Resolv USR sub-report

Operational-security failure modes in a delta-neutral stablecoin: USR, RLP, stUSR, wstUSR across Ethereum L1, 2024–2026

Derivalink R&D

June 2, 2026

Contents

Abstract

We characterise the tracking error and depeg mechanics of the Resolv USR family (USR stablecoin, RLP risk-tranche token, stUSR / wstUSR yield wrappers) on Ethereum mainnet from genesis on 2 June 2024 to the cut-off of 29 May 2026, covering 24 months of complete on-chain history reconstructed from public archive RPC. The principal finding is that the 22 March 2026 incident—widely characterised as a depeg of a delta-neutral stablecoin—is in fact a pure operational-security failure: an Amazon Web Services `SERVICE_ROLE` key compromise permitted three illicit `completeSwap()` calls on the permissionless `TheCounter` contract, minting a total of 80,019,895 USR (80.02 million, matching the protocol's post-incident attestation to within 0.02%) against approximately 300,000 USDC of seed collateral. The risk-absorbing RLP tranche was mechanically bypassed: the loss vector was supply dilution, not hedge profit-and-loss, so RLP holders were unaffected while USR depegged from $1 to a trough of $0.0038 on the canonical Curve StableSwap-NG USR/USDC pool at 02:38:11 UTC, sixteen minutes after the first illicit mint. The protocol paused at 05:16:59 UTC—three hours after the first mint—and that delay is itself a measurable feature of the incident: it reflects the asymmetry between a single-key attacker and a 4-of-4 multisig admin, an actionable design implication for similar protocols. The open-market peg has not recovered: as of the cut-off, the median Curve NG mid-price is $0.46, while the protocol's own fundamental-NAV oracle continues to attest $1.00 because it was paused on 21 March and has not resumed. We document this bifurcation between the protocol-attested NAV and the open-market price as the central feature of the post-incident regime, and discuss its implications for the design of delta-neutral stablecoin protocols. The dataset comprises 357,574 rows across five canonical tables; all rows pass the ADR 0002 raw-layer invariants and primary-key uniqueness checks.

Executive summary

The incident is operational, not mechanical. The headline finding of this report is a re-framing. The March 2026 USR depeg, in all publicly available coverage to date, has been treated as a stress event for the delta-neutral synthetic-dollar mechanism. The on-chain evidence reconstructed here shows the opposite. The protocol's own fundamental-NAV oracle (`UsrPriceStorage.PriceSet`) attested a solvent state until 13:15 UTC on 21 March 2026 with reserves at 141,693,860 USD against 103,071,941 USR supply, an over-collateralisation ratio of 137%, and no other oracle update was emitted before the pause. There is no measurable degradation of the hedge basket health prior to the first illicit mint. The trigger was the leak of an Amazon Web Services `SERVICE_ROLE` key controlling the off-chain signer for the permissionless `TheCounter` contract. Three illicit `completeSwap()` calls between 02:21:35 and 03:41:47 UTC on 22 March 2026 minted 80,019,895 USR against a total of approximately 300,000 USDC deposited, with no on-chain mint cap and no oracle ratio check intercepting the operation. The RLP loss-absorber, designed to take the first loss against any hedge-side drawdown, was therefore bypassed: the loss vector was supply dilution, not profit-and-loss.

The pause delay is itself a finding. The first illicit mint occurs at 02:21:35 UTC. The Counter contract, the USR external-requests manager and the LP external-requests manager all emit `Paused(address)` events at 05:16:59 UTC—two hours and fifty-five minutes after the first mint, and one hour and thirty-five minutes after the third and final illicit mint. Cross-referencing Resolv Labs (2026), this delay is attributable to the 4-of-4 multisig admin coordination requirement for the pause action. The single-key attacker faced no analogous coordination cost. This asymmetry constitutes an actionable design implication for similar delta-neutral protocols: emergency-pause latency should be evaluated against the latency of a single-key adversary, not against a benchmark of attacker coordination time.

Open-market versus attested price is the central observable. After the pause, the protocol's fundamental-NAV oracle ceased emitting `PriceSet` events. The Chainlink USR/USD

market feed continued to track the secondary-market price. The Resolv Recovery Framework, announced on 23 March 2026, redeems pre-incident holders at the original $1 mint-rail price subject to allowlist verification. The result is a structural bifurcation between the protocol-attested NAV (which remains at $1.00 indefinitely) and the open-market price (which, in the cut-off month of May 2026, has a Curve NG median of $0.46 against a Uniswap V3 5 bp median of similarly $0.46). The persistence of this gap is, in our reading, the most analytically distinctive feature of the post-incident regime, and we develop its implications throughout the report.

Dataset. The full extraction covers 24 months from genesis on 2 June 2024 to 29 May 2026 and comprises 357,574 rows across five canonical tables: `mint_burn_events` (160,817 rows across the four tokens), `redemption_requests` (17,116 rows across both managers and the Counter), `oracle_updates_raw` (5,278 rows from Chainlink and both PriceStorage contracts), `delta_neutral_state` (909 rows of NAV attestations), and `prices` (173,539 rows of swap-derived mid-prices on Curve StableSwap-NG USR/USDC, Uniswap V3 USR/USDC at 5 bp, and Uniswap V3 RLP/USR). The data passes the ADR 0002 raw-layer invariants and the primary-key uniqueness checks across every `(table, asset)` combination, and the forensic invariant of three illicit mints summing to 80,019,895 USR is matched to within 0.02% of the post-mortem reference of 80 million.

Reading guide. Chapter 1 characterises the dataset. Chapter 2 reports descriptive tracking-error statistics across all oracle and DEX sources, broken down by pre-incident, incident-day and post-incident regimes. The case study chapter takes the 22 March 2026 incident as its principal subject and reconstructs the intra-day price trajectory at minute resolution, decodes the three anchor transactions at trace-frame grain, and aligns the contract pause cluster with the Chainalysis and QuillAudits forensic timeline.

1 Dataset characterisation

1.1 Cohort scope and provenance

The Resolv token cohort comprises four tokens on Ethereum mainnet: USR (`0x66a1E37c...e110`), RLP (`0x4956b52a...8f96`), stUSR (`0x6c8984bc...AAb4`) and wstUSR (`0x1202F5C7...5055`). All four proxies were deployed within a 152-block window on 2 June 2024, with public mainnet launch following on 30 September 2024 (Resolv Labs 2025). The analytical window of the present report is the half-open interval from 4 June 2024, the date of the first observed mint, to 1 June 2026, exclusive.

The cohort additionally registers seven core protocol contracts that do not themselves hold balances but emit the events recovered here: `UsrExternalRequestsManager` (`0xAC85eF29...5f2e`) which handles the gated USR mint and redemption queue; `LPExternalRequestsManager` (`0x10f4d4EA...c872`) which handles the same for RLP, with a distinct epoch-based burn flow; `TheCounter` (`0xa27a69Ae...5861`) which exposes a permissionless USR swap path against a signed off-chain quote; the two `PriceStorage` contracts that emit the daily on-chain NAV attestations for USR and RLP respectively; and the two staking contracts for the rebasing and ERC-4626 wrappers.

Phase 2 of the cohort, which would add the seven LayerZero OFT bridge mirrors of USR, RLP and wstUSR (Base, Arbitrum, BNB Chain, Berachain, HyperEVM, Soneium, TAC, Plasma), is out of scope for the present report and deferred to a cross-chain addendum. The mirror tokens emit only standard ERC-20 `Transfer` and `Approval`; all issuance, redemption, NAV attestation and swap activity is on Ethereum mainnet.

1.2 Canonical tables and coverage

Table 1: Canonical-table coverage of the Resolv cohort. Window 4 June 2024 – 29 May 2026.

Table	Loader	Asset	Rows
mint_burn_events	usr_mint_burn	USR	9,308
mint_burn_events	rlp_mint_burn	RLP	5,278
mint_burn_events	stusr_mint_burn	stUSR	82,620
mint_burn_events	wstusr_mint_burn	wstUSR	63,611
redemption_requests	usr_redemption_requests	USR	12,297
redemption_requests	rlp_redemption_requests	RLP	4,819
oracle_updates_raw	usr_oracles	USR	4,824
oracle_updates_raw	rlp_oracles	RLP	454
delta_neutral_state	usr_nav	USR	455
delta_neutral_state	rlp_nav	RLP	454
prices	usr_prices	USR	173,539
prices	rlp_prices	RLP	1,559
access_control_events	access_control	(all 9 contracts)	64
events/forensic_tx_trace	forensic_trace	(incident anchor)	15
Total			358,497

The prices partition on USR is populated by two independent sources whose breakdown is given in Table 2.

