ONYX AML

INVESTIGATION REPORT

The Binance hack of 29 October 2026: how $6.3 billion left the hot wallets, where it is now and whether it is being cashed out

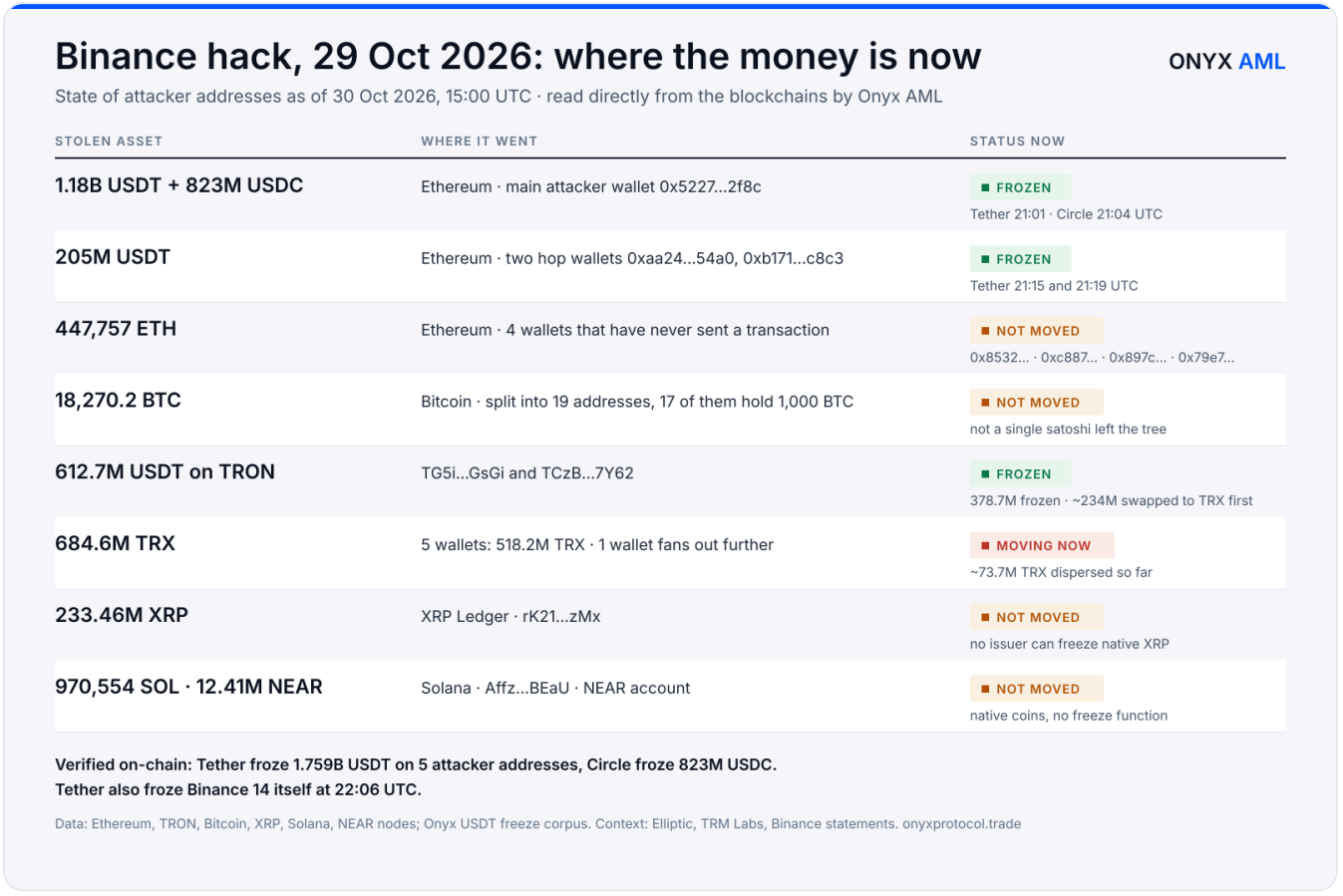
On the evening of 29 October an attacker emptied Binance hot wallets on ten blockchains in about four hours. Most reports stop at the headline figure. We read every attacker address directly from the chains, matched the freezes against our own corpus of Tether contract events, and checked where each coin is right now. Short version: about $2.6 billion in stablecoins is frozen, bitcoin and ether have not moved yet, and the only active outflow is TRX.

