CASE FILE / WORKING REPORT / REVISION 6.0

The Binance Hot Wallet Drain

Four Chainflip swaps, a pass-through to an FBI-listed terminal, the TRX trail back to the conversion hub, and the intrusion that reached Binance's signing service. The findings, stated plainly, with the limits of what the public record can prove.

- Data cut 4 November 2026, 04:50 UTC / 10:20 IST. Fixed chain cutoffs 1 November; principal positions re-checked 4 November. Prepared 4 November 2026.

TEN CHAINS

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

R6

$6.36B VALUE TAKEN, TRM ESTIMATE	**4** CHAINFLIP SWAPS, ONE RECIPIENT	**$2.272B** FOUR-TOKEN FROZEN, MEASURED
44.23M OP AT A RECEIVING ADDRESS	**18,270** BTC PRINCIPAL, 19 OUTPOINTS	**0** ESTABLISHED AS RETURNED

The four Chainflip swaps paid 272.055399550493021580 ETH. The common recipient moved 272.055383921583158580 ETH to 0x5915F563399b5d2C3A42A08F77E290Ae8121B260, which is on the FBI list and still holds it. The TRX that bought the USDT was spent from TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki. Two branches had fed that hub before the swap: 46,383,069.129019 TRX directly from TG5iB, and 120,000,000 TRX from the first of five fan-out wallets. Four more fan-out wallets delivered 518,200,902 TRX on 31 October, after the swap. Vendor totals differ in scope: TRM counts ten chains, Elliptic eleven, Bitquery nine. This report does not force them into one number.

Prepared by **Keshav Maheshwari**
withkeshav.com

Executive summary / six findings

The theft is established. The route is established. The signer and the terminal's controller are not. This report keeps those statements separate.

01 One window emptied two Ethereum hot wallets.

EVIDENCE At 20:20:59 a type-0x04 carrier applied an EIP-7702 tuple to Binance 14 at nonce 18,914,809. At 20:24:23 the wallet sent 167,464.247856 ETH, 1,615,409,498.97 USDT and 62 tokens. Twenty-four seconds after that sweep, 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 and its own signature.

02 The Tron route is four Chainflip swaps, not three.

EVIDENCE Deposits total 607,249 USDT. Payouts total 272.055399550493021580 ETH before gas and 272.055383921583158580 after. All four pay 0xc6ca6f2f2dc4b59193be61971462a527529cdac0, which moved the balance, less gas, to 0x5915F563399b5d2C3A42A08F77E290Ae8121B260.

03 The TRX came through a fan-out, not from a market maker.

EVIDENCE 1,672,000 TRX was paid into a public AMM and 573,892.358889 USDT came back. Before 13:38:18 the hub had received 166,383,069.13 TRX in transfers of 10 TRX or more: 46,383,069.13 from TG5iB and 120,000,000 from one branch of a five-way fan-out. Four further branches, 518,200,902 TRX, arrived on 31 October, after the swap. Qualifying receipts through the cutoff total 684,583,971.13 TRX from six addresses.

04 The FBI named the actor. It did not identify the signer.

EVIDENCE The 31 October advisory attributes the theft to TraderTraitor and lists 608 ETH addresses, 19 BTC addresses and one SOL address. The 19 BTC addresses are exactly the 19 terminal addresses. 0x5915F563 is also listed. A list is an attribution instrument, not proof of every wallet's controller.

05 Nothing is established as returned.

EVIDENCE The 44.23M OP sits at a receiving address on Optimism with no code, nonce 0 and no outbound. The Arbitrum ETH and ARB sit in governance escrow. All 19 Bitcoin principal outpoints were still unspent on 4 November. Binance's 90% and 95% updates, and the 98% in its 3 November blog, are replenishment from company resources, not stolen funds recovered.

06 The intrusion is documented. The signer is still not.

EVIDENCE Binance's 3 November account describes a June Homebrew download, a September fake recruitment, a 20 October move through an internal AI tool and a container token, and a 29 October container deployment that reached the wallet signing service. That is company evidence, not a chain proof. It explains the route, not the person who produced the signatures or how the MPC quorum was satisfied.

167,464	607,249	272.0554	0
ETH FROM BINANCE 14	USDT THROUGH FOUR SWAPS	ETH AT THE TERMINAL	ESTABLISHED AS RETURNED

What the public record can and cannot say. A valid transaction or authorization proves a signature was accepted. It does not show when it was created, who created it, or who held the signing system at inclusion. It does not distinguish the custodian, a compromised signing service, copied key material, an MPC workflow or an earlier signature broadcast later. The named records that would narrow it are listed at the end.

The money flow / ten chains

What left each chain, and what the record shows happened to it. Status at the 4 November cut. Parked means unmoved. Held means in an attacker-associated wallet or a locked position.

