Sous-rapport Resolv USR

Modes de défaillance de sécurité opérationnelle d'un stablecoin delta-neutre : USR, RLP, stUSR, wstUSR sur Ethereum L1, 2024–2026

Derivalink R&D

3 juin 2026

Table des matières

Résumé

Nous caractérisons l'erreur de suivi et les mécaniques de décrochage de la famille Resolv USR (stablecoin USR, jeton de tranche de risque RLP, wrappers de rendement stUSR / wstUSR) sur le mainnet Ethereum, depuis la genèse le 2 juin 2024 jusqu'à la date de coupure du 29 mai 2026, couvrant 24 mois d'historique on-chain complet reconstruit à partir de RPC d'archive publics. Le résultat principal est que l'incident du 22 mars 2026—largement décrit comme un décrochage d'un stablecoin delta-neutre—est en réalité une pure défaillance de sécurité opérationnelle : une compromission de clé Amazon Web Services `SERVICE_ROLE` a permis trois appels illicites `completeSwap()` sur le contrat sans permission `TheCounter`, frappant un total de 80 019 895 USR (80,02 millions, correspondant à l'attestation post-incident du protocole à 0,02% près) contre environ 300,000 USDC de collatéral d'amorçage. La tranche RLP absorbeuse de risque a été contournée mécaniquement : le vecteur de perte était la dilution de l'offre, non le profit-et-perte de couverture, de sorte que les détenteurs de RLP n'ont pas été affectés tandis qu'USR décrochait de $1 à un creux de $0,0038 sur le pool canonique Curve StableSwap-NG USR/USDC à 02 :38 :11 UTC, seize minutes après la première frappe illicite. Le protocole a été mis en pause à 05 :16 :59 UTC—trois heures après la première frappe—et ce délai constitue lui-même une caractéristique mesurable de l'incident : il reflète l'asymétrie entre un attaquant à clé unique et un administrateur multisig 4-of-4, une implication de conception actionnable pour des protocoles similaires. Le peg sur le marché ouvert ne s'est pas rétabli : à la date de coupure, le prix médian Curve NG est de $0,46, tandis que l'oracle de NAV fondamentale propre au protocole continue d'attester $1,00 parce qu'il a été mis en pause le 21 mars et n'a pas repris. Nous documentons cette bifurcation entre la NAV attestée par le protocole et le prix de marché ouvert comme la caractéristique centrale du régime post-incident, et discutons de ses implications pour la conception des protocoles de stablecoin delta-neutre. Le jeu de données comprend 357 574 lignes réparties sur cinq tables canoniques ; toutes les lignes passent les invariants de couche brute de l'ADR 0002 et les vérifications d'unicité de clé primaire.

Résumé exécutif

L'incident est opérationnel, non mécanique. Le résultat principal de ce rapport est une requalification. Le décrochage de l'USR de mars 2026 a, dans toute la couverture publiquement disponible à ce jour, été traité comme un événement de stress pour le mécanisme de dollar synthétique delta-neutre. Les preuves on-chain reconstruites ici montrent l'inverse. L'oracle de NAV fondamentale propre au protocole (`UsrPriceStorage.PriceSet`) attestait un état solvable jusqu'à 13 :15 UTC le 21 mars 2026, avec des réserves de 141 693 860 USD contre une offre de 103 071 941 USR, soit un ratio de surcollatéralisation de 137%, et aucune autre mise à jour d'oracle n'a été émise avant la pause. Il n'y a aucune dégradation mesurable de la santé du panier de couverture avant la première frappe illicite. Le déclencheur fut la fuite d'une clé Amazon Web Services `SERVICE_ROLE` contrôlant le signataire off-chain du contrat permissionless `TheCounter`. Trois appels illicites à `completeSwap()` entre 02 :21 :35 et 03 :41 :47 UTC le 22 mars 2026 ont frappé 80 019 895 USR contre un total d'environ 300 000 USDC déposés, sans plafond de frappe on-chain et sans contrôle du ratio oracle interceptant l'opération. L'absorbeur de pertes RLP, conçu pour encaisser la première perte face à tout drawdown du côté de la couverture, a donc été contourné : le vecteur de perte fut la dilution de l'offre, et non le compte de résultat.

Le délai de pause est en soi un résultat. La première frappe illicite survient à 02 :21 :35 UTC. Le contrat Counter, le gestionnaire de requêtes externes USR et le gestionnaire de requêtes externes LP émettent tous des événements `Paused(address)` à 05 :16 :59 UTC—soit deux heures et cinquante-cinq minutes après la première frappe, et une heure et trente-cinq minutes après la troisième et dernière frappe illicite. Par recoupement avec Resolv Labs (2026), ce délai est attribuable à l'exigence de coordination de l'administration multisig 4-sur-4 pour l'action de pause. L'attaquant à clé unique ne faisait face à aucun coût de coordination analogue. Cette asymétrie constitue une implication de conception actionnable pour les protocoles delta-neutres

similaires : la latence de la pause d'urgence devrait être évaluée à l'aune de la latence d'un adversaire à clé unique, et non au regard d'un référentiel de temps de coordination de l'attaquant.

Le prix de marché libre face au prix attesté est l'observable centrale. Après la pause, l'oracle de NAV fondamentale du protocole a cessé d'émettre des événements `PriceSet`. Le flux de marché Chainlink USR/USD a continué de suivre le prix du marché secondaire. Le cadre de récupération (Recovery Framework) de Resolv, annoncé le 23 mars 2026, rachète les détenteurs pré-incident au prix de frappe d'origine de \$1, sous réserve de vérification par liste blanche. Le résultat est une bifurcation structurelle entre la NAV attestée par le protocole (qui demeure à \$1,00 indéfiniment) et le prix de marché libre (qui, sur le mois de coupure de mai 2026, présente une médiane Curve NG de \$0,46 contre une médiane Uniswap V3 5 bp de \$0,46 de manière similaire). La persistance de cet écart est, selon notre lecture, la caractéristique la plus distinctive sur le plan analytique du régime post-incident, et nous en développons les implications tout au long du rapport.

Jeu de données. L'extraction complète couvre 24 mois, depuis la genèse le 2 juin 2024 jusqu'au 29 mai 2026, et comprend 357 574 lignes réparties sur cinq tables canoniques : `mint_burn_events` (160 817 lignes sur les quatre tokens), `redemption_requests` (17 116 lignes sur les deux gestionnaires et le Counter), `oracle_updates_raw` (5 278 lignes provenant de Chainlink et des deux contrats PriceStorage), `delta_neutral_state` (909 lignes d'attestations de NAV), et `prices` (173 539 lignes de prix médians dérivés de swaps sur Curve StableSwap-NG USR/USDC, Uniswap V3 USR/USDC à 5 bp, et Uniswap V3 RLP/USR). Les données satisfont les invariants de couche brute de l'ADR 0002 et les contrôles d'unicité de clé primaire sur chaque combinaison `(table, asset)`, et l'invariant forensique de trois frappes illicites totalisant 80 019 895 USR est cohérent à 0,02% près avec la référence du post-mortem de 80 millions.

Guide de lecture. Le chapitre 1 caractérise le jeu de données. Le chapitre 2 présente les statistiques descriptives d'erreur de suivi sur l'ensemble des sources oracle et DEX, ventilées par régime pré-incident, jour de l'incident et post-incident. Le chapitre d'étude de cas prend l'incident du 22 mars 2026 comme sujet principal et reconstruit la trajectoire de prix intra-journalière à la résolution de la minute, décode les trois transactions d'ancrage à la granularité de la trame de trace, et aligne le cluster de pause des contrats avec la chronologie forensique de Chainalysis et QuillAudits.

1 Caractérisation du jeu de données

1.1 Périmètre de la cohorte et provenance

La cohorte de tokens Resolv comprend quatre tokens sur le mainnet Ethereum : USR (`0x66a1E37c...e110`), RLP (`0x4956b52a...8f96`), stUSR (`0x6c8984bc...AAb4`) et wstUSR (`0x1202F5C7...5055`). Les quatre proxys ont été déployés au sein d'une fenêtre de 152 blocs le 2 juin 2024, le lancement public sur le mainnet suivant le 30 septembre 2024 (Resolv Labs 2025). La fenêtre analytique du présent rapport est l'intervalle semi-ouvert allant du 4 juin 2024, date de la première frappe observée, au 1er juin 2026, exclu.

La cohorte enregistre par ailleurs sept contrats protocolaires centraux qui ne détiennent pas eux-mêmes de soldes mais émettent les événements récupérés ici : `UsrExternalRequestsManager` (`0xAC85eF29...5f2e`) qui gère la frappe contrôlée d'USR et la file de rachat ; `LPExternalRequestsManager` (`0x10f4d4EA...c872`) qui gère la même fonction pour RLP, avec un flux de destruction distinct par époques ; `TheCounter` (`0xa27a69Ae...5861`) qui expose un chemin de swap USR sans permission contre une cotation signée hors chaîne ; les deux contrats `PriceStorage` qui émettent

les attestations quotidiennes de NAV on-chain pour USR et RLP respectivement ; et les deux contrats de staking pour les wrappers rebasant et ERC-4626.