Data as of 30 October 2026, 15:00 UTC
Onyx AML · onyxprotocol.trade · report ONYX-INC-2026-10-BNB

Data as of 30 October 2026, 15:00 UTC. Balances, freeze times and transfers below were read by Onyx AML directly from Ethereum, TRON, Bitcoin, XRP Ledger, Solana and NEAR nodes and from our corpus of USDT freeze events. Totals, attribution and the first-hour swaps come from Binance, Elliptic, TRM Labs and CoinDesk and are marked as such. The root cause has not been officially confirmed yet; we separate what is known from what is likely.

The short version

What	Figure	Source
Stolen in total	about $6.3B (Binance), $6.36B (TRM), $6.43B (Elliptic), 10 networks	Binance, TRM, Elliptic
Frozen by Tether on attacker addresses	1,759.2M USDT on 5 addresses (Ethereum 3, TRON 2)	on-chain, Onyx
Frozen by Circle	823M USDC on the main wallet, plus 1.56M on a bridge hop	on-chain, Onyx
Ether held by the attacker	447,757 ETH on 4 wallets that have never sent a transaction	on-chain, Onyx
Bitcoin held by the attacker	18,270.2 BTC on 19 addresses, nothing spent	on-chain, Onyx
Other untouched coins	233.46M XRP, 970,554 SOL, 12.41M NEAR	on-chain, Onyx
Actively moving	TRX: about 73.7M of 684.6M fanned out to fresh addresses	on-chain, Onyx
Attribution	North Korea's TraderTraitor, "high confidence" (TRM), "likely" (Elliptic); no government statement yet	TRM, Elliptic



How it happened: the weak points

Binance's first statement pointed to a compromised laptop of a DevOps engineer, which gave the attacker access to a service container from which withdrawal transactions could be submitted. Binance also said it found no evidence that private keys leaked. A later update said the investigation had found "additional points of breach". The full technical report has not been published, so the list below is what the chain data and the public statements support today.

1. The signing system obeyed the attacker on ten chains at once. Bitcoin, TRON, XRP, Solana, Avalanche, Polygon, Arbitrum, Optimism and Base were drained with ordinary signed transfers from Binance wallets, within minutes of each other. When a system can be told to sign transfers on ten networks without the keys leaving it, the weak point is not a key but the layer that decides what gets signed. Both Elliptic and TRM reach the same conclusion. This is also why "no private keys leaked" is not reassuring: the keys did not need to leave.

2. The hot wallet signed an EIP-7702 delegation. EIP-7702 (live since the Pectra upgrade in May 2025) lets an ordinary address attach smart-contract code to itself with one signed authorization. The attacker submitted one transaction carrying 50 such authorizations, each signed by the Binance 14 key for a different nonce. Only one matched. That detail matters: whoever requested the signatures could get them, but did not know the wallet's live state, which fits access to a signing service rather than possession of the key. We confirmed in the chain state that from block 26,300,753 (20:20:59 UTC) Binance 14 carried the delegation marker pointing to contract `0x63e842b054bd624a465454d533c33f573e9c6fae`. That contract has verified source code under the name "Target" and was deployed by `0x7c8601d4645b93cea45f71e118a729332e6b5ca0`, an address on the attacker's side that was funded through Tornado Cash the day before. A hot wallet that only ever sends plain transfers has no business signing a type-4 authorization. A signing policy that allowed it is the clearest single control failure visible on chain.