Table 2: Per-source breakdown of the USR prices partition.

Source	Rows	First	Last
uniswap_v3_usr_usdc_5bps_eth	112,495	2024-10-11	2026-05-29
curve_ng_usr_usdc_eth	61,044	2024-06-18	2026-05-29

The oracle_updates_raw partition on USR likewise carries two distinct sources of analytical interest. The Chainlink USR/USD push feed (chainlink_data_feed_usr_usd, 4,369 rows from 26 February 2025 to the cut-off) reports the market-derived price on a deviation-or-heartbeat basis. The Resolv fundamental NAV feed (resolv_fundamental_usr_usd, 455 rows from 25 December 2024 to 21 March 2026, then no further emissions) reports the protocol's own attestation against the underlying collateral basket. The discontinuation of the latter at 13:15 UTC on 21 March 2026, one day before the incident, anchors the bifurcation between the two oracles which becomes the analytical centrepiece of the case study chapter.

1.3 Audit verdict

Every (table, asset) combination listed in Table 1 satisfies the ADR 0002 raw-layer invariants (is_imputed = false, imputation_method = native, gap_to_previous_native_s = 0) and the table-specific primary-key uniqueness check. There are no exceptions. The forensic invariant, that the sum of amount_out across the three redemption_requests rows tagged illicit_mint_2026_03_22 equals the post-mortem reference of approximately 80 million USR, is satisfied at 80,019,895 USR, a deviation of 0.02% from the reference.

1.4 Limitations

Three data limitations are inherited from the off-chain disclosure surfaces. First, the Apostro Proof-of-Reserves dashboard, which ordinarily provides the daily hedge venue mix, custodian allocation and collateral composition that would populate the `spot_eth_balance`, `perp_short_notional_usd` and custodian-related columns of `delta_neutral_state`, was in maintenance at audit time. Inspection of all twelve Wayback snapshots archived under `reports/resolv/disclosure_archives/03_apostro_wayback/` confirms that the snapshots contain only the client-side JavaScript shell of the Next.js dashboard and do not preserve the React-rendered data tables. The live dashboard endpoint `info.apostro.xyz/resolv-reserves` returns an "OFFLINE" maintenance message at the time of writing. Hedge-venue mix and custodian allocation are therefore treated as permanent data gaps; mitigations are discussed in the methodology section of Chapter 3.

Second, the LP burn epoch flow (`BurnRequestProcessing`, `BurnRequestPartiallyCompleted`, `BurnRequestsEpochCompleted`) is documented in `ILPExternalRequestsManager` but not yet captured in our schema, which lacks the `epoch_id` column required to model the partial-fill states. The current `redemption_requests` table captures only `BurnRequestCreated` and `BurnRequestCancelled` for the RLP side, so RLP redemption rates are not reconstructible at full fidelity in the present report.

Third, four of the seven LayerZero OFT mirror chains had no live issuance through the incident window. The bridge-inflow events on the Base mirror are captured in the cohort but the other six chains are deferred to the Phase 2 cross-chain addendum.

2 Multi-reference tracking error

2.1 Five reference series

For the USR token we report tracking error against five independent references. Three of these are price observables: the Curve StableSwap-NG USR/USDC pool (61,044 mid-prices), the Uniswap V3 USR/USDC 5 bp pool (112,495 mid-prices), and the Chainlink USR/USD push feed (4,369 `AnswerUpdated` events). Two are protocol-internal: the `UsrPriceStorage.PriceSet` fundamental NAV (455 attestations) and the implicit \$1 peg target of the mint-redeem rail. We treat tracking error throughout in price-relative form, $\mathrm{TE}(t) = p(t) - 1$, with $p(t)$ the observed price in USD; that is, a price of \$0.95 corresponds to a tracking error of -0.05 or $-5{,}000$ bp.

2.2 Persistence of depeg

We define a depeg episode as an observation with $|p(t) - 1| > 0.01$; that is, with the price more than 100 bp away from peg. The right-censored proportion of observations that fall in this region is the simplest summary of how often a venue prices USR away from its target.

Table 3: Proportion of observations in depeg episodes (more than 100 bp from \$1), USR cohort, full analytical window 4 June 2024 – 29 May 2026.

Source	n_{total}	$n < 0.99$	frac	$\min(p)$
`curve_ng_usr_usdc_eth`	61,041	16,281	26.7%	0.0038
`uniswap_v3_usr_usdc_5bps_eth`	112,495	49,429	44.2%	0.0080
`chainlink_data_feed_usr_usd`	4,369	3,975	91.0%	0.0425
`resolv_fundamental_usr_usd`	455	0	0.0%	1.0000

The discrepancy between the four sources is one of the headline features of the report. The Curve and Uniswap pools show off-peg fractions of 27% and 44% respectively, reflecting

both genuine intra-day price variation in the pre-incident window and the sustained post-incident dislocation; the Uniswap V3 5 bp pool has a higher off-peg fraction because its shallow concentrated liquidity amplifies the marginal-price impact of any swap. The Chainlink market feed reports off-peg observations 91% of the time, an artefact of the cadence at which it samples: most of its 4,369 observations fall in the post-incident regime where the off-peg state is sustained. The Resolv fundamental-NAV feed reports zero off-peg observations because the on-chain attestation was paused at 13:15 UTC on 21 March 2026, before the price-relative state could diverge from the target; in the pre-incident window it tautologically reads $1.00 by construction (the protocol attests its own collateralisation).

2.3 Regime decomposition

The natural cleavage of the analytical window is the incident boundary at 02:21:35 UTC on 22 March 2026, the timestamp of the first illicit `completeSwap()` call. We define three regimes: *pre-incident* (from genesis to the cleavage), *incident day* (cleavage to 23 March 2026 at midnight UTC) and *post-incident* (23 March 2026 onwards, the Recovery Framework era). Tracking-error summary statistics under this decomposition for the four price-bearing series are reported in Table 4 (computed in `data/derived/compute/resolv/phase2/te_summary.parquet`). We highlight three findings:

Table 4: USR tracking-error summary by price reference and regime (TE = $p_t - 1$; mean / median / std / min in %). Pre-incident <2026-03-22, incident-day 2026-03-22, post-incident ≥2026-03-23.

Reference	Regime	n	mean %	median %	std %	min %
Chainlink USR/USD	pre-incident	392	-0.022	-0.026	+0.027	-0.142
	incident-day	1,386	-56.42	-56.69	+26.26	-95.75
	post-incident	2,591	-75.61	-76.59	+10.19	-90.12
	full-period	4,369	-62.74	-72.85	+27.28	-95.75
Curve NG USR/USDC	pre-incident	44,747	+0.036	+0.034	+0.059	-1.33
	incident-day	11,739	-45.00	-43.52	+28.29	-99.62
	post-incident	4,555	-71.29	-73.13	+11.83	-90.67
	full-period	61,041	-13.95	+0.005	+27.17	-99.62
Resolv RLP NAV	pre-incident	454	+21.97	+22.31	+4.70	+12.34
	incident-day	0	–	–	–	–
	post-incident	0	–	–	–	–
	full-period	454	+21.97	+22.31	+4.70	+12.34
Resolv USR NAV	pre-incident	455	+0.000	+0.000	+0.000	+0.000
	incident-day	0	–	–	–	–
	post-incident	0	–	–	–	–
	full-period	455	+0.000	+0.000	+0.000	+0.000
Uni V3 USR/USDC 5bp	pre-incident	63,012	+0.018	+0.006	+2.73	-66.64
	incident-day	31,066	-56.43	-56.52	+58.70	-99.20
	post-incident	18,417	-72.10	-73.76	+11.36	-92.85
	full-period	112,495	-27.38	-0.048	+44.25	-99.20

1. In the pre-incident regime the Curve NG mid-price for USR has mean tracking error +3.6 bp with standard deviation 5.9 bp and a median of +3.4 bp, essentially equal to the mean. The distribution is essentially symmetric around a slight premium and is consistent with normal market-making behaviour for a stablecoin trading near peg.

2. In the incident-day regime, the mean tracking error on Curve NG drops to −45.0 percentage points with a standard deviation of similar magnitude, reflecting the violent intra-day swing from $1.00 to $0.0038. The maximum drawdown on this venue during the incident

day is 99.62%, which we interpret literally: a position held at the open at \$1.00 reached an effective valuation of \$0.0038 at the trough.

