

Vector (SG) — Sample Initial Tracing Report

Methodology demonstration based on a public incident. Not legal advice. Not a statement about any person.

Incident used: BNB Smart Chain "Token Hub" (BNB Bridge) exploit, 6 October 2022 (UTC)

Prepared by: Vector (SG), Singapore on-chain forensics and risk intelligence ·

cryptosec@mail.grokbots.com

Report type: Stage 1 — Initial Tracing Report (sample)

Data snapshot: fetched 27 October 2026, 23:35–23:50 (Asia/Shanghai, UTC+8)

Times: every time is shown in UTC and, in brackets, Asia/Shanghai (CST = UTC+8).

How to read this sample. This is the deliverable format of our paid Stage 1 service, produced on a *public historical* incident so that nothing here concerns a client. Every transaction hash, address, amount and timestamp in this document was taken from chain data that we fetched ourselves (§7). Names of services come only from cited public sources, each with a confidence level. We do not identify natural persons and we make no accusation. Verification marks: ✓ opened/fetched and verified in this work · ♦ secondary source only · ? not verified.

1. Executive summary

- **What happened (on-chain).** The exploiter address `0x489A8756C18C0b8B24EC2a2b9FF3D4d447F79BEc` received **two payouts of 1,000,000 BNB** from the BNB Token Hub system contract (tx `0xebf83628...efe3b8b` at 2022-10-06 18:26:46 UTC and tx `0x05356fd0...e5c57a` at 20:43:18 UTC; 02:26:46 and 04:43:18 CST next day). Both are decoded from receipt logs ✓.
- **Where it went on BSC.** Within about three and a half hours the address (a) deposited 900,000 BNB into Venus and borrowed 62.5M BUSD + 50M BSC-USD + 35M USDC, (b) swapped $\approx 79,956$ BNB and 10M BUSD on PancakeSwap, and (c) bridged **136,043,518.63** units of stablecoins (face value, USDT/BUSD/USDC) out of BSC in 27 Stargate and 19 Multichain calls (Stargate 62,043,518.63; Multichain 74,000,000.00). The address's complete BSC history is 94 transactions (nonces 0–93), all captured.
- **Where it landed.** Bridged funds went to the *same address* on Ethereum, Avalanche, Polygon, Arbitrum, Optimism and Fantom. On Ethereum we traced arrivals, DEX swaps, issuer freezes and later consolidation: **33,771.03 ETH** moved to a second address on 2022-10-07 18:15:35 UTC (02:15:35 CST on 10-08), swapped to stETH in January 2023 and moved to a third address in February 2023.
- **Freeze touchpoints.** Tether blacklisted the exploiter at 2022-10-06 21:24:59 UTC and Circle at 2022-10-07 01:34:35 UTC (both read from on-chain events ✓). The funding of the address came through the instant-exchange service ChangeNOW (High confidence for the service; Medium for the address-level label). **No centralized-exchange deposit address was identified in the window we traced** — we say so rather than force one.
- **What this sample does not do.** It does not trace the Avalanche, Fantom, Polygon, Arbitrum or Optimism legs, does not reconstruct every swap output on Ethereum, and does not claim any funds are recoverable. See §8.

2. Scope and sources

Scope. (i) BSC activity of the exploiter address from first funding to its last bridging transaction; (ii) Ethereum-side arrivals, swaps, issuer freezes and consolidation of the same actor; (iii) public attribution of the services touched. Out of scope: the vulnerability root cause, other chains' legs, identification of any person.

#	Source	Used for	Status
S 1	BSC public RPC <code>bsc-dataseed.binance.org</code> (full-block scan, receipts, logs, <code>eth_call</code> symbol/decimals)	all BSC facts	✓ fetched
S 2	Blockscout Ethereum API (<code>eth.blockscout.com</code> , v2 and Etherscan-compatible <code>/api</code>)	Ethereum transfers, address labels, issuer freeze events	✓ fetched (third-party indexer)
S 3	Coinbase, "BSC Token Hub Compromise investigation and analysis", 2022-10-31	cross-validation of timeline, funder, ChangeNow and Binance statements	✓ opened; statements taken from it are unless re-derived on-chain ◆
S 4	ChangeNOW press release (GlobeNewswire, 2022-10-11 12:46 ET)	funding via ChangeNOW; address blocked	✓ opened (excerpts saved in <code>sources/</code>)
S 5	Stargate V1 and PancakeSwap v2 contract-address documentation	router/pool address identity	✓ opened
S 6	Multichain (Anyswap) router label	router identity	◆ secondary only; Ethereum-side counterpart carries Blockscout label "Multichain: Fantom Bridge" ✓
S 7	SlowMist and SharkTeam incident analyses	—	? not opened; not relied on

Confidence scale. *High*: on-chain fact or ≥ 2 independent sources agree. *Medium*: one public label/source, or an inference from direct transfers. *Low*: pattern similarity only (none used for conclusions in this sample). Confidence applies to attributions, not to on-chain facts.

