CASE FILE / PRELIMINARY REPORT / REVISION 2.2

The Binance Hot Wallet Drain

Binance hot wallets across ten blockchains were emptied in one window on 29 October 2026. This document records what the on-chain evidence shows. Every address in the table is hyperlinked in the PDF and on this site.

- Snapshot 30 October 2026, 13:06 UTC. Updated 31 October 2026, 09:19 UTC.

TEN CHAINS

Ethereum | Bitcoin | XRP | Solana | Tron | Arbitrum | Avalanche | Polygon | Optimism | Base

PRELIMINARY

$6.36B VALUE TAKEN, TRM ESTIMATE	**10** CHAINS HIT	**~$2.27B** FROZEN, MEASURED SUBTOTAL
~$2.4B ATTACKER-HELD ETH/BTC	**481,581** ETH ETH TRACKED	**18,270** BTC UNSPENT

481,581 ETH tracked = 474,338 in six tracked wallets + 7,242.76 ETH converted from AVAX on 30 October. In USD, 6.36B taken (TRM estimate) = 2.27B frozen + 2.4B attacker-held + 1.69B not reconciled. The 2.4B is ETH and BTC only; the 2.27B is four stablecoins. On 31 October, 44.23M OP was moved by the Optimism portal admin. Frozen estimates: 2.27B measured, 2.85B Elliptic, 3B Binance.

Prepared by **Keshav Maheshwari**
withkeshav.com

What changed / 31 October update

Three movements since the first note. Two are material. None changes the main picture.

01 / OPTIMISM

44.23M OP moved by the Optimism portal admin

One Ethereum transaction upgraded the Optimism portal, produced a deposit record and restored the real implementation. The OP now sits in an Optimism Safe alias. This is not an attacker return.

L1 tx 0xd80476b3... / block 26309074 / 00:10:59 UTC

02 / AVALANCHE

2.06M AVAX converted into 7,242.76 ETH

Eight swaps sold AVAX for USDC, CCTP burned and minted it on Ethereum, and the USDC was swapped into ETH. The ETH sits in a new wallet that has never sent a transaction.

30 October 2026, 12:44 UTC / 0x294828705974ad04d86a24a2ff6efe762505a0ed

03 / BLOCKLIST

34 of 51 case addresses are listed by Elliptic

All 19 Bitcoin wallets match. List presence is a publisher label, not proof of control or value allocation. The list changed between snapshots.

3,295 rows / sha256 f527db39... / 08:52 UTC

WHAT IS LIMITED

No public Optimism statement was found explaining the move, so intent is unknown. The AVAX swap-by-swap route table was not available to replay, so only the end state is verified. The blocklist is a label, not proof. The Safe's native internal history is incomplete. These are limits, not negative results.

19 / 19	970,554	$2.27B
BITCOIN WALLETS STILL UNSPENT	SOL STILL PARKED	FROZEN STABLECOINS UNCHANGED (SUBTOTAL)

Timeline / 28 to 31 October 2026

One window, plus the recovery actions that followed. All dates and times are UTC.

28 October 2026 UTC

Morning — Main wallet funded through Tornado Cash, three withdrawals of 0.1 ETH on 28 and 29 October.

29 October 2026 UTC

15:59 — **Sweeper contract deployed** on Ethereum `0x63e842B054Bd624a465454D533C33F573e9c6fAe`

20:05 — **XRP Ledger emptied**, 233.46M XRP from five wallets.

20:10 — **Solana and Optimism** hot wallets emptied.

20:20 — 50 EIP-7702 authorizations submitted in one batch, **one matched the nonce**.

20:24 — **Binance 14 emptied**, 167,464 ETH and 1.615B USDT taken.

20:25 — Ten more hot wallets emptied across four chains.

20:41 — More sweeps using the same access.

21:01 — **Tether froze 971.1M USDT, 1.38B in total including the 1.175B holding balance.**

21:04 — **Circle froze 823M USDC.**

22:10 — World Liberty froze 27.8M USD1; Ripple froze 40.5M RLUSD.

23:05 — **Second wave** on Avalanche and Polygon.

23:35 — Binance reported $2.54B frozen, later about $3B (company figures; measured inventory $2.27B).