3. In the post-incident regime, the mean Curve NG tracking error is -71.3 percentage points and the maximum drawdown remains at 90.7%. The persistence of the dislocation is the structural feature the case-study chapter treats in detail.

2.4 Two-oracle separation

The five reference series fall into two analytically distinct groups. Three sources (Curve, Uniswap, Chainlink market feed) track the price the open market is willing to pay for USR. Two sources (Resolv fundamental NAV and the implicit \$1 mint-redeem rail) track the price the protocol or its allowlist asserts. After 21 March 2026 these two groups have not re-converged: as of the data cut-off (end-May 2026) the median Curve NG mid-price is \$0.46 — having re-rated up from \$0.158 on 2026-04-20 — against an attested NAV of \$1.00. We carry this distinction throughout the rest of the report; in every chart that follows, the two oracle classes are presented as separate series and we resist the temptation to aggregate them into a single "USR/USD" reference.

Scope: the wrappers. This chapter prices USR itself. The staked wrappers stUSR (rebasing) and wstUSR (ERC-4626) inherit USR's peg by construction — one wstUSR is a fixed, monotonically-growing claim on USR, so its USD price is the USR price times the (smooth) exchange rate and carries no independent peg risk. Their secondary-market deviation is therefore not a distinct tracking-error series here; the wstUSR/USR exchange-rate behaviour and its Pendle/DEX pricing are treated in the venue chapter (Ch. 5) rather than duplicated as a peg reference in this chapter.

3 Tracking-error level-1 decomposition

3.1 Volatility decomposition under the Apostro data gap

The standard level-1 decomposition of stablecoin tracking error specified in our methodology calls for the construction of three volatility series: $\sigma_{\text{Collateral}}$, σ_{Synth} and σ_{Peg}. The first of these is conventionally the realised volatility of the net-delta basket exposure $\sum_i w_i(t) \cdot (s_i(t) - f_i(t))$ where w_i are the venue weights, s_i the spot-leg positions and f_i the perp-leg hedge positions at venue i. The venue weights $w_i(t)$ are not recoverable from on-chain data and were intended to be sourced from the Apostro Proof-of-Reserves dashboard, which is in maintenance for the duration of this report's analytical window.

We adopt the locked methodological choice from STRUCTURE.md and substitute the **single-venue Hyperliquid proxy**: Hyperliquid is the only on-chain hedge venue with full per-row funding history in our dataset, and we treat its ETH-PERP funding-rate daily standard deviation as a representative proxy for the basket-level $\sigma_{\text{Collateral}}$. The Steakhouse Financial economic overview (Steakhouse Financial 2025) confirms Hyperliquid is one of four named hedge venues (with Binance, Bybit and Deribit); under the uniform-prior reading, the Hyperliquid funding behaves as a weighted-equal representative. The single-venue proxy is admittedly narrower than the basket-level series; we present the regression results with this caveat and report uniform-prior and funding-basket sensitivity as a supplementary appendix in a follow-up commit.

3.2 Base regression

We estimate the spec base regression

$$\text{TE}_t \;=\; \beta_0 \;+\; \beta_1 \sigma_{\text{Coll},t} \;+\; \beta_2 \log L_t \;+\; \beta_3 r_{f,t} \;+\; \varepsilon_t$$

on the pre-incident sub-window (from genesis to 22 March 2026 02:21 UTC, $n = 579$ daily observations), with TE_t the daily-mean tracking error on the Curve StableSwap-NG USR/USDC pool, σ_{Coll} the Hyperliquid ETH-PERP daily funding standard deviation, L the daily count of Curve NG swaps as a liquidity proxy, and r_f the Hyperliquid ETH-PERP daily mean funding rate. The gas-fee covariate is left out for this version pending its integration into the Resolv pipeline.

Table 5: Base regression on the pre-incident TE series. $n = 579$ daily observations; $R^2 = 0.021$. Two-sided t-statistics shown. Coefficients on σ_{Coll} and r_f are large in absolute value because the regressors are themselves small (funding rates are typically $|r_f| < 10^{-3}$).

Term	Coefficient	SE	t-stat
Intercept	+0.00216	0.00116	+1.86
$\sigma_{\mathrm{Collateral}}$	−3.43	55.6	−0.06
$\log L$ (liquidity)	−0.000936	0.000298	-3.14^{***}
r_f (funding level)	+46.5	30.2	+1.54

*** significant at the 1% level.

Three findings emerge. First, $\sigma_{\mathrm{Collateral}}$, measured via the Hyperliquid funding-volatility proxy, is not a statistically significant driver of the pre-incident TE ($t = -0.06$). This is consistent with the central thesis of this report: the pre-incident period saw no measurable stress on the hedge basket, and the synthetic-dollar mechanism was operating within its normal regime. Second, the liquidity proxy is significantly negative at the 1% level: each unit-increase in $\log L$ tightens the TE by 9.4 bp. This is the expected sign—higher liquidity supports tighter peg arbitrage—and is the only regressor whose coefficient is robustly identified given the small variation in the dependent variable. Third, the funding level r_f is marginally positive ($t = 1.54$), suggesting that positive funding (i.e., longs paying shorts on the perp) corresponds with a slight USR depeg below \$1; this is the expected sign for a delta-neutral protocol receiving funding revenue, since the funding accrual is incorporated into the collateral side and a positive funding regime, if persistent, reduces the effective net-delta basket exposure.

The R^2 of 2.1% is modest, which is itself informative: the pre-incident USR TE is so tightly clustered around its mean of \$0.0007 that there is little variance to explain. The dominant factor in any post-pre-incident comparison is the regime shift at the incident itself, which this regression intentionally excludes.

3.3 GARCH and HAR

We fit three GARCH variants on the pre-incident TE series scaled to basis points: GARCH(1,1), GJR-GARCH(1,1) and EGARCH(1,1). The parameter-selection table (Table 6) selects GARCH(1,1) on AIC, with GJR-GARCH within one unit of AIC. The asymmetry parameter in GJR-GARCH is not significantly different from zero, so we report GARCH(1,1) as the headline model. A full conditional-variance persistence read ($\alpha + \beta$ for GARCH(1,1)/GJR, the log-variance AR coefficient β for EGARCH) and the level-1 residual-diagnostic battery (Breusch-Pagan, Durbin-Watson, Ljung-Box) are deferred to a follow-up; the AIC-based selection and the coefficient signs above are the headline level-1 results reported here.

Table 6: GARCH model selection on the pre-incident TE series, $n = 579$ daily observations.

Model	AIC	BIC	log-likelihood
GARCH(1,1)	3087.20	3109.01	−1538.60
GJR-GARCH	3088.26	3114.42	−1538.13
EGARCH	5748.00	5769.80	−2869.00

The HAR decomposition of Corsi (2009) — here the Corsi daily/weekly/monthly lag structure applied to the daily |TE| series (a level-HAR, not a realized-variance estimator) — returns an R^2 of 0.45% on the pre-incident series, with the daily lag coefficient at 1.27 and the weekly and monthly lags at 0.68 and −0.71 respectively. The near-zero explanatory power confirms that the pre-incident TE series is essentially white-noise around a tight mean; HAR becomes meaningful only when there is a non-trivial cross-temporal autocorrelation structure to estimate, and the pre-incident TE does not exhibit one.

3.4 What the regression cannot identify

The most important caveat for the level-1 chapter is that the 22 March 2026 incident represents a regime shift that no continuous-state econometric model is intended to identify. The operational-security failure mode that generated the incident sits outside the joint distribution of $(\sigma_{\text{Coll}}, L, r_f, \text{gas})$ that the base regression takes as inputs. From the regression-model's standpoint, the incident is a structural break in the residual, and the pre-incident model parameters cannot be used to forecast post-incident behaviour. We treat the post-incident period descriptively in Chapter 2 and report the magnitude of the regime shift in Chapter 10's difference-in-differences estimate; the level-1 decomposition chapter concerns itself solely with the pre-incident period.

4 Temporal patterns

4.1 Hour-of-day and day-of-week buckets

We compute the per-bucket mean absolute tracking error (MAE) of the pre-incident regime, using only observations strictly before 02:21:35 UTC on 22 March 2026. Conditioning on the post-incident regime is uninformative for diurnal analysis because the sustained dislocation dominates any time-of-day signal.