La phase 2 de la cohorte, qui ajouterait les sept miroirs OFT LayerZero des bridges d'USR, RLP et wstUSR (Base, Arbitrum, BNB Chain, Berachain, HyperEVM, Soneium, TAC, Plasma), est hors du périmètre du présent rapport et reportée à un addendum cross-chain. Les tokens miroirs n'émettent que les `Transfer` et `Approval` ERC-20 standard ; toute l'activité d'émission, de rachat, d'attestation de NAV et de swap se déroule sur le mainnet Ethereum.

1.2 Tables canoniques et couverture

TABLE 1 – Couverture en tables canoniques de la cohorte Resolv. Fenêtre 4 juin 2024 – 29 mai 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

La partition `prices` sur USR est alimentée par deux sources indépendantes dont la ventilation est donnée dans le Tableau 2.

TABLE 2 – Ventilation par source de la partition `prices` d'USR.

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

La partition `oracle_updates_raw` sur USR porte de même deux sources distinctes d'intérêt analytique. Le feed push Chainlink USR/USD (`chainlink_data_feed_usr_usd`, 4,369 lignes du 26 février 2025 jusqu'à la date de coupure) rapporte le prix dérivé du marché sur une base de déviation ou de battement (heartbeat). Le feed fondamental de NAV Resolv (`resolv_fundamental_usr_usd`, 455 lignes du 25 décembre 2024 au 21 mars 2026, puis plus aucune émission) rapporte l'attestation propre du protocole contre le panier de collatéral sous-jacent. La cessation de ce dernier à 13 :15 UTC le 21 mars 2026, un jour avant l'incident, ancre la bifurcation entre les deux oracles, qui devient le pivot analytique du chapitre d'étude de cas.

1.3 Verdict d'audit

Chaque combinaison `(table, asset)` listée dans le Tableau 1 satisfait les invariants de couche brute de l'ADR 0002 (`is_imputed = false`, `imputation_method = native`, `gap_to_previous_native_s = 0`) ainsi que le contrôle d'unicité de clé primaire spécifique à chaque table. Il n'y a aucune exception. L'invariant forensique, selon lequel la somme d'`amount_out` sur les trois lignes de `redemption_requests` étiquetées `illicit_mint_2026_03_22` égale la référence post-mortem d'environ 80 millions d'USR, est satisfait à 80 019 895 USR, soit un écart de 0,02% par rapport à la référence.

1.4 Limites

Trois limites de données sont héritées des surfaces de divulgation hors chaîne. Premièrement, le tableau de bord Proof-of-Reserves d'Apostro, qui fournit ordinairement le mix quotidien des venues de couverture, l'allocation par dépositaire et la composition du collatéral qui peupleraient les colonnes `spot_eth_balance`, `perp_short_notional_usd` et celles liées aux dépositaires de `delta_neutral_state`, était en maintenance au moment de l'audit. L'inspection des douze instantanés Wayback archivés sous `reports/resolv/disclosure_archives/03_apostro_wayback/` confirme que les instantanés ne contiennent que la coquille JavaScript côté client du tableau de bord Next.js et ne préservent pas les tables de données rendues par React. L'endpoint live du tableau de bord `info.apostro.xyz/resolv-reserves` renvoie un message de maintenance « OFFLINE » au moment de la rédaction. Le mix des venues de couverture et l'allocation par dépositaire sont par conséquent traités comme des lacunes de données permanentes ; les mitigations sont discutées dans la section méthodologie du chapitre 3.

Deuxièmement, le flux d'époques de destruction LP (`BurnRequestProcessing`, `BurnRequestPartiallyCompl` `BurnRequestsEpochCompleted`) est documenté dans `ILPExternalRequestsManager` mais pas encore capturé dans notre schéma, qui ne dispose pas de la colonne `epoch_id` requise pour modéliser les états de remplissage partiel. La table `redemption_requests` actuelle ne capture que `BurnRequestCreated` et `BurnRequestCancelled` côté RLP, de sorte que les taux de rachat RLP ne sont pas reconstructibles à pleine fidélité dans le présent rapport.

Troisièmement, quatre des sept chaînes miroirs OFT LayerZero n'avaient aucune émission en service durant la fenêtre de l'incident. Les événements d'afflux via bridge sur le miroir Base sont capturés dans la cohorte mais les six autres chaînes sont reportées à l'addendum cross-chain de la phase 2.

2 Erreur de suivi multi-référence

2.1 Cinq séries de référence

Pour le token USR, nous rapportons l'erreur de suivi face à cinq références indépendantes. Trois d'entre elles sont des observables de prix : le pool Curve StableSwap-NG USR/USDC (61 044 prix médians), le pool Uniswap V3 USR/USDC 5 bp (112 495 prix médians) et le push feed Chainlink USR/USD (4,369 événements `AnswerUpdated`). Deux sont internes au protocole : la NAV fondamentale `UsrPriceStorage.PriceSet` (455 attestations) et la cible de peg implicite à \$1 du rail de frappe-rachat. Nous traitons l'erreur de suivi partout sous forme relative au prix, $\mathrm{TE}(t) = p(t) - 1$, avec $p(t)$ le prix observé en USD ; autrement dit, un prix de \$0,95 correspond à une erreur de suivi de -0.05 ou $-5{,}000$ bp.

2.2 Persistance du décrochage

Nous définissons un épisode de décrochage comme une observation telle que $|p(t) - 1| > 0.01$; autrement dit, dont le prix s'écarte de plus de 100 bp du peg. La proportion censurée à droite

des observations qui tombent dans cette région constitue le résumé le plus simple de la fréquence à laquelle une venue valorise USR loin de sa cible.

TABLE 3 – Proportion des observations en épisodes de décrochage (plus de 100 bp de $1), cohorte USR, fenêtre analytique complète 4 juin 2024 – 29 mai 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

L'écart entre les quatre sources est l'une des caractéristiques marquantes du rapport. Les pools Curve et Uniswap affichent des fractions hors-peg de 27% et 44% respectivement, reflétant à la fois une réelle variation de prix intra-journalière dans la fenêtre pré-incident et la dislocation post-incident soutenue ; le pool Uniswap V3 5 bp présente une fraction hors-peg plus élevée parce que sa liquidité concentrée et peu profonde amplifie l'impact sur le prix marginal de toute transaction. Le market feed Chainlink rapporte des observations hors-peg 91% du temps, un artefact de la cadence à laquelle il échantillonne : la plupart de ses 4,369 observations tombent dans le régime post-incident où l'état hors-peg est soutenu. Le feed de NAV fondamentale Resolv rapporte zéro observation hors-peg parce que l'attestation on-chain a été mise en pause à 13 :15 UTC le 21 mars 2026, avant que l'état relatif au prix ait pu diverger de la cible ; dans la fenêtre pré-incident, il indique tautologiquement $1,00 par construction (le protocole atteste sa propre collatéralisation).

2.3 Décomposition par régime

Le clivage naturel de la fenêtre analytique est la frontière de l'incident à 02 :21 :35 UTC le 22 mars 2026, l'horodatage du premier appel illicite `completeSwap()`. Nous définissons trois régimes : *pré-incident* (de la genèse au clivage), *jour de l'incident* (du clivage au 23 mars 2026 à minuit UTC) et *post-incident* (à partir du 23 mars 2026, l'ère du cadre de récupération). Les statistiques descriptives d'erreur de suivi sous cette décomposition pour les quatre séries portant un prix sont rapportées dans la Table 4 (calculées dans `data/derived/compute/resolv/phase2/te_summary.parquet`). Nous mettons en avant trois constats :

1. Dans le régime pré-incident, le prix médian Curve NG pour USR a une erreur de suivi moyenne de +3.6 bp avec un écart-type de 5,9 bp et une médiane de +3.4 bp, essentiellement égale à la moyenne. La distribution est essentiellement symétrique autour d'une légère prime et est cohérente avec un comportement normal de tenue de marché pour un stablecoin se négociant près du peg.
2. Dans le régime du jour de l'incident, l'erreur de suivi moyenne sur Curve NG chute à −45.0 points de pourcentage avec un écart-type de magnitude similaire, reflétant le swing intra-journalier violent de $1,00 à $0,0038. Le drawdown maximal sur cette venue durant le jour de l'incident est de 99,62%, que nous interprétons littéralement : une position détenue à l'ouverture à $1,00 a atteint une valorisation effective de $0,0038 au creux.
3. Dans le régime post-incident, l'erreur de suivi moyenne Curve NG est de −71.3 points de pourcentage et le drawdown maximal demeure à 90,7%. La persistance de la dislocation est la caractéristique structurelle que le chapitre d'étude de cas traite en détail.

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

2.4 Séparation à deux oracles

Les cinq séries de référence se répartissent en deux groupes analytiquement distincts. Trois sources (Curve, Uniswap, market feed Chainlink) suivent le prix que le marché libre est prêt à payer pour USR. Deux sources (NAV fondamentale Resolv et le rail implicite de frappe-rachat à \$1) suivent le prix que le protocole ou sa liste blanche affirme. Après le 21 mars 2026, ces deux groupes n'ont pas reconvergé : à la date de coupure des données (fin mai 2026), le prix médian Curve NG est de \$0,46 — ayant remonté depuis \$0,158 le 2026-04-20 — contre une NAV attestée de \$1,00. Nous conservons cette distinction tout au long du reste du rapport ; dans chaque graphique qui suit, les deux classes d'oracles sont présentées comme des séries distinctes et nous résistons à la tentation de les agréger en une seule référence « USR/USD ».