3. The delegation stayed on for almost four hours. A 7702 delegation persists until it is replaced. Once set, every new deposit into Binance 14 could be swept without another signature. The attacker swept the wallet again at 20:41, 20:59, 21:04, 21:44, 22:39 and 23:56 (TRM). In the chain state the marker disappears only at block 26,301,896, at 00:10:35 UTC on 30 October: 3 hours 49 minutes 36 seconds of exposure. Tether eventually blacklisted Binance 14 itself at 22:06:23 UTC so that USDT arriving there could not be pulled out. An issuer freezing the exchange's own hot wallet to protect it from its own delegation is, as far as we know, a first.

4. Too much money in one hot wallet. Ethereum accounted for about $3.8B of the theft, almost all of it from Binance 14. It was also the executor of a Binance smart account, which is how 823M USDC was pulled. A hot wallet is meant to hold a working float. These same wallets are listed in Binance's proof of reserves, which is why CoinDesk estimates that ether backing fell to about 94% until the replacement funds arrive.

5. Hours of visible preparation. The operator wallet received three 0.1 ETH withdrawals from Tornado Cash on 28 October, the sweeper contract was deployed at 15:59 UTC on 29 October and, according to TRM, rehearsed on test wallets about four hours before use. None of that is invisible; it was simply not linked to Binance until the money moved.

What exchanges should take from it. Sign by policy, not by request: hot wallets should be allowed a whitelist of transaction types, and a 7702 authorization should be denied outright. Monitor your own addresses for code: `eth_getCode` returning anything other than empty on an exchange hot wallet is an instant alarm. Cap hot wallet balances and velocity per chain, and treat simultaneous large outflows on several chains as a single incident. Keep freeze channels with issuers warm: the money that was saved on 29 October was saved by Tether, Circle, Ripple and World Liberty Financial within 40 minutes to two hours, and only for tokens that have a freeze function.

Timeline (UTC)

Time	Event	Source
28 Oct	Three 0.1 ETH withdrawals from Tornado Cash fund the operator wallet	Elliptic, TRM
29 Oct 15:59	Sweeper contract deployed	Elliptic
~20:05	233.46M XRP leave five Binance XRP Ledger wallets	TRM
20:20	18,270.2 BTC leave Binance and are split into 1,000 BTC chunks	TRM, on-chain
20:20:59	EIP-7702 delegation active on Binance 14 (block 26,300,753)	on-chain, Onyx
20:22:45	612,729,468 USDT move from Binance-Hot 7 on TRON to TG5iBMQPrDzJJAUM8GMVBf1hRaJ1wvzsGi	on-chain, Onyx
~20:24	167,464 ETH and 63 tokens swept out of Binance 14	TRM, CoinDesk
20:45:51, 20:56:09	100M and 200M USDT forwarded on TRON to TPBkSjkCMn2ckrMuAP8n2J1jdjbw76bKN4, then about 234M pushed into SunSwap pools for TRX	on-chain, Onyx
21:01:35	First Tether freezes: the main Ethereum wallet 0x5227…2f8c and three other attacker wallets, blocks 26,300,954 to 26,300,960	Onyx freeze corpus
21:04	Circle freezes 823M USDC	TRM, Elliptic; confirmed on-chain
21:09:12	Tether freezes TG5i…GsGi with 312.73M USDT still on it	Onyx freeze corpus
21:14:59, 21:18:59	Tether freezes two Ethereum hop wallets holding 175.0M and 30.0M USDT	Onyx freeze corpus
21:16:18 to 21:21:12	65.99M USDT forwarded to TCzBTkqn66yApqbYoPezaEQosM5DAd7Y62 and frozen there 4 min 54 s later	on-chain, Onyx
22:06:23	Tether blacklists Binance 14 itself	Onyx freeze corpus
22:15	Binance pauses withdrawals	Binance
23:56	Last sweep of Binance 14	TRM, Elliptic
30 Oct 00:06	46.38M stolen TRX sent to a new address, TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki	on-chain, Onyx
00:10:35	Delegation on Binance 14 removed (block 26,301,896)	on-chain, Onyx
06:36	Token dumping on DEXs stops	Elliptic
10:20 to now	120M TRX join TRBd…PRki, which sends 30k to 950k TRX chunks to freshly created addresses	on-chain, Onyx