3. Incident summary

On 2022-10-06 attackers abused the BNB Beacon Chain ↔ BSC cross-chain bridge so that the system contracts released $2 \times 1,000,000$ BNB to a single address. Public post-mortems describe a flaw in cross-chain proof verification ◆ (this sample does not analyse it). The BNB Chain network was halted by validators for several hours afterwards (Coinbase gives 22:19 UTC for the announcement ◆). Coinbase estimates that about US\$110M left BSC ◆; our decoded stablecoin bridging total is 136,043,518.63 units at face value (including a 15 BUSD test). We have **not** reconciled the two figures.

On-chain preparation (nonces 0-13, 2022-10-05 22:11 → 2022-10-06 16:55 UTC). The address was funded with 101.54371362 BNB in two transfers from `0x975d9bd9...cd94b`, ran small tests (Venus, Alpaca, WBNB, a 15 BUSD Stargate transfer, a 0.1 BNB transfer to `0xcfb55da...b4ca`), then sent 100 BNB to the system contract `0x...1006` (RelayerHub per Coinbase ◆).

Exploit and cash-out (18:26 → 21:44 UTC). Two successful exploit calls (nonces 14 and 86; 15 reverted attempts in between, nonces 71-85). Funds were borrowed against, swapped and bridged, always to the exploiter's own address on the destination chain (decoded from calldata, \$7).

4. Fund-flow graph

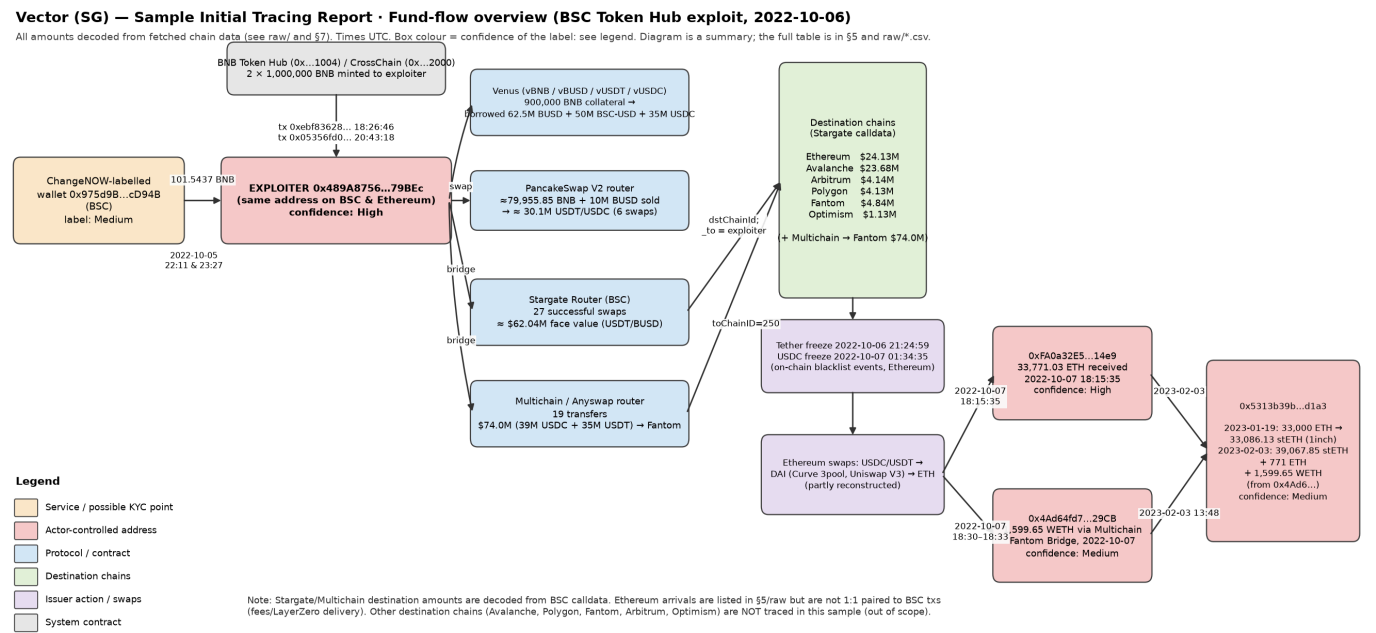


Figure 1. Summary of the traced flow. Stablecoin figures are face value (1 unit ≈ US\$1, not a market price). Stargate/Multichain amounts are decoded from BSC calldata; Ethereum arrivals are listed separately and are not paired 1:1 with BSC calls.