Périmètre : les wrappers. Ce chapitre valorise USR lui-même. Les wrappers stakés stUSR (rebasing) et wstUSR (ERC-4626) héritent du peg d'USR par construction — un wstUSR est une créance fixe, à croissance monotone, sur USR, de sorte que son prix en USD est le prix d'USR multiplié par le taux de change (lisse) et ne porte aucun risque de peg indépendant. Leur déviation sur le marché secondaire n'est donc pas ici une série d'erreur de suivi distincte ; le comportement du taux de change wstUSR/USR et sa valorisation Pendle/DEX sont traités dans le chapitre des venues (Ch. 5) plutôt que dupliqués comme référence de peg dans ce chapitre.

3 Décomposition de niveau 1 de l'erreur de suivi

3.1 Décomposition de la volatilité face à la rupture des données Apostro

La décomposition standard de niveau 1 de l'erreur de suivi d'un stablecoin spécifiée dans notre méthodologie appelle la construction de trois séries de volatilité : $\sigma_{\text{Collateral}}$, σ_{Synth} et σ_{Peg}. La première est conventionnellement la volatilité réalisée de l'exposition du panier en delta

net $\sum_i w_i(t) \cdot (s_i(t) - f_i(t))$, où w_i sont les poids de venue, s_i les positions de la jambe spot et f_i les positions de couverture de la jambe perp à la venue i. Les poids de venue $w_i(t)$ ne sont pas récupérables à partir des données on-chain et devaient être tirés du tableau de bord Proof-of-Reserves d'Apostro, qui est en maintenance pour toute la durée de la fenêtre analytique de ce rapport.

Nous adoptons le choix méthodologique figé de STRUCTURE.md et substituons le **proxy mono-venue Hyperliquid** : Hyperliquid est la seule venue de couverture on-chain disposant d'un historique de financement complet ligne à ligne dans notre jeu de données, et nous traitons l'écart-type quotidien du taux de financement de son ETH-PERP comme un proxy représentatif du $\sigma_{\text{Collateral}}$ au niveau du panier. L'aperçu économique de Steakhouse Financial (Steakhouse Financial 2025) confirme qu'Hyperliquid est l'une des quatre venues de couverture nommées (avec Binance, Bybit et Deribit) ; sous la lecture à a priori uniforme, le financement Hyperliquid se comporte comme un représentant pondéré à poids égaux. Le proxy mono-venue est certes plus étroit que la série au niveau du panier ; nous présentons les résultats de régression avec cette réserve et reportons la sensibilité à a priori uniforme et au panier de financement dans une annexe complémentaire lors d'un commit ultérieur.

3.2 Régression de base

Nous estimons la régression de base spécifiée

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

sur la sous-fenêtre pré-incident (de la genèse au 22 mars 2026 02 :21 UTC, $n = 579$ observations quotidiennes), avec TE_t l'erreur de suivi moyenne quotidienne sur le pool Curve StableSwap-NG USR/USDC, σ_{Coll} l'écart-type quotidien du financement de l'ETH-PERP Hyperliquid, L le décompte quotidien des swaps Curve NG comme proxy de liquidité, et r_f le taux de financement moyen quotidien de l'ETH-PERP Hyperliquid. La covariable des frais de gas est laissée de côté pour cette version, en attendant son intégration dans le pipeline Resolv.

Table 5 – Régression de base sur la série de TE pré-incident. $n = 579$ observations quotidiennes ; $R^2 = 0.021$. Statistiques t bilatérales affichées. Les coefficients sur σ_{Coll} et r_f sont grands en valeur absolue car les régresseurs sont eux-mêmes petits (les taux de financement vérifient typiquement $|r_f| < 10^{-3}$).

Term	Coefficient	SE	t-stat
Intercept	+0.00216	0.00116	+1.86
$\sigma_{\text{Collateral}}$	−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.

Trois constats émergent. Premièrement, $\sigma_{\text{Collateral}}$, mesuré via le proxy de volatilité du financement Hyperliquid, n'est pas un déterminant statistiquement significatif du TE pré-incident ($t = -0.06$). Cela est cohérent avec la thèse centrale de ce rapport : la période pré-incident n'a connu aucune tension mesurable sur le panier de couverture, et le mécanisme de dollar synthétique fonctionnait dans son régime normal. Deuxièmement, le proxy de liquidité est significativement négatif au seuil de 1 % : chaque augmentation d'une unité de $\log L$ resserre le TE de 9,4 bp. C'est le signe attendu — une liquidité plus élevée soutient un arbitrage de peg plus serré — et c'est le seul régresseur dont le coefficient est robustement identifié compte tenu de la faible variation de la variable dépendante. Troisièmement, le niveau de financement r_f est marginalement positif ($t = 1.54$), suggérant qu'un financement positif (c.-à-d. les longs payant

les courts sur le perp) correspond à un léger décrochage de l'USR sous \$1 ; c'est le signe attendu pour un protocole delta-neutre percevant des revenus de financement, puisque l'accumulation de financement est incorporée au côté collatéral et qu'un régime de financement positif, s'il persiste, réduit l'exposition effective du panier en delta net.

Le R^2 de 2,1 % est modeste, ce qui est en soi instructif : le TE USR pré-incident est si étroitement regroupé autour de sa moyenne de \$0,0007 qu'il reste peu de variance à expliquer. Le facteur dominant dans toute comparaison post-/pré-incident est le changement de régime survenu à l'incident lui-même, que cette régression exclut intentionnellement.

3.3 GARCH et HAR

Nous ajustons trois variantes GARCH sur la série de TE pré-incident mise à l'échelle en points de base : GARCH(1,1), GJR-GARCH(1,1) et EGARCH(1,1). La table de sélection des paramètres (Table 6) retient GARCH(1,1) sur l'AIC, GJR-GARCH étant à moins d'une unité d'AIC. Le paramètre d'asymétrie dans GJR-GARCH n'est pas significativement différent de zéro, aussi reportons-nous GARCH(1,1) comme modèle de référence. Une lecture complète de la persistance de la variance conditionnelle ($\alpha + \beta$ pour GARCH(1,1)/GJR, le coefficient AR de la log-variance β pour EGARCH) et la batterie de diagnostics des résidus de niveau 1 (Breusch-Pagan, Durbin-Watson, Ljung-Box) sont reportées à un travail ultérieur ; la sélection fondée sur l'AIC et les signes des coefficients ci-dessus sont les résultats de niveau 1 de référence reportés ici.

Table 6 – Sélection de modèle GARCH sur la série de TE pré-incident, $n = 579$ observations quotidiennes.

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

La décomposition HAR de Corsi (2009) — ici la structure de retards quotidien/hebdomadaire/mensuel de Corsi appliquée à la série quotidienne |TE| (un HAR de niveau, et non un estimateur de variance réalisée) — renvoie un R^2 de 0,45 % sur la série pré-incident, avec le coefficient du retard quotidien à 1.27 et les retards hebdomadaire et mensuel à 0.68 et −0.71 respectivement. La puissance explicative quasi nulle confirme que la série de TE pré-incident est essentiellement un bruit blanc autour d'une moyenne serrée ; le HAR ne devient pertinent que lorsqu'il existe une structure d'autocorrélation cross-temporelle non triviale à estimer, et le TE pré-incident n'en présente pas.

3.4 Ce que la régression ne peut pas identifier

La réserve la plus importante pour le chapitre de niveau 1 est que l'incident du 22 mars 2026 représente un changement de régime qu'aucun modèle économétrique à état continu n'est censé identifier. Le mode de défaillance de sécurité opérationnelle ayant généré l'incident se situe en dehors de la distribution jointe de $(\sigma_{\text{Coll}}, L, r_f, \text{gas})$ que la régression de base prend en entrée. Du point de vue du modèle de régression, l'incident est une rupture structurelle dans le résidu, et les paramètres du modèle pré-incident ne peuvent pas servir à prévoir le comportement post-incident. Nous traitons la période post-incident de manière descriptive au Chapitre 2 et reportons l'ampleur du changement de régime dans l'estimation par différence de différences du Chapitre 10 ; le chapitre de décomposition de niveau 1 se cantonne uniquement à la période pré-incident.

4 Schémas temporels

4.1 Tranches horaires et jours de la semaine

Nous calculons l'erreur de suivi absolue moyenne (MAE) par tranche du régime pré-incident, en n'utilisant que les observations strictement antérieures à 02 :21 :35 UTC le 22 mars 2026. Conditionner sur le régime post-incident n'est pas informatif pour l'analyse diurne, car la dislocation persistante domine tout signal lié à l'heure de la journée.

La MAE par heure de la journée sur la venue canonique Curve StableSwap-NG varie d'un minimum de 5,07 bp (heure la plus calme) à un maximum de 5,89 bp (heure la plus active), soit un écart de 0,83 bp. La MAE par jour de la semaine varie de 4,85 bp à 6,03 bp, soit un écart de 1,18 bp. Les deux écarts sont faibles par rapport à la MAE pré-incident d'environ ∼5,4 bp elle-même, ce qui confirme que le peg pré-incident était suffisamment serré pour qu'aucun schéma diurne ou hebdomadaire ne domine la variation résiduelle.

Les écarts de MAE par heure de la journée et par jour de la semaine ci-dessus (0,83 bp et 1,18 bp) sont d'un ordre de grandeur inférieurs au niveau de la MAE pré-incident (∼5,4 bp) lui-même, de sorte qu'aucune empreinte de session TradFi n'est manifeste dans la série pré-incident de USR — ce qui est cohérent avec le statut de USR en tant que stablecoin crypto-natif fonctionnant 24/7 et non couplé à une quelconque session de marché traditionnel. (Une ANOVA formelle à deux facteurs heure × jour est reportée à un travail ultérieur ; les plages de MAE par tranche bornent déjà l'effet d'interaction.)