Where the money went, chain by chain

Ethereum stablecoins: mostly caught. The main attacker wallet `0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c` now holds 1,175,464,713 USDT and 823,000,000 USDC, both frozen. The race was close: the USDT arrived around 20:24 and was frozen at 21:01, 37 minutes later. In that window the attacker sold roughly 325M to 434M USDT to market makers and through UniswapX and 1inch for ether at a discount of more

than 10% (TRM, Elliptic); a buyer who pays 10% over market for ether is a buyer in a hurry. Two hop wallets with 175.0M and 30.0M USDT were frozen on the way. Those two, `0xaa246bf639586a6ba46762d378ce50ca4fc654a0` and `0xb171ca86f82070282138352ff7111b494060c8c3`, are not yet in Elliptic's public blocklist; we found them through our freeze corpus, frozen within the same twenty minutes. A third address frozen in that window, `0x7aa4d3029e4c6a8e916300014ad95b6d6c03bfd1`, is delegated to the same smart-account code as a listed attacker wallet.

Ether: parked. 413,477 ETH sit on three wallets: `0x8532fa14acaf483729c449b8458aeddb900543d4` (197,460 ETH), `0xc887af690e0301cd4edbbce8f8d31b4ec65b286a` (137,602 ETH) and `0x897c80d1a9729e94460e2bd93178bd5215158df3` (78,415 ETH). None of them has ever sent a transaction (nonce 0). A fourth parking wallet, `0x79e70d139fc05aa75f75611fdf2680e9952b544a`, holds another 34,280 ETH collected on the morning of 30 October from three listed attacker wallets; it is not in Elliptic's public list either. That makes 447,757 ETH parked on four wallets. The traffic you see on explorers is incoming dust and messages from onlookers, not outflows. About 19,760 ETH were also borrowed on Aave against 59.9M USDT of collateral before Aave froze the markets (Elliptic).

Bitcoin: split, not sold. The 18,270.2 BTC were broken up within minutes into 19 addresses: 17 hold exactly 1,000 BTC, one 832.5 and one 437.7. We walked the whole tree: the sum of unspent outputs is 18,270.2 BTC, so not a single coin has left it. Round 1,000 BTC lots are convenient for over-the-counter sales, which is the most likely next stage, but nothing has moved yet. Bitcoin has no issuer and nobody can freeze it.

TRON: a race against Tether, mostly lost. 612.7M USDT left Binance-Hot 7 at 20:22:45. The attacker managed to forward 300M before the freeze: about 234M went into SunSwap pools and came out as roughly 638M TRX, 65.99M was forwarded and frozen within five minutes, and 312.73M were frozen on the first receiving wallet. The TRX was then consolidated on one address and split into five: four wallets with 158.2M, 120M, 120M and 120M TRX have not moved. The fifth sent 120M TRX to `TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki`, which also received the 46.38M TRX stolen from Binance directly. That address was created at 00:06 UTC on 30 October and has since sent about 73.7M TRX in 30k to 950k chunks to dozens of brand-new addresses. This is the only part of the theft that is actively being laundered right now. Elliptic also reports that part of the TRON flow reached an address that holds proceeds of the September Bitget exploit.

