CASE FILE / WORKING REPORT / REVISION 4.0

The Binance Hot Wallet Drain

Binance hot wallets across ten blockchains were emptied in one window on 29 October 2026. Revision 3 adds the Optimism authorization chain, the EIP-7702 rehearsal, a chain-by-chain reconciliation, and the questions only Binance can answer.

- First snapshot 30 October 2026, 13:06 UTC. Revision 2 31 October, 09:19 UTC. Revision 2.2 31 October, 11:00 UTC. This revision 31 October, 14:30 UTC.

TEN CHAINS: Ethereum | Bitcoin | XRP | Solana | Tron | Arbitrum | Avalanche | Polygon | Optimism | Base

R 4

$6.36B VALUE TAKEN, TRM ESTIMATE	**10** CHAINS HIT	**~$2.27B** FROZEN, FOUR-TOKEN MEASURED
170,426 ETH TRACED TO BINANCE 14	**18,270 BTC** UNSPENT, 19 WALLETS	**0** ESTABLISHED AS RETURNED

6.36B taken (TRM estimate) = 2.27B frozen in four stablecoins + 2.4B attacker-held ETH and BTC (third-party estimate, no price basis) + 1.69B residual. The 481,581 ETH figure is a balance in six tracked wallets, not a stolen amount: only 170,426 ETH traces to Binance 14. On 31 October, 44,231,858.7 OP was moved by the Optimism portal admin into the System Owner Safe alias and 8,426.0477 ETH plus 74,559,805.2 ARB was frozen in escrow on Arbitrum. A JustLend receipt-token route was traced from deposit to convergence on a contract named Vault. Nothing is established as returned to Binance.

Prepared by **Keshav Maheshwari**
withkeshav.com

Executive summary / what this revision establishes

Five statements, each carried by evidence in this document. No new claim appears here that is not proved or labelled later.

01

One coordinated window emptied two Ethereum hot wallets and nine other chains

Between 20:20 and 21:04 UTC on 29 October, 167,464.247856 ETH and 1,615,409,498.97 USDT left Binance 14 in one sweep. Twenty-four seconds later Binance 16 sent about 28,006 ETH, 55.7M USDT, 25.9M RLUSD and 84.5 WBTC to the same collection address with no delegation, signed by its own key. Further assets left on nine other chains.

02

Containment is real, but nothing has been returned to Binance

Four stablecoins measured at 2,271,952,865.67 are frozen at par. 44,231,858.7 OP sits at the Optimism System Owner Safe alias. 8,426.047679407546 ETH and 74,559,805.2 ARB are quarantined on Arbitrum pending a governance decision. 19 of 19 Bitcoin outpoints remain unspent. The returned-to-Binance category is zero on every chain.

03

Most of the money is located, but the ETH figure in Revision 2.2 was a balance

Of 481,581 ETH held, 170,426.16 traces to Binance 14 native outflow, 156,892.88 came from converted stablecoins, 19,762.41 is debt-encumbered Aave borrowing, and 127,256.59 is unexplained. The remaining attacker-held stablecoins are located and count 1,002,729,468 at par.

04

The method was prepared, not improvised

One EIP-7702 authorization applied at 20:20:59, chosen from a batch of 50 all signed by Binance 14. The same operator cluster rehearsed the full delegation-and-sweep pipeline four times on three self-funded dust accounts between 13:51 and 16:47 that afternoon, and deployed two sweeper contracts.

05

Four questions stay open, and one of them is not answerable from public data

Who held Binance 14's key at 00:10:35. Where 127,256.59 ETH came from. Whether XRP, Tron, Polygon and Base moved as recorded, since the record holds no full address for any of them. How the AVAX reached Ethereum, since no burn, message or mint evidence survives in the record. Each is stated on page 18.

2.27B	44.23M	28,006	0
FROZEN AND MEASURED	OP MOVED BY GOVERNANCE	ETH FROM BINANCE 16	ESTABLISHED AS RETURNED

WHAT CHANGED FROM REVISION 2.2

Seven corrections. The 481,581 ETH figure is a balance, not a stolen amount. The EIP-7702 sweep was named as the wrong transaction and the accepted nonce was described as inferred when it is measured. The 4.39 ETH outflow is really 4.839787807 ETH across twelve transfers. "Seized" became "moved" for the Optimism action. The AVAX 2.06M figure now carries its 200,116.19 AVAX gap. The frozen gap is reconciled to about 2.6946B against TRM's 2.7B. Binance 16 and its 28,006 ETH are added.

Confirmed and unresolved / read this first

The left column is measured on-chain. The right column is not established, even where this document uses the figure.

ESTABLISHED ON-CHAIN	
Binance 14 sweep, 167,464 ETH and 1.615B USDT	MEASURED
Binance 16 outflow, no delegation	REPORTED
50 authorizations, one applied at nonce 18,914,809	MEASURED
Rehearsal: 4 installs, 3 accounts, 2 sweepers	MEASURED
Post-drain 78 transactions and the revocation	MEASURED
OP portal upgrade, deposit, restore in one L1 tx	MEASURED
OP Safe hash approved by two parent multisigs	MEASURED
L1 to L2 sourceHash match	MEASURED
44,231,858.70442318 OP at the alias, zero outbound	MEASURED
19 of 19 Bitcoin outpoints unspent	MEASURED
7,242.76435545017 ETH at the Avalanche end state	MEASURED
8,426.0477 ETH and 74,559,805.2 ARB quarantined	MEASURED
Frozen four-token total 2,271,952,865.67	MEASURED
4.839787807 ETH outflow, 12 transfers	MEASURED

NOT ESTABLISHED	
Who held Binance 14's key at 00:10:35	OPEN
Whether the 45 post-drain transfers were a rescue	OPEN
Who authorized the OP move, and why	OPEN
Any off-chain compromise mechanism	ASSESSMENT
The Arbitrum L1 trigger transaction	NOT FOUND
The AVAX CCTP route and message	NO EVIDENCE
The Stargate source chain	UNDECODED
127,256.59 ETH of the parked balance	UNEXPLAINED
XRP, Tron, Polygon, Base quantities	THIRD PARTY
The $2.4B attacker-held figure	NO PRICE BASIS
Attribution to a named group	EXTERNAL ONLY
Any return to Binance	NONE FOUND
Whether Binance owned the OP	INFERENCE
Control of 0xC2096a12 and its 7,002.79 ETH	UNKNOWN

Open question this revision cannot close. Who held Binance 14's key at 00:10:35 UTC on 30 October, when the account signed its own zero-delegate revocation? The chain shows the key was usable at that minute. It cannot show who used it. Only Binance's signer-service request log, HSM or MPC audit trail, and revocation request record can answer this. No public technique reaches it. The question is restated on page 18 with the exact records that would settle it.