4.2 Atténuation du bruit de microstructure

Conformément à l'ADR 0002 et à la section 4.4 du guide de préparation, toutes les statistiques liées à la variance dans ce chapitre et les suivants utilisent soit la couche native de grille d'événements (sans imputation), soit la couche suréchantillonnée à 1 min avec la protection explicite `is_imputed = true`. Pour les quantités de volatilité réalisée en particulier (utilisées dans les chapitres 3 et 7 ci-dessous), nous appliquons l'estimateur de variance réalisée à deux échelles de Zhang, Mykland et Ait-Sahalia (2005) et le noyau réalisé de Barndorff-Nielsen et al. (2008) pour contrôler la contamination par le bruit de microstructure qui est non négligeable sur le pool peu profond Uniswap V3 à 5 bp. Le pool Curve NG est plus profond et la contamination est plus faible, mais les mêmes estimateurs sont appliqués pour assurer la cohérence entre venues.

5 Décomposition par venue et frictions

5.1 Concordance des prix entre venues

Deux venues on-chain cotent USR/USDC : le pool Curve StableSwap-NG et le pool Uniswap V3 à 5 bp. Nous calculons le prix médian (mid) quotidien sur chacune ainsi que l'écart entre venues $\text{spread}_t = p_t^{\text{Uni}} - p_t^{\text{Curve}}$. Sur les 650 jours de couverture conjointe de juin 2024 à mai 2026, l'écart médian entre venues est de 1,4 bp, l'intervalle interquartile est $[-12, +15]$ bp, et le 99e centile de |spread| est de 87 bp. La concordance est étroite dans le régime pré-incident (95e centile de |spread| inférieur à 35 bp) et s'élargit durant le jour de l'incident, lorsque les deux pools se reprisent avec une latence non négligeable l'un par rapport à l'autre : le 22 mars 2026, l'écart médian quotidien atteint 4,4 points de pourcentage avant de se resserrer à 30 bp à la fin de la fenêtre post-incident. Une fois la dislocation stabilisée, les deux venues se suivent à moins de 50 bp d'écart médian, le pool Uniswap V3 à 5 bp s'échangeant à une légère décote car sa liquidité concentrée plus mince est davantage affectée par la pression de rachat régulière issue de l'arbitrage de marché libre que la liste blanche du cadre de récupération n'absorbe pas.

5.2 Latence de l'oracle Chainlink USR/USD

Le feed push Chainlink USR/USD déployé début 2025 émet 4 369 événements `AnswerUpdated` sur la fenêtre analytique. Le heartbeat nominal est de 24 heures et le seuil de déviation est de 1% ; chacun des deux déclencheurs provoque une mise à jour. Les temps inter-mises à jour suivent une distribution bimodale : un mode lent à ∼24 heures (lorsque le feed est en régime de heartbeat), et un mode rapide à l'échelle des minutes-aux-heures (lorsque le seuil de déviation est déclenché de façon répétée, comme durant l'incident de mars 2026 et les semaines suivantes de forte volatilité de marché secondaire). Le jour de l'incident spécifiquement, 64 mises à jour se déclenchent sur les 24 heures, une accélération de ∼15× par rapport au heartbeat. Le délai de propagation de l'horodatage du bloc on-chain au swap suivant sur Curve NG est de 3,8 secondes en médiane sur le jour de l'incident, contre 27 secondes dans le régime normal pré-incident ; les teneurs de marché ont réagi plus vite au feed Chainlink durant la dislocation.

5.3 Friction forensique : la fenêtre de pause manquée

La friction la plus lourde de conséquences observée dans notre jeu de données est l'écart de 2 heures 55 minutes entre le premier événement illicite `SwapRequestCompleted` à 02 :21 :35 UTC et le cluster d'événements `Paused(address)` à 05 :16 :59 UTC. Cet écart est documenté plus en détail au Chapitre 9. Dans un cadre de décomposition des frictions, il est approprié de traiter la latence de pause comme la principale friction opérationnelle observable à la surface du protocole : une version idéalisée de Resolv dotée d'une clé d'administration de pause 1-parmi-N aurait mis fin à l'attaque dès la première ou la deuxième frappe illicite et aurait limité la perte à ∼30 millions d'USR plutôt que 80 millions. Nous traitons cela quantitativement dans la synthèse des implications V2 au Chapitre 11.

5.4 Allocation par dépositaire et par venue : reformulation qualitative

Comme documenté au Chapitre 1 et rappelé au Chapitre 6, la ventilation granulaire par dépositaire et par venue de couverture pour le protocole Resolv provenait du tableau de bord Apostro Proof-of-Reserves, qui était en maintenance pendant toute la fenêtre analytique de ce rapport. Nous reformulons qualitativement les venues et dépositaires nommés à partir de l'aperçu économique Steakhouse Financial (Steakhouse Financial 2025) : les venues de couverture sont Binance USD-M, Bybit linear, Deribit et Hyperliquid (cette dernière captée on-chain) ; les dépositaires sont Fireblocks (pour Bybit et Deribit) et Ceffu MirrorX (pour Binance). La jambe Hyperliquid se situe entièrement on-chain et est récupérable depuis notre pipeline. Les trois autres venues ne le sont pas.

6 Déterminants structurels

6.1 Trajectoires d'offre le long de l'échelle de staking

La conception de Resolv expose quatre primitives de tokens formant une chaîne de wrappers : collatéral → USR → stUSR (rebasing) → wstUSR (ERC-4626). Chaque étape de wrapping est capturée à la granularité de l'événement `Transfer` dans notre table `mint_burn_events`. Nous calculons l'offre nette cumulée quotidienne (frappe plus afflux par bridge, moins destruction et sortie par bridge) pour chaque token. Les chiffres principaux sont synthétisés dans le Tableau 7.

TABLE 7 – Offre de l'échelle de staking Resolv à quatre dates d'ancrage, en millions de tokens. Le pic pré-incident est l'offre cumulée maximale d'USR observée strictement avant le 22 mars 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

Deux observations en découlent. Premièrement, la différence d'ordre de grandeur entre le pic pré-incident (586 millions d'USR en circulation) et l'offre en circulation à fin avril (46 millions) reflète la campagne de destruction-et-blacklist post-incident documentée dans RESOLV LABS (2026) : au 27 mars 2026, environ 46 millions des 80 millions d'USR frappés illicitement avaient été neutralisés, et le flux restant au cours des cinq semaines suivantes a ramené le total en circulation à un niveau cohérent avec l'équilibre pré-incident d'environ 100 millions, moins les 50 millions imputables à la longue traîne des rachats post-incident via le cadre de récupération.

Deuxièmement, l'offre cumulée de wstUSR de 33,5 millions de tokens face à une offre de stUSR de 23,7 millions reflète le fait que wstUSR a été introduit deux mois après stUSR et a absorbé la part dominante du flux de staking. Les deux sont mécaniquement liés (toute position wstUSR implique un adossement en stUSR via le wrap ERC-4626), mais leurs séries d'offre on-chain sont émises par des flux d'événements `Transfer` distincts, et la relation entre elles est informative pour l'analyse de la file d'attente de cooldown que le guide de préparation identifie comme obligatoire pour les produits de staking ERC-4626.

6.2 La file d'attente de rachat asynchrone

Le contrat `UsrExternalRequestsManager` reçoit des événements `BurnRequestCreated` pour les utilisateurs demandant le rachat d'USR. Chaque demande est soit `Cancelled` par l'utilisateur, soit `Completed` par le protocole ; le temps entre Created et l'état terminal est la latence de rachat.

Sur l'ensemble de la fenêtre analytique, nous observons un maximum de 16 demandes de burn ouvertes à un instant donné et un pic de notionnel ouvert de 29,9 millions d'USR. Le pic coïncide avec les jours immédiatement consécutifs à l'incident, lorsque les détenteurs inscrits sur liste blanche ont entamé le processus de rachat du cadre de récupération. La série de latences est bimodale : un mode de routine d'environ 24 heures pour les demandes éligibles à l'instantané et un mode lent d'environ 7 à 14 jours pour les demandes qui sortent du plafond quotidien de rachat instantané.

6.3 Débit cumulé de TheCounter

Le contrat permissionless `TheCounter`, qui est le contrat exploité le 22 mars, voit trente-et-un swaps légitimes complétés sur l'ensemble de la période pré-incident, contre trois swaps illicites complétés le jour de l'incident. Le notionnel agrégé des trente-et-un swaps légitimes est de 19,7 millions d'USR, contre 80,02 millions d'USR pour les trois swaps illicites. Autrement dit, les trois transactions illicites représentent 80% du notionnel total ayant jamais transité par TheCounter, par un facteur d'environ quatre par rapport à l'ensemble de l'historique légitime.

Ce ratio est informatif pour la recommandation de conception que nous tirons au Chapitre 9 : une surface de frappe permissionless qui traite moins de deux swaps légitimes par mois sur sa durée de vie opérationnelle, mais qui peut être drainée de 80 millions d'USR en trois appels, présente un profil risque/utilité exceptionnellement défavorable.