CHAIN	WHAT MOVED	AMOUNT	STATE
Ethereum	Two wallets swept; terminal unmoved at 4 November	167,464 ETH + ~28,006 ETH	HELD
Bitcoin	19 principal outpoints, none moved at 4 November	18,270.1999 BTC	PARKED
XRP	Moved to six new addresses on 2 November	233.46M XRP	MOVED
Solana	About 87,000 SOL moved by 3 November; 825,000 remains	970,554 SOL	PARTLY MOVED
Tron	Four swaps settled; distribution stopped 1 November	607,249 USDT in / 272.0554 ETH out	MOVED
Arbitrum	Forced transfer into governance escrow	8,425.9977 ETH + 74.6M ARB	QUARANTINED
Avalanche	2.06M AVAX sold, converted and consolidated	7,242.76 ETH	CONVERTED
Polygon	No address located in this record	not re-pulled	NO ADDRESS
Optimism	Receiving address, nonce 0, unmoved at 4 November	44,231,858.70 OP	HELD
Base	No address located in this record	not recorded	NO ADDRESS

Read this column carefully. Quarantined is a governance escrow, not an issuer freeze and not a return. Held means the address is associated with the movement, not that every unit in it is stolen principal. Converted is still proceeds. A freeze is not a recovery, and replenishment is not a return.

CONTAINMENT ACTIONS, 29 TO 31 OCTOBER

21:01
Tether freezes 1.380B USDT

21:04
Circle freezes 823.1M USDC

22:10
RLUSD 40.5M; USD1 27.8M

00:18
Arbitrum escrows 8,425.9977 ETH and 74.6M ARB

31 Oct
OP moved to a receiving address

The 7702 sweep / and the second wallet

A single authorization turned Binance 14 into a sweeper. The second wallet needed no delegation, which is the strongest public hint that the compromise sat in the signing path.

ROLE	HASH AND POSITION	AMOUNT AND READING
Authorization carrier	`tx 0xad99264d5532ae0dd04b2004eebda05f25657e70dacb764f7ac8d4ccd051298b` `block 26,300,753, index 138`	Fifty EIP-7702 tuples. One applied to Binance 14 at nonce 18,914,809.
First sweep	`0x53bd38b816c23e74134786c29a8c18d792777998a3b9326047b583100e88e2f3` `block 26,300,770, index 189`	167,464.247856 ETH, 1,615,409,498.97 USDT and 62 tokens. 64 logs.
Revocation	`Included 30 October 00:10:35 UTC`	Zero-delegate authorization. Inclusion is not signing time.

18,914,809	15 / 34	18,914,825	49
NONCE THAT APPLIED	TUPLES ABOVE / BELOW IT	NONCE AFTER THE SWEEP	TUPLES THAT COULD NOT APPLY LATER

The carrier holds fifty authorizations, from nonce 18,914,824 down to 18,914,775. At execution the account nonce was 18,914,809, so fifteen tuples sat above it and thirty-four below. One applied. After the sweep the nonce was 18,914,825, above every tuple, so none of the unused forty-nine could apply later. The batch shape is consistent with several signing workflows. It does not prove the signer could not read the nonce, and it does not prove the batch was assembled minutes before inclusion.

Binance 16 is the second wallet. It 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. The convergence on one collection address is evidence of a coordinated window. It is not proof that one person held both keys.

> WHAT THE CHAIN CAN AND CANNOT SAY
>
> A valid transaction or authorization proves a signature was accepted at that block. It does not show when the signature was created, who created it, or who held the signing system at inclusion. It does not distinguish the custodian, a compromised signing service, copied key material, an MPC workflow or an earlier signature broadcast later. The signer-request log, the HSM or MPC audit trail and the policy configuration are the records that would narrow it. A public reconstruction cannot reach them. Binance's 3 November account names the route: unauthorised access to the internal signing service, with MPC and no single key. It does not name who produced the signatures.

The Tron route / four swaps, one recipient

The three Vault collections are collections, not user deposits. A fourth swap completes the route. All four pay the same Ethereum address, the last of them 24 seconds before the pass-through. The fourth deposit entered at 13:34:39, four minutes before the 13:38:18 purchase, and its upstream source is separate and not traced here.

LEG	DEPOSIT, 30 OCTOBER	USDT IN	SWAP	ETH OUT
1	13:43:54 / channel 15475449-Tron-21318	100,000	1985522, completed	44.852680413328560808
2	13:50:24 / channel 15475526-Tron-5945	200,000	1985591, completed	89.998671361744510528
3	13:57:18 / channel 15475595-Tron-19290	272,892	1985638, completed	121.785629276330845590
4	13:34:39 / channel 15475340-Tron-21305	34,357	1985494, completed	15.418418499089104654
Total	Four channels, four completed swaps	607,249	One recipient	272.055399550493021580