Timeline / 28 October to 31 October 2026

One window, plus the containment and the later movement. All times UTC.

TIME	EVENT	DETAIL
28 Oct	**Funding**	The operator wallet is funded through Tornado Cash in three small withdrawals.
29 Oct 02:28	**Sweeper A**	Operator EOA deploys sweeper contract 0x19bee294, 1,256 bytes. Preparation begins.
13:51 to 16:47	**Rehearsal**	Four EIP-7702 installs on three self-funded dust accounts. 6 USDT, 3 USDT and 2.54 USDT swept. Sweeper B deployed 15:59.
20:20:59	**Install**	50 authorizations in one type-0x04 transaction. One applies to Binance 14 at nonce 18,914,809.
20:24:23	**Binance 14**	167,464.247856 ETH, 1,615,409,498.97 USDT and 62 tokens leave in one sweep. 64 logs.
20:24:47	**Binance 16**	About 28,006 ETH and four further assets leave with no delegation, signed by its own key.
20:41 to 21:04	**More USDC**	780,000,000 and 43,000,000 USDC, then 23 token transfers.
21:01	**Tether freeze**	Tether freezes 971.1M USDT. Circle follows three minutes later with 823M USDC.
22:55 to 00:07	**Binance 14 signs**	78 ordinary transactions after the drain, 45 of them to a publicly Binance-labelled hub.
30 Oct 00:10:35	**Revocation**	Binance 14 signs its own zero-delegate authorization. Nobody is identified as the signer.
30 Oct 00:18	**Arbitrum**	Emergency upgrade locks the inbox. 8,426.0477 ETH and 74,559,805.2 ARB frozen in escrow.
30 Oct 01:17:47	**3,000 ETH**	Exactly 3,000 ETH reaches 0xC2096a12. Its later total is 7,002.786415 ETH.
30 Oct 12:44	**AVAX to ETH**	AVAX sold, bridged and consolidated into 7,242.76435545017 ETH at 0x29482870.
31 Oct 00:04:47	**OP approved**	OP Foundation Safe, 5 of 7, approves the Safe transaction hash.
00:08:47	**OP approved**	Security Council Safe, 10 of 13, approves the same hash.
00:10:59	**OP L1**	Portal implementation replaced, one deposit emitted, implementation restored, in one transaction.
00:12:15	**OP L2**	Deposit settles on OP Mainnet. 44,231,858.7 OP moves to the System Owner Safe alias.
04:39 to 08:17	**12 transfers**	The holding wallet sends 4.839787807 ETH in twelve native transfers.
08:40 to 08:48	**Consolidation**	Five senders move 2,815.957147 ETH into 0xC2096a12.
09:25 to 10:04	**Stargate**	1,182.539533 ETH arrives at 0x11861b31, which forwards 1,186.829269 ETH to 0xC2096a12.
12:26	**Cutoff**	Last observation for this revision. Bitcoin tip 973,976.

THE FIVE ACTIONS THAT CHANGED THE POSITION

20:24
Binance 14 emptied in one sweep, 64 logs.

21:01
Tether freezes 971.1M, Circle follows within three minutes.

00:10
Optimism governance moves 44.23M OP to its own Safe alias.

00:18
Arbitrum locks its inbox, quarantining ETH and ARB.

12:26
Snapshot. 19 of 19 Bitcoin outpoints still unspent.

The Optimism movement / 44,231,858.7 OP

A single L1 transaction, authorized through Optimism's own governance stack, moved the OP out of the collection wallet. It is not an attacker return and not a legal seizure. The 44.2M OP reported as stolen by Blockaid and the 44M OP recorded by Elliptic as this move are the same tokens, counted once.

TIME (UTC)	ACTOR	ACTION
00:04:47	**OP Foundation Safe**	approveHash(0xbd93c5a3...d56956), threshold 5 of 7, five signatures
00:08:47	**Security Council Safe**	approveHash(0xbd93c5a3...d56956), threshold 10 of 13, ten signatures
00:10:59	**Executor EOA**	Nonce 42 calls System Owner Safe.execTransaction; Safe nonce 47, L1 block 26,309,074
00:12:15	**OP Mainnet**	Deposit executes, 44,231,858.7 OP transfers to the Safe alias, block 158,903,379

The Safe transaction hash `0xbd93c5a30b07e95fb36dfa11b66b06b5a340fd52690179d8479dadd8cdd56956` was recomputed from the EIP-712 domain, the struct hash and Safe nonce 47. It matches the ExecutionSuccess log byte for byte. Both parent multisigs approved that exact hash, not a near-identical payload. First approval to settlement: seven minutes twenty-eight seconds.

5 / 7	10 / 13	2	0
FOUNDATION APPROVAL	SECURITY COUNCIL APPROVAL	IMPLEMENTATION CHANGES, BOTH IN ONE TX	OUTBOUND OP SINCE THE MOVE

The recipient is the System Owner Safe's L2 alias, derived rather than asserted. `0x5a0aae59d09fccbddb6c6cceb07b7279367c3d2a +` `0x1111000000000000000000000000000000001111 =` `0x6b1bae59d09fccbddb6c6cceb07b7279367c4e3b`. The offset is 0x1111 in the first two bytes and 0x1111 in the last two, with sixteen zero bytes between.