Bridged out of BSC, by destination (successful calls, stablecoin face value):

Destination chain	Units
Fantom	78,835,427.31
Ethereum	24,128,349.08
Avalanche	23,678,045.83
Arbitrum	4,138,255.06
Polygon	4,130,898.75
Optimism	1,132,542.59

5. Hop-by-hop trace table

Times: UTC with Asia/Shanghai (CST) in brackets. Chain: BSC = BNB Smart Chain, ETH = Ethereum mainnet. Hashes are abbreviated; full hashes are in Appendix A and in raw/trace_table.csv. "Basis" says how the row was established.

Hop	Time	Chain	From → To	Asset / amount	Tx	Basis
H1	10-05 22:11:04 UTC (10-06 06:11:04 CST)	BSC	0x975d9B... cD94B → exploiter 0x489A...79BEc	0.44889193 BNB	0xaa6ce682...bc3ae4	On-chain ; funder label: Coinbase 2022- 10-31 (Medium)
H2	10-05 23:27:54 UTC (10-06 07:27:54 CST)	BSC	0x975d9B... cD94B → exploiter	101.09482169 BNB	0xa84f85e1...6d0d1d	On-chain
H3	10-06 15:19:57 → 15:54:15 UTC (10-06 23:19:57 → 23:54:15 CST)	BSC	exploiter → Venus vBNB, Alpaca ibBNB, WBNB, Stargate (15 BUSD → Avalanche); last test: 0.1 BNB → 0xcfb55...b4ca	Test txs, nonces 0-12 (≈0.1-0.4 BNB, 15 BUSD)	0x1b7b6b15...0179a5 0xe83050fe...d2d292 0xb64a9986...cb5d57	On-chain ; Coinbase calls nonce 12 a 'transfer to ChangeNow'