DEPOSIT TRANSACTIONS, LEG 1 TO LEG 4

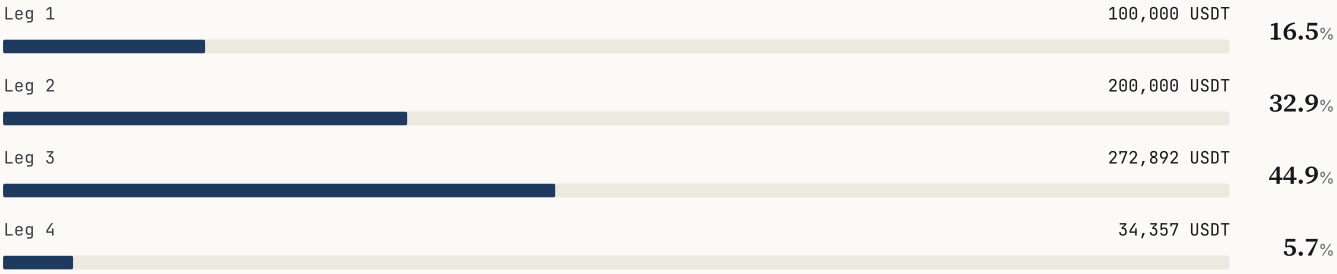
1. 0x3249ac4ae6fbcee06cefec663aaab671a79943c7a68a4536c3b14a45d42c3d15
2. 0xae9aec2f0ca7a68da439c6751834490ccc6638116241d96fa811b6fbeb533fa3
3. 0x60c7d100a831cbbc35f5f8c0b56d5c2425409fd639751a520a041db58f608cd7
4. 0xe3376b0802de413da397722c05596e318b565ea1cb6ada80c2b662e99db778e5

ETHEREUM EGRESS TRANSACTIONS, LEG 1 TO LEG 4. ALL FOUR PAY 0XC6CA6F2F2DC4B59193BE61971462A527529CDAC0

1. 0xf3dbbf5c957e39dff0a9c7dbc9122745324653ad39cda9f7d45c2e12bf8ce43a
2. 0x5e49f89204b1511c8b51f94873f480ee6d0c4de3ecdb61506735f77a2c3db0b5
3. 0x3a0dae994d41f9bf53ec727c91439a2080fe696d11f0c39f2da3fb5723f5a766
4. 0xd129192842c87242074e910015d412d7df6a9174cf9a2f8644c4bd2ad24e7bd0

USDT deposited into each Chainflip swap

607,249 USDT total

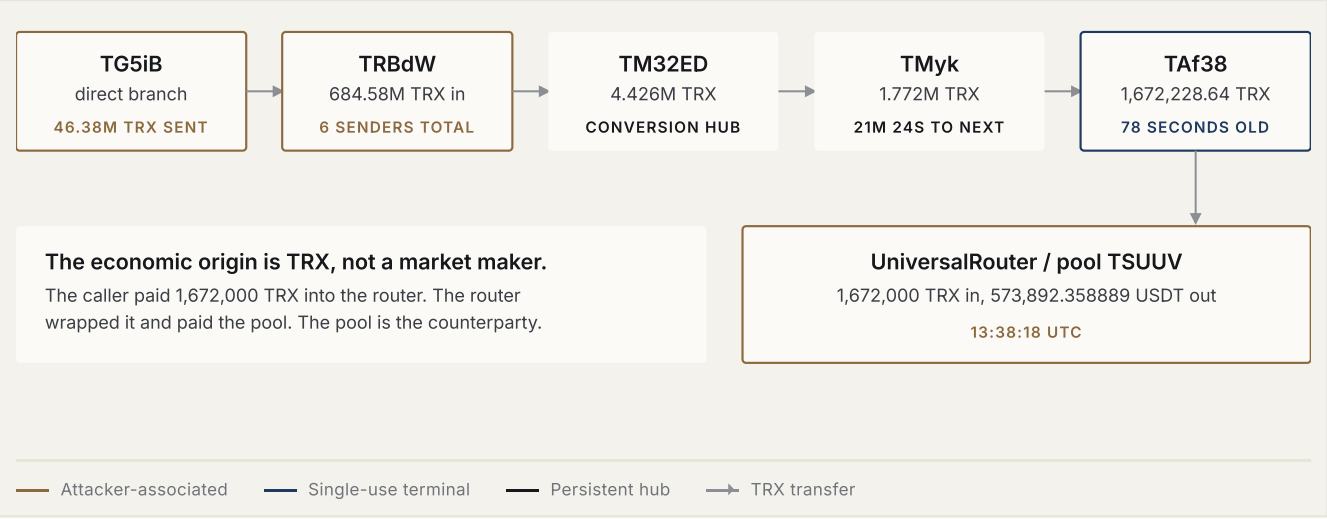


Share of the 607,249 USDT deposited. The ETH paid is not proportional: each leg priced at its own settlement minute.

> THE TERMINAL IS FBI-LISTED, AND IT IS NOT A FREEZE
>
> 0xc6ca6f2f2dc4b59193be61971462a527529cdac0 received the four payouts and sent 272.055383921583158580 ETH to 0x5915F563399b5d2C3A42A08F77E290Ae8121B260 at 14:03:59, 24 seconds after the last payout. The outbound plus 0.000015628909863 ETH of gas equals the four payouts exactly. The destination is a fresh EOA: nonce 0, code 0x. It holds the ETH and has no outbound. The FBI list places it in the campaign. The list does not freeze it, and the funds are not returned.