XRP, Solana, NEAR: untouched. 233,461,943 XRP sit on `rK21t6nGLy4MNDqhvy3pGwcLFy25qgfzMx`, 970,554 SOL on `AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU` and 12.41M NEAR on one account. These are native coins with no freeze function, so the issuers cannot help here. The Arbitrum Security Council did move 8,426 ETH and 74.6M ARB out of the attacker's reach at 00:08 UTC (TRM).

Is the hacker dumping?

Not at scale, not yet. The dumping happened in the first hours and only where speed mattered: stablecoins were sold or swapped before the issuers could freeze them, and the long tail of tokens was dumped on DEXs until 06:36 UTC (Elliptic). Since then bitcoin, the parked ether, XRP, SOL and NEAR have not moved. The one active flow is TRX, fanned out through fresh addresses, which is typical preparation for swap services and OTC desks. If the pattern of earlier large thefts holds, the next stage is bridges and OTC brokers, and it can take weeks. The market impact so far came from fear rather than selling: bitcoin fell about 4% and liquidations reached about $1.6B on 30 October.

The FUN dump: what happened to a small token

The Binance 14 sweep at 20:24 UTC also took 714,911,344 FUN (FUNToken, formerly FunFair) to the main attacker wallet. At 23:28:47 UTC the whole amount was moved to a fresh address, `0x06ea1ab3ecf570`

`029eb1f94dbb9eac06bc79685f`, which sold into the thin FUN/WETH pool on Uniswap in 154 transactions. It got rid of 134,145,256 FUN and received only 111.48 ETH, about $250,000; the pool price collapsed by more than 90% (CoinDesk). At 06:30 UTC the attacker gave up and sent the remaining 580,766,088 FUN, about 5.4% of the supply, back to the main wallet, where they still sit. The 111.85 ETH of proceeds went to the parking wallet 0x79e7...544a. FUNToken asked exchanges to pause FUN deposits. The lesson for holders of small tokens: an exchange hot wallet can hold a large share of your token's supply, and if it is stolen, the overhang stays in the market for as long as the attacker keeps it. Someone has also started sending zero-value FUN transfers from a look-alike address, a classic address-poisoning trick, this time aimed at the hacker.

What it means for Binance users

Binance says client balances are not affected because the stolen funds were the exchange's own hot wallets, and that it has set aside more than $6.34B to cover the loss, about $5B of it already in the affected tokens. Withdrawals were paused at 22:15 UTC on 29 October; the exchange gives about 40 hours as a preliminary target, and has promised a full proof of reserves by Monday. Deposits keep working.

- **Ignore anyone who offers "compensation" or a "refund" from Binance.** After every large hack, fake support accounts appear within hours. Binance does not ask for seed phrases, payments or "verification transfers".
- **Do not rush to buy USDT or TRX from strangers on P2P this week.** Stolen TRX is being fanned out right now. Coins that touched these addresses can get your account frozen at the next exchange, even if you did nothing wrong.
- **Check the counterparty address before a deal.** Our free checker reads the USDT and USDC blacklists straight from the contracts, so the frozen attacker addresses show up there immediately. The full list of attacker addresses is in the PDF.
- **Watch the proof of reserves.** The question is not the total but token by token: whether the replacement ether and bitcoin are actually on the listed wallets.

Method and limits

We started from Elliptic's public blocklist of 48 addresses and the hot wallet and transaction hashes published by CoinDesk, read the current balances, contract code and USDT and USDC blacklist status of every address, walked the bitcoin and TRX trees until the coins stopped moving, and matched every freeze against our own corpus of events from the USDT contracts on Ethereum and TRON. The delegation window was found by reading the code of Binance 14 at historical blocks. Dollar totals, the first-hour swaps, the Aave position and attribution come from the sources named in the table. The root cause is not confirmed until Binance publishes its report; we will update this page when it does.

Funds frozen and you think it is a mistake? Describe your case in a free assessment: we will tell you honestly what the chances are and where to start.