Hop	Time	Chain	From → To	Asset / amount	Tx	Basis
H4	10-06 16:55:06 UTC (10-07 00:55:06 CST)	BSC	exploiter → 0x...1006 (RelayerHub, per Coinbase)	100 BNB	0xe1fe5fef...3396d6	On-chain ; system-contract identity
H5	10-06 18:26:46 UTC (10-07 02:26:46 CST)	BSC	0x...2000 (CrossChain) call → 0x...1004 (TokenHub) pays exploiter	1,000,000 BNB minted (log data 0xd3c21bce...a1000000 = 1e24 wei); block 21,957,793	0xebf83628...fe3b8b	On-chain (receipt log decoded)
H6	10-06 18:30:13 → 18:36:07 UTC (10-07 02:30:13 → 02:36:07 CST)	BSC	exploiter → Venus vBNB (mint)	600,000 BNB (→ 27,521,993.91 vBNB) + 300,000 BNB (→ 13,760,996.56 vBNB)	0xf9d91162...4a70ab 0x30a2e002...04ca77	On-chain ; vBNB contract name via on-chain symbol()
H7	10-06 18:31:04 → 18:37:28 UTC (10-07 02:31:04 → 02:37:28 CST)	BSC	Venus vBUSD / vUSDT / vUSDC → exploiter (borrow)	62,500,000 BUSD; 50,000,000 BSC-USD (symbol 'USDT'); 35,000,000 USDC	0xbda0344d...6dd3be 0x049ba44a...5758ff 0xad3b410e...297041	On-chain (token transfers decoded)
H8	10-06 18:32:58 → 20:05:52 UTC (10-07 02:32:58 → 04:05:52 CST)	BSC	exploiter → Stargate Router 0x4a364f...18D8 (swap; <code>_to</code> = exploiter's own address on dst chain)	Wave 1: Ethereum 10x, 24,128,349.08; Avalanche 6x, 19,995,428.67; Arbitrum 3x, 4,138,255.06; Polygon 3x, 4,130,898.75; Optimism 1x, 1,132,542.59; Fantom 1x, 898,087.00	0x79067c22...99eec5 0x967dd1d3...9e8ae3	Calldata decoded ; router/pool addresses match Stargate docs
H9	10-06 18:52:59 → 20:15:21 UTC (10-07 02:52:59 → 04:15:21 CST)	BSC	exploiter → Multichain router 0xd1c596...b5f3 (anySwapOutUnd erlying, toChainID 250 = Fantom)	Wave 1: anyUSDC 10x, 39,000,000.00; anyUSDT 7x, 27,000,000.00	0xb82cebec...bf0dd3 0xa13cc857...b0dda4	Calldata decoded ; router label
H10	10-06 20:12:10 → 20:17:53 UTC (10-07 04:12:10 → 04:17:53 CST)	BSC	exploiter → PancakeSwap V2 router 0x10ED43...024E	10,000,000 BUSD → 9,064,835.32 USDT; 15,655.85 BNB → 4,000,000 USDC; 34,300 BNB → 8,863,252.62 USDT	0x0cc52b19...f48037 0xa0c7203e...335952 0x98fd7e0e...c2aa61	On-chain ; router per PancakeSwap docs
H11	10-06 20:32:00 → 20:42:54 UTC (10-07 04:32:00 → 04:42:54 CST)	BSC	exploiter → 0x...2000 (CrossChain)	15 reverted calls (status 0), nonces 71-85	0xf2c714b6...047dc9 0xcf127483...61c9f7	On-chain
H12	10-06 20:43:18 UTC (10-07 04:43:18 CST)	BSC	0x...2000 call → 0x...1004 pays exploiter	1,000,000 BNB minted; block 21,960,470 (Coinbase text repeats the first hash by typo; on-chain tx is this one)	0x05356fd0...e5c57a	On-chain
H13	10-06 20:50:00 → 21:43:36 UTC (10-07 04:50:00 → 05:43:36 CST)	BSC	exploiter → PancakeSwap V2 router	3 × 10,000 BNB → 2,773,134.38 / 2,724,315.23 / 2,707,999.87 USDT	0x00a1be26...e8ab61 0x0b6e7e59...ab3978 0xb55cbd53...c86e28	On-chain
H14	10-06 20:50:41 → 20:51:17 UTC (10-07 04:50:41 → 04:51:17 CST)	BSC	exploiter → Stargate Router	Wave 2: Fantom 1x, 3,937,340.31; Avalanche 1x, 3,682,602.16	0xf84deb63...d31f88 0xa7beda0c...ee9f03	Calldata decoded
H15	10-06 21:32:28 → 21:43:59 UTC (10-07 05:32:28 → 05:43:59 CST)	BSC	exploiter → Multichain router	Wave 2: anyUSDT 2x, 8,000,000.00 (last tx on BSC = 4,000,000 USDT)	0x61cf9882...5726aa 0x9e45bfc...4a674a	Calldata decoded
H16	10-06 18:35:35 → 21:32:11 UTC (10-07 02:35:35 → 05:32:11 CST)	ETH	Stargate <i>SUSDT</i> / <i>SUSDC</i> pools → exploiter 0x489A...	12 arrivals: USDT 21,135,251.05; USDC 6,709,374.37	0x72eab47e...f86502 0x07c846c8...5830c0	Blockscout transfers (indexer); labels from Blockscout metadata
H17	10-06 19:09:47 → 21:20:47 UTC (10-07 03:09:47 → 05:20:47 CST)	ETH	Multichain: Fantom Bridge and 'Avalanche: Bridge' → exploiter	Fantom bridge: 8,999,000 USDC + 7,497.25 WETH; Avalanche bridge: 12,879,246.65 USDC + 855,317.03 USDT + 2,299.97 WETH	0xcc43c00a...0fb2d6 0x81f45296...ec9918	Blockscout