The TRX origin / a fan-out and a direct branch

The 1,672,000 TRX that bought the USDT did not appear at the swap. It was spent from the hub's working balance, which two branches had fed before 13:38:18.



TIME, 30 OCTOBER	HOP	TRX
10:12:57	TKdLoLkYLpVygaknB2q3YPHaoL9o3AXbce to TM32EDad1ZiMob3S5Rx8VJB6dnjMjD1NTY	3,859,596.431033
11:33:57	TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki to TM32EDad1ZiMob3S5Rx8VJB6dnjMjD1NTY	566,513.374523
13:15:39	TM32EDad1ZiMob3S5Rx8VJB6dnjMjD1NTY to TMyk6fKnBoXG2Au7wrnd64HATugCMcYi7r	1,772,362.450336
13:37:03	TMyk6fKnBoXG2Au7wrnd64HATugCMcYi7r to TAf38EfW1EdNJ3jfVuka3KK2S4ZxUYvokL	1,672,228.637946
13:38:18	TAf38EfW1EdNJ3jfVuka3KK2S4ZxUYvokL to UniversalRouter at TQqgNg13s2DjvXhW1ky4v6TsR8wZGvb7Y4	1,672,000.000000

684,583,971.13	166.38M	220	78 s
TRX INTO TRBDW	TRX RECEIVED BEFORE THE SWAP	RECIPIENTS OF 1,113 OUTFLOWS	TAF38 EXISTED BEFORE THE SWAP

TRBdW ran 1,113 outflows to 220 recipients over 51 hours with zero contract calls. The five fan-out wallets forwarded at different times: one at 10:20:48 on 30 October, four on 31 October between 01:01 and 18:44. TRBdW funded TKdLoL, TM32ED and TNhpf. TAf38 used 99.986% of its balance at 13:38:18 and has been empty since. The terminal addresses are single-use. The upstream layer is a set of persistent conversion hubs.

WHAT THIS LINKS, AND WHAT IT DOES NOT

The Chainflip route and the TNhpf flow share the TRBdW hub. Above it, TSpe5HC3PRD2svJcr1YoGszhHk2mtkyZ8A received 638,190,941.68 TRX from TPBkSjkCMn2ckrMuAP8n2J1jdjbw76bKN4 and 9,986.91 TRX from TCzBTkqn66yApqbYoPezaEQosM5DAd7Y62, then sent 638,200,900 TRX out in five transfers on 30 October. The five recipients delivered 638,200,902 TRX, because one of them held 2 TRX of its own dust and forwarded it with the rest. TG5iB is a separate branch that paid the hub 46,383,069.13 TRX directly. It received 612,729,468 USDT and 46,394,098 TRX on 29 October. Whether the 638,190,941.68 TRX that TPBk sent to TSpe came from a TG5iB USDT conversion is not established by the TRX transfer record: TPBk's recorded TRX inflows on 29 October total 11,009.000025 TRX, so it spent a balance the transfer history does not show. Only two branches had delivered by the swap. Aggregate receipts cannot be allocated to a particular spend: the hub is an account, not a set of marked coins. The reconciliation is on the evidence page.

The intrusion / four stages, one signing service

Binance's own account of how the attacker reached the signing service. It is company evidence, not a chain proof. It explains the route without naming the person who produced the signatures.

STAGE	DATE	WHAT BINANCE SAYS HAPPENED	WHAT IT GAVE THE ATTACKER
01 Foothold	June 2026	Wallet DevOps Engineer A downloaded a tampered Homebrew build while searching for an AI coding tool. Binance detected it, replaced the device and rotated credentials.	The engineer's role and his wallet-team colleagues were exposed.
02 Recruitment	September 2026	Software Engineer B was contacted on a job platform by a fake Project Director. Two interviews followed. The second asked him to download an "assignment" repository onto his work computer.	Malware ran at setup. The endpoint tools did not detect it.
03 Lateral move	20 October 2026	The attacker used Engineer B's computer and an internal AI tool to take control of Engineer A and Wallet Software Engineer C.	A container deployment permission token on Engineer A's computer.
04 Signing	29 October 2026 17:15-19:56 UTC	The attacker logged onto Engineer C's computer, used credentials stolen from Engineer A, deployed a container and ran a script.	Unauthorised access to the internal wallet signing service. Transfers began at 20:05.

3	50	2,961.9	57
ENGINEERS IN THE PATH	AUTHORIZATIONS IN ONE CARRIER	ETH, FINAL UNAUTHORISED TRANSFER	DPRK-LINKED CASES PREVENTED IN 2026

What this connects. The report already showed one transaction carrying 50 EIP-7702 authorizations, with one landing at nonce 18,914,809. Binance describes the same batch as 50 signing transactions used to manipulate the nonce. The two accounts agree on the shape and differ on the noun. The company's account also explains the three-hour containment window: the hot wallet used MPC, so there was no single key to revoke the delegation. The final unauthorised transfer was 2,961.9 ETH at 23:56 UTC, and the delegation was cleared at 00:10:35 on 30 October.