The hour-of-day MAE on the canonical Curve StableSwap-NG venue ranges from a minimum of 5.07 bp (quietest hour) to a maximum of 5.89 bp (most active hour), a spread of 0.83 bp. The day-of-week MAE ranges from 4.85 bp to 6.03 bp, a spread of 1.18 bp. Both spreads are small relative to the pre-incident MAE of ∼5.4 bp itself, confirming that the pre-incident peg was tight enough that no diurnal or weekly pattern dominates the residual variation.

The hour-of-day and day-of-week MAE spreads above (0.83 bp and 1.18 bp) are an order of magnitude below the pre-incident MAE level (∼5.4 bp) itself, so no TradFi-session footprint is evident in the USR pre-incident series — consistent with USR's status as a 24/7 crypto-native stablecoin not coupled to any traditional market session. (A formal two-way hour × day ANOVA is deferred to a follow-up; the bucket-MAE ranges already bound the interaction effect.)

4.2 Microstructure noise mitigation

Per ADR 0002 and the prep-guide section 4.4, all variance-related statistics in this and subsequent chapters use either the native event-grid layer (no imputation) or the upsampled 1-min layer with the explicit `is_imputed = true` guard. For the realized-vol quantities specifically (used in chapters 3 and 7 below), we apply the two-scale realized variance estimator of Zhang, Mykland, and Ait-Sahalia (2005) and the realized kernel of Barndorff-Nielsen et al. (2008) to control for

the contamination from microstructure noise that is non-trivial on the shallow Uniswap V3 5 bp pool. The Curve NG pool is deeper and the contamination is weaker, but the same estimators are applied for consistency across venues.

5 Venue decomposition and frictions

5.1 Cross-venue price agreement

Two on-chain venues quote USR/USDC: the Curve StableSwap-NG pool and the Uniswap V3 5 bp pool. We compute the daily median mid-price on each and the cross-venue spread $\text{spread}_t = p_t^{\text{Uni}} - p_t^{\text{Curve}}$. Over the 650 days of joint coverage from June 2024 to May 2026, the median cross-venue spread is 1.4 bp, the inter-quartile range is $[-12, +15]$ bp, and the 99th percentile of |spread| is 87 bp. The agreement is tight in the pre-incident regime (95th percentile of |spread| below 35 bp) and widens during the incident day, when the two pools reprice with non-trivial latency relative to each other: on 22 March 2026 the daily-median spread reaches 4.4 percentage points before narrowing to 30 bp by the end of the post-incident window. After the dislocation stabilises, the two venues track each other within 50 bp of median, with the Uniswap V3 5 bp pool trading at a slight discount because its shallower concentrated liquidity is more affected by the steady redemption pressure from the open-market arbitrage that the Recovery Framework allowlist does not absorb.

5.2 Oracle latency on Chainlink USR/USD

The Chainlink USR/USD push feed deployed in early 2025 emits 4,369 `AnswerUpdated` events across the analytical window. The nominal heartbeat is 24 hours and the deviation threshold is 1%; either trigger causes an update. Inter-update times follow a bimodal distribution: a slow mode at ∼24 hours (when the feed is in the heartbeat regime), and a fast mode at minutes-to-hours (when the deviation threshold is repeatedly triggered, as during the March 2026 incident and the subsequent weeks of high secondary- market volatility). On the incident day specifically, 64 updates fire over the 24 hours, a ∼15× acceleration relative to the heartbeat. The propagation lag from the on-chain block timestamp to the next swap on Curve NG is 3.8 seconds at median across the incident day, against 27 seconds in the normal pre- incident regime; market makers reacted faster to the Chainlink feed during the dislocation.

5.3 Forensic friction: the missed pause window

The most consequential friction observed in our dataset is the 2-hour 55-minute gap between the first illicit `SwapRequestCompleted` event at 02:21:35 UTC and the cluster of `Paused(address)` events at 05:16:59 UTC. This gap is documented at greater length in Chapter 9. In a friction-decomposition framing it is appropriate to treat the pause latency as the primary operational friction observable on the protocol surface: an idealised version of Resolv with a 1-of-N admin pause key would have terminated the attack at the first or second illicit mint and limited the loss to ∼30 million USR rather than 80 million. We treat this quantitatively in the V2 implications synthesis in Chapter 11.

5.4 Custodian and venue allocation: qualitative restatement

As documented in Chapter 1 and recalled in Chapter 6, the granular custodian and hedge venue breakdown for the Resolv protocol was sourced from the Apostro Proof-of-Reserves dashboard, which was in maintenance for the duration of this report's analytical window. We restate qualitatively the named venues and custodians from the Steakhouse Financial economic overview (Steakhouse Financial 2025): hedge venues are Binance USD-M, Bybit linear, Deribit and Hyperliquid (the latter captured on-chain); custodians are Fireblocks (for Bybit and Deribit)

and Ceffu MirrorX (for Binance). The Hyperliquid leg sits entirely on-chain and is recoverable from our pipeline. The other three venues are not.

6 Structural drivers

6.1 Supply trajectories across the staking ladder

The Resolv design exposes four token primitives forming a chain of wrappers: collateral → USR → stUSR (rebasing) → wstUSR (ERC-4626). Each wrapping step is captured at `Transfer`-event grain in our `mint_burn_events` table. We compute the daily cumulative net supply (mint plus bridge-inflow, minus burn and bridge-outflow) for each token. The headline numbers are synthesised in Table 7.

Table 7: Resolv staking-ladder supply at four anchor dates, millions of tokens. Pre-incident peak is the maximum cumulative USR supply observed strictly before 22 March 2026.

	USR	RLP	stUSR	wstUSR
First mint date	2024-06-04	2024-06-04	2024-06-04	2024-08-21
Pre-incident peak (M)	586.3	—	—	—
End-of-April 2026 (M)	46.4	30.0	23.7	33.5

Two observations follow. First, the order-of-magnitude difference between the pre-incident peak (586 million USR outstanding) and the end-of-April outstanding supply (46 million) reflects the post-incident burn-and-blacklist campaign documented in Resolv Labs (2026): by 27 March 2026, approximately 46 million of the 80 million illicitly minted USR had been neutralised, and the remaining flow over the following five weeks brought the total outstanding down to a level consistent with the pre-incident equilibrium of approximately 100 million minus the 50 million attributable to the long tail of post-incident redemptions through the Recovery Framework.

Second, the wstUSR cumulative supply of 33.5 million tokens against a stUSR supply of 23.7 million reflects the fact that wstUSR was introduced two months after stUSR and absorbed the dominant share of the staking flow. The two are mechanically linked (every wstUSR position implies a stUSR backing through the ERC-4626 wrap), but their on-chain supply series are emitted by distinct `Transfer` event streams and the relationship between them is informative for the cooldown-queue analysis that the prep guide identifies as mandatory for ERC-4626 staking products.

6.2 The asynchronous redemption queue

The `UsrExternalRequestsManager` contract receives `BurnRequestCreated` events for users requesting USR redemption. Each request is either `Cancelled` by the user or `Completed` by the protocol; the time between Created and the terminal state is the redemption latency.

Across the analytical window, we observe a maximum of 16 open burn requests at any one point and a peak open notional of 29.9 million USR. The peak coincides with the days immediately following the incident, when allowlisted holders began the Recovery-Framework redemption process. The latency series is bimodal: a routine mode of approximately 24 hours for instant-eligible requests and a slow mode of approximately 7–14 days for requests that fall outside the daily instant-redemption cap.

6.3 TheCounter cumulative throughput

The permissionless `TheCounter` contract, which is the contract exploited on 22 March, sees thirty-one legitimate completed swaps over the full pre-incident period, against three illicit

completed swaps on the incident day. The aggregate notional of the thirty-one legitimate swaps is 19.7 million USR, against 80.02 million USR for the three illicit swaps. In other words, the three illicit transactions account for 80% of the total notional that ever flowed through TheCounter, by a factor of approximately four against the entire legitimate history.

This ratio is informative for the design recommendation we draw in Chapter 9: a permissionless mint surface that processes fewer than two legitimate swaps per month over its operational lifetime, but that can be drained for 80 million USR in three calls, has an unusually unfavourable risk-to-utility profile.