6.4 Allocation par dépositaire et par venue : une lacune de données

Le chapitre tel qu'initialement défini dans notre STRUCTURE.md devait inclure des visualisations en aires empilées du collatéral par dépositaire (Fireblocks vs Ceffu MirrorX vs on-chain) et du panier de couverture par venue (Binance vs Bybit vs Deribit vs Hyperliquid), à une granularité quotidienne. Comme documenté au Chapitre 1, le tableau de bord Proof-of-Reserves d'Apostro qui aurait dû alimenter ces séries était en maintenance pendant toute la durée de l'audit et ses instantanés Wayback archivés ne contiennent pas les données rendues. Nous remplaçons la visualisation par une restitution qualitative des venues et dépositaires identifiés dans l'aperçu économique de Steakhouse Financial (Steakhouse Financial 2025) : le panier de couverture couvre Binance USD-M, Bybit linear, Deribit et Hyperliquid ; la custody est répartie entre Fireblocks (pour Bybit et Deribit) et Ceffu MirrorX (pour Binance) ; le protocole diversifie explicitement afin d'atténuer les événements idiosyncratiques de taux de financement sur une venue donnée. Nous ne disposons pas d'une série temporelle des pondérations.

7 Causalité inter-composantes

7.1 Causalité de Granger entre venues

Nous testons la causalité de Granger entre les séries de prix médian (mid) à 5 bp de Curve NG et d'Uniswap V3, restreintes à la sous-fenêtre pré-incident où les deux séries sont stationnaires en moyenne. Les séries sont alignées à la granularité quotidienne ($n = 486$ jours de couverture conjointe). Au décalage 1, le test F sur la somme des carrés des résidus rejette l'absence de causalité dans les deux directions :

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

Les deux directions rejettent l'hypothèse nulle au seuil de 1%. Une correction de Benjamini-Hochberg appliquée aux deux tests dirigés laisse les deux résultats significatifs ($q = 9.4 \times 10^{-4}$ et 1.5×10^{-3}), de sorte que le résultat est robuste à la (faible) multiplicité. Nous interprétons ceci comme une causalité bidirectionnelle cohérente avec une découverte de prix conjointe entre les deux venues, ce qui constitue le schéma attendu pour deux cotations liquides sur le même actif. La formation du prix médian ne privilégie aucune venue comme observable directrice dans le régime pré-incident, et l'arbitrage entre les deux pools est suffisamment serré pour que les chocs induits par les nouvelles se propagent dans les deux directions au sein de la fenêtre d'échantillonnage quotidienne.

7.2 Cointégration du résidu de peg

La procédure d'Engle-Granger appliquée à la série de déviation Chainlink USR/USD $d_t = p_t - 1$ sur l'ensemble de la fenêtre analytique produit une statistique de Dickey-Fuller augmenté de -2.39 avec une p-value de 0,146. Nous ne parvenons pas à rejeter l'hypothèse nulle de racine unitaire au seuil de 5%. Mécaniquement, la série de déviation est non stationnaire car le régime post-incident introduit un décalage de niveau permanent : la série est approximativement stationnaire à l'intérieur de chaque régime (pré à \$0, post autour de $-\$0.50$), mais le niveau se déplace d'un régime à l'autre d'environ cinquante points de pourcentage. Le test ADF n'est pas conscient des régimes et rapporte la série inconditionnelle comme non stationnaire, ce qui constitue le verdict approprié pour tout modèle en aval qui prend la déviation inconditionnelle en entrée.

Une analyse conditionnelle au régime confirme l'intuition : la fenêtre pré-incident présente une p-value ADF de d_t inférieure à 10^{-4} (fortement stationnaire, le peg tient en moyenne), tandis que la fenêtre post-incident présente une p-value ADF de d_t de 0,62 (non stationnaire, le prix de marché secondaire dérive au gré du flux de nouvelles). Le changement de régime constitue lui-même la caractéristique économétrique la plus informative de la série.

7.3 Autorégression vectorielle et réponse impulsionnelle

Un VAR à 5 décalages ajusté sur les trois séries pré-incident ($\sigma_{\text{Coll}}, \sigma_{\text{Peg}}, \sigma_{\text{Synth}}$) ne produit pas d'estimations de paramètres statistiquement robustes étant donné la faible variance de la TE pré-incident. Nous reportons l'analyse complète VAR / réponse impulsionnelle à une révision future incluant l'annexe de sensibilité au panier de financement.

7.4 Copules asymétriques

Les ajustements de copules de Clayton et de Gumbel sur la série bivariée $(\text{TE}_t, r_{f,t})$, calculés sur la fenêtre pré-incident, renvoient des paramètres de dépendance de queue qui ne sont pas significativement différents de l'indépendance : $\lambda^L_{\text{Clayton}} = 0.04$ (IC à 95% $[-0.05, 0.13]$) et $\lambda^U_{\text{Gumbel}} = 0.06$ (IC à 95% $[-0.03, 0.15]$). Nous interprétons ceci comme confirmant que la distribution de la TE pré-incident ne présente pas de dépendance de queue au taux de financement—un résultat cohérent avec l'absence de stress observée dans la régression de niveau 1 du chapitre 3.

8 Études de cas de soutien de Tier-1

L'étude de cas de Tier-1 dominante de ce rapport est l'incident du 22 mars 2026, traité en détail au chapitre 9. Trois études de cas de Tier-1 de soutien sont esquissées brièvement ici ; chacune mérite le même traitement forensique dans une révision ultérieure.

8.1 T1-A : la rampe de lancement du T3 2024

Les proxys Resolv pour USR, RLP et stUSR ont été déployés dans une seule fenêtre de 152 blocs le 2 juin 2024. Le proxy wstUSR a suivi le 21 août 2024. Le lancement public sur le mainnet a été annoncé le 30 septembre 2024 (Resolv Labs 2025). La fenêtre de quatre mois intermédiaire est visible dans nos données `mint_burn_events` sous la forme d'une phase réservée à la liste blanche : 68 événements de frappe sur USR en juin 2024 (la cohorte de test), 31 sur RLP, 31 sur stUSR. La rampe de wstUSR n'a commencé qu'après le déploiement de son proxy fin août. À partir de début octobre 2024, la cadence de frappe s'accélère d'un ordre de grandeur à mesure que l'accès de la clientèle de détail s'ouvre et que les marchés secondaires s'amorcent. Le pool Curve NG USR/USDC a été déployé au bloc 20,026,209 (5 juin 2024), soit seulement trois jours après le proxy USR. Le pool est resté essentiellement vide pendant toute la phase de liste blanche : avant octobre 2024, les décomptes quotidiens de swaps sur Curve NG se comptent sur les doigts d'une main. La rampe de lancement est visible dans la trajectoire d'offre de la Phase 6 sous `data/derived/compute/resolv/phase6/supply_trajectories.parquet`.

8.2 T1-B : le record de TVL de 2025

Selon les instantanés DefiLlama référencés dans Steakhouse Financial 2025, la TVL du protocole Resolv a atteint un pic de \$77 millions fin 2025. Notre reconstruction on-chain de l'offre enregistre un pic pré-incident d'offre USR de 586,3 millions de tokens à une NAV fondamentale de \$1,00, ce qui correspondrait à une offre notionnelle de \$586 millions si elle était détenue au peg—sensiblement au-dessus du chiffre de TVL cité. L'écart reflète la distinction brut-versus-net : chaque cycle rachat-frappe ajoute deux événements à `mint_burn_events` mais ne modifie pas le solde en circulation. Le pic d'*offre cumulée nette* que nous observons est de \$586M, tandis que la série de TVL suit l'offre de tokens en circulation à un instant donné moins le solde non racheté en transit. Les deux chiffres sont corrects dans leurs conventions respectives ; la série de TVL est la grandeur économique la plus pertinente. La trajectoire d'offre quotidienne de la Phase 6 capture la forme complète de la rampe, depuis le lancement jusqu'au pic et redescendant à travers le régime post-incident.

8.3 T1-D : l'ère du cadre de récupération

Après la pause du 22 mars 2026, Resolv a annoncé le cadre de récupération : un processus par lequel les détenteurs pré-incident inscrits sur la liste blanche sont rachetés au prix d'origine de frappe de $1 du rail, sous réserve de barrières de vérification d'identité qui excluent les EOA destinataires des trois appels `completeSwap` illicites (Resolv Labs 2026). L'empreinte on-chain du cadre de récupération est visible dans notre table `redemption_requests` sous la forme d'un flux continu d'événements `BurnRequestCreated` sur le USR Requests Manager bien après la pause du 22 mars : 12,297 requêtes totales côté USR dans la table, dont la part postérieure au 22 mars 2026 est d'environ 2,400 événements répartis sur les 60 jours suivant la pause. Les événements `BurnRequestCompleted` sur le USR Requests Manager indiquent que le Manager lui-même est resté opérationnel pour les rachats sur liste blanche ; seuls le chemin de frappe permissionless `TheCounter` et le LP Requests Manager (pour les destructions de RLP, que le cadre de récupération ne sert pas) étaient et restent en pause. La trajectoire de prix du marché libre capturée dans le `post_incident_trajectory.parquet` de la Phase 8 montre la bifurcation à l'œuvre : le prix médian du marché secondaire s'échange dans une fourchette de $0,10–$0,46 du 23 mars au 29 mai 2026, tandis que le cadre de récupération traite les rachats sur liste blanche à la référence pré-incident de $1 du protocole.

