CASE FILE / PRELIMINARY REPORT

The Binance Hot Wallet Drain

Binance hot wallets across ten blockchains were emptied in one coordinated window on 29 October 2026. This document records what the on-chain evidence shows. Every address is clickable to its explorer.

- On-chain snapshot taken 30 October 2026, 13:06 UTC

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

PRELIMINARY

$6.36B VALUE TAKEN	**10** CHAINS HIT	**~$2.27B** FROZEN
~$2.4B STILL WITH ATTACKER	**413,477** ETH PARKED	**18,270** BTC UNSPENT

Prepared by **Keshav Maheshwari**
withkeshav.com

Timeline / 28 to 30 October 2026

One coordinated window. All dates and times are UTC. The cluster on the evening of 29 October carries most of the case.

28 October 2026

UTC

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

29 October 2026

UTC

15:59	**Sweeper contract deployed** on Ethereum `0x63e842B054Bd624a465454D533C33F573e9c6fAe`
20:05	**XRP Ledger emptied**, 233.46M XRP from five wallets.
20:10	**Solana and Optimism** hot wallets emptied.
20:20	50 signing requests sent to Binance 14, **one accepted**.
20:24	**Binance 14 emptied**, 167,464 ETH and 1.615B USDT taken.
20:25	Ten more hot wallets emptied across four chains.
20:41	More sweeps using the same access.
21:01	**Tether froze 971.1M USDT.**
21:04	**Circle froze 823M USDC.**
22:10	World Liberty Financial froze 27.8M USD1.
23:05	**Second wave** on Avalanche and Polygon.
23:35	Binance reported $2.54B frozen.