CURRENT STATE OF THE ALIAS	
OP balance, read at block 158,925,143	44,231,858.70442318 OP
Nonce and code	NONCE 0, 0 BYTES
Outbound OP, 11 chunks scanned, 0 failed	ZERO EVENTS
Balance reconciliation	44,231,858.7 + 0.00442318587 DUST
Dust source	COLLECTOR LOOKALIKE, 00:12:33

> WHAT THIS PROVES ABOUT CONTROL
>
> The OP left the collection wallet and sits at an address controlled through the System Owner Safe's L1 alias, with no separate key. The authorization is cryptographic: two independent multisigs approved this payload, and the L2 deposit hash derives from the L1 block and log index. The tokens have not moved since. What is not proven is intent: who decided, why, whether this is recovery, seizure, or a treasury action, and whether Binance has any claim.

The Optimism mechanism / replayable

One L1 transaction at block 26,309,074. Everything below is in that transaction or derives from it.

STEP	CALL	RESULT
1	**Safe execTransaction**	operation = 1, DELEGATECALL into Multicall3
2	**CreateX deploy**	CREATE2 address 0x6d971b07...c9bb derives from salt and initcode. Deployed code is byte-identical to the runtime.
3	**upgradeAndCall**	Portal proxy points at the shim. ProxyAdmin owner unchanged.
4	**Shim emits deposit**	mint 0, value 0, gasLimit 1,000,000, calldata transfer(alias, 44,231,858.7 OP)
5	**upgrade back**	Portal restored to the official implementation in the same transaction

The L1 to L2 link is cryptographic. The L2 transaction carries a sourceHash recomputed from the L1 block hash and log index 1846. It matches exactly, and no neighbouring index matches. Across a 20,000-block scan, the portal's implementation changed exactly twice, both inside this transaction, and the ProxyAdmin owner never changed.

VERIFIED AND NOT VERIFIED

The mechanism: upgrade, deposit, restore	PROVEN
The authorization: two multisigs on this hash	PROVEN
The control: alias balance, nonce 0, no outbound	PROVEN
Behavioural replay of the shim	NO ENDPOINT ACCEPTED STATE OVERRIDES
Any Optimism statement explaining the action	NONE FOUND
Legal character of the move	NOT ESTABLISHED

> COVERAGE, STATED HONESTLY
>
> Elliptic reported this move in one sentence on 31 October: "Optimism's governance appears to have done the same, moving 44 million OP". So the existence of the move is public. This document's contribution is the mechanism-level reconstruction, which no public source provides. That is a different claim from discovery, and this revision does not make the discovery claim. A search of the Optimism governance forum, blog and public statements found no explanation of the action. That is a negative result from a bounded search, not proof of silence.

HOW OTHER PUBLIC WORK COVERS THIS MOVE

Elliptic, 31 October	ONE SENTENCE, SAME CONCLUSION
TRM Labs	NOT MENTIONED
Chainalysis	NOT MENTIONED
Blockaid, Hypernative, Bitquery	L2 OUTFLOW ONLY
Optimism governance, blog, X	NO EXPLANATION FOUND

The EIP-7702 install / 50 authorizations

Two transactions, two roles. Revision 2.2 named the second one as the first. The distinction is what proves the design.

ROLE	HASH AND POSITION	TYPE AND TIME
Authorization carrier	`0xad99264d5532ae0dd04b2004eebda05f25657e70dacb764f7ac8d4ccd051298b`	0x04, block 26,300,753 index 138, 20:20:59
First sweep	`0x53bd38b816c23e74134786c29a8c18d792777998a3b9326047b583100e88e2f3`	0x02, block 26,300,770 index 189, 20:24:23

The attacker installed authority once, then used ordinary transactions for three hours forty-six minutes and never needed a second authorization. The nonce arithmetic closes exactly: 18,914,825 after the sweep block, plus 78 ordinary transactions equals 18,914,903, the revocation transaction's nonce, then 18,914,905 after the revocation and its applied authorization.

50	1	50 / 50	18,914,809
AUTHORIZATIONS IN ONE TX	CHAIN ID IN EVERY ENTRY	RECOVER TO BINANCE 14	ACCEPTED NONCE, ENTRY 15

THE AUTHORIZATION BATCH

Count and carrier	50, ONE TRANSACTION
Delegate in every entry	0X63E842B0...C6FAE, SWEEPER B
Nonces	18,914,824 DOWN TO 18,914,775
Signer recovery	INDEPENDENT SECP256K1, 50 OF 50
Applied	EXACTLY ONE, NONCE 18,914,809
Delegation designator	0XEF0100 + DELEGATE, 23 BYTES
Cross-chain replay	EXCLUDED, CHAIN ID 1

WHY A BATCH OF FIFTY

An entry above the account nonce is invalid when the transaction executes, but it becomes valid if the account's nonce later reaches it; nothing in the tuple expires it. At that block, 15 entries were above the account nonce and 34 below it. Only the entry at 18,914,809 could apply in that transaction; the 15 higher entries remained available for later nonces. A band of 50 is still what an operator builds when it can obtain signatures but cannot read the account's live nonce. It also suggests the signed batch was assembled minutes, not hours, before its 20:20:59 inclusion. This is an inference from batch shape; inclusion time is not signature time.

The rehearsal / eighteen hours of preparation

The same operator cluster ran the whole pipeline on accounts it controlled before touching Binance 14.

TIME	EVENT
02:28:59	Operator deploys sweeper A 0x19bee294, 1,256 bytes
13:51:35	Type-0x04 to 0x837810E3, 2 authorizations, sweeper A
13:51:59	Type-0x04 to 0x9C29BA2D, 3 authorizations, sweeper A
13:57	0xFD41dA53 funds both accounts with 0.001 and 0.002 ETH
14:19:59	0x837810E3 swept: 6.000000 USDT and 1.000000 USDC
14:24:11	0x9C29BA2D swept: 3.000000 USDT and 1.000000 USDC
15:59:11	Operator deploys sweeper B 0x63e842B0, 1,674 bytes
16:20:47	Type-0x04 to 0x43AEdb9B, 2 authorizations, sweeper B
16:24:11	Known case address 0xe4F9070e funds it with 1.01 ETH
16:25:59	Type-0x04 to the same account again, 2 authorizations
16:30:11	0x43AEdb9B swept: 2.541994 USDT

Self-funded, self-delegated, dust-valued. No exchange hot wallet holds those combinations. This excludes an improvised technique at Binance 14. It does not show the same infrastructure obtained Binance 14's signature: the rehearsals only prove the attacker could obtain authorizations for accounts it controlled.