Hop	Time	Chain	From → To	Asset / amount	Tx	Basis
H18	10-06 18:56:23 → 20:46:59 UTC (10-07 02:56:23 → 04:46:59 CST)	ETH	exploiter → Curve 3pool (USDC→DAI), Uniswap V3 pools, two Vyper contracts (USDT)	USDC 3,998,094.20 + 8,999,000 → DAI 12,995,494.74 (→ Uniswap V3); USDC 12,879,246.65 → Uniswap V3; USDT 8,006,919.37 + 3,121,602.31 + 6,083,954.48 → Vyper contracts	0x07d6ce86...01b4600x249aeb65...966b020x77eca758...e0a3310x925eed1d...9107da0x557252ff...c978c40x7973605a...ab41a50x16a3f3a1...b55466	Blockscout ; swap outputs not fully reconstructed (see §8)
H19	10-06 21:24:59 UTC (10-07 05:24:59 CST)	ETH	Tether: AddedBlackList(exploiter)	USDT freeze of 0x489A... (block 15,691,728)	0xaaafa4200...dd8dc8	On-chain event (matches Coinbase 21:24:59)
H20	10-07 01:34:35 UTC (10-07 09:34:35 CST)	ETH	Circle: Blacklisted(exploiter)	USDC freeze of 0x489A... (block 15,692,969; Coinbase says 01:34:34)	0x5ea742c3...cd9f86	On-chain event
H21	10-07 18:09:23 → 18:15:35 UTC (10-08 02:09:23 → 02:15:35 CST)	ETH	exploiter → 0xFA0a32E5...14e9 ('BNB Bridge Exploiter 2', Blockscout); also unwrap of WETH at 18:14:35	1 ETH test (18:09:23); 9,797.218063 WETH unwrapped (18:14:35); 33,771.03279121 ETH (18:15:35, block 15,697,931)	0xb2f3148c...697ba00x22f19d7d...2afe7b0x74701d88...ff26d9	Blockscout . NB: Coinbase timeline dates the '33K ETH' move at 18:09:23; on-chain 18:09:23 is the 1 ETH test
H22	10-07 18:30:23 → 18:33:47 UTC (10-08 02:30:23 → 02:33:47 CST)	ETH	Multichain: Fantom Bridge → 0x4Ad64fd7...18F29CB	99.9 WETH + 1,499.75 WETH (= 1,599.65 WETH)	0x3e63eeb1...40f9830xf273ef09...5c75d7	Blockscout ; link to exploiter via Coinbase timeline
H23	01-19 01:40:47 UTC (01-19 09:40:47 CST)	ETH	0xFA0a... → 1inch AggregationRoute v4 → 0xFA0a...	33,000 ETH sent → 33,086.13038 stETH received (block 16,437,632)	0x087db327...acd3df	Blockscout
H24	01-19 01:42:59 → 01:59:47 UTC (01-19 09:42:59 → 09:59:47 CST)	ETH	0x68EA8490... (unlabelled) → 0xFA0a...	4,588.04538 stETH + 1,308.621821 stETH — source not analysed	0x87dfee02...b3a19b0x532cfd92...73ffad	Blockscout
H25	02-03 13:46:35 → 13:48:11 UTC (02-03 21:46:35 → 21:48:11 CST)	ETH	0xFA0a... and 0x4Ad6... → 0x5313b39B...D1a3 ('BNB Bridge Exploiter', Blockscout)	39,067.85303 stETH + 771 ETH (from 0xFA0a...); 1,599.65 WETH (from 0x4Ad6...)	0x390c3e9f...75ba4d0x96db0ae8...1b489f0x043313a4...57b47e	Blockscout
H26	10-20 13:08:11 UTC (10-20 21:08:11 CST)	ETH	Polygon (Matic) ERC20 bridge exit → exploiter 0x489A... (exit()) sent by unlabelled EOA 0xCB66...d3d9)	3,631,976.429995 USDT (block 26,233,996)	0x143b7031...f33e96	Blockscout (post-incident; relation of caller unknown)

Failed bridge calls (nonces 26, 43, 49; Stargate) are excluded from totals.

6. Service touchpoints, confidence and recommended requests

Our rule: a "touchpoint" must be a service that actually received, held, or can restrict the funds — not a label that merely appears next to an address.

Service	Where	What we can show	Confidence	Recommended request (illustrative; for counsel to decide)
ChangeNOW (instant swap service)	BSC funder 0x975d9B...cD94B → exploiter (H1, H2); nonce 12 test transfer	S4 states the initial funds were swapped through ChangeNOW and the recipient address was blocked; S3 shows the two funding txs and calls nonce 12 a "transfer to ChangeNow"	High (service); Medium (address-level label: Blockscout has no label for the funder; address label rests on S3)	Preserve and disclose order/swap records for the two funding txs (order IDs, deposit address, any KYC/IP data) via the proper legal channel

Service	Where	What we can show	Confidence	Recommended request (illustrative; for counsel to decide)
Tether (USDT)	Ethereum; exploiter address	AddedBlackList event, block 15,691,728, 2022-10-06 21:24:59 UTC . No Tether freeze event found for the other three addresses in blocks 15,690,000–16,500,000 . On 2026-10-20 the exploiter address received 3,631,976.43 USDT via the Polygon bridge (H26)	High	Confirm freeze scope for USDT held by the exploiter address, including the 2026-10-20 arrival; ask whether other actor-linked addresses are in scope
Circle (USDC)	Ethereum; exploiter address	Blacklisted event, block 15,692,969, 2022-10-07 01:34:35 UTC (Coinbase: 01:34:34 — one-second difference, we use the block timestamp)	High	Confirm status; note most USDC had already been swapped (Curve/Uniswap V3, H18)
Stargate / LayerZero	BSC router; Ethereum pools (H8, H16)	Calldata and pool addresses ; no custody of the funds after delivery	High (identity)	Information request only: delivery records, destination-chain transaction links
Multichain (bridge)	BSC router; "Multichain: Fantom Bridge" on Ethereum (H9, H17, H22)	Calldata decoded ; router label	Medium-High	Information request; verify the service's current operating status before sending any request
Venus Protocol	BSC lending (H6, H7)	900,000 BNB deposited; 147.5M stablecoins borrowed	High	Position data (liquidation/repayment outcome) — not traced here
Binance (BNB Chain)	BSC	Per S3, blocklisted the exploiter for cross-chain transfers at 22:19 UTC on 2022-10-06	Medium	Not re-verified on-chain
1inch, Uniswap, Curve, PancakeSwap, Lido (stETH)	routing / liquidity	Non-custodial protocols; used as routing evidence only. No issuer-level freeze path identified in our sources	n/a	None
Centralized-exchange deposit address	—	None identified in the traced window	—	—