WHAT THIS DOES NOT PROVE

This is Binance's account, not a chain read. Binance says some technical detail stays confidential and that an independent review is being engaged. It does not name the person who produced the signatures, publish the MPC audit trail, or show how the quorum was satisfied. It does not turn every FBI-listed intermediary into a TraderTraitor wallet, and it does not identify the terminal's controller. The company account and the on-chain record are separate instruments; this report keeps them separate.

Lesson. The signing service was the target. A fake recruiter, a tampered Homebrew build and an internal AI tool were the route. Model the human and tooling path as part of the transaction path.

Attribution / the FBI list and what it proves

The actor-level question is answered. The wallet-level question is not. A list is an attribution instrument, not a controller certificate.

LIST	ETH	BTC	SOL	TRON	OTHER	ROWS
FBI advisory, 31 October	608 unique	19 unique	1	0	0	628
Elliptic v1, 08:54:23	2,659 rows	56	1	5,585	8	8,309
Elliptic v2, 08:54:23	2,737 rows	56	1	5,603	11	8,408

378 / 608	19 / 19	230	2,277
FBI ETH ADDRESSES ON ELLIPTIC V1	FBI BTC ADDRESSES MATCHED EXACTLY	FBI ETH ADDRESSES NOT ON V1	UNIQUE EVM ADDRESSES ONLY ON ELLIPTIC

The 19 BTC addresses on the FBI list are exactly the 19 terminal addresses in this case, and the single SOL address is also an exact match. That is set equality, not similarity. A further exact match is 0x5915F563399b5d2C3A42A08F77E290Ae8121B260, the terminal of the Chainflip pass-through. 0x294828705974ad04d86a24a2ff6efe762505a0ed is on the FBI list but not on Elliptic v1, which shows that an official list and a vendor list are different instruments with different update times.

On 3 November Kim Yo-jong denied the attribution, calling it "absurd rhetoric". The FBI list is unchanged at 608 Ethereum addresses, 19 Bitcoin and one Solana address on 4 November. Elliptic's free blocklist has grown from 8,408 to more than 9,500. A bounded search found no arrest, indictment, seizure or OFAC designation of TraderTraitor.

> THE FBI'S OWN SCOPE, QUOTED
>
> "The following addresses are holding or have held assets from the theft, and are operated by or closely connected to North Korean TraderTraitor actors." That is wider than "controlled by" and narrower than "every stolen dollar". Non-membership is not exoneration, and membership is not proof of the balance or the provenance of every unit at that address.

What the attribution changes. It removes the old "no government attribution" caveat and places the campaign at the actor level. It does not identify the person who produced the signatures or how the MPC quorum was satisfied. It does not turn every listed intermediary into a TraderTraitor wallet, and it does not resolve the terminal's controller.

Controls / what they did, and did not do

Three controls, three different scopes. A recommendation is not an execution, a per-chain halt is not a global halt, and a bridge claim without a request identifier does not establish a bridge route.

AAVE V3 CORE, ETHEREUM, BLOCK 26,318,925

RESERVE	ASSET	FROZEN	LTV	LIQ. THRESHOLD	SLOPE2 AT CUT
USDC	0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48	0	0	78%	5.50%
USDT	0xdAC17F958D2ee523a2206206994597C13D831ec7	0	0	78%	5.50%
DAI	0x6B175474E89094C44Da98b954EedeAC495271d0F	0	0	77%	15.00%
USDtb	0xC139190F447e929f090Edeb554D95AbB8b18aC1C	0	0	0%	30.00%

The 31 October LlamaRisk notice says the reserves are no longer frozen and recommends restoring pre-incident Slope2 to 10.00 / 10.00 / 35.00 / 50.00%. At the cut the reserves are unfrozen, LTV is still 0 and Slope2 still reads 5.50 / 5.50 / 15.00 / 30.00%. No event in the supplementary scan to block 26,319,190, 265 blocks past the declared checkpoint, restores the recommended curves. A 4 November read shows all four restored to 10.00 / 10.00 / 35.00 / 50.00%; the execution happened after this report's fixed cut. A zero-LTV setting is a collateral restriction, not a seizure, and a restored curve is not a return.

THREE CONTROLS, THREE SCOPES

CONTROL	OBSERVED STATE	WHAT IT DOES NOT PROVE
THORChain	10 of 13 inbound chains halted at 09:03 UTC on 1 November; 3 of 13 on 4 November (BSC, GAIA, SOL); ETH, BTC and Tron open.	That the halt is global. HALTTHORCHAIN, HALTCHAINGLOBAL and HALTTRADING all read 0.
Issuers	Four-token freeze 2,271,952,865.67 at par; candidate bridge 2,694,599,999.67. Binance reports 2.85B frozen or intercepted; Elliptic independently verifies 2.85B.	That the candidate lines are additive, or that a freeze is a return.
Relay	The queried index returns no request for TNhpfKq83wufEKGjBhQFnT7jnxYmyBzH6F; its 349-transaction history has no Relay depository call.	That no Relay request exists through another address or role, or that the $38M figure is a Relay measurement.