Open question. Binance 14 kept signing after the drain: 78 ordinary transactions from 20:24:35 to 00:07:11, 45 of them to an address publicly labelled Binance 8, then its own zero-delegate revocation at 00:10:35. Two readings fit. Binance retained the key and moved remaining tokens to its own wallet, which is a rescue executed with the same key the attacker had just used. Or the attacker retained it and the convergence on a Binance hub is coincidence. The first is far more economical. The chain cannot separate them.

COMPETING EXPLANATIONS, NONE ESTABLISHED

Private key theft	NOT EXCLUDED
Signing service compromise	MOST CONSISTENT, NOT PROVEN
Malicious insider	NOT EXCLUDED
Cross-chain replay	EXCLUDED, CHAIN ID 1
Same-chain replay of unused entries	NOT TESTED
Build pipeline compromise	ONLY A ROUTE TO THE ABOVE
Approval-control bypass only	PLAUSIBLE COMPONENT

Asset reconciliation / seven categories

One row per position. Par-valued assets at par. Everything else unpriced, because this record has no price table and its internal ETH ratios disagree by up to 2.2 times.

CATEGORY	PRICED TOTAL	UNPRICED OR NOTE
Removed from Binance	3,051,138,966.97	Stablecoins only. Fourteen further removed rows carry an unpriced native quantity.
Issuer-frozen	2,273,516,678.45	USDT 1.380B, USDC 823.1M, RLUSD 40.5M, USD1 27.8M, Avalanche USDC 1.56M
Quarantined or administrative	not valued	8,426.0477 ETH and 74,559,805.2 ARB on Arbitrum; 44,231,858.7 OP
Returned to Binance	0	No asset on any chain is established as returned
Attacker-held	1,002,729,468	Stablecoins only: Tron 312.7M, 0x8d53f50a 190M, Helper 2 500M. ETH, BTC, XRP, SOL unpriced.
Swapped or bridged	not additive	Every leg is represented at source or destination. Summing counts value twice or three times.
Unresolved	453,099,600.51	Tron 300M and Safe MEXC 153.1M. Other unresolved rows are unpriced or diagnostic.

2.27B	1.00B	0	453M
FROZEN, MEASURED	ATTACKER-HELD STABLECOINS LOCATED	RETURNED	UNRESOLVED, PRICED

WHY THE CATEGORIES CANNOT SIMPLY BE ADDED

The collection wallet retained 1,175,464,712.88 USDT and dispatched 1,200,000,000, for 2,375,464,712.88, against a documented inflow of 1,615,409,498.97. That is a 760,055,213.91 gap. The three priced rows sum to 3,729,345,746.96 against 3,051,138,966.97 removed. The 678,206,779.99 excess is the measure of overlap between the rows, not a fourth category and not value removed. The helper wallets overlap and cannot be summed. "Quarantined" is this document's term for held in escrow pending a governance decision; the sources, including Arbitrum's notice, say "frozen".

LARGEST SINGLE POSITIONS IN THE LEDGER

Tether USDT, frozen	1,380,464,585.20
Circle USDC, frozen	823,123,175.53
Helper 2 USDT, held	500,000,000
Tron USDT, held	312,729,468
Safe MEXC USDT, unresolved	153,099,600.51

The frozen bridge / 2.27B to 2.69B

Revision 2.2 called the gap between its 2.27B and TRM's 2.7B unreconciled. It reconciles in seven lines, with one caution.

LINE	USD	EVIDENCE
USDT, Ethereum	1,380,464,585.20	Tether blacklist, four addresses
USDC	823,123,175.53	Circle blacklist, collection wallet
RLUSD	40,541,065.00	48M sent onward before the 22:00:59 pause
USD1	27,824,039.94	World Liberty freeze
Four-token measured	2,271,952,865.67	Published subtotal in Revision 2.2
Tron USDT	~378,047,134	Tether freeze, Tron
Avalanche USDt	~8,400,000	Issuer freeze after the swap
Polygon USDT0	~6,200,000	Issuer freeze
Arbitrum	~30,000,000	Quarantined, not frozen by an issuer
Total	~2,694,600,000	Against TRM's 2.7B

> CAUTION BEFORE THIS IS TREATED AS CLOSED
>
> The Tron USDT line may already sit inside the 1.380B Tether total. Until each line is tied to a separate issuer freeze event, this table is a hypothesis with strong arithmetic, not a finding. The remaining roughly 160M to Elliptic's 2.85B is Paxos, First Digital, tokenised gold, WBETH and smaller issuers, not itemised here.

VALUATION RULES USED IN THIS DOCUMENT

Par instruments at par	USDT, USDC, RLUSD, USD1
Everything else	UNPRICED WITHOUT A NAMED SOURCE
The $2.4B attacker-held claim	ONE EQUATION, TWO UNKNOWN PRICES
Totals from TRM, Elliptic, Chainalysis	THIRD-PARTY ESTIMATES
Binance's approximately $3B	COMPANY CLAIM
6.36B residual	1.69B, ACCOUNTING ONLY

The totals also differ and Revision 2.2 did not say so: TRM 6.36B, Elliptic 6.43B, Chainalysis 6.4B, Binance, Blockaid and Bitquery about 6.3B, and a case-card figure of 5.912B that could not be traced to a Chainalysis publication. A seven percent spread deserves the same labelling as the frozen figures.

The money flow / ten chains

Where each chain's funds went. State is what the evidence supports, not what the outcome may become.