Why label hits are not touchpoints. The exploiter's Ethereum history contains inbound dust (e.g. two 2-USDT transfers from an address Blockscout labels "Okx 7", 2022-10-07 04:53:59 and 05:15:11 UTC) and spam-token airdrops. Receiving dust from a labelled wallet says nothing about where the stolen funds went, so we exclude it.

7. Evidence integrity

How the data was fetched. BSC: `src/fetch_bsc_scan.py` scans blocks 21,933,517 → 21,962,264 on `bsc-datasee d.binance.org` with batched `eth_getBlockByNumber` (full transactions) and keeps every transaction sent by or to the watched addresses; `src/fetch_bsc_receipts.py` fetches receipts/logs; `src/decode_bsc.py` decodes ERC-20 transfers and system-contract logs; `src/analyze_bridges.py` decodes Stargate `swap()` (selector `0x9fbf10fc`: word 0 = LayerZero dst chain id, word 1/2 = src/dst pool id, word 4 = amount, word 7 = offset of `_to`) and Multichain `any SwapOutUnderlying` (`0xeddbf5e2`; `toChainID` 250 = Fantom). Ethereum: `src/fetch_eth_blockscout.py`, `src/derive_eth_le g.py` and `src/fetch_freeze_events.py` (Blockscout; logs for Tether/Circle blacklist events). `src/build_report.py` assembles the tables from the raw files; `src/make_graph.py` draws Figure 1.

Completeness check. The exploiter's BSC transaction count is 94 (nonces 0–93); the scan found 94 outgoing transactions plus inbound ones. Post-incident inbound transactions from third parties (dust/message transactions) are not part of the flow; their payloads are untrusted data and were not acted on.

Fetch times and heads (Asia/Shanghai). BSC scan: 2026-10-27 23:39:50 CST. Ethereum Blockscout pull: 2026-10-27 23:39:13 CST. Chain heads when checked: Ethereum block 26,284,995 (2026-10-27 15:38:35 UTC = 23:38:35 CST); BSC head block 130,115,925 (`0x7c16955`) at about 23:47 CST. Block numbers of key events are

in §5. Blockscout counters (113–114 transactions, 302–328 token transfers for the exploiter on Ethereum) changed slightly between calls; treat them as a snapshot.

Integrity. SHA-256 of every raw file is in `raw/SHA256SUMS.txt`. Reproduce: `cd sample-report && python3 src/fetch_bsc_scan.py && python3 src/fetch_bsc_receipts.py && python3 src/decode_bsc.py && python3 src/analyze_bridges.py && python3 src/fetch_eth_blockscout.py && python3 src/fetch_freeze_events.py && python3 src/derive_eth_leg.py && python3 src/build_report.py`. Ethereum data depends on a third-party indexer; for evidence use, key facts should be re-confirmed on an archive node. Public BSC RPC nodes are pruned (no historical balances/nonces), so historical state was not used.