Appendix A. Address register

Every address below was read directly from its blockchain at 15:00 UTC on 30 October 2026. Freeze times come from the Onyx corpus of USDT contract events (Tether). "Not in Elliptic list" marks addresses we identified that are absent from Elliptic's public blocklist at the time of writing.

Address	Network	Role	Holdings now	Status
`0x28c6c06298d514db089934071355e5743bf21d60`	Ethereum	Binance 14 hot wallet, EIP-7702 delegated 20:20:59 to 00:10:35	1,352,018 USDT	Binance (victim); frozen by Tether 22:06:23
`0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c`	Ethereum	Main attacker wallet, received the sweeps	4.50 ETH, 1,175,464,713 USDT, 823,000,000 USDC, 580,766,088 FUN	frozen by Tether 21:01:35; USDC frozen by Circle
`0x9749292d74fd460982d0912ea9515ea24736c762`	Ethereum	Attacker wallet	~0	frozen by Tether 21:01:35
`0x0ddf0480016e6bcb2c1f5d190d221fba1320697e`	Ethereum	Attacker wallet	0.06 ETH	frozen by Tether 21:01:47
`0x8d53903625b8e839b9df4bd28b0efb1cd6b8639a`	Ethereum	Attacker wallet	0.10 ETH	frozen by Tether 21:02:47
`0xaa246bf639586a6ba46762d378ce50ca4fc654a0`	Ethereum	Hop wallet *(not in Elliptic list)*	174,999,872 USDT	frozen by Tether 21:14:59
`0xb171ca86f82070282138352ff7111b494060c8c3`	Ethereum	Hop wallet *(not in Elliptic list)*	30,000,000 USDT	frozen by Tether 21:18:59
`0xccbef95633adb5cd2b5038db5a38d77e726ca263`	Ethereum	Hop wallet *(not in Elliptic list)*	0.03 ETH	frozen by Tether 21:16:47
`0x7aa4d3029e4c6a8e916300014ad95b6d6c03bfd1`	Ethereum	Attacker wallet, delegated to smart-account code *(not in Elliptic list)*	0.04 ETH	frozen by Tether 21:12:35
`0x77edef23fbd05921c26fe29fcc3a65e14d2ac3eb`	Ethereum	Attacker wallet, delegated to smart-account code	0.01 ETH	
`0x8532fa14acaf483729c449b8458aeddb900543d4`	Ethereum	Holding wallet, never sent a transaction	197,460 ETH	not moved
`0xc887af690e0301cd4edbbce8f8d31b4ec65b286a`	Ethereum	Holding wallet, never sent a transaction	137,602 ETH	not moved
`0x897c80d1a9729e94460e2bd93178bd5215158df3`	Ethereum	Holding wallet, never sent a transaction	78,415 ETH	not moved
`0x7c8601d4645b93cea45f71e118a729332e6b5ca0`	Ethereum	Operator, deployed the sweeper contract	1.18 ETH	
`0x63e842b054bd624a465454d533c33f573e9c6fae`	Ethereum	Sweeper contract "Target", target of the Binance 14 delegation *(not in Elliptic list)*	~0	
`0x19bee294a6daab49c9e5ab69a5da6c035c70f2bf`	Ethereum	Contract deployed by the operator	~0	
`0xa97bf7836f8a08f9ed91d41453d371493fae8d10`	Ethereum	Swap wallet	0.37 ETH, 123,176 USDC	USDC frozen by Circle
`0xc39e690bea48448cc47e7acddfe30e6453e09824`	Ethereum	Bridge hop from Avalanche	1,563,813 USDC	USDC frozen by Circle
`0xb3ddec0ccc5c3ba733fcdf5a15f98c95ec5a5fdb`	Ethereum	Swap wallet	33,005 USDC	USDC frozen by Circle