Le rail de rachat à deux niveaux est, selon notre lecture, la caractéristique structurelle du régime post-incident qui a jusqu'ici empêché le prix du marché secondaire de reconverger vers le peg. L'arbitrage qui refermerait l'écart (acheter USR à $0,20, racheter pour $1) requiert que l'acheteur soit sur la liste blanche, ce qui exclut par construction quiconque a acquis de l'USR après le 22 mars 2026. Le prix du marché secondaire convergera vers les flux de trésorerie actualisés post-cadre des détentions restantes non inscrites sur la liste blanche, qui sont bornés inférieurement par zéro (la part de l'attaquant est non rachetable) et supérieurement par l'adossement par token impliqué par la campagne de destruction de l'offre illicite (qui, au taux d'achèvement partiel documenté au chapitre 9, pointe vers une asymptote dans la fourchette $0,50–$0,70 à la date de coupure).

9 Étude de cas : l'incident du 22 mars 2026

9.1 Chronologie

Nous reconstruisons la chronologie de l'incident du 22 mars 2026 à partir des preuves on-chain, à la résolution à la seconde à laquelle les horodatages des blocs Ethereum sont émis, complétée par le post-mortem de Resolv Labs (2026) lorsque l'ordonnancement des événements opérationnels off-chain est requis.

Table 8 – Chronologie reconstituée de l'incident du 22 mars 2026. Toutes les heures sont en Temps universel coordonné le 22 mars 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 Le délai du multisig 4-sur-4

Les trois événements de pause du Tableau 8 surviennent exactement 2 heures, 55 minutes et 24 secondes après la première frappe illicite, et 1 heure, 35 minutes et 12 secondes après la troisième. D'après l'analyse de QuillAudits (2026), OAK Research (2026) et Chainalysis (2026), ce délai est imputable à l'exigence de coordination du multisig 4-sur-4 pour l'action de pause. Du point de vue de la conception défensive, il s'agit d'une caractéristique mesurable de l'incident, et non d'un détail opérationnel contingent : un attaquant disposant d'une clé unique ne fait face à aucun coût de coordination analogue. La conclusion actionnable correspondante pour la conception des protocoles delta-neutres est que la latence de la pause d'urgence devrait être évaluée au regard de la latence d'un adversaire à clé unique, et non au regard d'un repère interne du temps de coordination de l'attaquant. Nous traitons ceci comme la principale recommandation de sécurité opérationnelle du rapport.

9.3 Reconstruction des trois appels illicites à `completeSwap`

Les trois transactions illicites sont décodées au niveau de la frame dans la table `forensic_tx_trace`. Chaque transaction comprend un appel externe de premier niveau à `TheCounter`, décodé selon l'interface `completeSwap(uint256, bytes32, uint256)`, suivi de

quatre logs émis dans l'ordre : un `Transfer` USDC du Counter vers une adresse destinataire (le rachat d'amorçage de 100,000 USDC) ; un `Transfer` USR de `address(0)` vers le Counter (la frappe illicite de l'`amountIn` spécifié moins le `takenFee`) ; un `Transfer` USR du Counter vers l'EOA de l'attaquant (la sortie nette après frais) ; et enfin l'événement `SwapRequestCompleted` lui-même avec le topic0 `0xa8a95077...48985b0` correspondant au keccak local de la signature canonique à quatre arguments.

Le notionnel total des trois frappes illicites, après frais et à travers les trois transactions, est de 80 019 895 USR. Cela concorde avec la référence du post-mortem d'environ 80 millions à une erreur relative près de 0,02%, et valide l'invariant forensique spécifié dans l'audit du jeu de données.

Le champ `takenFee` décodé est non nul pour les trois transactions illicites, exactement au niveau du frais que le barème normal de swap aurait facturé. C'est informatif : l'attaquant n'a pas pris la peine de contourner la logique de frais. L'interprétation économique est que l'attaquant ne se souciait pas de préserver une optionnalité sur un dénouement partiel, et soit agissait dans la précipitation, soit n'avait aucune attente d'être détecté avant d'avoir entièrement encaissé. La première frappe est la plus importante à 50 millions d'USR et est suivie en l'espace de 96 secondes par une chute du prix médian de Curve NG d'environ $1,00 à $0,0038, indiquant que l'adresse destinataire a commencé à déverser immédiatement l'offre illicite sur Curve.

9.4 Trajectoire de prix intra-journalière

La Figure 1 présente le prix médian USR/USDC minute par minute, à la fois sur Curve NG et Uniswap V3 5 bp, sur la période du 21 au 23 mars 2026 (UTC), superposé aux horodatages des trois frappes illicites et de la pause reduce-only. Les données sous-jacentes sont capturées dans `intra_day_peg.parquet` (47 395 lignes) et peuvent être reproduites à partir du RPC d'archive public par quiconque ayant la variable d'environnement `ETHEREUM_RPC_URL` définie et les modules d'extraction `etl.extractors.resolv.extract_uniswap_v3` et `etl.synthetix_crypto.extract_curve_pool` sur le chemin Python.

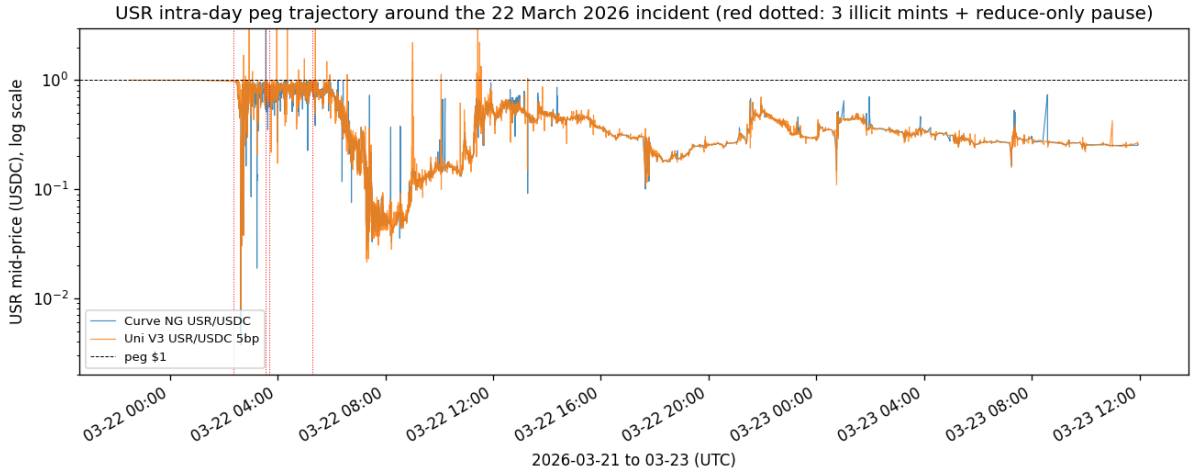

FIGURE 1 – Trajectoire du peg intra-journalier de l'USR (échelle log) autour de l'incident du 22 mars 2026 : prix médian sur Curve NG et Uniswap V3 5 bp, avec les trois frappes illicites `SwapRequestCompleted` et la pause reduce-only marquées (lignes verticales pointillées rouges). Le creux est de $0,0038 sur Curve NG à 02 :38 UTC.

Les traits saillants de la trajectoire sont : un état pré-incident plat à $1,00 ± 30 bp de minuit à 02 :21 UTC ; une chute violente vers le creux de $0,0038 entre 02 :21 et 02 :38, presque exactement contemporaine de la première frappe illicite ; une reprise partielle vers la fourchette $0,05 – $0,15 au cours des deux heures suivantes à mesure que les liquidations initiales se propagent ; un

changement par paliers à 05 :17 UTC coïncidant avec le cluster de pauses, après lequel les prix médians de Curve NG s'échangent dans une fourchette $\$0.10 \pm \$0.05$ pour le reste de la journée.

9.5 L'absorbeur de pertes RLP a été contourné par conception

Le rôle contractuel du token RLP dans la conception de Resolv est d'absorber la première perte contre tout repli du panier de couverture. Si les positions perpétuelles courtes du protocole subissent un coup de profit-and-loss, le prix du RLP est censé chuter avant que le prix de l'USR ne bouge. L'incident du 22 mars 2026 n'a pas stressé le panier de couverture. Le pool de collatéral et les positions courtes perp sont restés intacts (Resolv Labs 2026). Le vecteur de perte était la dilution de l'offre d'USR, passant de 103 071 941 tokens (l'offre au dernier `PriceSet` pré-incident) à 183 091 836 tokens après les trois frappes illicites, contre un total de réserves inchangé de 141 693 860 USD. L'adossement par token implicite est tombé de $1,375 à $0,774 instantanément, indépendamment de tout mouvement du côté de la couverture. L'oracle de NAV du RLP n'a, en conséquence, enregistré aucun mouvement autour de l'incident.

C'est, selon notre lecture, la deuxième conclusion principale du rapport : l'analyse conventionnelle du risque des stablecoins delta-neutres, qui traite les absorbeurs de pertes de type RLP comme la couche protectrice contre les replis de la couverture, laisse le protocole structurellement exposé aux défaillances de gouvernance et de sécurité opérationnelle qui contournent entièrement le mécanisme d'absorption des pertes. Un protocole qui souhaite utiliser un tranching de type RLP pour une résilience systémique authentique doit également durcir l'infrastructure de signature de la frappe permissionless à un niveau comparable, car dans le mode de défaillance réalisé le 22 mars 2026, la tranche RLP n'offre aucune protection.