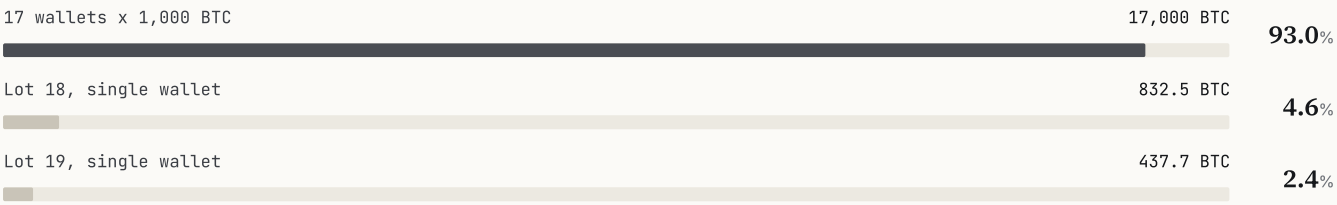
Binance's own numbers are replenishment, not recovery. Update 3 reports about 90% of the impacted amount covered and more than $6.34B of company funds set aside, with a PoR snapshot at 31 October 00:00 UTC and a zero-knowledge proof expected by 3 November. Update 4 reports about 95%, with phase-one withdrawals scheduled for 06:00-09:00 UTC on 1 November. The 3 November blog says 98% as of 31 October; the company's own documents are not reconciled. Company funds replacing customer balances is customer backing. It is not stolen funds returned. The containment took hours because the hot wallet used MPC: there was no single key to revoke the delegations.

Bitcoin / principal, change and dust

The principal did not move. The balances rose because dust and change arrived. The 19 principal outpoints are unspent at tip 974,107 and again at the 4 November re-check; the rest is change and unsolicited dust.

The 18,270 BTC principal

19 outpoints, none spent



Share of 18,270.19988827 BTC. The 1,000 BTC round lots are a distribution pattern, not a single transfer.

THE 19 PRINCIPAL HOLDINGS, IN BLOCK ORDER

01. bc1qxrxujwxfnvz040jw76d26zhjdg5jura7hs968s	1,000.00000000	02. bc1qepc70u3u476vgvg3hfcwjgu4mecxe2uchs4lag	1,000.00000000
03. bc1qdfhmlrdvg4tm87zjl0vyf0xflp5ql50q3g88gw	1,000.00000000	04. bc1qnq6jj9jmlf3945m3l8s0kxnqehrsga300k8t3s	1,000.00000000
05. bc1qz8hdwv8gmml0u96dsvnzsagz6krjyzxmgxupdp	1,000.00000000	06. bc1q42flhayrzy3zh8lkyevw8qcjduurt9a35wlsyx	1,000.00000000
07. bc1q63qrfrpsg5hh0zzn3kp2xx9vljl7dq7tatsjxp	1,000.00000000	08. bc1q0ts8gaf9ht0rr4u02hr56f8thndqsc4kmkmfv3	1,000.00000000
09. bc1q2wvz0kcsn4hqmajwtey30ud27fl25w8pveznn6	1,000.00000000	10. bc1qalwnl7dtaa73fsq5tyn0ghfy3fgfpqkt69tca8	1,000.00000000
11. bc1qjwdw6vrzq4vf6hckutvx4ucj86awwv99mxnz7w	1,000.00000000	12. bc1qs3aej5tmcdz0vctz8y9rjcxtxg8v5385577s56	1,000.00000000
13. bc1qm2j6v3247khlwzxl7p9vqnfkghcllyhv9wjaat	1,000.00000000	14. bc1qs6xnmhar38z44g2za93pv8ygdcwurrh8l87w3v	1,000.00000000
15. bc1qf5cyvv9w50tx9xx9s3xwsne0z87wvjj9l8a35u	1,000.00000000	16. bc1qg3nrzpuvq2pxqx74tcrywr09dc208ze96n3t53	1,000.00000000
17. bc1qm8v88m5fy6kuq9myva2eemwycxqd3e0zcrs2l8	1,000.00000000	18. bc1qrg025e2pgx0rwya2kpgtj30972p64jt0hn6zyt	832.49990088
19. bc1qxg0l4p6xc50zuv9cl5f0l0wmaxjpg8wcy7s9ra	437.69998739		

PRINCIPAL IS NOT THE SAME AS BALANCE

Principal is 18,270.19988827 BTC. Non-principal receipts add 0.00111282 BTC: 0.00063719 in dust-pattern receipts that include 1,111-sat outputs, 0.00046563 in change, and 0.00001000 in new 700-sat and 300-sat dust. The three components are exclusive and sum to the balance difference exactly. Aggregate balance is 18,270.20100109 BTC at the report cut. At the 4 November re-check it was 18,270.20105832 BTC, 0.00005723 BTC higher, all of it inbound dust; no principal outpoint had been spent. The three 30 October multi-output rounds are dust-pattern receipts, not change, and the balance increase is not a movement of principal.