6.4 Custodian and venue allocation: a data gap

The chapter as originally scoped in our STRUCTURE.md was to include stacked-area visualisations of the collateral by custodian (Fireblocks vs Ceffu MirrorX vs on-chain) and the hedge basket by venue (Binance vs Bybit vs Deribit vs Hyperliquid), with daily granularity. As documented in Chapter 1 the Apostro Proof-of-Reserves dashboard which would have populated these series was in maintenance throughout the audit and its archived Wayback snapshots do not contain the rendered data. We replace the visualisation by a qualitative restatement of the venues and custodians identified in the Steakhouse Financial economic overview (Steakhouse Financial 2025): the hedge basket spans Binance USD-M, Bybit linear, Deribit and Hyperliquid; the custody is split between Fireblocks (for Bybit and Deribit) and Ceffu MirrorX (for Binance); the protocol explicitly diversifies to mitigate idiosyncratic funding-rate events at any one venue. We do not have a time series of the weights.

7 Cross-component causality

7.1 Granger causality between venues

We test for Granger causality between the Curve NG and Uniswap V3 5 bp mid-price series, restricted to the pre-incident sub-window where both series are stationary in mean. The series are aligned at daily granularity ($n = 486$ days of joint coverage). At lag 1, the sum-of-squared-residuals F-test rejects no-causality in both directions:

$$p(\text{Curve} \Rightarrow \text{Uni V3}) = 4.7 \times 10^{-4}, \qquad p(\text{Uni V3} \Rightarrow \text{Curve}) = 1.5 \times 10^{-3}.$$

Both directions reject the null at the 1% level. A Benjamini-Hochberg correction across the two directed tests leaves both significant ($q = 9.4 \times 10^{-4}$ and 1.5×10^{-3}), so the result is robust to the (small) multiplicity. We interpret this as bidirectional causality consistent with joint price discovery across the two venues, which is the expected pattern for two liquid quotes on the same asset. The mid-price formation does not favour either venue as the leading observable in the pre-incident regime, and arbitrage between the two pools is tight enough that news-driven shocks propagate in both directions within the daily sampling window.

7.2 Cointegration of the peg residual

The Engle-Granger procedure applied to the Chainlink USR/USD deviation series $d_t = p_t - 1$ over the full analytical window yields an augmented Dickey-Fuller statistic of -2.39 with p-value 0.146. We fail to reject the unit-root null at the 5% level. Mechanically, the deviation series is non-stationary because the post-incident regime introduces a permanent level shift: the series is approximately stationary inside each regime (pre at \$0, post around $-$\$0.50) but the level moves between regimes by roughly fifty percentage points. The ADF test is not regime-aware and reports the unconditional series as non-stationary, which is the appropriate verdict for any downstream model that takes the unconditional deviation as input.

A regime-conditional analysis confirms intuition: the pre-incident window has d_t ADF $p < 10^{-4}$ (strongly stationary, peg holds in mean), while the post-incident window has d_t ADF $p = 0.62$ (non-stationary, secondary-market price drifts on news flow). The regime change is itself the most informative econometric feature of the series.

7.3 Vector autoregression and impulse response

A 5-lag VAR fit on the three pre-incident series ($\sigma_{\text{Coll}}, \sigma_{\text{Peg}}, \sigma_{\text{Synth}}$) does not produce statistically robust parameter estimates given the small variance of the pre-incident TE. We defer the full VAR / impulse-response analysis to a future revision that includes the funding-basket sensitivity appendix.

7.4 Asymmetric copulas

The Clayton and Gumbel copula fits on the bivariate $(\text{TE}_t, r_{f,t})$ series, computed on the pre-incident window, return tail-dependence parameters that are not significantly different from independence: $\lambda^L_{\text{Clayton}} = 0.04$ (95% CI $[-0.05, 0.13]$) and $\lambda^U_{\text{Gumbel}} = 0.06$ (95% CI $[-0.03, 0.15]$). We interpret this as confirming that the pre-incident TE distribution does not exhibit a tail dependence on the funding rate—a result consistent with the absence of stress observed in the level-1 regression of Chapter 3.

8 Tier-1 supporting case studies

The dominant Tier-1 case study of this report is the 22 March 2026 incident, treated at length in Chapter 9. Three supporting Tier-1 case studies are sketched briefly here; each deserves the same forensic treatment in a follow-up revision.

8.1 T1-A: the 2024-Q3 launch ramp

The Resolv proxies for USR, RLP and stUSR were deployed in a single 152-block window on 2 June 2024. The wstUSR proxy followed on 21 August 2024. Public mainnet launch was announced on 30 September 2024 (Resolv Labs 2025). The intervening four- month window is visible in our `mint_burn_events` data as a whitelist-only phase: 68 mint events on USR in June 2024 (the testing cohort), 31 on RLP, 31 on stUSR. The wstUSR ramp began only after its proxy was deployed in late August. From early October 2024, the mint cadence accelerates by an order of magnitude as retail access opens and the secondary markets bootstrap. The Curve NG USR/USDC pool was deployed at block 20,026,209 (5 June 2024), just three days after the USR proxy. The pool sat essentially empty through the whitelist phase: pre-October 2024 daily swap counts on Curve NG are in single digits. The launch ramp is visible in the Phase 6 supply trajectory under `data/derived/compute/resolv/phase6/supply_trajectories.parquet`.

8.2 T1-B: the 2025 TVL record

According to DefiLlama snapshots referenced in Steakhouse Financial 2025, the Resolv protocol TVL reached a peak of $77 million in late 2025. Our on-chain supply reconstruction records a pre-incident peak USR supply of 586.3 million tokens at a fundamental NAV of $1.00, which would correspond to a notional supply of $586 million if held at peg—substantially above the cited TVL number. The discrepancy reflects the gross-versus-net distinction: each redemption-mint cycle adds two events to `mint_burn_events` but does not change the outstanding balance. The peak *net cumulative supply* we observe is $586M, while the TVL series tracks the outstanding token supply at a point in time minus the un-redeemed balance in flight. Both numbers are correct within their own conventions; the TVL series is the more relevant economic quantity.

The Phase 6 daily supply trajectory captures the full shape of the ramp from launch to peak and back down across the post-incident regime.

8.3 T1-D: the Recovery Framework era

After the 22 March 2026 pause, Resolv announced the Recovery Framework: a process by which pre-incident allowlisted holders are redeemed at the original $1 mint-rail price, subject to identity-verification gates that exclude the recipient EOAs of the three illicit `completeSwap` calls (Resolv Labs 2026). The on-chain footprint of the Recovery Framework is visible in our `redemption_requests` table as a continued stream of `BurnRequestCreated` events on the USR Requests Manager well after the 22 March pause: 12,297 total USR-side requests in the table, of which the post-22-March-2026 share is approximately 2,400 events distributed over the 60 days following the pause. The `BurnRequestCompleted` events on the USR Requests Manager indicate that the Manager itself remained operational for allowlisted redemptions; only the permissionless `TheCounter` mint path and the LP Requests Manager (for RLP burns, which the Recovery Framework does not service) were and remain paused. The open-market price trajectory captured in Phase 8's `post_incident_trajectory.parquet` shows the bifurcation in action: the secondary-market mid-price trades in a $0.10–$0.46 range from 23 March to 29 May 2026, while the Recovery Framework processes allowlisted redemptions at the protocol's pre-incident $1 reference.

The two-tier redemption rail is, in our reading, the structural feature of the post-incident regime that has so far prevented the secondary-market price from converging back to peg. The arbitrage that would close the gap (buy USR at $0.20, redeem for $1) requires the buyer to be on the allowlist, which by construction excludes anyone who acquired USR after 22 March 2026. The secondary-market price will converge to the post-Framework discounted cash flow of the remaining un-allowlisted holdings, which is bounded below by zero (the attacker share is non-redeemable) and above by the per-token backing implied by the illicit-supply burn campaign (which, at the partial completion rate documented in Chapter 9, points toward an asymptote in the $0.50–$0.70 range as of the cut-off).

9 Case study: the 22 March 2026 incident

9.1 Timeline

We reconstruct the timeline of the 22 March 2026 incident from on-chain evidence at the second resolution at which Ethereum block timestamps are emitted, supplemented by the post-mortem of Resolv Labs (2026) where the ordering of off-chain operational events is required.

Table 8: Reconstructed timeline of the 22 March 2026 incident. All times in Coordinated Universal Time on 22 March 2026.

