls:

- Strategies may be fully invested; small redemptions may require partial unwinds, which increases gas but does not jeopardise solvency.
- Weekly harvests confirm principal deposits; a mismatch of more than 5 basis points halts new allocations.
- The buffer absorbs any realised loss before impacting RV.

7.6 Operational Risk

- Collateral manager: Can allocate only within pre-set caps and whitelist; cannot change protocol rules.
- Fail-safe principle: The protocol prioritises halting over minting/redeeming against stale or incorrect data.

8. Operations and Governance

gmUSD minimises discretionary control. Protocol behaviour is deterministic; governance and operators act only at the margins to whitelist assets, manage parameters, or pause in emergencies. The following protocol defined roles exist:

1. Vault Manager (Vault) - manages asset allocation across strategies on each collateral vault
2. Price Feed Manager (Controller) - determines the oracle/price feed
3. Vault Manager (Controller) - can add/remove collateral and change collateral vault parameters (each collateral has a single dedicated vault)

4. Fee Manager (Controller) - sets the protocol fee
5. Rebalancing Manager (Controller) - rebalances collateral across vaults
6. Periphery Manager (Controller) - manages swap and distribution contracts
7. Yield Distribution Manager (Controller) - triggers yield distribution
8. Controller Admin (Controller) - upgrades the controller implementation
9. Pause Authority (Controller) - can pause/unpause the protocol in extreme cases

In the V1 implementation, Steakhouse Financial will hold roles 1,5, and 7, with the remaining roles held by the protocol security multisig.

Upgrade Path

- All contract upgrades are subject to a **48-hour timelock**.
- Public diffs and third-party audits are required for each major release.
- Minor parameter changes (caps, harvest interval, α) pass through governance but do not require contract upgrades.

9. Collateral Onboarding

The initial collateral set includes USDC, USDT, and USDS. Only canonical assets on Ethereum L1 could serve as collateral backing for gmUSD. Additional assets may be listed in accordance with the policy below.

9.1 Pass/Fail Eligibility

- An independent USD reference (e.g. Chainlink or other oracle provider) and at least one liquid DEX venue suitable for TWAP pricing feed.
- Observable, stable peg and adequate onchain depth over a 180-day window.
- Contract transparency - canonical contract published; upgrade/admin semantics and freeze/blacklist behaviour documented; protocol addresses not blocked.
- A reasonable public view into how the peg is maintained (mechanism summary, venues relied on, or equivalent).

9.2 Evaluation Dimensions

- Peg mechanism and failure modes.
- Liquidity profile (primary and secondary markets) and routing impact.

- Counterparty/venue dependencies (exchanges, custodians, keeper networks).
- Contract/control surface and incident history.
- Oracle quality, observability and redundancy (multiple provider availability).

9.3 Listing

- Sandbox vaults with conservative per-asset caps and target weights.
- Increase limits only after a trial period with stable observed behaviour
- A global per-asset ceiling applies in v1.

As the protocol matures, additional evaluation dimensions may be considered. In particular, issuers of RWA-backed stablecoins may provide private disclosures on reserves and controls, complementing public data.

10. Roadmap & Future Extensions

gmUSD v1 delivers a fully functional stablecoin with peg defence, yield distribution, and collateral management. Future releases focus on automation, capital efficiency, and expanded safety mechanisms. Timelines are indicative only.

10.1 v1.1 — Usability and Transparency Upgrades

Target timeline: Q1 2026

- Gas-aware routing: Mint/redeem logic chooses the cheapest path for the user (direct vs. swap) if the spread exceeds a defined threshold.
- Public dashboards: as outlined in sections 4.4 and 5.4

10.2 v1.2 — Capital-efficiency Upgrades

Target timeline: Q2 2026

- Time-weighted yield distribution: Rewards allocated by liquidity-days rather than snapshots, reducing manipulation.
- Mint proxies on rollups: Users can initiate gmUSD mints on L2; collateral locked and finalized on L1.

10.3 v2.0 — Risk & Treasury Upgrades

Target timeline: Q3 2026

- Automated rebalancing: Onchain trigger and routing of rebalancing swaps replace the manual multisig process.
- Automated buffer overflow release: In v1, surplus above the 1% buffer target is released manually; in v2 this process becomes automated, ensuring consistent routing of excess value.

10.4 v2.x — Strategic Extensions

Target timeline: TBC

- Direct issuer lanes: Onchain depegs of USDC/USDT with a percentage change of≥1% can be closed via direct redemption/mint with issuers, thereby restoring balance.
- Native L2 minting: Lightweight vaults on supported rollups accept L2-native collateral, batch-bridged to L1 for canonical issuance.
- Solver/intent integration: gmUSD becomes a first-class asset in intent-based routing (e.g. CoW, Anoma), enabling zero-hop cross-chain swaps