CHAIN	MOVED	STATE	NOTE
Ethereum	167,464 ETH 1.615B USDT 62 tokens	HELD	Binance 14 sweep plus Binance 16, about 28,006 ETH. Frozen, converted, consolidated.
Bitcoin	18,270.1999 BTC	PARKED	19 addresses, 19 principal outpoints unspent at tip 973,976.
XRP	233,461,943.1 XRP	THIRD PARTY	Five payments, no outgoing. No full address in this record.
Solana	970,554.1 SOL	PARKED	Receiver holds 970,552.399646237 SOL, no outgoing.
Tron	612.7M USDT 46,394,098 TRX	HELD	312.7M USDT retained. A JustLend receipt-token route is reconstructed on pages 13 and 14; TRX activity is still not reproduced.
Arbitrum	8,426.0477 ETH 74,559,805.2 ARB	QUARANTINED	At 0x0000...0da0 pending a governance decision. Not returned.
Avalanche	1.81M AVAX 444,536.6 later	CONVERTED	2,058,519.71 sold, 200,116.19 unexplained. End state 7,242.7644 ETH.
Polygon	46,626,593.5 POL	THIRD PARTY	No full address in this record.
Optimism	44,231,858.7 OP	MOVED	System Owner Safe alias. Not a seizure, not a return.
Base	not recorded	THIRD PARTY	In the ten-chain scope. No quantity or address in this record.

Read the state column literally. Parked means unmoved at the cutoff. Held means in an attacker-associated wallet or a located position. Quarantined means in escrow pending another party's decision. Moved means it left under an authority whose intent is not public. Returned is used nowhere, because nothing is established as returned to Binance.

CONTAINMENT, BY MECHANISM

Issuer
Tether, Circle, Paxos, World Liberty and others freeze stablecoins at par.

Governance
Optimism moves OP to its Safe alias; Arbitrum quarantines ETH and ARB.

Chain halt
Arbitrum's inbox upgrade is the mechanism that makes quarantine possible.

No action
Bitcoin and Solana are unmoved. No issuer controls either asset.

Returned
Zero. No asset on any chain is established as back with Binance.

The Ethereum branch / detail

The holding wallet's full morning outflow, and the fan-out that followed it. Revision 2.2 counted 4.39 ETH. The real figure is 4.839787807 ETH across twelve transfers.

UTC	ETH	FULL TRANSACTION HASH
04:39:23	0.05	0x9aff3c1854a38ef57d96d86acefa6dae631669d36c927bedf824ddeec72d9a37
04:57:47	0.05	0xdaadf0eb50aa6082bee8febda2efa38353cc2150d53841774ffaca0fd4b19d27
06:53:59	0.05	0x8d8f98e82986e2279cafc9162446afb87da269194b2584a2af0e31779ef34fb4
07:09:11	0.05	0x60ee7b7a641eae44af841e6308d625978b9c62e189f280b06662bfe9eabeb577
07:15:35	0.05	0x0efd2af086cb245454ba2c3f307beef8e11421afbba668403eababed01860657
07:18:23	0.05	0x4540b85076d86498b11376674af775dcc598d3811f7c90593c45cb11da1ad404
07:26:47	0.05	0x975eef82bfe9e286810ad4c0fbee47afed1a4f115b19658507868057865e6f14
07:30:47	0.05	0x62e1e63fbe8f2c163fa8e8e64a5e345d0e91fe0847db06f3bd3f187f62ba43de
07:33:59	0.05	0x6fe43641ec78468b7393e56bb6f91208b3cf5e52215d788625ca03618a7a85a2
07:35:59	0.05	0xb0de506a0e4f90533aa08cc0ddfcb80b643f6878dc596789da49cd37ae8624bf
07:53:35	0.05	0x219f57350b545993f1922a1acb5c4cf0c1be27004ad6c28bc8f5b20a0d76c892
08:17:59	4.289787807491628	0x35f0a5f57012656fcad01107b1f1c627f458e513a6d76c472b3ea9f7d368ce90

Destinations for the twelve transfers are listed in the fan-out table at the foot of this page. Total 4.839787807491628 ETH, plus gas. The balance rebuild from 1,046 normal and 633 internal records reconciles to the on-chain balance of 0.00002873 ETH, so this list is complete. Revision 2.2 counted the 4.289787807 transfer and two of the 0.05 legs, and missed nine.

> NEW: THE DRIP FUNDED A TOKEN-SALE FAN-OUT THAT CONSOLIDATED 2,815.96 ETH
>
> Five of the wallets that received a 0.05 ETH leg later sold tokens through a Uniswap router and sent the proceeds to 0xC2096a12. Their router inflows total 2,801.146675 ETH; they consolidated 2,815.957147 ETH between 08:40:17 and 08:47:31. That is 99.5 percent of what they forwarded. 0xC2096a12 holds 7,002.786415 ETH with nonce 0 and no outbound, including exactly 3,000 ETH received on 30 October at 01:17:47. Two inbound value paths tie it to the holding wallet's fan-out, four of the five senders being downstream of the same 0.05 ETH drip, so it is almost certainly part of the same cluster. Control is inferred and this document does not label it as proven attacker custody.

THE FIVE FAN-OUT WALLETS, AND WHAT THEY FORWARDED

0x73EE90554fd0954490B072ca11e6422642aB4593	1,104.056222
0xa3E1A5b5eC04907932101962a2fbEC614B1Cbb04	931.776554
0x7B12eA0960D92349a8FD2d07757C354dF166837a	470.364414
0x76044CF6Afb2d8E85719AD35e2D1C95473BF9F89	156.593080
0x4271B78E7eFe2669482ED4E3312bb7f2d2bfB8AF	153.166877
Total consolidated to 0xC2096a12	2,815.957147

The Tron route / deposit to convergence

A receipt-token route through JustLend, reconstructed on addresses Elliptic attributes to this incident. The mechanism is Chainalysis's; this reconstruction is ours, and it is not their $500,000 example.