30 October 2026 UTC

00:10 — **Attacker access revoked**, sweeper could no longer move funds.

00:18 — Arbitrum forced 8,426 ETH and 74.6M ARB out of the attacker wallet (emergency call at 00:08).

11:41 — **AVAX converted.** 2.06M AVAX sold per route update (register: 1.81M received + 444.5K later), bridged by CCTP to Ethereum, 7,242.76 ETH by 12:44.

Ongoing — Money moved through Aave and decentralised exchanges; Bitcoin split into 19 wallets, none moved.

31 October 2026 UTC

00:10 — **Optimism portal upgraded** in one transaction, a deposit record produced, the implementation restored. 44.23M OP moved.

00:12 — The deposit executes on L2, paying the OP to the Safe alias `0x6b1bae59...`

00:39 — A lookalike token forges a transfer to a similar address, aimed at the new holder.

08:17 — The holding wallet sends 4.29 ETH in the main transfer, 4.39 ETH in total, to a new wallet. Frozen stablecoins stay in place.

08:52 — Elliptic blocklist updates to 3,295 rows. 34 of 51 case addresses are listed.

The money flow / ten chains

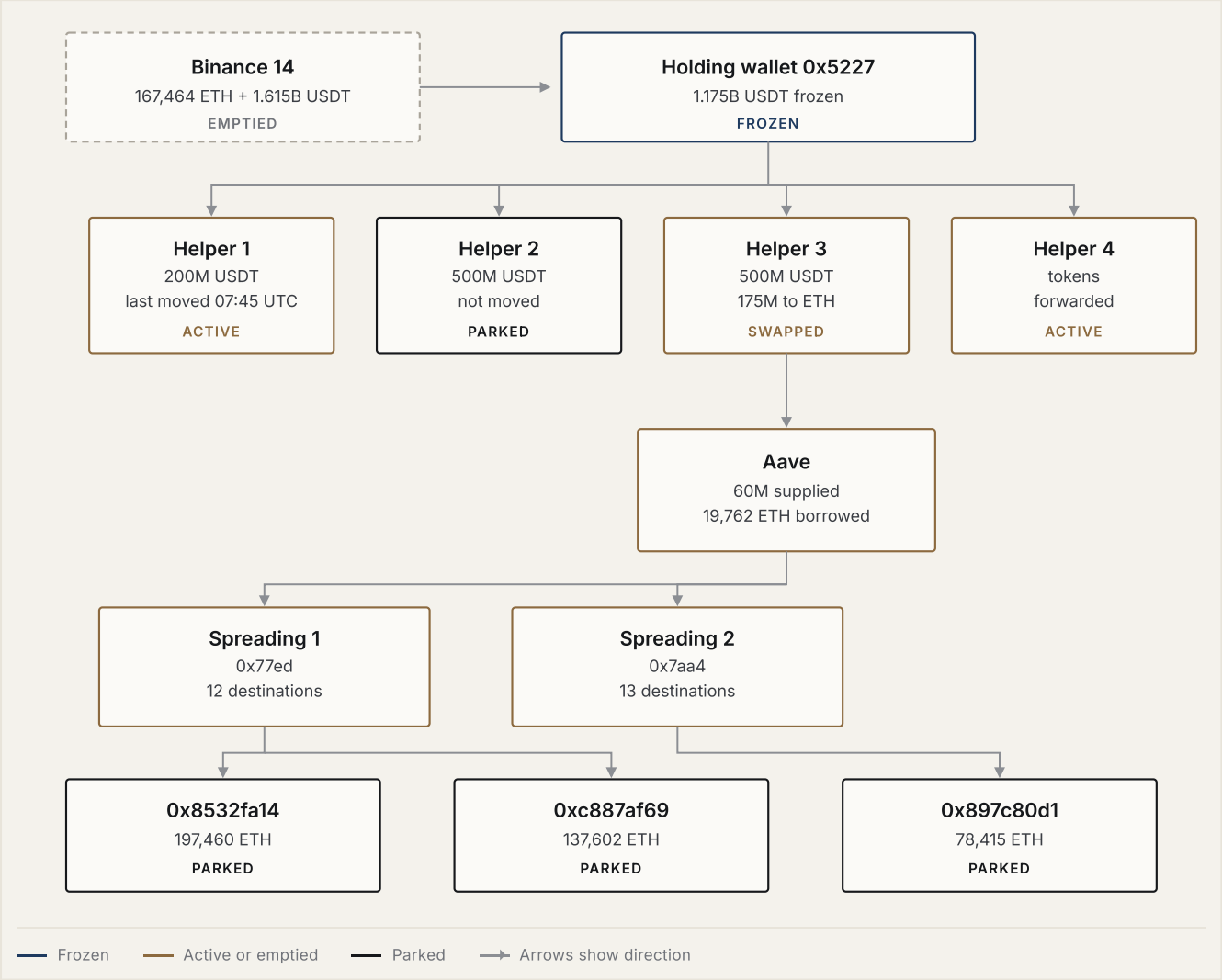
Where each chain's funds went. The Ethereum branch is detailed on the next page.