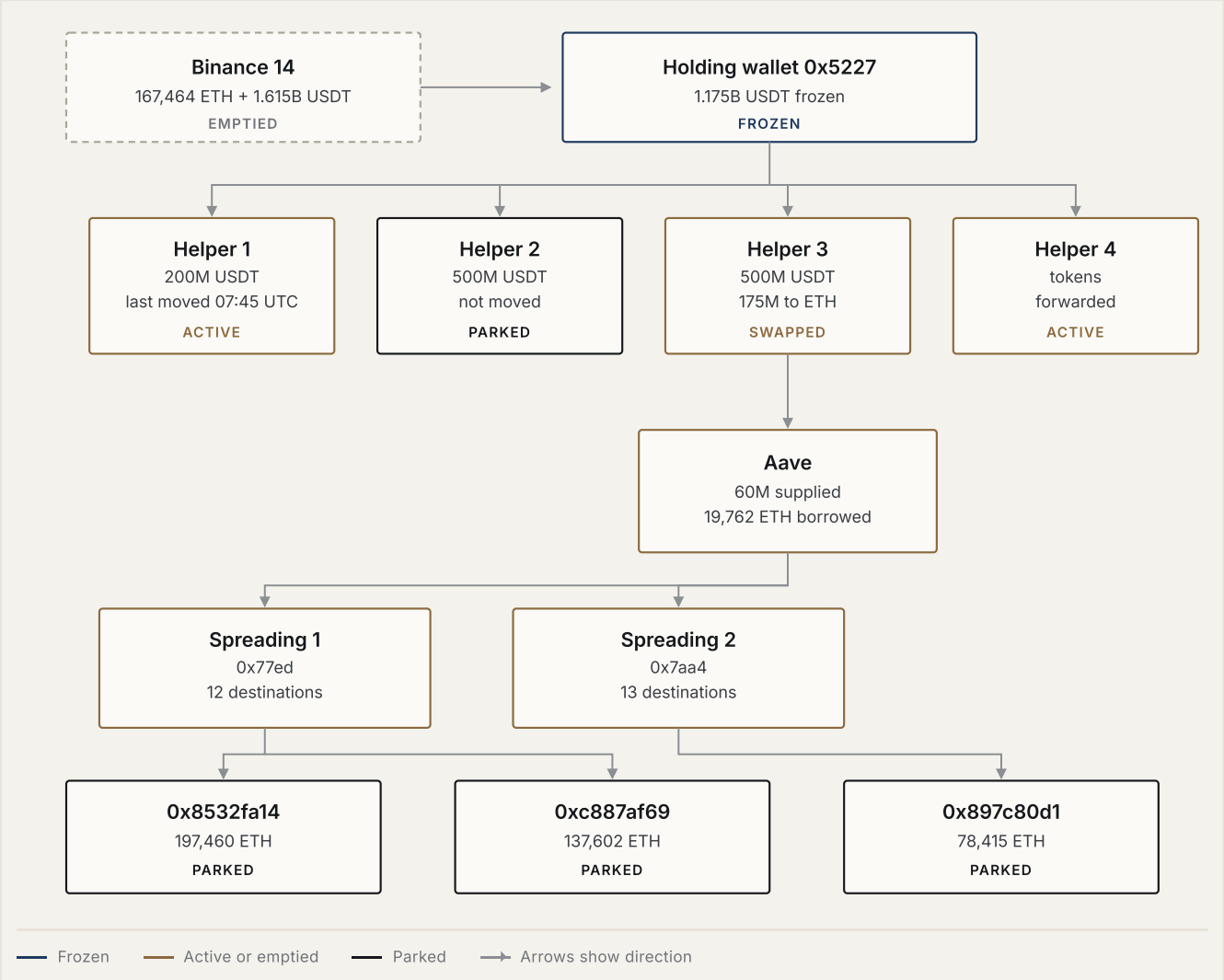
30 October 2026

UTC

00:10	**Attacker access revoked**, sweeper could no longer move funds.
00:18	Arbitrum forced 8,426 ETH and 74.6M ARB out of the attacker wallet (emergency call at 00:08).
Ongoing	Money moved through Aave and decentralised exchanges; Bitcoin split into 19 wallets, none moved.

The money flow / Ethereum

Traced on-chain from the emptied hot wallet to the wallets still holding the ETH.
Boxes are labelled by role and status.



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

167,464 ETH	1.175B USDT	100M USDT	413,477 ETH
TAKEN FROM BINANCE 14	FROZEN IN THE HOLDING WALLET	SWAPPED ON UNISWAP	PARKED IN THREE WALLETS

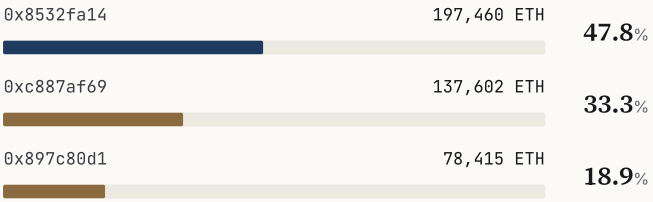
Where the money is now

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

CHAIN	STATUS	AMOUNT	STATE
Ethereum	Parked in three wallets	413,477 ETH	● PARKED
Bitcoin	Split into 19 wallets, none moved	18,270 BTC	● PARKED
XRP	Taken from five wallets, no outgoing seen	233.46M XRP	● PARKED
Solana	Parked, no outgoing seen	970,554 SOL	● PARKED
Tron	Received 612.7M, 312.7M retained	312.7M USDT	● PARTLY HELD
Arbitrum	Forced out by the Security Council	8,426 ETH	● RECOVERED
Avalanche	Received 1.81M, 444.5K moved later	1.37M AVAX	● PARTLY HELD
Polygon	Collected	46.6M POL	● MOVED
Optimism and Base	Hot wallet emptied	Small	● EMPTIED

Where the 413,477 ETH sits

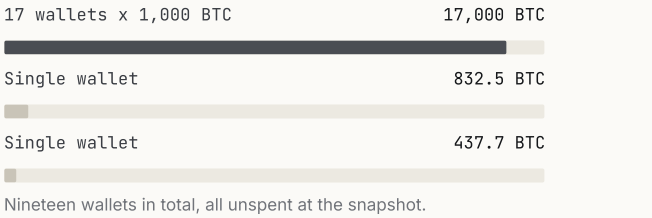
share of parked ETH



The chart shows where the ETH sits, not what it is worth.