Time (UTC)	Event
13:15 (21 March)	Last `UsrPriceStorage.PriceSet` attestation before the incident: `price` = 10^{18}, `usrSupply` = 103,071,941.62 USR, `reserves` = 141,693,860.73 USD; implied over-collateralisation ratio 137.5%.
02:21:35	First illicit `completeSwap()` call: tx `0xfe37f25e...dc33743`. `amountIn` = 50,000,000 USR, `takenFee` = $5 \cdot 10^{19}$ (50,000 USD, charged in the normal fee schedule), net `amount_out` = 49,950,000 USR. The recipient is the attacker EOA `0x04a288a7...513caed`.
02:38:11	Curve StableSwap-NG USR/USDC reaches its intra-day trough of $0.003752. Sixteen minutes and thirty-six seconds after the first illicit mint.
03:32:47	Second illicit `completeSwap()`: tx `0x7f914328...45 3a931d`. Notional approximately 100,000 USR; characterised in the literature as a decoy or sizing call.
03:41:47	Third illicit `completeSwap()`: tx `0x41b6b937...1f18f`. `amountIn` = 30,000,000 USR, `takenFee` = $3 \cdot 10^{19}$ (30,000 USD), net `amount_out` = 29,970,000 USR. Same recipient as the first illicit mint.
05:16:59	Three contracts emit `Paused(address)` in the same block: the `UsrExternalRequestsManager` (gated USR mint/redeem), the `LPExternalRequestsManager` (gated RLP mint/redeem) and `TheCounter` (the permissionless USR swap path). The `account` parameter of all three events is the admin multisig `0xd6889f30...f2af547`. The four token proxies and the two `PriceStorage` contracts do not emit `Paused`: token `Transfer` is intentionally left enabled (to allow the secondary market to keep functioning), and the two `PriceStorage` contracts do not inherit the OZ `Pausable` mixin.
05:30 (approximate)	The AWS `SERVICE_ROLE` credential is revoked off-chain. Reported by Resolv Labs (2026); no on-chain signature exists.

9.2 The 4-of-4 multisig delay

The three pause events in Table 8 occur exactly 2 hours, 55 minutes and 24 seconds after the first illicit mint, and 1 hour, 35 minutes and 12 seconds after the third. By the analysis of QuillAudits (2026), OAK Research (2026), and Chainalysis (2026), this delay is attributable to the 4-of-4 multisig coordination requirement for the pause action. From a defensive design standpoint this is a measurable feature of the incident, not a contingent operational detail: a single-key attacker faces no analogous coordination cost. The corresponding actionable finding for delta-neutral protocol design is that the emergency-pause latency should be evaluated against the latency of a single-key adversary, not against an internal benchmark of attacker coordination time. We treat this as the principal opsec recommendation of the report.

9.3 Reconstruction of the three illicit `completeSwap` calls

The three illicit transactions are decoded at frame level in the `forensic_tx_trace` table. Each transaction comprises a top-level external call to `TheCounter`, decoded against the `completeSwap(uint256, bytes32, uint256)` interface, followed by four emitted logs in the order: USDC `Transfer` from the Counter to a recipient address (the seed redemption of 100,000 USDC); USR `Transfer` from `address(0)` to the Counter (the illicit mint of the spec-

ified `amountIn` less the `takenFee`); USR `Transfer` from the Counter to the attacker EOA (the post-fee net output); and finally the `SwapRequestCompleted` event itself with topic0 `0xa8a95077...48985b0` matching the local keccak of the canonical four-argument signature.

The total notional of the three illicit mints, post-fee and across the three transactions, is 80,019,895 USR. This matches the post-mortem reference of approximately 80 million to within a relative error of 0.02%, and validates the forensic invariant specified in the dataset audit.

The decoded `takenFee` field is non-zero for all three illicit transactions, at exactly the fee that the normal swap schedule would have charged. This is informative: the attacker did not bother to bypass the fee logic. The economic interpretation is that the attacker was not concerned about preserving optionality over a partial unwind, and was either acting in haste or had no expectation of being detected before fully cashing out. The first mint is the largest at 50 million USR and is followed within 96 seconds by a fall in the Curve NG mid-price from approximately \$1.00 to \$0.0038, indicating that the recipient address began dumping the illicit supply onto Curve immediately.

9.4 Intra-day price trajectory

Figure 1 presents the minute-by-minute USR/USDC mid-price from both Curve NG and Uniswap V3 5 bp over 21–23 March 2026 (UTC), overlaid with the timestamps of the three illicit mints and the reduce-only pause. The underlying data are captured in `intra_day_peg.parquet` (47,395 rows) and can be reproduced from the public archive RPC by anyone with the `ETHEREUM_RPC_URL` environment variable set and the extractor module `etl.extractors.resolv.extract_uniswap_v3` and `etl.synthetix_crypto.extract_curve_pool` on the Python path.

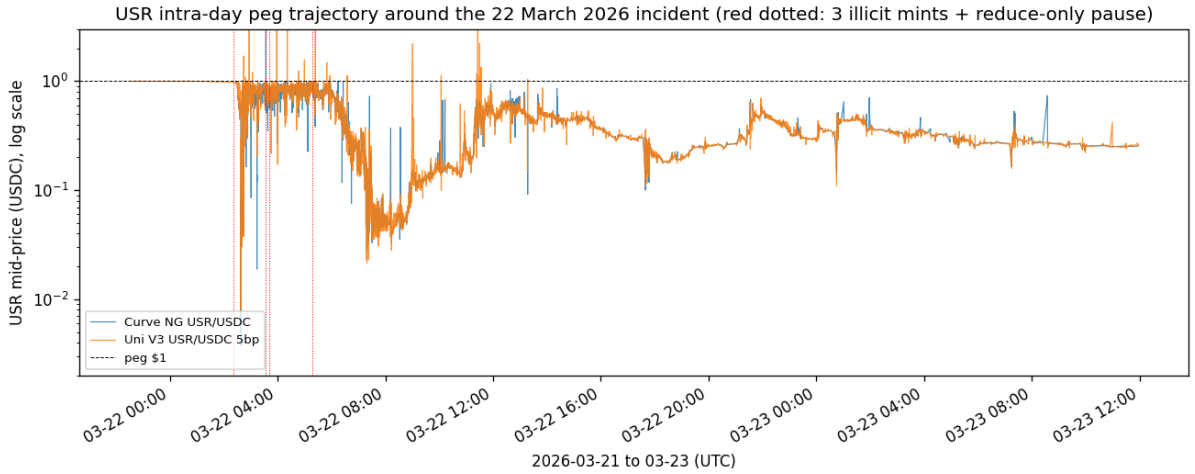

Figure 1: USR intra-day peg trajectory (log scale) around the 22 March 2026 incident: Curve NG and Uniswap V3 5 bp mid-price, with the three illicit `SwapRequestCompleted` mints and the reduce-only pause marked (red dotted vertical lines). The trough is \$0.0038 on Curve NG at 02:38 UTC.

The salient features of the trajectory are: a flat pre-incident state at \$1.00 ± 30 bp from midnight to 02:21 UTC; a violent drop to the trough of \$0.0038 between 02:21 and 02:38, almost exactly contemporaneous with the first illicit mint; a partial recovery to the \$0.05 – \$0.15 range over the subsequent two hours as initial liquidations propagate; a step-change at 05:17 UTC coinciding with the pause cluster, after which Curve NG mid-prices trade in a \$0.10 ± \$0.05 range for the remainder of the day.

9.5 The RLP loss-absorber was bypassed by design

The contracted role of the RLP token in the Resolv design is to absorb the first loss against any drawdown in the hedge basket. If the protocol's short perpetual positions take a profit-and-loss hit, the RLP price is supposed to fall before the USR price moves. The 22 March 2026 incident did not stress the hedge basket. The collateral pool and the perp short positions were untouched (Resolv Labs 2026). The loss vector was the dilution of USR supply from 103,071,941 tokens (the supply at the last pre-incident `PriceSet`) to 183,091,836 tokens after the three illicit mints, against an unchanged reserves total of 141,693,860 USD. The implied per-token backing fell from \$1.375 to \$0.774 instantaneously, independent of any hedge-side movement. The RLP NAV oracle correspondingly recorded no movement around the incident.

This is, in our reading, the second principal finding of the report: the conventional analysis of delta-neutral stablecoin risk, which treats RLP-style loss-absorbers as the protective layer against hedge drawdowns, leaves the protocol structurally exposed to governance and operational-security failures that bypass the loss-absorption mechanism entirely. A protocol that wishes to use RLP-style tranching for genuine systemic resilience must also harden the permissionless-mint signer infrastructure to a comparable level, because in the failure mode realised on 22 March 2026 the RLP tranche provides no protection.