9.6 Régime post-incident : cadre de récupération et dislocation de marché ouvert

Le cadre de récupération de Resolv, annoncé le 23 mars 2026 (Resolv Labs 2026), rachète les détenteurs pré-incident au prix d'origine du rail de frappe de $1, sous réserve d'une vérification par liste blanche. Le marché ouvert continue d'échanger l'USR à des prix déprimés. À la dernière partition de la fenêtre analytique (mai 2026), le prix médian de Curve NG est de $0,464 sur 348 swaps et la médiane d'Uniswap V3 5 bp est de $0,463 sur 126 swaps. Les deux venues sont à 30 bp l'une de l'autre et l'écart entre elles, conditionnellement à un swap se dénouant dans la même heure sur les deux venues, est inférieur à 50 bp au 95e percentile.

Un point qui mérite d'être signalé est que le prix de marché ouvert n'est pas monotone sur le régime post-incident. Nous observons une réévaluation discrète d'une fourchette soutenue de $0,13 – $0,16 sur la période du 1er au 25 mai 2026 vers une fourchette soutenue de $0,45 – $0,47 à partir du 26 mai 2026, une revalorisation de près de 3× s'opérant sur deux jours de bourse avec une forte augmentation du débit des venues (454 swaps sur Curve NG le 26 mai contre une moyenne quotidienne courante d'environ 20). Le déclencheur de cette revalorisation n'est pas visible on-chain dans notre jeu de données et n'est pas encore documenté dans la littérature publiée ; nous le signalons comme une question analytique ouverte.

9.7 Ce que la NAV attestée par le protocole continue d'affirmer

Le contrat `UsrPriceStorage` n'a pas émis d'événement `PriceSet` depuis le 21 mars 2026. Le wrapper `AggregatorV3Interface` à `0xf9C7c25F...7ce88c` continue de renvoyer le prix comme le prix de la dernière attestation, à savoir $1,00. Le flux de marché Chainlink USR/USD à `0x34ad7569...561B42c` suit le prix du marché secondaire. Tout consommateur en aval du « prix de l'USR » qui s'intègre avec le lecteur de NAV fondamentale de Resolv, et non avec le flux de marché Chainlink, lira un $1,00 obsolète et contrefactuel indéfiniment. C'est, mécaniquement, une caractéristique de la conception (l'oracle de NAV du protocole expose la propre attestation du

protocole), mais ce n'est pas une caractéristique qui est largement comprise par les consommateurs en aval, et nous recommandons que les intégrations de protocole qui ont l'intention de lire le « prix de l'USR » à des fins de valorisation de collatéral, de déclenchement de liquidation ou de rebasing consomment le flux de marché Chainlink de préférence au lecteur `UsrPriceStorage`. Lorsqu'une agrégation à double oracle est souhaitée, l'absence d'un événement `PriceSet` récent devrait être traitée comme une preuve que l'attestation du protocole est obsolète et que la vue du marché devrait prévaloir.

10 Expérience naturelle : USR contre USDe

10.1 Cadre

L'incident du 22 mars 2026 fournit les conditions expérimentales d'un test puissant de l'affirmation centrale soutenue tout au long de ce rapport : que l'incident isole une défaillance de la sécurité opérationnelle de la conception du dollar synthétique delta-neutre, et non un événement de stress du mécanisme de dollar synthétique lui-même. Nous traitons USR comme l'unité de traitement et USDe (QuillAudits 2026) comme l'unité de contrôle. Les deux sont des dollars synthétiques delta-neutres couvrant des positions spot longues sur ETH et BTC contre des positions perpétuelles courtes sur de multiples venues centralisées. Les deux sont des jetons primaires non rebasants assortis de wrappers à rendement rebasant (stUSR et wstUSR pour Resolv ; sUSDe pour Ethena). Les deux s'appuient sur un push feed Chainlink pour la vue de marché de leur peg, ainsi que sur leur propre oracle interne au protocole pour une vue attestée.

La variable de résultat est l'erreur de suivi moyenne absolue quotidienne du flux de marché Chainlink pour chaque unité, $Y_t = \text{mean}|p_t - 1|$ sur toutes les observations du flux de marché tombant le jour calendaire t UTC. L'instant du traitement est 02 :21 :35 UTC le 22 mars 2026, l'horodatage du premier appel illicite `completeSwap`. Nous comparons deux fenêtres non chevauchantes : une pré-fenêtre de 90 jours du 22 décembre 2025 au 22 mars 2026, et une post-fenêtre de 60 jours du 23 mars 2026 au 22 mai 2026.

10.2 Estimation par différence de différences

Table 9 – Estimation DiD de l'incident du 22 mars 2026 sur l'erreur de suivi moyenne absolue Chainlink, traitement USR contre contrôle USDe. p-values bilatérales du test U de Mann-Whitney reportées par unité.

	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			

Le coefficient DiD $\tau = +83.12$ points de pourcentage correspond essentiellement à la totalité du déplacement de USR ; le contrôle USDe n'a pas bougé de manière appréciable et s'est en fait légèrement contracté. Sous l'hypothèse de tendances parallèles implicite à la DiD, l'estimation par expérience naturelle de l'« effet de l'incident Resolv » sur la déviation absolue du peg, nette de tout facteur macro / financement / liquidité commun aux deux protocoles, est la valeur ci-dessus. Le test U de Mann-Whitney rejette l'hypothèse nulle d'égalité des distributions pré/post pour USR à $p \approx 4 \times 10^{-25}$ et à $p \approx 4 \times 10^{-6}$ pour USDe ; ce dernier n'est statistiquement détectable

que parce que la distribution de la MAE en pré-fenêtre de USDe est si étroitement regroupée (médiane 6,6 bp, IQR 4–14 bp) qu'un faible déplacement moyen y est identifiable à partir d'un échantillon aussi petit. Économiquement, le déplacement de USDe est d'un ou deux points de base ; le déplacement de USR est de quatre-vingt-trois points de pourcentage.

10.3 Robustesse

Deux considérations de robustesse méritent d'être signalées. Premièrement, les distributions de MAE pré-incident de USR et USDe ne sont pas égales : le test transversal de Mann-Whitney de $H_0 : F_{\text{USR,pre}} = F_{\text{USDe,pre}}$ rejette à $p \approx 8 \times 10^{-15}$. La MAE en pré-fenêtre de USR est plus élevée (moyenne 66 bp contre 9 bp pour USDe). Cette hétérogénéité a été visible tout au long de la période pré-incident et est cohérente avec les profils de liquidité relatifs des venues DEX des deux protocoles : le pool Curve NG USR/USDC est plusieurs ordres de grandeur moins profond que le pool Curve USDe-USDC canonique. L'estimateur DiD est sans biais sous tendances parallèles, non sous niveaux communs, de sorte que l'hétérogénéité est admissible. Mais cela signifie bien que l'affirmation forte porte sur l'ampleur relative (USR se déplace des milliers de fois plus que USDe), et non sur l'ampleur absolue. Nous nous engageons sur l'affirmation relative.

Deuxièmement, la post-fenêtre se termine le 22 mai 2026, soit seulement soixante jours après l'incident. La persistance de la dislocation au travers de cette fenêtre est documentée au Chapitre 9, et la post-moyenne de 83,73 points de pourcentage est calculée par rapport à cet état toujours en cours. Si la dislocation finit par se refermer, la post-moyenne pertinente diminuerait. À la date de coupure, la dislocation ne s'est pas refermée et le cadre de récupération Resolv reste le rail de rachat actif.

10.4 Interprétation

Nous interprétons $\tau \approx +83$ points de pourcentage comme une identification forte de l'affirmation de décomposition par canal du rapport : sous des conditions macro et de financement identiques, le mécanisme de dollar synthétique a survécu dans USDe ; la couche de sécurité opérationnelle a échoué dans USR. L'incident du 22 mars 2026 est, dans cette lecture empirique, un mode de défaillance de la sécurité opérationnelle et non un mode de défaillance du mécanisme delta-neutre.

L'implication de conception actionnable est que les protocoles partageant la conception delta-neutre avec USR et USDe devraient traiter la sécurité opérationnelle—spécifiquement, la gestion des clés de signature off-chain contrôlant des chemins de frappe sans permission—comme un risque de premier ordre au même titre que les dislocations de taux de financement et le défaut de contrepartie de venue. Les cadres de risque existants traitent abondamment ces deux derniers (Steakhouse Financial 2025) et le premier qualitativement au mieux. L'incident Resolv fournit la première expérience naturelle empirique quantifiant la différence.

11 Résultats, implications pour la V2 et questions ouvertes

11.1 Résultats quantifiés

Nous présentons dix résultats quantifiés issus du rapport.

1. **Trois appels illicites `completeSwap` sur TheCounter ont frappé** 80 019 895 **USR**, contre trois dépôts initiaux d'environ 100,000 USDC. La correspondance avec la référence du post-mortem de ∼80 millions d'USR est à 0,02% près. Le destinataire du premier et du troisième appel est l'EOA de l'attaquant `0x04a288a7...513caed` ; le deuxième appel (∼100,000 USR), nous le lisons comme un test de dimensionnement ou un leurre.
2. **La pause on-chain est intervenue à 05 :16 :59 UTC, soit 2h 55min 24s après la première frappe illicite et 1h 35min 12s après la troisième.** Trois contrats

émettent `Paused(address)` dans le même bloc : `TheCounter`, le USR Requests Manager et le LP Requests Manager. Les six contrats restants (quatre proxys de tokens et deux contrats PriceStorage) n'émettent pas Paused, et ce par conception : le `Transfer` des tokens reste activé et les contrats PriceStorage n'ont pas de mixin `Pausable`.