SOURCE — Binance hot wallets on ten chains, 29 October 2026

Ethereum	167,464 ETH + 1.615B USDT	Holding, four helpers, Aave, two spreading wallets	● 474,338 ETH PARKED
Bitcoin	18,270 BTC	Split into 19 wallets, none has moved	● PARKED
XRP	233.46M XRP	Taken from five wallets, no outgoing seen	● PARKED
Solana	970,554 SOL	Receiver holds the balance, no outgoing	● PARKED
Tron	612.7M USDT	Received, 312.7M later retained	● PARTLY HELD
Arbitrum	8,426 ETH + 74.6M ARB	Forced out by the Security Council	● QUARANTINED
Avalanche	2.06M AVAX (route update)	Sold, bridged by CCTP, swapped into ETH	● 7,242.76 ETH
Optimism	44.23M OP	Seized by the Optimism portal admin	● MOVED
Polygon	46.6M POL	Collected, later moved	● MOVED
Base	small	Hot wallet emptied	● EMPTIED

The Ethereum branch / detail

The largest branch, traced on-chain from the emptied hot wallet to the wallets still holding the ETH.



No funds from the spreading wallets reached an exchange deposit. Still on-chain.

167,464 ETH	1.175B USDT	100M USDT	413,477 ETH
TAKEN FROM BINANCE 14	FROZEN IN THE HOLDING WALLET (PART OF 1.38B)	SWAPPED ON UNISWAP, SEPARATE LEG	PARKED IN THREE WALLETS

Reading the totals. The parked ETH includes other native inflows to the same wallets, not only the Binance 14 sweep. The helper balances overlap; the same USDT can pass through more than one wallet.

New branch, 30 October. The route update reports 2.06M AVAX sold (the register records 1.81M received plus 444.5K later), bridged to Ethereum by CCTP and swapped into 7,242.76 ETH. That ETH now sits at 0x294828705974ad04d86a24a2ff6efe762505a0ed, which has never sent a transaction.

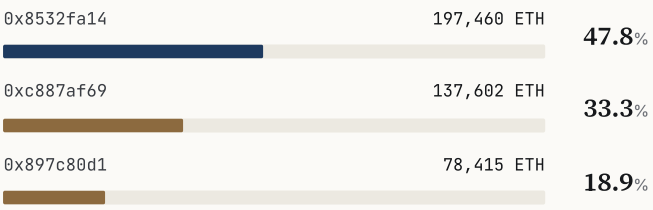
Where the money is now

Status by chain at the 31 October check, followed by the shape of the Ethereum holdings and the overall recovery position.