8. Limitations

1. **Not traced:** the Avalanche, Fantom, Polygon, Arbitrum and Optimism legs. We only know what was sent (BSC calldata) and, for Ethereum, what arrived. In particular the 2026-10-20 Polygon-bridge exit (H26) shows funds were still moving on those legs years later.
2. **Not reconciled:** per-transaction pairing of BSC bridge calls with Ethereum arrivals (fees and delivery delays); our 136,043,518.63 bridged total versus Coinbase's $\approx$ US\$110M estimate; the roughly 1.02M BNB (2,000,000 minus 900,000 deposited to Venus minus $\approx$ 79,956 sold) that was neither deposited nor sold (its fate was not traced; BSC historical balances are unavailable on pruned RPC).
3. **Ethereum swap outputs** (ETH/WETH legs, internal transactions) were not reconstructed in full; the path from stablecoins to the 33,771 ETH is therefore partly inferred from input amounts and timing.
4. **Open item:** Blockscout lists a USDC transfer transaction by the exploiter at 2022-10-07 18:11:11 UTC (tx `0x9ae7e324...447031`, block 15,697,910) after the USDC blacklist, with no token transfer attached. We draw no conclusion from it.
5. **Discrepancies noted:** Coinbase's timeline places the 33K ETH transfer at 18:09:23 UTC; on-chain that time is the 1 ETH test and the 33,771 ETH transfer is at 18:15:35. Coinbase's text repeats the first exploit hash for the second exploit; on-chain it is `0x05356fd0...`. Circle freeze: Coinbase 01:34:34 vs block timestamp 01:34:35.
6. **Labels** are public, mostly single-source; the funder label and the labels for `0x4Ad6...18F29CB` and `0x5313b39B...D1a3` are Medium confidence. "Same actor" for addresses linked by direct transfers is an inference, not proof of identity of any person.
7. S7 sources were not opened. This is a methodology demonstration, not legal advice; Vector (SG) is not a law firm, does not custody funds and does not promise recovery.

9. Next steps — what Stage 2 adds

A real engagement would add: (1) the full multi-chain trace of every destination chain; (2) reconstruction of swap outputs and internal transactions to close value gaps; (3) corroboration of labels with at least two sources and a documented clustering method; (4) identification of exchange/OTC deposit endpoints, if any, with per-service freeze-request packages formatted for counsel; (5) monitoring of the identified addresses and services with alerts; (6) a reproducible evidence bundle (hashes, scripts, node/indexer versions). Stage 2 depends on the matter and is quoted separately; see the Vector (SG) one-pager for commercial terms. Nothing in this report is a promise of recovery.

Appendix A — Full transaction hashes referenced in §5

Hop	Tx hash
H1	<code>0xaa6ce682daef66aa2bfc2741e5ec30ce93958fd86d2d4d256c416a58e2bc3ae4</code>
H2	<code>0xa84f85e1afc3e1b8ed5111ba16e11325f8fc5d6081cb6958becd6a333f6d0d1d</code>
H3	<code>0x1b7b6b151435b2a1d925e4165ff5ff886d72de54c3bcfb6e0a602033520179a5</code>
H3	<code>0xe83050fefadd55d2e9c72bfeacc334b28e1116506f2af256e1ed986929d2d292</code>
H3	<code>0xb64a99866ba0c727482919ceee149b761005c4d40c11dc1676ad02cad9cb5d57</code>
H4	<code>0xe1fe5fef26e93e6389910545099303e4fee774427d9e628d2aab80f1b53396d6</code>
H5	<code>0xebf83628ba893d35b496121fb8201666b8e09f3cbadf0e269162baa72efe3b8b</code>
H6	<code>0xf9d911624b5294652ec7f0b9fa7817f2a5953860411325e7f6e73d87f14a70ab</code>
H6	<code>0x30a2e002b7e5c634199b6e71efaad806454d2df752eb3d7897027f6f0404ca77</code>