Accounting / positions, not a waterfall

The positions have different scopes. They are not a waterfall that sums to the theft.
The one rule is that overlapping rows are never added.

POSITION	USD AT PAR	SCOPE
Four-token issuer-frozen	2,271,952,865.67	USDT 1,380.5M; USDC 823.1M; RLUSD 40.5M; USD1 27.8M
Tron USDT, candidate	~378,047,134	Tether freeze event on Tron, per the R4 record
Avalanche USDt, candidate	~8,400,000	Issuer freeze after the swap
Polygon USDT0, candidate	~6,200,000	Issuer freeze
Arbitrum quarantined	~30,000,000	8,425.997679954399336 ETH deposited, 8,426.047679407546 ETH held at the cut, plus 74,559,805.2 ARB in governance escrow
Candidate bridge total	2,694,599,999.67	Arithmetic of the five lines above, not deduplicated
Attacker-held stablecoins	1,002,729,468	Tron 312.7M; 0x8d53f50a 190M; Helper 2 500M
Unresolved, priced	453,099,600.51	Tron 300M; Safe MEXC 153.1M
Stablecoins removed	3,051,138,966.97	Fourteen stablecoin rows; not the total theft
Returned to Binance	0 established	No public record at this cut
Replenishment	90% then 95%	Company funds, SAFU, Futures insurance fund, treasury

The priced positions

different scopes; do not add



Bars are scaled to the 3.051B removed stablecoin subtotal. They are shown side by side to compare scope, not to total.

WHY THE ROWS DO NOT ADD

The frozen row is a subset of the removed stablecoins and may overlap the Tron line. The held row includes stablecoins that may have been removed and then moved, plus helper wallets that overlap each other. The unresolved row includes a Safe position that may be a service. The withdrawn R4 total added three mixed-scope rows and reached 3.729B against its own 3.051B subtotal. The 678.2M difference was an arithmetic consequence of mixing scopes, not a measure of overlap. The rows on this page are not a partition either, and they are not a waterfall that sums to the theft. After the cut, Binance reports 2.85B frozen or intercepted and Elliptic reports 3.18B still in linked addresses. Both are wider scopes than the four-token measurement and are not added to it.

The scoreboard / measured, claimed, open

The quantities this case is trying to close, separated by basis. A company figure, a vendor estimate and a chain read are not interchangeable, and none of them is a waterfall.

QUANTITY	VALUE	BASIS	STATUS
Value taken	`6.34B / 6.36B / 6.43B`	Binance / TRM / Elliptic	A range, not a point
Frozen or intercepted	`2.85B`	Binance; verified by Elliptic	Official plus vendor
Four-token freeze	`2,271,952,865.67`	Chain inventory	Measured
Still in linked addresses	`3.18B`	Elliptic, 3 November	Vendor, moving
Returned to Binance	`0 established`	Public record	Open
Replenished	`95% or 98%`	Binance updates / Binance blog	Company documents disagree
BTC principal	`18,270.19988827`	Chain, 19 outpoints	Measured, 19/19 unspent
ETH terminal	`272.055383921583158580`	Chain, nonce 0	Measured, unmoved
OP receiving address	`44,231,858.70442319`	Chain, nonce 0	Measured, unmoved
Tron distribution	`1,113 outflows`	Chain, 220 recipients, 51 hours	Measured, dormant since 1 November

THE NUMBERS STILL TO CLOSE

OPEN QUANTITY	THE RECORD THAT WOULD CLOSE IT
Source of TPBk's 638,190,941.68 TRX	TPBk's full TRC-20 and contract-call history, including any USDT-to-TRX swap, not only native transfers.
Composition of the 2.85B frozen	Issuer freeze ledgers by token, chain and time, reconciled against the on-chain inventory.
Amount converted before the freezes	DEX pool trades in the 37-minute window between arrival and the Tether freeze.
Amount bridged out of Tron	Bridge deposit and payout pairs, not deposit-side estimates alone.
MPC quorum behind the authorizations	Signer-request log, MPC audit trail and policy configuration for 20:20:59 and 00:10:35.
Controller of the terminal	A service link, an operator record, or a later movement that survives scrutiny.

The rule. Do not add a company figure to a vendor estimate and call it a measurement. The four-token freeze is measured; the 2.85B is broader and official; the 3.18B is a vendor snapshot that moves. They answer different questions.

Open questions / what the public record cannot settle

Seven questions. Each one has a named record that would close it. None is filled by inference.

01 **Who produced the authorizations included at 20:20:59 and at 00:10:35, and how was the MPC quorum satisfied?** The chain proves a valid signature was accepted in those blocks. It does not show when it was created, who produced it, or who controlled the signing system at inclusion. Binance says the signing service was reached with stolen credentials and a deployed container. It does not name the person or publish the MPC audit trail. The signer-request log, the audit trail, the revocation request record and the policy configuration would narrow it.