CHAIN	STATUS	AMOUNT	STATE
Ethereum	474,338 ETH in six tracked wallets	474,338 ETH	● PARKED
Bitcoin	Split into 19 wallets, none moved	18,270 BTC	● PARKED
XRP	Taken from five wallets, no outgoing seen	233.46M XRP	● PARKED
Solana	Parked, no outgoing seen	970,554 SOL	● PARKED
Tron	Received 612.7M, 312.7M retained; 300M not in subtotal	312.7M USDT	● PARTLY HELD
Arbitrum	Forced out by the Security Council	8,426 ETH + 74.6M ARB	● QUARANTINED
Avalanche	2.06M AVAX sold, converted to ETH	7,242.76 ETH	● CONVERTED
Optimism (OP)	Hot wallet emptied; 44.23M OP moved by the portal admin	44.23M OP	● MOVED
Polygon	Collected	46.6M POL	● MOVED
Base (hot wallet)	Hot wallet emptied	Small	● EMPTIED

Where the 413,477 ETH sits

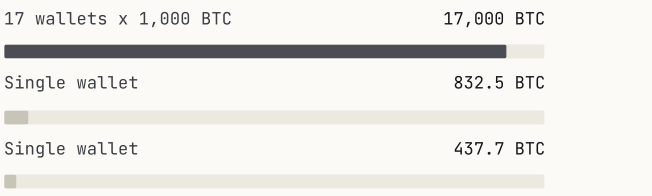
share of parked ETH



Three main wallets, 413,477 of 474,338 tracked. Share, not market value.

How the 18,270 BTC is split

none moved



Nineteen wallets in total, all unspent at the snapshot.

Recovery position of $6.36B

6.36 = 2.27 + 2.4 + 1.69



2.27B frozen + 2.4B attacker-held + 1.69B not reconciled = 6.36B taken. The residual is an accounting figure, not a confirmed position.

CONTAINMENT ACTIONS

21:01 Tether freezes 1.38B USDT

21:04 Circle freezes 823M USDC

22:10 World Liberty 27.8M; Ripple 40.5M

23:35 Binance reports $2.54B frozen

00:18 Arbitrum quarantines 8,426 ETH

Key addresses

The addresses that carry this case. Each one opens on its own explorer.

20 of 51 in this case

CHAIN	ROLE	FULL ADDRESS	STATE
ETHEREUM	**Operator** funded through Tornado Cash, origin	0x7C8601d4645b93cea45F71e118A729332e6B5CA0	ORIGIN
ETHEREUM	**Sweeper** deployed 15:59 UTC	0x63e842B054Bd624a465454D533C33F573e9c6fAe	CONTRACT
ETHEREUM	**Holding wallet** 1.175B USDT frozen	0x5227f603C1eE34CE3C06eFe6477003BDfCCB2f8c	FROZEN
ETHEREUM	**Binance 14** the hot wallet that was emptied	0x28C6c06298d514Db089934071355E5743bf21d60	EMPTIED
ETHEREUM	**Helper 1** 200M received; last move 07:45 UTC	0x0ddf0480016e6bcb2c1f5d190d221fba1320697e	ACTIVE
ETHEREUM	**Helper 2** 500M USDT not moved	0x9749110a86941480dbefca1efdc0ceb528a0c762	PARKED
ETHEREUM	**Helper 3** 500M USDT, 175M to ETH	0x9749292d74fd460982d0912ea9515ea24736c762	SWAPPED
ETHEREUM	**Helper 4** received tokens, forwarded	0x42cdf00c85005630cc8605731b9364f712077810	FORWARDED
ETHEREUM	**Spreading 1** sent to 12 destinations	0x77edef23fbd05921c26fe29fcc3a65e14d2ac3eb	ACTIVE
ETHEREUM	**Spreading 2** sent to 13 destinations	0x7aa4d3029e4c6a8e916300014ad95b6d6c03bfd1	ACTIVE
ETHEREUM	**ETH storage** 197,460 ETH parked	0x8532fa14acaf483729c449b8458aeddb900543d4	PARKED
ETHEREUM	**ETH storage 2** 137,602 ETH parked	0xc887af690e0301cd4edbbce8f8d31b4ec65b286a	PARKED
ETHEREUM	**ETH storage 3** 78,415 ETH parked	0x897c80d1a9729e94460e2bd93178bd5215158df3	PARKED
ETHEREUM	**Safe MEXC 27** 153M USDT, MEXC-labelled	0xf016e1d45ef23bdd414e7a2e4d46e1b34577b508	ATTRIBUTED
BITCOIN	**BTC source** Binance Bitcoin wallet	bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h	SOURCE
BITCOIN	**BTC receiver** all 18,270 BTC arrived here	bc1q0mtc2f5agpkvlq6hhahmfr3hlr55kyfjhl2mnm	PARKED
SOLANA	**SOL receiver** 970,554 SOL parked	AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU	PARKED
OPTIMISM	**OP Safe alias** 44.23M OP moved	0x6b1bae59d09fccbddb6c6cceb07b7279367c4e3b	MOVED
ETHEREUM	**AVAX to ETH** 7,242.76 ETH, never moved	0x294828705974ad04d86a24a2ff6efe762505a0ed	PARKED
ETHEREUM	**Holding outflow** 4.29 + 0.1 ETH, purpose unknown	0x11861b31b97c5c6550d49b03b1eed1a105774084	UNCLEAR