0xcf4ca2bdf21bc3a467a00b6afe72b833982723e0	Ethereum	Attacker wallet	~0	emptied
0x42cdf00c85005630cc8605731b9364f712077810	Ethereum	Attacker wallet	~0	emptied
0xe7024ab80143b1ef843efe6a58368696cb87958d	Ethereum	Attacker wallet	0.02 ETH	
0x7f9dc988b46336ad536828fad50fa8fa1e5415e3	Ethereum	Attacker wallet	~0	emptied
0x8c7111e9a3270457b76f0bd137209089047a6aa4	Ethereum	Attacker wallet	~0	emptied
0x0084847bb9384d2fc5e8836e663689467e3e4c81	Ethereum	Attacker wallet	0.05 ETH	
0xa3b3dee870f01560fdbe5af659c9c9135748886f	Ethereum	Attacker wallet	~0	emptied
0x600d6f00eadabdb514561ceeb43730a7103e8298	Ethereum	Attacker wallet	~0	emptied
0x811f15855476156ebf86ba3b84fafb8ceaa4e84c	Ethereum	Attacker wallet	~0	emptied
0x79e70d139fc05aa75f75611fdf2680e9952b544a	Ethereum	Parking wallet, collected 34,280 ETH from three attacker wallets *(not in Elliptic list)*	34,280 ETH	not moved
0x06ea1ab3ecf570029eb1f94dbb9eac06bc79685f	Ethereum	FUN seller: sold 134.1M FUN on Uniswap for 111.48 ETH *(not in Elliptic list)*	~0	emptied
TDqSquXBgUCLYvYC4XZgrprLK589dkhSCf	TRON	Binance-Hot 7 (TRON), source of 612.7M USDT		Binance (victim)
TG5iBMQPrDzJJAUM8GMVBf1hRaJ1wvzsGi	TRON	First TRON receiver	312,729,468 USDT	frozen by Tether 21:09:12
TPBkSjkCMn2ckrMuAP8n2J1jdjbw76bKN4	TRON	TRON forwarder to SunSwap	~0	frozen by Tether 21:17:39
TCzBTkqn66yApqbYoPezaEQosM5DAd7Y62	TRON	TRON hop *(not in Elliptic list)*	65,990,000 USDT	frozen by Tether 21:21:12
TSpe5HC3PRD2svJcr1YoGszhHk2mtkyZ8A	TRON	TRX consolidation *(not in Elliptic list)*	~0	emptied
TKkH2vH6kyi2QKcMbqym53WMuvdd1xvw6K	TRON	TRX holding wallet *(not in Elliptic list)*	158,200,902 TRX	not moved
TJajtPqDqUGh1Sr1j8ugHoSXBVpaFLLHKT	TRON	TRX holding wallet *(not in Elliptic list)*	120,000,000 TRX	not moved
TCBAz7itvtX5CjBzVMPQdrbwQLN63ao1fk	TRON	TRX holding wallet *(not in Elliptic list)*	120,000,000 TRX	not moved
TL2F4GhnaFVZBZPncHYjwfYZFW44NcfVwj	TRON	TRX holding wallet *(not in Elliptic list)*	120,000,000 TRX	not moved
TAk1xJNWuBYvJHLsUiBFLeuK6xvpQUFYP5	TRON	TRX wallet, forwarded 120M TRX *(not in Elliptic list)*	~0	emptied
TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki	TRON	TRX disperser, created 30 Oct 00:06 *(not in Elliptic list)*	92,717,498 TRX	moving
bc1q0mtc2f5agpkvlq6hhahmfr3hlr55kyfjhl2mnm	Bitcoin	BTC root, split 18,270.2 BTC	~0	emptied