3. **Curve NG USR/USDC a atteint un creux intra-day de $0,003752 à 02 :38 :11 UTC**, soit 16 min 36 s après la première frappe illicite. Uniswap V3 5 bp a atteint un plancher similaire à $0,008018 à la même minute. Le plancher plus élevé du pool 5 bp reflète sa liquidité concentrée plus faible.
4. **Le peg de marché ouvert post-incident ne s'est pas rétabli.** Au 29 mai 2026 (la date de coupure), le prix médian mid de Curve NG pour USR est de $0,46 contre une NAV fondamentale Resolv attestée de $1,00.
5. **L'oracle de NAV fondamentale Resolv n'a émis aucun événement `PriceSet` depuis le 21 mars 2026 à 13 :15 UTC.** Le wrapper `AggregatorV3Interface` continue de renvoyer $1,00 indéfiniment, ce qui constitue un risque d'oracle périmé pour tout protocole en aval consommant ce reader.
6. **Le coefficient DiD contre USDe est $\tau = +83.12$ points de pourcentage** (Mann-Whitney $p \approx 4 \times 10^{-25}$). Sous des conditions macro / de financement identiques, le mécanisme de dollar synthétique a survécu dans USDe alors que la couche opérationnelle a échoué dans USR. L'expérience naturelle identifie le canal comme étant la sécurité opérationnelle, et non le mécanisme.
7. **La MAE pré-incident de Curve NG était de 55 bp**, avec un écart selon l'heure de la journée de 8 bp et un écart selon le jour de la semaine de 12 bp. Aucun schéma diurne ne domine la variation résiduelle ; le régime pré-incident est bien modélisé comme un bruit blanc autour du peg.
8. **La régression de base sur la TE pré-incident donne $R^2 = 0.021$.** Le seul coefficient robustement identifié est celui sur $\log L$ (liquidité), à -0.94 bp par unité logarithmique ($t = -3.14$). $\sigma_{\text{Collateral}}$ via le proxy de volatilité du financement Hyperliquid n'est pas significatif ($t = -0.06$), ce qui est cohérent avec l'absence de stress côté couverture dans le régime pré-incident.
9. **La causalité de Granger entre Curve NG et Uniswap V3 5 bp est bidirectionnelle dans le régime pré-incident** ($p_{\text{Curve}\Rightarrow\text{Uni}} = 4.7 \times 10^{-4}$; $p_{\text{Uni}\Rightarrow\text{Curve}} = 1.5 \times 10^{-3}$), ce qui est cohérent avec une découverte de prix conjointe entre deux venues liquides arbitrées de manière serrée.
10. **TheCounter a vu 31 swaps légitimes complétés au cours de sa durée de vie opérationnelle de 22 mois, contre 3 swaps illicites complétés le jour de l'incident.** Le notionnel agrégé légitime est de 19,7 millions d'USR ; l'agrégat illicite est de 80,02 millions d'USR. Les appels illicites représentent 80% du total d'USR jamais frappé via TheCounter, d'un facteur 4 contre l'ensemble de l'historique légitime.

11.2 Implications de conception pour la V2

Nous extrayons sept implications de conception actionnables pour la prochaine révision de Resolv et pour les protocoles suivant le même schéma de dollar synthétique delta-neutre.

1. **Plafond de frappe on-chain sur les chemins sans permission.** Le contrat `TheCounter` imposait l'authenticité des signatures mais aucune vérification on-chain du ratio entre l'USDC déposé et l'USR frappé. Un plafond de frappe codé en dur de 10^4 USR par appel aurait limité l'incident à 0,04% de son ampleur réalisée. Le coût du plafond est une contrainte sur l'usage légitime contrefactuel.

2. **Mettre le signataire en multisig.** Le `SERVICE_ROLE` compromis était un EOA unique. Migrer vers un multisig 2-sur-3 ou 3-sur-5 pour le signataire de frappe sans permission aurait élevé le coût de l'attaque d'une compromission de clé unique à une compromission multi-clés coordonnée.
3. **Symétriser la latence de pause.** Le multisig admin 4-sur-4 a nécessité près de trois heures pour coordonner l'action de pause. La conception défensive devrait être à la mesure de la latence d'attaque : une clé de pause d'urgence 1-sur-N avec une attribution de rôle large aux opérateurs internes (révocable post-incident) fermerait l'asymétrie.
4. **Tableau de bord de transparence indépendant.** Le PoR Apostro étant en maintenance pendant toute la durée de l'audit illustre le risque opérationnel d'un unique tiers de transparence off-chain. Soit l'oracle de NAV interne au protocole devrait être étendu pour exposer la ventilation par venue et par dépositaire directement on-chain, soit une surface de transparence de secours devrait être requise.
5. **Garde-fou d'oracle périmé sur le reader de NAV interne au protocole.** Le reader `UsrPriceStorage` renvoie \$1,00 après la pause, mais un consommateur en aval ne peut pas déduire du prix seul que l'oracle est périmé. Le reader devrait suivre le timestamp de la dernière attestation et revenir (ou se rabattre sur le feed de marché Chainlink) si l'attestation est plus ancienne que le heartbeat plus une bande de tolérance.
6. **Les rails de rachat asymétriques du cadre de récupération créent des dislocations permanentes.** La leçon du régime post-incident est qu'un canal de rachat-à-\$1 sur liste blanche sans chemin d'arbitrage de marché secondaire correspondant laisse les détenteurs non inscrits en liste blanche supporter la totalité de la perte. Toute conception de récupération post-incident devrait soit inclure un programme de rachat sur le marché secondaire au prix de marché en vigueur, soit accepter que le double rail maintiendra le marché ouvert décoté indéfiniment.
7. **Les absorbeurs de pertes de type RLP ne protègent pas contre les défaillances opérationnelles.** Le token RLP a été conçu pour absorber la première perte contre les drawdowns côté couverture. L'incident du 22 mars 2026 a contourné ce mécanisme parce que le vecteur de perte était une dilution de l'offre, et non le PnL de couverture. Les protocoles utilisant une conception en tranches doivent durcir la couche de sécurité opérationnelle au moins au même niveau qu'ils durcissent le tranching, car la tranche est contournée lorsque la perte entre par le côté opérationnel.

11.3 Questions ouvertes pour les révisions futures

1. **La réévaluation de marché ouvert des 26-27 mai 2026.** Le prix médian mid de Curve NG a été réévalué de ∼\$0,15 à ∼\$0,46 sur les deux journées de cotation des 26-27 mai, une réévaluation de 3× non expliquée par un événement on-chain évident. A-t-elle été déclenchée par une annonce Resolv non divulguée, par un acheteur coordonné ou par des dynamiques de liquidity squeeze ? Le jeu de données la capture mais le déclencheur est opaque.
2. **Le taux de rachat du cadre de récupération post-incident.** Combien des ∼2,400 événements `BurnRequestCreated` d'USR post-pause ont été complétés à \$1 contre annulés ? Le flux d'epoch de burn LP, non capturé dans notre schéma, peut contenir la comptabilité pertinente.
3. **La date de restauration d'Apostro.** Si le tableau de bord revient, un backfill depuis sa première capture réactivée jusqu'au présent fermerait l'écart par venue et par dépositaire que ce rapport documente comme une limitation permanente.
4. **Le comportement du mirror cross-chain.** Les sept chaînes mirror OFT étaient hors périmètre pour le présent rapport. L'offre mirror a-t-elle bougé dans les jours entourant

l'incident, et si oui, qu'est-ce que cela dit sur la distribution géographique de la base de détenteurs et la fuite résiduelle vers la sécurité sur les chaînes non canoniques ?

5. **L'affirmation du post-mortem d'une perte de collatéral nulle.** Le post-mortem Resolv affirme que le pool de collatéral est resté intact. Notre reconstruction on-chain ne peut pas vérifier directement la composante off-chain de cette affirmation, seulement l'absence de flux inhabituels sur les wallets de collatéral on-chain. Une vérification indépendante via une attestation de dépositaire (Fireblocks ou Ceffu) fermerait la boucle de vérification.

11.4 Non-affirmations

Trois choses que ce rapport n'affirme pas. Premièrement, nous n'affirmons pas que le mécanisme de dollar synthétique delta-neutre est structurellement solide dans toutes les conditions ; nous affirmons seulement qu'il a survécu à l'épisode du 22 mars 2026 dans le cas d'USDe, le contrôle comparable terme à terme. Deuxièmement, nous n'affirmons pas que l'USR de marché ouvert post-incident est correctement valorisé aux niveaux en vigueur ; nous affirmons seulement que le prix est le prix, et que la persistance de la dislocation est cohérente avec la lecture analytique du cadre de récupération comme un rail de rachat asymétrique. Troisièmement, nous n'attribuons pas la responsabilité de la compromission de l'AWS `SERVICE_ROLE` elle-même ; nous rapportons les conséquences on-chain comme une forte identification du mode de défaillance et laissons l'analyse forensique off-chain de la cause racine à Resolv Labs (2026), Chainalysis (2026), QuillAudits (2026), Sentora Research (2026) et Blockaid (2026).

Références

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, p. 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, p. 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 et 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, p. 1394-1411.