UTC, 30 OCT	EVENT	AMOUNT	TRANSACTION
13:38:18	Market maker to swap service	573,892.358889 USDT	f04e52e584f5fed9c949972d7630fca434dc4fe65261a6d48f920c5a26136295
13:39:03	Intermediary to depositor	573,892.358889 USDT	c7fd7a9c96b869047302fdb7f886c94da77c48437493709350ac1e71adc6cb24
13:39:42	Mint, USDT in, jUSDT out	52,696,142.619763 jUSDT	f74a30e4441f9376ce55460b3cb0e6bb6a5f2ddc1bc0f7c6dc78b00e436795e8
13:40:33	Receipt transferred in full	52,696,142.619763 jUSDT	3393fe86907b0ae42d62dceac146519e5ee3075730aa848315761a60ac4fc62c
13:41:15	Redeem, round underlying	9,182,234.323089 jUSDT to 100,000.000000 USDT	5c2d29777956d83006a3b18f1d109510dc2daf4a6feeca351f44851501610095
13:43:54	Out to pass-through	100,000.000000 USDT	3249ac4ae6fbcee06cefec663aaab671a79943c7a68a4536c3b14a45d42c3d15
13:46:54	Redeem, round underlying	91,822.333924 jUSDT to 1,000.000000 USDT	dc0c5b1faf11bc163d81956258aa83c09711b5467e715a77f9dd8baf180a3fd2
13:47:12	Pass-through to Vault	99,999.999999 USDT	2b3b6433cdd9cdba607a47d8ca617fe412b108e62d7c21f403e405ecbc75cbb0
13:49:12	Redeem, round underlying	18,364,466.027098 jUSDT to 200,000.000000 USDT	db07aae2d7d1ee3267ac2f72ec0542ed5943d20dc81028eabc244eb1e394be62
13:50:24	Out to pass-through	200,000.000000 USDT	ae9aec2f0ca7a68da439c6751834490ccc6638116241d96fa811b6fbeb533fa3
13:54:12	Pass-through to Vault	200,000.000000 USDT	5403055c8b31503089cf8aff00403215ebd06f8dce4e20266fed455d38027292
13:54:42	Receipt transferred onward	25,057,619.935653 jUSDT	5af3ed7d424629d1b2064e10b8206352f3e20fb352a10edc3a445958f91702eb
13:55:27	Redeem, full balance	25,057,619.935653 jUSDT to 272,892.473047 USDT	d43426f4497f9157a2856fdfb32db73de47f8bc0e287df9a0e6e475e7e14e389
13:57:18	Out to created contract	272,892.000000 USDT	60c7d100a831cbbc35f5f8c0b56d5c2425409fd639751a520a041db58f608cd7
13:59:06	Pass-through to Vault	272,892.000000 USDT	c749b4aa58ded8e37115aefedc180ab3f39cd8029d3452510ca664681dd47a7f

Exits: 100,000 + 200,000 + 272,892 to the Vault, plus 1,000 returned to the market maker, equals 573,892 against 573,892.358889 deposited. The 0.358889 USDT difference is protocol fee and rounding. Receipt units: 9,182,234.323089 + 91,822.333924 + 18,364,466.027098 + 25,057,619.935653 = 52,696,142.619764 against 52,696,142.619763 minted, one unit. The first three redemptions are `redeemUnderlying`, round USDT out and non-round jToken burn; the fourth is `redeem`. JustLend's mint emits a Transfer from the market contract, not the zero address.

The Tron route / provenance, falsification, controls

What the route proves, where the trail stops, and the test that weakens the single-actor reading.

WHERE PROVENANCE STOPS

Intermediary to depositor, 41 seconds, both blocklisted	PROVEN ON-CHAIN
Above the intermediary: a swap service and a market maker	MASKS THE TRAIL
Link from a hack collection wallet to the depositor	VENDOR LABEL ONLY
Vault contract owner and role	UNKNOWN

FALSIFICATION: THE PIPELINE IS OLDER THAN THE INCIDENT

The same accumulator chain moved 3,475,486.43 USDT in 52 edges between 29 October 01:42:21 and 18:06:00 UTC, before the 20:24:23 drain. Only three distinct senders fed it in that period, and one hub both sent to and received from another. The Tron pipeline is not incident-specific infrastructure. It is consistent with a settlement or laundering service used by more than one client, and it weakens any single-actor reading of the Tron side.

METHOD DEFECT: THE PROVIDER REPORTS APPROVALS AS TRANSFERS

64 records in the collected feed carry the canonical USDT address and a value of 2^256-1. Six were checked against their raw receipts: every one contains an Approval event and no Transfer. Summing the feed without checking the log topic inflates volume by about twenty orders of magnitude. The rows mean "unlimited approval granted", not "value moved". Two route addresses granted unlimited USDT approvals to a contract, which is an approval-pull relationship, not poisoning.

CONTROL SURFACE, MEASURED

Per-account freeze or blacklist of receipt tokens	DOES NOT EXIST
Global transfer pause, one EOA guardian, two-day restart	EXISTS, NOT ACTIVE
Redemption pause	DOES NOT EXIST
Redemption bounded by cash	56.7 PERCENT LIQUID
Issuer blacklist on the pool	SELECTORS LIVE, POOL NOT LISTED

So "receipt tokens cannot be frozen" is too absolute. There is no per-account freeze, but transfers can be stopped globally by one guardian signature, and large redemptions can fail on cash. The observed timing, transfer within 51 seconds and redemption within minutes, is consistent with moving before a control could be applied. It does not prove intent.

What this route does not show. It does not show that the depositor is the incident actor rather than a service client, that the Vault is attacker-controlled, or that the receipt token preserved control rather than economic continuity. H1 stays low for control, medium for linkage; H8 (common tooling) and H9 (multiple operators) fit the pre-incident activity better. No probability is assigned.

Where the money is now / 31 October, 12:26 UTC

Five groups, no double counting. The old three-bucket waterfall is retired because it put located stablecoins into an "unreconciled" bucket.