bc1qxrxujwxfnvz040jw76d26zhjdg5jura7hs968s	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1qepc70u3u476vgvg3hfcwjgu4mecxe2uchs4lag	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1qnq6jj9jmlf3945m3l8s0kxnqehrsga300k8t3s	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1qdfhmlrdvg4tm87zjl0vyf0xflp5ql50q3g88gw	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1qz8hdwv8gmml0u96dsvnzsagz6krjyzxmgxupdp	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1q42flhayrzy3zh8lkyevw8qcjduurt9a35wlsyx	Bitcoin	BTC holding address *(not in Elliptic list)*	1,000.0 BTC	not moved
bc1qjwdw6vrzq4vf6hckutvx4ucj86awwv99mxnz7w	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1q0ts8gaf9ht0rr4u02hr56f8thndqsc4kmkmfv3	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1qalwnl7dtaa73fsq5tyn0ghfy3fgfpqkt69tca8	Bitcoin	BTC holding address *(not in Elliptic list)*	1,000.0 BTC	not moved
bc1q2wvz0kcsn4hqmajwtey30ud27fl25w8pveznn6	Bitcoin	BTC holding address *(not in Elliptic list)*	1,000.0 BTC	not moved
bc1qs3aej5tmcdz0vctz8y9rjcxtxg8v5385577s56	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1qs6xnmhar38z44g2za93pv8ygdcwurrh8l87w3v	Bitcoin	BTC holding address *(not in Elliptic list)*	1,000.0 BTC	not moved
bc1qm2j6v3247khlwzxl7p9vqnfkghcllyhv9wjaat	Bitcoin	BTC holding address	1,000.0 BTC	not moved
bc1q63qrfrpsg5hh0zzn3kp2xx9vljl7dq7tatsjxp	Bitcoin	BTC holding address *(not in Elliptic list)*	1,000.0 BTC	not moved
bc1qg3nrzpuvq2pxqx74tcrywr09dc208ze96n3t53	Bitcoin	BTC holding address *(not in Elliptic list)*	1,000.0 BTC	not moved
bc1qm8v88m5fy6kuq9myva2eemwycxqd3e0zcrs2l8	Bitcoin	BTC holding address *(not in Elliptic list)*	1,000.0 BTC	not moved
bc1qf5cyvv9w50tx9xx9s3xwsne0z87wvjj9l8a35u	Bitcoin	BTC holding address *(not in Elliptic list)*	1,000.0 BTC	not moved
bc1qrg025e2pgx0rwya2kpgtj30972p64jt0hn6zyt	Bitcoin	BTC holding address	832.5 BTC	not moved
bc1qxg0l4p6xc50zuv9cl5f0l0wmaxjpg8wcy7s9ra	Bitcoin	BTC holding address	437.7 BTC	not moved
rK21t6nGLy4MNDqhvy3pGwcLFy25qgfzMx	XRP Ledger	XRP holding	233,461,943 XRP	not moved
AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU	Solana	SOL holding	970,554 SOL	not moved
efd224256518a7cacd209867963276efed302a8e222c013c43f4b1bd369ae5af	NEAR	NEAR holding	12,410,068 NEAR	not moved

Appendix B. Sources

- Binance, official statements, 29-30 Oct 2026 (via CoinDesk, crypto.news)
- Elliptic, "The largest theft in history: North Korea likely behind the $6.4 billion Binance hack", elliptic.co/insights/binance-largest-hack-in-history, and public blocklist data-

cdn.elliptic.co/blocklists/binance-hack-blocklist.csv

- TRM Labs, "North Korea steals USD 6.36 billion from Binance in the largest hack in history", trmlabs.com
- CoinDesk, "Binance says customer money is safe after huge hack drains key reserve wallets", 30 Oct 2026; "Binance arranges $6.34 billion to cover losses", 30 Oct 2026
- CNBC, 29-30 Oct 2026; Yahoo Finance, 30 Oct 2026 (market impact)
- Ethereum node (eth.drpc.org, archive state), Blockscout; TronGrid, Tronscan; mempool.space; XRP Ledger s1.ripple.com; Solana mainnet-beta RPC; NEAR RPC
- Onyx AML corpus of USDT contract events (AddedBlackList) on Ethereum and TRON