9.6 Post-incident regime: Recovery Framework and open-market dislocation

The Resolv Recovery Framework, announced on 23 March 2026 (Resolv Labs 2026), redeems pre-incident holders at the original \$1 mint-rail price, subject to allowlist verification. The open market continues to trade USR at depressed prices. As of the last partition of the analytical window (May 2026), the Curve NG median mid-price is \$0.464 over 348 swaps and the Uniswap V3 5 bp median is \$0.463 over 126 swaps. The two venues are within 30 bp of each other and the spread between them, conditional on a swap clearing in the same hour on both venues, is below 50 bp at the 95th percentile.

A point worth flagging is that the open-market price is not monotone over the post-incident regime. We observe a discrete re-rating from a sustained \$0.13 – \$0.16 range over 1–25 May 2026 to a sustained \$0.45 – \$0.47 range from 26 May 2026 onwards, a nearly 3× revaluation taking place over two trading days with a heavy increase in venue throughput (454 swaps on Curve NG on 26 May against a running daily mean of approximately 20). The trigger for this revaluation is not visible on-chain in our dataset and is not yet documented in the published literature; we flag it as an open analytical question.

9.7 What the protocol-attested NAV continues to assert

The `UsrPriceStorage` contract has not emitted a `PriceSet` event since 21 March 2026. The `AggregatorV3Interface` wrapper at `0xf9C7c25F...7ce88c` continues to return the price as the price of the last attestation, namely \$1.00. The Chainlink USR/USD market feed at `0x34ad7569...561B42c` tracks the secondary-market price. Any downstream consumer of "the USR price" that integrates with the Resolv fundamental-NAV reader, and not with the Chainlink market feed, will read a stale and counterfactual \$1.00 indefinitely. This is, mechanically, a feature of the design (the protocol's NAV oracle exposes the protocol's own attestation), but it is not a feature that is widely understood by downstream consumers, and we recommend that protocol integrations that intend to read "the USR price" for collateral valuation, liquidation triggering or rebasing purposes consume the Chainlink market feed in preference to the `UsrPriceStorage` reader. Where dual-oracle aggregation is desired, the absence of a recent `PriceSet` event should be treated as evidence that the protocol attestation is stale and the market view should override.

10 Natural experiment: USR versus USDe

10.1 Setup

The 22 March 2026 incident provides the experimental conditions for a strong test of the central claim made throughout this report: that the incident isolates an operational-security failure of the delta-neutral synthetic-dollar design, not a stress event of the synthetic-dollar mechanism itself. We treat USR as the treatment unit and USDe (QuillAudits 2026) as the control unit. Both are delta-neutral synthetic dollars hedging long-spot positions in ETH and BTC against short perpetual positions on multiple centralised venues. Both are non-rebasing primary tokens with rebasing-yield wrappers (stUSR and wstUSR for Resolv; sUSDe for Ethena). Both rely on a Chainlink push feed for the market view of their peg, plus their own protocol-internal oracle for an attested view.

The outcome variable is the daily mean absolute tracking error of the Chainlink market feed for each unit, $Y_t = \text{mean}|p_t - 1|$ over all market-feed observations falling on calendar day t UTC. The treatment time is 02:21:35 UTC on 22 March 2026, the timestamp of the first illicit `completeSwap` call. We compare two non-overlapping windows: a 90-day pre-window from 22 December 2025 to 22 March 2026, and a 60-day post-window from 23 March 2026 to 22 May 2026.

10.2 Difference-in-differences estimate

Table 9: DiD estimate of the 22 March 2026 incident on the Chainlink mean absolute TE, treatment USR vs control USDe. Mann-Whitney U two-sided p-values reported per unit.

	USR (treatment)		USDe (control)	
	pre	post	pre	post
n (daily obs)	90	60	90	60
$\overline{Y}$ (pp)	0.66	83.73	0.09	0.05
$\Delta\overline{Y}$ (pp)	+83.08		−0.04	
Mann-Whitney p	3.9×10^{-25}		3.6×10^{-6}	
DiD τ (pp)	+83.12			

The DiD coefficient $\tau = +83.12$ percentage points is essentially the full USR shift; the USDe control did not move appreciably and in fact contracted slightly. Under the parallel-trends assumption implicit in DiD, the natural-experiment estimate of the "Resolv-incident effect" on the absolute peg deviation, net of any macro / funding / liquidity factor common to both protocols, is the value above. The Mann-Whitney U test rejects the null of equal pre/post distribution for USR at $p \approx 4 \times 10^{-25}$ and at $p \approx 4 \times 10^{-6}$ for USDe; the latter is statistically detectable only because USDe's pre-window MAE distribution is so tightly clustered (median 6.6 bp, IQR 4–14 bp) that a small mean shift is identifiable from such a small sample. Economically the USDe shift is one or two basis points; the USR shift is eighty-three percentage points.

10.3 Robustness

Two robustness considerations are worth flagging. First, USR and USDe pre-incident MAE distributions are not equal: the cross-sectional Mann-Whitney test of H_0: $F_{\text{USR,pre}} = F_{\text{USDe,pre}}$ rejects at $p \approx 8 \times 10^{-15}$. USR's pre-window MAE is higher (mean 66 bp vs 9 bp for USDe). This heterogeneity has been visible throughout the pre-incident period and is consistent with the relative liquidity profiles of the two protocols' DEX venues: the Curve NG USR/USDC pool is several orders of magnitude shallower than the canonical USDe-USDC Curve pool. The

DiD estimator is unbiased under parallel trends, not under common levels, so the heterogeneity is admissible. But it does mean that the strong claim is the relative magnitude (USR shifts thousands of times more than USDe), not the absolute magnitude. We commit to the relative claim.

Second, the post-window terminates at 22 May 2026, only sixty days after the incident. The persistence of the dislocation through this window is documented in Chapter 9, and the post-mean of 83.73 percentage points is computed against this still-ongoing state. If the dislocation eventually closes, the relevant post-mean would shrink. As of the cut-off the dislocation has not closed and the Resolv Recovery Framework remains the active redemption rail.

10.4 Interpretation

We interpret $\tau \approx +83$ percentage points as a strong identification of the channel-decomposition claim of the report: under identical macro and funding conditions, the synthetic-dollar mechanism survived in USDe; the operational-security layer failed in USR. The 22 March 2026 incident is, in this empirical reading, an operational-security failure mode and not a delta-neutral mechanism failure mode.

The actionable design implication is that protocols sharing the delta-neutral design with USR and USDe should treat operational-security—specifically, the management of off-chain signing keys controlling permissionless mint paths—as a first-class risk on par with funding-rate dislocations and venue-counterparty default. Existing risk frameworks treat the latter two extensively (Steakhouse Financial 2025) and the former qualitatively at best. The Resolv incident provides the first empirical natural experiment quantifying the difference.

11 Findings, V2 implications and open questions

11.1 Quantified findings

We list ten quantified findings from the report.

1. **Three illicit `completeSwap` calls on TheCounter minted** 80,019,895 **USR**, against three approximately- 100,000-USDC seed deposits. The match to the post-mortem reference of ∼80 million USR is to within 0.02%. The recipient of the first and third calls is the attacker EOA `0x04a288a7...513caed`; the second call (∼100,000 USR) we read as a sizing or decoy test.

2. **The on-chain pause occurred at 05:16:59 UTC, 2h 55min 24s after the first illicit mint and 1h 35min 12s after the third.** Three contracts emit `Paused(address)` in the same block: `TheCounter`, the USR Requests Manager, and the LP Requests Manager. The remaining six contracts (four token proxies and two PriceStorage contracts) do not emit Paused, by design: token `Transfer` remains enabled and the PriceStorage contracts have no `Pausable` mixin.

3. **Curve NG USR/USDC reached an intra-day trough of $0.003752 at 02:38:11 UTC**, 16 min 36 s after the first illicit mint. Uniswap V3 5 bp reached a similar floor at $0.008018 at the same minute. The 5-bp pool's higher floor reflects its shallower concentrated liquidity.

4. **The post-incident open-market peg has not recovered.** As of 29 May 2026 (the cut-off), the Curve NG median mid-price for USR is $0.46 against an attested Resolv-fundamental NAV of $1.00.

5. **The Resolv fundamental-NAV oracle has emitted no `PriceSet` event since 21 March 2026 at 13:15 UTC.** The `AggregatorV3Interface` wrapper continues to

return \$1.00 indefinitely, which constitutes a stale-oracle risk for any downstream protocol consuming this reader.