Hop	Tx hash
H7	0xbda0344dc9c96bbc5cab60bae8c7622195e68c392cf45f64ecb7c8c5806dd3be
H7	0x049ba44ab978687b26f8d45d48b446f5db30ae9c47d77dce6ec11124cb5758ff
H7	0xad3b410e3adeb9193bfcc0b185cf1b20314a02b03f8cf9a1b5adae9f6297041
H8	0x79067c22ab23cc142a59f82641a6d634474780fc54c985286317b2626499eec5
H8	0x967dd1d3ec76c32afe202f7a3753ae3484219c73571c4f335ece7ecb3a9e8ae3
H9	0xb82cebece047f4089961e9e1bdbc90a653ac8f8d8cd8763bb051a1a82bf0dd3
H9	0xa13cc857bd8eed4cbd8465b441a3da001f93a21674aed82c3e6046b0c4b0dda4
H10	0x0cc52b19aac4c2032358fb757d0800177e5a0d27f7ca5398b58fc7fd24f48037
H10	0xa0c7203ec666805f1666634144835d1a87241483222a536b02e0285619335952
H10	0x98fd7e0e4f1be0949421a796d82498fce1940c3b270c421fd096f7fe78c2aa61
H11	0xf2c714b6b006fc9c633d5d95ddec05a76402f9607e114fcece30656f25047dc9
H11	0xcf127483bd05d5cfb4ee6d113dcabe7b7c3c45ae3eb7c65efb4a687c6161c9f7
H12	0x05356fd06ce56a9ec5b4eaf9c075abd740cae4c21eab1676440ab5cd2fe5c57a
H13	0x00a1be26863411fba6d17666c1dfbc48cf7a3a85527ab532f885a02ac1e8ab61
H13	0x0b6e7e5928bdb935feeb0d73bad3513e12a0eac464c11d97cfc491ce1aab3978
H13	0xb55cbd538b7775b3d87586ba2ebf32de7fac1fa1e6a06bae1dfa28af9bc86e28
H14	0xf84deb6346f1460f48a69cb5df339c63dbc0497e9c235e895d5fa1f436d31f88
H14	0xa7beda0c43f45d57efd88fb3ccaf26e1f4ec60706b10556897717a3288ee9f03
H15	0x61cf9882d529f04a79d9ce5fcb0a3c8433c3c4d6740c9012f48aed5c3f5726aa
H15	0x9e45bfca33157998df92fae3eacb5815c02f74217899ccfe554dcc6e8e4a674a
H16	0x72eab47e822de2dd4ee554f02f678be72cac656f8d00479e1362d32f95f86502
H16	0x07c846c80f69e1b75979175e602d3756948028ed21ca5a53cd0174dc495830c0
H17	0xcc43c00a61c98d3cb446881b3fe2583bba42287f94df6ef8ea4685491a0fb2d6
H17	0x81f45296f6fc1db01938b12351eeef0ec78251aa6be7f1e036d42ac8aec9918
H18	0x07d6ce86197cc608368f75f7d062ebfa0705eeea52e9789d9161d3e86c01b460
H18	0x249aeb65b6335d01a53e92e832b1d59469b9a874f27b4a8a6124e657ea966b02
H18	0x77eca75801b98a4effcae267561ef39e60eaf2889c6f27d6535a55efd6e0a331
H18	0x925eed1d337a39f1020e03aa79f72357224252a987bdf93915a98b31139107da
H18	0x557252ffbebfcb79fba9e7e8818eb02bae8321c3df4a852a6d33feb88bc978c4
H18	0x7973605ab2611c025acbebfdddee95103993789784bb650a91d39b74debab41a5
H18	0x16a3f3a1481d8a8384ac8e3279b7270896796577a1e1f728e56b42ae0cb55466
H19	0xaaafa4200c567b429a9ac2353162d551188d2bf01221ebbbcf09e170dfdd8dc8
H20	0x5ea742c33f82662d8b68455abcf5605051a6ca24073b3bae84a00c1d38cd9f86
H21	0xb2f3148ce03ad509d107ab00b571497ba3c72167e342b008fd3fc30353697ba0
H21	0x22f19d7def2a6e3b40a99fe151f300c1c5c43432cb4d62ce59fd32f8712afe7b
H21	0x74701d8816a4b3b6c377dfb1dab2edd5abfe7ad92d114905aaf151a701ff26d9
H22	0x3e63eeb1f2d200499d19ce795042b366fa8b416739b985f9e512a2646040f983
H22	0xf273ef09ec26c6a67c8b7b7cd72d3322fc3337a31724df841356d4b7795c75d7
H23	0x087db3274281971534697405e238b7d2dd1bb5e1bc53c8cea1ce569890acd3df
H24	0x87df00c949f66a64e4a5832f38c5b255ca6ae8fa747856900c696d8eb3a19b
H24	0x532cf92b6667769ae57d7033179626deb66a0ce0eaf444f9de45d9b1a73ffad
H25	0x390c3e9f9ce83277cb1e74ca2825b7146354a7d8c4429948bafc2c07cf75ba4d
H25	0x96db0ae8afe7f6c40287a7a27f152a4cf48653865fb8cc60466a0357f71b489f
H25	0x043313a41c8fa779c1e9236f5033dfc5a14ce4d7dae600b3169f0519db57b47e
H26	0x143b703122f4bac0dfc87217f758d00fd8b0d2e44ee73a02650e73a095f33e96

Key addresses. Exploiter 0x489A8756C18C0b8B24EC2a2b9FF3D4d447F79BEC · funder 0x975d9bd9928f398c7e01f6ba236816fa558cd94b · Stargate Router 0x4a364f8c717cAAD9A442737Eb7b8A55cc6cf18D8 · Multichain router 0xd1C5966f9F5Ee6881Ff6b261BBE4a5972B1B5f3 · PancakeSwap V2 router 0x10ED43C718714eb63d5aA57B78B54704E256024E · consolidation 0xFA0a32E5C3386

123122b6B68099001D9371d14e9, 0x4Ad64fd7cA6D6150614179B9bCE4094Bc18F29CB, 0x5313b39bf226ced2332c81eB97BB28c6fD50d1a
3.