02 **Who controls 0x5915F563399b5d2C3A42A08F77E290Ae8121B260?** It is a fresh EOA, nonce 0, code 0x, holding 272.055383921583158580 ETH, and it is on the FBI list. A list is not control. The operator's records, or a later movement that links it to a service, would narrow the hypothesis. A service link would not identify the controller.

03 **Who is above TSFET and TSiY1f?** TSiY1f was fed by 35 bulk wallets created between 02:30 and 02:47 on 30 October. TSFET is a single-use pass-through. Their funders and TRBdW's other 217 recipients are not traced.

04 **What is the full approval population?** One Approval is confirmed by the raw receipt, with value 2^256-1 and spender TTJxU3P8rHycAyFY4kVtGNfmnMH4ezcuM9. The 64-record count is not re-established. A complete re-pull and raw-topic decode would establish it.

05 **Did an Ethereum reorg cause a duplicate 10 ETH refund?** Chainalysis asserts it. A 10 ETH refund can be 9.99988939 ETH after the fee, so an exact-10 filter is not a valid negative. A primary reorg dataset and the two refunds would close it.

06 **Which Aave implementation was live at the event block?** The freeze, unfreeze and rate events are recovered and the reserves are unfrozen. The implementation slot and the exact before and after state remain open.

07 **Where did TPBk's 638,190,941.68 TRX come from?** TPBk sent it to TSpe, but its recorded TRX inflows on 29 October total 11,009 TRX. A USDT-to-TRX conversion would not appear in the native transfer history. The full TRC-20 and contract-call record for TPBk and its counterparties would close it.

Why these are listed. A report that hides its open questions is less useful than one that names them. These are the limits of the public record, not a verdict on the findings above. The method and the correction history are on the notes page. The checkable rows, the fixed cutoffs and the source register are on the evidence page.

Key addresses / and what this rests on

Full addresses, not truncated, each linked to a public explorer. Ten checkable rows, the nineteen Bitcoin outpoints, the fixed cutoffs and the primary sources are on the evidence page.

ENTITY	CHAIN	ADDRESS
Binance 14 Emptied. Hot wallet, 20:24:23	ETHEREUM	0x28C6c06298d514Db089934071355E5743bf21d60
Authorization carrier tx Transaction. EIP-7702 batch, block 26,300,753	ETHEREUM	0xad99264d5532ae0dd04b2004eebda05f25657e70dacb764f7ac8d4ccd051298b
Four-swap recipient Pass-through. All four Chainflip payouts	ETHEREUM	0xc6ca6f2f2dc4b59193be61971462a527529cdac0
Terminal FBI-listed. Holds 272.055383921583158580 ETH, plus 0.00001 ETH dust	ETHEREUM	0x5915F563399b5d2C3A42A08F77E290Ae8121B260
Chainflip ETH Vault Service. Official Chainflip mainnet Vault	ETHEREUM	0xF5e10380213880111522dd0efD3dbb45b9f62Bcc
Theft hub Hub. Received 612,729,468 USDT and 46,394,098 TRX	TRON	TG5iBMQPrDzJJAUM8GMVBf1hRaJ1wvzsGi
Conversion hub Hub. 1,113 outflows to 220 recipients	TRON	TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki
Swap terminal Single-use. 1,672,228.637946 TRX in	TRON	TAf38EfW1EdNJ3jfVuka3KK2S4ZxUYvokL
AMM pool Counterparty. 573,892.358889 USDT out	TRON	TSUUVjysXV8YqHytSNjfkNXnnB49QDvZpx
Optimism receiving address Held. 44,231,858.70442319 OP, no code, no outbound	OPTIMISM	0x6b1bae59d09fccbddb6c6cceb07b7279367c4e3b
Governance escrow Quarantined. 8,425.997679954399336 ETH deposited	ARBITRUM	0x0000000000000000000000000000000000000da0

> Every address above is written in full and links to a public explorer. The evidence page carries the ten rows that carry this case, all nineteen Bitcoin outpoints with their transaction ids and satoshi values, the fixed cutoffs and the source register. The working register, the query recipes and the capture files stay internal.

WHAT THIS REPORT RESTS ON

Verified on-chain: a hash, block, receipt, balance or log read	VERIFIED
Official statement: the issuing party's own words	OFFICIAL
Vendor assessment: a named firm's published reading	VENDOR
Analytical inference: derived, not directly observed	INFERENCE
Unresolved at this cut	OPEN

> Fixed cutoffs: Ethereum 26,318,925; Optimism finalized 158,962,082; Arbitrum 520,232,606; Bitcoin tip 974,107; Tron solid 87,616,878. Principal positions re-checked 4 November. Event time, data cutoff, retrieval time and release time are kept separate throughout. Block hashes, the nineteen Bitcoin outpoints and the source register are on the evidence page.