> Click any address to open it on its block explorer and check it yourself. Explorer: Etherscan for Ethereum, the Optimism explorer for the OP alias, mempool.space for Bitcoin, Solscan for Solana.

What the evidence shows

Five findings the on-chain record supports, and the limits of what it can prove.

01 **The evidence points to a compromised signing layer, not one private key.**

EVIDENCE Ten chains produced valid signatures in one short window.

02 **The access was prepared in advance.**

EVIDENCE Fifty EIP-7702 authorizations were submitted in one batch; one matched the nonce.

03 **The attacker wallets were new.**

EVIDENCE They were funded through Tornado Cash before the sweep.

04 **The tracked money stayed on-chain.**

EVIDENCE No exchange deposit observed from the spreading wallets. One 50M USDT leg from the Aave branch reached a wallet labelled MEXC 27.

05 **The Optimism portal admin moved 44.23M OP to its own L2 alias.**

EVIDENCE A separate 2-of-2 Safe owning the portal admin upgraded the portal, produced a deposit record and restored it in one transaction. Intent is not stated publicly.

ATTRIBUTION

TraderTraitor / North Korea

External assessment by TRM Labs and Chainalysis, not proven on-chain; sources on p11. Consistent with the signing pattern, the Tornado Cash funding and how the money was moved.

DPRK

121	116	9
CLAIMS LOGGED, 97 VERIFIED	ADDRESS RECORDS, 99 DISTINCT, 51 IN THIS CASE	CHAINS READ DIRECTLY

WHAT IS PROVEN, WHAT IS ASSESSED

Compromised signing layer	INFERRED FROM CHAIN
50 EIP-7702 authorizations, one matched the nonce	PROVEN ON-CHAIN
Attacker wallets were new	PROVEN ON-CHAIN
No exchange deposit observed from the spreading wallets	OBSERVED ON-CHAIN
Optimism OP move	PROVEN ON-CHAIN
TraderTraitor attribution	EXTERNAL ASSESSMENT

Last on-chain verification: 31 October 2026, 09:19 UTC. The three main storage wallets were unchanged apart from dust. The 4.29 ETH main transfer, 4.39 ETH in total, came from the holding wallet. The OP move and the AVAX consolidation were verified at that time.

Live case. This is a snapshot of a live investigation based on public blockchain data as of 31 October 2026. Details may change as new activity appears. For information only. This is not legal, financial or investment advice. Please check every address and figure yourself. Corrections: contact withkeshav.com.

Archive / how this note developed

Each note is dated and kept. The numbers below are the record, not a promise.

NOTE	DATE AND TIME	PAGES	CLAIMS	VERIFIED
Notes 1	30 October 2026, 13:06 UTC	6	101	82
Notes 2	31 October 2026, 09:19 UTC	11	121	97

NOTES 1 / 30 OCT

The first note

The Ethereum laundering chain, the Bitcoin peel chain of 19 wallets, the Solana receiver, the frozen inventory and the key addresses.

NOTES 2 / 31 OCT

The recovery actions

The Optimism move of 44.23M OP, the AVAX to ETH conversion, the Elliptic blocklist cross-check, and the limits page.

EVIDENCE TRAIL

Case wkoc-CFBW6. Claims register: 121 claims, 97 verified. Address registry: 116 records, 99 distinct, 51 in this case. Revision 2.2 adds the evidence index, the 19 Bitcoin addresses, 20 published addresses, and the moved/produced wording. Revision 2.1 corrected the Arbitrum status to quarantined, the EIP-7702 authorization wording, the 4.29/4.39 ETH scope, and the frozen subtotal labels. The Notes 1 PDF is retained but superseded; its Arbitrum status is out of date. The claim register and address list are in the case archive; raw captures are in the CSI evidence store.