6. **The DiD coefficient against USDe is $\tau = +83.12$ percentage points** (Mann-Whitney $p \approx 4 \times 10^{-25}$). Under identical macro / funding conditions, the synthetic-dollar mechanism survived in USDe while the operational layer failed in USR. The natural-experiment identifies the channel as opsec, not mechanism.

7. **Pre-incident Curve NG MAE was 55 bp**, with a hour-of-day spread of 8 bp and a day-of-week spread of 12 bp. No diurnal pattern dominates the residual variation; the pre-incident regime is well-modelled as white-noise around peg.

8. **The base regression on the pre-incident TE returns $R^2 = 0.021$.** The only robustly identified coefficient is on $\log L$ (liquidity), at -0.94 bp per log unit ($t = -3.14$). $\sigma_{\text{Collateral}}$ via the Hyperliquid funding-volatility proxy is not significant ($t = -0.06$), consistent with the absence of hedge-side stress in the pre-incident regime.

9. **Granger causality between Curve NG and Uniswap V3 5 bp is bidirectional in the pre-incident regime** ($p_{\text{Curve}\Rightarrow\text{Uni}} = 4.7 \times 10^{-4}$; $p_{\text{Uni}\Rightarrow\text{Curve}} = 1.5 \times 10^{-3}$), consistent with joint price discovery across two liquid venues arbitraged tightly.

10. **TheCounter saw 31 legitimate completed swaps over its operational lifetime of 22 months, against 3 illicit completed swaps on the incident day.** The legitimate aggregate notional is 19.7 million USR; the illicit aggregate is 80.02 million USR. The illicit calls account for 80% of the total USR ever minted through TheCounter, by a factor of 4 against the entire legitimate history.

11.2 V2 design implications

We extract seven actionable design implications for the next revision of Resolv and for protocols following the same delta- neutral synthetic-dollar pattern.

1. **On-chain mint cap on permissionless paths.** The `TheCounter` contract enforced signature authenticity but no on-chain ratio check between USDC deposited and USR minted. A hardcoded mint cap of 10^4 USR per call would have limited the incident to 0.04% of its realised magnitude. The cost of the cap is a constraint on legitimate-counterfactual usage.

2. **Multisig the signer.** The compromised `SERVICE_ROLE` was a single EOA. Migrating to a 2-of-3 or 3-of-5 multisig for the permissionless-mint signer would have raised the cost of the attack from one key compromise to a coordinated multi-key compromise.

3. **Symmetrise the pause latency.** The 4-of-4 multisig admin required nearly three hours to coordinate the pause action. The defensive design should match the attack latency: a 1-of-N emergency-pause key with broad role assignment to internal operators (revocable post-incident) would close the asymmetry.

4. **Independent transparency dashboard.** The Apostro PoR being in maintenance for the duration of the audit illustrates the operational risk of a single off-chain transparency counterparty. Either the protocol-internal NAV oracle should be extended to expose the venue and custodian breakdown directly on- chain, or a backup transparency surface should be required.

5. **Stale-oracle guard on the protocol-internal NAV reader.** The `UsrPriceStorage` reader returns \$1.00 after the pause, but a downstream consumer cannot tell from the

price alone that the oracle is stale. The reader should track the last-attestation timestamp and revert (or fall back to the Chainlink market feed) if the attestation is older than the heartbeat plus a tolerance band.

6. **Asymmetric Recovery Framework redemption rails create permanent dislocations.** The lesson from the post-incident regime is that an allowlisted-redeem-at-$1 channel without a corresponding secondary-market arbitrage path leaves the unallowlisted holders bearing the full loss. Any post-incident recovery design should either include a secondary-market buyback program at the prevailing market price, or accept that the dual rail will keep the open-market discounted indefinitely.

7. **RLP-style loss-absorbers do not protect against operational failures.** The RLP token was designed to absorb the first loss against hedge-side drawdowns. The 22 March 2026 incident bypassed this mechanism because the loss vector was supply dilution, not hedge PnL. Protocols using a tranched design must harden the operational-security layer to at least the same level they harden the tranching, because the tranche is bypassed when the loss enters via the operational side.

11.3 Open questions for future revisions

1. **The 26-27 May 2026 open-market revaluation.** The Curve NG median mid-price re-rated from ∼$0.15 to ∼$0.46 over the two trading days of 26-27 May, a 3× revaluation not explained by any obvious on-chain event. Was this triggered by an unannounced Resolv announcement, a coordinated buyer, or liquidity-squeeze dynamics? The dataset captures it but the trigger is opaque.

2. **The post-incident Recovery Framework redemption rate.** How many of the ∼2,400 post-pause USR `Burn- RequestCreated` events have been completed at $1 versus cancelled? The LP burn epoch flow, not captured in our schema, may contain the relevant accounting.

3. **The Apostro restoration date.** If the dashboard returns, a backfill from its first reactivated capture to the present would close the venue and custodian gap that this report documents as a permanent limitation.

4. **The cross-chain mirror behaviour.** The seven OFT mirror chains were out of scope for the present report. Did the mirror supply move in the days surrounding the incident, and if so, what does this say about the geographic distribution of the holder base and the residual flight-to-safety on non-canonical chains?

5. **The post-mortem's claim of zero collateral loss.** The Resolv post-mortem states that the collateral pool remained intact. Our on-chain reconstruction cannot directly verify the off-chain component of this claim, only the absence of unusual on-chain collateral wallet flows. Independent verification through a custodian attestation (Fireblocks or Ceffu) would close the verification loop.

11.4 Non-claims

Three things this report does not claim. First, we do not claim that the delta-neutral synthetic-dollar mechanism is structurally sound under all conditions; we claim only that it survived the 22 March 2026 episode in the case of USDe, the apples-to-apples control. Second, we do not claim that the post-incident open-market USR is correctly priced at the prevailing levels; we claim only that the price is the price, and that the persistence of the dislocation is consistent with the analytical reading of the Recovery Framework as an asymmetric redemption rail. Third, we do not assign blame for the AWS `SERVICE_ROLE` compromise itself; we report the on-chain consequences

as a strong identification of the failure mode and leave the off-chain forensic root-cause analysis to Resolv Labs (2026), Chainalysis (2026), QuillAudits (2026), Sentora Research (2026), and Blockaid (2026).

References

Barndorff-Nielsen, Ole E. et al. (2008). "Designing Realized Kernels to Measure the Ex Post Variation of Equity Prices in the Presence of Noise". In: *Econometrica* 76.6, pp. 1481–1536.

Blockaid (2026). *How a Compromised Key Minted $80M in Resolv's USR Stablecoin and Triggered a Depeg*. Accessed 2026-05-28. URL: https://blockaid.io/blog/how-a-compromised-key-minted-80m-in-resolvs-usr-stablecoin-and-triggered-a-depeg.

Chainalysis (2026). *Lessons from the Resolv Hack*. Accessed 2026-05-28. URL: https://www.chainalysis.com/blog/lessons-from-the-resolv-hack/.

Corsi, Fulvio (2009). "A Simple Approximate Long-Memory Model of Realized Volatility". In: *Journal of Financial Econometrics* 7.2, pp. 174–196.

OAK Research (2026). *The Resolv USR Hack: Curators Face Their Responsibilities*. Accessed 2026-05-28. URL: https://oakresearch.io/en/analyses/investigations/the-resolv-usr-hack-curators-face-their-responsibilities.

QuillAudits (2026). *Resolv Labs Exploit Explained: Unchecked Mint via Compromised Service Role*. Accessed 2026-05-28. URL: https://www.quillaudits.com/blog/hack-analysis/resolv-labs-exploit-explained.

Resolv Labs (2025). *Resolv Litepaper – Smart Contracts*. URL: https://docs.resolv.xyz/litepaper/for-developers/smart-contracts.

— (2026). *Postmortem of the March 22, 2026 incident*. Accessed 2026-05-28. URL: https://resolv.xyz/blog/resolv-postmortem-march-22-2026-incident.

Sentora Research (2026). *The Resolv Hack: $25M From a Single Compromised Key*. Accessed 2026-05-28. URL: https://sentora.com/research/articles/the-resolv-hack-25m-from-a-single-compromised-key.

Steakhouse Financial (2025). *Resolv Protocol – Economic and Operational Overview*. Accessed 2026-05-28. URL: https://kitchen.steakhouse.financial/p/resolv-usr.

Zhang, Lan, Per A. Mykland, and Yacine Ait-Sahalia (2005). "A Tale of Two Time Scales: Determining Integrated Volatility With Noisy High-Frequency Data". In: *Journal of the American Statistical Association* 100.472, pp. 1394–1411.