Position of the headline, priced rows only

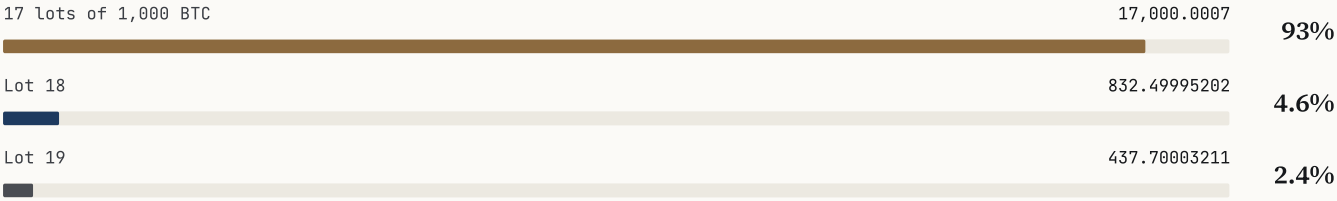
USD at par



Bars are scaled to the 3.05B removed subtotal, not to the 6.36B headline, so they are not a recovery percentage.

Where the 18,270.19988827 BTC sits

19 addresses



Every principal outpoint returns unspent at tip 973,976. The dust in each lot is change, not movement.

170,426	127,257	19 / 19	0
ETH TRACED TO BINANCE 14	ETH GENUINELY UNEXPLAINED	BITCOIN OUTPOINTS UNSPENT	ASSETS RETURNED

THE 481,581 ETH, DECOMPOSED

Proven native ETH from Binance 14	170,426.16
Converted from stablecoins and tokens	156,892.88
Aave borrowing, debt-encumbered	19,762.41
Genuinely unexplained	127,256.59
Held in tracked wallets, not a theft amount	474,338.04
Avalanche end state, converted	7,242.76
Total	481,580.80

THE ONE SENTENCE THIS PAGE EXISTS TO SUPPORT

Only about 35 percent of the ETH this investigation tracks was taken from Binance as ETH. The rest was bought with stolen stablecoins, borrowed against stolen collateral, or cannot be explained from the record. Valuing all 481,581 ETH as stolen ETH overstates the ETH theft by roughly a factor of two to three.

Key addresses / the ones that carry the case

Full addresses, no truncation. Every one opens on a public explorer.

ENTITY	CHAIN	ADDRESS
Binance 14 delegated hot wallet	ETH	0x28C6c06298d514Db089934071355E5743bf21d60
Collection wallet main holding	ETH	0x5227f603C1eE34CE3C06eFe6477003BDfCCB2f8c
Operator EOA authorization carrier	ETH	0x7C8601d4645b93cea45F71e118A729332e6B5CA0
Sweeper B delegate contract	ETH	0x63e842B054Bd624a465454D533C33F573e9c6fAe
Conduit Stargate receiver	ETH	0x11861b31b97C5C6550D49b03B1eed1A105774084
Consolidation 7,002.786415 ETH	ETH	0xC2096a12eBE0944f4d39E59979F485AfD92d850a
OP Safe System Owner	ETH	0x5a0aae59d09fccbddb6c6cceb07b7279367c3d2a
OP alias holds 44.23M OP	OP	0x6b1bae59d09fccbddb6c6cceb07b7279367c4e3b
Executor Safe signer	ETH	0xe10a25d4ec17a94ca455f3cda84137189843b4f2
Arbitrum escrow frozen in escrow	ARB	0x0000000000000000000000000000000000000da0
Arbitrum attacker reported by ZachXBT	ARB	0x3E2bf1ac6bf0934BBba6456C341c2EcbCED632d5
Avalanche end state 7,242.7644 ETH	ETH	0x294828705974ad04d86a24a2ff6efe762505a0ed
BTC receiver 18,270.2 BTC	BTC	bc1q0mtc2f5agpkvlq6hhahmfr3hlr55kyfjhl2mnm
SOL receiver 970,552.4 SOL	SOL	AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU
OP token canonical	OP	0x4200000000000000000000000000000000000042

The nineteen Bitcoin terminal addresses are in the appendix on page 17. The five fan-out wallets are listed on page 12 and the rehearsal accounts on page 8, not repeated here, because they are not established as controlled by the same party.

Appendix / Bitcoin and bridges

The nineteen terminal addresses, then what is and is not proven about the two bridge routes.

LOT	ADDRESS	BALANCE BTC
01	bc1qxrxujwxfnvz040jw76d26zhjdg5jura7hs968s	1,000.00005885
02	bc1qepc70u3u476vgvg3hfcwjgu4mecxe2uchs4lag	1,000.00005812
03	bc1qdfhmlrdvg4tm87zjl0vyf0xflp5ql50q3g88gw	1,000.00005810
04	bc1qnq6jj9jmlf3945m3l8s0kxnqehrsga300k8t3s	1,000.00005810
05	bc1qz8hdwv8gmml0u96dsvnzsagz6krjyzxmgxupdp	1,000.00004828
06	bc1q42flhayrzy3zh8lkyevw8qcjduurt9a35wlsyx	1,000.00004852
07	bc1q63qrfrpsg5hh0zzn3kp2xx9vljl7dq7tatsjxp	1,000.00004181
08	bc1q0ts8gaf9ht0rr4u02hr56f8thndqsc4kmkmfv3	1,000.00004772
09	bc1q2wvz0kcsn4hqmajwtey30ud27fl25w8pveznn6	1,000.00004772
10	bc1qalwnl7dtaa73fsq5tyn0ghfy3fgfpqkt69tca8	1,000.00004736
11	bc1qjwdw6vrzq4vf6hckutvx4ucj86awwv99mxnz7w	1,000.00004736
12	bc1qs3aej5tmcdz0vctz8y9rjcxtxg8v5385577s56	1,000.00004713
13	bc1qm2j6v3247khlwzxl7p9vqnfkghcllyhv9wjaat	1,000.00004772
14	bc1qs6xnmhar38z44g2za93pv8ygdcwurrh8l87w3v	1,000.00004109
15	bc1qf5cyvv9w50tx9xx9s3xwsne0z87wvjj9l8a35u	1,000.00003403
16	bc1qg3nrzpuvq2pxqx74tcrywr09dc208ze96n3t53	1,000.00003772
17	bc1qm8v88m5fy6kuq9myva2eemwycxqd3e0zcrs2l8	1,000.00002624
18	bc1qrg025e2pgx0rwya2kpgtj30972p64jt0hn6zyt	832.49995202
19	bc1qxg0l4p6xc50zuv9cl5f0l0wmaxjpg8wcy7s9ra	437.70003211

All 19 principal outpoints return unspent. Total 18,270.19988827 BTC principal; the BALANCE column includes 0.00089173 BTC of change. Checked at tip 973,975 to 973,976, 12:13:56Z to 12:26:28Z.