29 Oct **Case opened.** 36 claims logged, first addresses registered, first evidence bundle captured.

30 Oct **Chain mapped.** Ethereum laundering path, 19 Bitcoin wallets, Solana receiver, frozen inventory. 101 claims.

31 Oct **Recovery actions.** Optimism OP move, AVAX to ETH conversion, blocklist cross-check, limits page. 121 claims, 97 verified.

What is limited / and how to read this

Every investigation has edges. These are ours, stated plainly.

01 **Intent of the OP move.** The mechanism is proven on-chain. No public Optimism statement was found, so we do not claim to know why it happened.

02 **The AVAX route.** The end state is verified: 7,242.76 ETH in a wallet that has never moved it. The swap-by-swap route table was not available to replay.

03 **The blocklist.** Elliptic lists 34 of our 51 addresses, including all 19 Bitcoin wallets. A list is a publisher label, not proof of control, and it changes between snapshots.

04 **The Safe.** The 153M USDT balance and the owner set are verified. Its native internal history could not be refreshed completely.

05 **Cross-incident link.** Address ancestry to an earlier incident is established. Common operator control is not proven on-chain, so the same-actor claim remains an external assessment.

06 **The handoff package.** Some referenced evidence files were not present locally. The end states were re-checked on-chain; the per-hash route files were not replayed.

07 **Coverage of the exchange negative.** The 25 traced destinations are not an exhaustive sweep of every exchange deposit address.

08 **Not reconciled value.** About $1.69B of the $6.36B, or 26.6%, is an accounting residual, not a confirmed position.

09 **Price basis.** USD figures use prices at the time of the sweep, from public reporting, not today's price.

10 **Frozen figure.** Estimates differ in scope: our measured four-token subtotal is $2.27B, Elliptic reports about $2.85B frozen or seized, and Binance reports about $3B. The difference is not reconciled.

11 **Chain scope.** Ten chains follows TRM. Elliptic's 31 October assessment includes NEAR, making eleven. This note keeps the ten-chain scope.

Last on-chain verification: 31 October 2026, 09:19 UTC. Ethereum, Optimism, Bitcoin, Solana, XRP, Tron, Arbitrum, Avalanche and Polygon were read directly at that time.

Live case. This is a snapshot of a live investigation based on public blockchain data as of 31 October 2026. Details may change as new activity appears. For information only. This is not legal, financial or investment advice. Please check every address and figure yourself. Corrections: contact withkeshav.com.

Evidence index / replay the findings

Full hashes, blocks and timestamps. Every row is a handle a reader can open.

CLAIM	CHAIN	FULL HASH OR ADDRESS	BLOCK / UTC	VALUE	STATUS
C-047 Binance 14 sweep	ETH	0x53bd38b816c23e74134786c29a8c18d792777998a3b9326047b583100e88e2f3	26,300,770 20:24:23	167,464.247856 ETH 1,615,409,498.97 USDT	MEASURED
C-015 to ETH storage	ETH	0x551d7961652e6d9835b11988908adf86ebe480badb4ce2d7d52193b2b1b02c76	- 20:38:47	195,460 ETH	MEASURED
C-016/17/18 helpers	ETH	0x1fc0ef33a767132edad434834a5555b30fcb5a171206c03b86175ef6dafac81c 0xaf17432b71a40e5ec863622eb874181a5ea4527c003d875f80ad53a79a68711a 0x68d7d69deaeb9750c38020b4f8d3728146ca8d2267eba1e38cf9b56722ad659a	- 20:30-20:33	200M + 500M + 500M USDT	MEASURED
C-050 revocation	ETH	0xafbf94c92a8d749988411669fa14d4f8866d9b4420b4ebd299f28e958dac7209	- 00:10:35	delegation revoked	MEASURED
C-113 OP L1	ETH	0xd80476b3ec56283723804cf7bc2d96f800c81d3ebd0fea843555396ffe94f28f	26,309,074 00:10:59	44,231,858.7 OP	MEASURED
C-107 OP L2	OP	0x120aa6c2e6dac40c0795cace7db7dc8bc09465630c42d271847fc33d2e32bed7	158,903,379 00:12:15	44,231,858.7 OP	MEASURED
C-106 holding outflow	ETH	0x35f0a5f57012656fcad01107b1f1c627f458e513a6d76c472b3ea9f7d368ce90	- 08:17	4.289787807 ETH	MEASURED
C-106b 0.05 ETH legs	ETH	0xb0de506a0e4f90533aa08cc0ddfcb80b643f6878dc596789da49cd37ae8624bf 0x219f5755bb545993f1922a1acb5c4cf6c1be27004ad6c28bc8f5b20a0d7cc892	- 07:35 / 07:53	0.05 + 0.05 ETH	MEASURED
C-108 AVAX to ETH	ETH	0x294828705974ad04d86a24a2ff6efe762505a0ed	- 30 Oct 12:44	7,242.764355 ETH	END STATE
C-057 Arbitrum	ARB	0x0000000000000000000000000000000000000da0	- 00:18:20	8,425.9977 ETH 74,559,805.2 ARB	MEASURED
Elliptic blocklist	multi	sha256 f527db39071f82b31b41bc88cb2b3a6d91f1440322dc8f1fd3f0db5c6ef41482	08:52:19	3,295 rows 34 of 51 listed	THIRD-PARTY

4.39 ETH = 4.289787807 main transfer + 0.05 + 0.05. Further 0.05 ETH transfers the same morning are separate.

BITCOIN PEEL CHAIN, 19 TERMINAL WALLETS (ALL UNSPENT AT BLOCK 973,812)

bc1q0ts8gaf9ht0rr4u02hr56f8thndqsc4kmkmfv3
bc1q42flhayrzy3zh8lkyevw8qcjduurt9a35wlsyx
bc1qalwnl7dtaa73fsq5tyn0ghfy3fgfpqkt69tca8
bc1qepc70u3u476vgvg3hfcwjgu4mecxe2uchs4lag
bc1qg3nrzpuvq2pxqx74tcrywr09dc208ze96n3t53
bc1qm2j6v3247khlwzxl7p9vqnfkghcllyhv9wjaat
bc1qnq6jj9jmlf3945m3l8s0kxnqehrsga300k8t3s
bc1qs3aej5tmcdz0vctz8y9rjcxtxg8v5385577s56
bc1qxg0l4p6xc50zuv9cl5f0l0wmaxjpg8wcy7s9ra
bc1qz8hdwv8gmml0u96dsvnzsagz6krjyzxmgxupdp
bc1q2wvz0kcsn4hqmajwtey30ud27fl25w8pveznn6
bc1q63qrfrpsg5hh0zzn3kp2xx9vljl7dq7tatsjxp
bc1qdfhmlrdvg4tm87zjl0vyf0xflp5ql50q3g88gw
bc1qf5cyvv9w50tx9xx9s3xwsne0z87wvjj9l8a35u
bc1qjwdw6vrzq4vf6hckutvx4ucj86awwv99mxnz7w
bc1qm8v88m5fy6kuq9myva2eemwycxqd3e0zcrs2l8
bc1qrg025e2pgx0rwya2kpgtj30972p64jt0hn6zyt
bc1qs6xnmhar38z44g2za93pv8ygdcwurrh8l87w3v
bc1qxrxujwxfnvz040jw76d26zhjdg5jura7hs968s

Primary sources. Binance, Security Incident Update, 30 Oct 2026, binance.com/en/support/announcement/detail/c5a8729a97ac486d963784d96c5642d7. TRM Labs, North Korea steals $6.36B from Binance, 29 Oct 2026, trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history. Elliptic, Binance largest hack, 31 Oct 2026, elliptic.co/insights/binance-largest-hack-in-history/. Arbitrum Security Council, emergency action, 30 Oct 2026, forum.arbitrum.foundation/t/security-council-emergency-action-30-10-2026/31625. EIP-7702, eips.ethereum.org/EIPS/eip-7702.