BRIDGE ROUTES, PROVEN AND UNPROVEN

Avalanche end state, 7,242.76435545017 ETH, 11 inflows	PROVEN
1,545.8336998697919 ETH from 0x62b16E7E	PROVEN
CCTP burn, message, attestation, mint	NO EVIDENCE IN RECORD
Route legs visible	6 OF 8
AVAX received against sold	200,116.19 GAP
Stargate delivery at 0x11861b31	8 IDENTIFIERS
Stargate source chain	UNDECODED, SCAN 404
Arbitrum L2 forced transfer 0x410af166	BLOCK 519,514,685, TYPE 0X65
Arbitrum L1 trigger transaction	NOT FOUND

Method and limits / how to read this

Four evidence classes, two valuation rules, and the limits this revision did not overcome.

EVIDENCE CLASSES, USED CONSISTENTLY

Measured on-chain: a hash, block, balance or log read	CLASS 1
Confirmed official: the issuing party's own statement	CLASS 2
Third-party estimate: a named firm's published figure	CLASS 3
Accounting residual: derived, never a located asset	CLASS 4

RULES APPLIED

Par assets at par; everything else unpriced without a named source and time	VALUATION
A firm is named only where its claim is cited with title and date	ATTRIBUTION
"No public source found" means not found, not proven absent	NEGATIVES
No first-discovery claim without a documented search	ORIGINALITY
Frozen, quarantined, moved, returned and attacker-held are kept separate	LANGUAGE
A provider feed is not a transfer until the log topic is checked	NEW
Inclusion time is not signing time	NEW
Two agents reading one feed are not corroboration	NEW

LIMITS THIS REVISION DID NOT OVERCOME

XRP, Tron, Polygon and Base have no full address in this record, so four of the ten chains cannot be replayed by a reader. The AVAX route has no burn, message, attestation or mint evidence. The Stargate source chain is undecoded. The Arbitrum L1 trigger was not found in the blocks examined. No price table exists, so the $2.4B attacker-held figure cannot be tested. The Optimism shim could not be behaviourally replayed because no public endpoint accepted state overrides. Blog and X absences are partial retrievals, not proven silences. Binance 16 is carried from four third-party reports and was not independently re-read in this pass.

RECORDS THAT WOULD CLOSE THE SIGNING QUESTION, MOST USEFUL FIRST

Signer request log, 20:20 to 20:21 and 00:10:35	TIER 1
Whether the 50-entry batch was one request or fifty	TIER 1
HSM or MPC audit trail for Binance 14's key	TIER 1
The revocation request record at 00:10:35	TIER 1
Policy configuration in force at 20:20:59	TIER 2
IAM, CI/CD provenance, Kubernetes audit log	TIER 3

The open question this report states rather than answers. Who held Binance 14's key at 00:10:35 UTC on 30 October? The chain proves the key was usable at that minute and that the account signed its own revocation. It cannot show who used it. No public technique reaches that fact. The records that would settle it are Binance's signer-service request log for 20:20 to 20:21 and for 00:10:35, its HSM or MPC audit trail, its revocation request record, and its policy configuration at the time. Until Binance publishes or provides them, this question stays open in this report and is not resolved by inference.

Version history / what changed, and why

Three revisions in two days. Each one is kept, because a correction is part of the record.

VERSION	PUBLISHED	PAGES	WHAT IT ESTABLISHED
Notes 1	30 Oct 13:06	9	First snapshot: the sweep, the ten chains, the holding wallets, the initial freeze.
Notes 2, R2	31 Oct 09:19	11	Added the Optimism move, the AVAX conversion and the blocklist cross-check.
Notes 2, R2.2	31 Oct 11:00	11	Metadata, timeline and wording corrections from external review.
Notes 2, R3.0	31 Oct 12:45	17	OP authorization chain, EIP-7702 rehearsal, reconciliation, appendices, open question.
Notes 2, R4.0	31 Oct 14:30	19	This revision: the Tron receipt-token route, the pre-incident pipeline finding, the approval/transfer defect, and the publication corrections.

CORRECTIONS IN THIS REVISION

4.39 ETH outflow	CORRECTED TO 4.839787807 ACROSS 12 TRANSFERS
Sweep transaction type	CARRIER AND SWEEP ARE DIFFERENT HASHES
Accepted nonce	INFERRED, NOW MEASURED
Optimism wording	SEIZED, NOW MOVED
AVAX 2.06M	NOW CARRIES THE 200,116.19 GAP
ETH 474,338	A BALANCE, WITH 170,426 TRACED
Frozen gap	RECONCILED TO ABOUT 2.6946B
Five independent links	NOW TWO INBOUND VALUE PATHS
28-minute drip	NOW 19M25S MEAN, 7M24S MEDIAN
Approvals read as transfers	64 RECORDS RECLASSIFIED

ADDITIONS IN THIS REVISION

Binance 16, about 28,006 ETH with no delegation	NEW
Safe hash approved by two parent multisigs	NEW
18-hour EIP-7702 rehearsal on three accounts	NEW
Post-drain signing and the revocation	NEW
Seven-category reconciliation ledger	NEW
Token-sale fan-out consolidating 2,815.96 ETH	NEW
A complete JustLend receipt-token route, deposit to convergence	NEW
The Tron pipeline moved 3.47M USDT before the hack	NEW
64 provider records reclassified as approvals	NEW
Bitcoin and bridge appendices	NEW

> HOW TO CHECK THIS DOCUMENT
>
> Every hash, block and address can be opened in a public explorer. Balances were read at the heights stated. Vendor figures are named and labelled. Where this document states a limit, the limit is the finding.