How the 18,270 BTC is split

none moved



Nineteen wallets in total, all unspent at the snapshot.

Recovery position of $6.36B

share of value taken



CONTAINMENT ACTIONS

21:01 Tether freezes 971.1M USDT

21:04 Circle freezes 823M USDC

22:10 World Liberty freezes 27.8M USD1

23:35 Binance reports $2.54B frozen

00:18 Arbitrum recovers 8,426 ETH

Key addresses

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

14 of 47 in this case

CHAIN	ROLE	FULL ADDRESS	STATE
ETHEREUM	**Operator** funded through Tornado Cash, origin	0x7C8601d4645b93cea45F71e118A729332e6B5CA0	ORIGIN
ETHEREUM	**Sweeper** deployed 15:59 UTC	0x63e842B054Bd624a465454D533C33F573e9c6fAe	CONTRACT
ETHEREUM	**Holding wallet** 1.175B USDT frozen	0x5227f603C1eE34CE3C06eFe6477003BDfCCB2f8c	FROZEN
ETHEREUM	**Binance 14** the hot wallet that was emptied	0x28C6c06298d514Db089934071355E5743bf21d60	EMPTIED
ETHEREUM	**Helper 1** 200M USDT last moved 07:45 UTC	0x0ddf0480016e6bcb2c1f5d190d221fba1320697e	ACTIVE
ETHEREUM	**Helper 2** 500M USDT not moved	0x9749110a86941480dbefca1efdc0ceb528a0c762	PARKED
ETHEREUM	**Helper 3** 500M USDT, 175M to ETH	0x9749292d74fd460982d0912ea9515ea24736c762	SWAPPED
ETHEREUM	**Spreading 1** sent to 12 destinations	0x77edef23fbd05921c26fe29fcc3a65e14d2ac3eb	ACTIVE
ETHEREUM	**Spreading 2** sent to 13 destinations	0x7aa4d3029e4c6a8e916300014ad95b6d6c03bfd1	ACTIVE
ETHEREUM	**ETH storage** 197,460 ETH parked	0x8532fa14acaf483729c449b8458aeddb900543d4	PARKED
ETHEREUM	**Safe MEXC 27** 153M USDT, MEXC-labelled	0xf016e1d45ef23bdd414e7a2e4d46e1b34577b508	ATTRIBUTED
BITCOIN	**BTC source** Binance Bitcoin wallet	bc1qm34lsc65zpw79lxes69zkqmk6ee3ewf0j77s3h	SOURCE
BITCOIN	**BTC receiver** all 18,270 BTC arrived here	bc1q0mtc2f5agpkvlq6hhahmfr3hlr55kyfjhl2mnm	PARKED
SOLANA	**SOL receiver** 970,554 SOL parked	AffzFDKZbyMiU11zmVBoAqD25ugpr7xoWWyRyGigBEaU	PARKED

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

What the evidence shows

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

01 **The signing system was compromised, not one private key.**

EVIDENCE Ten chains produced valid signatures in one short window.

02 **The access lasted only a short time.**

EVIDENCE Fifty signing requests were sent in one batch.

03 **The attacker wallets were new and made for this attack.**

EVIDENCE They were funded through Tornado Cash before the sweep.

04 **Most of the money stayed on-chain.**

EVIDENCE No funds from the spreading wallets ended at an exchange deposit. One 50M USDT leg reached a wallet labelled MEXC 27.

ATTRIBUTION

TraderTraitor / North Korea

External assessment, not proven on-chain. Consistent with the signing pattern, the Tornado Cash funding and how the money was moved.

DPRK

101	112	8
CLAIMS LOGGED, 82 VERIFIED	ADDRESS RECORDS, 95 DISTINCT, 47 IN THIS CASE	CHAINS READ DIRECTLY

WHAT IS PROVEN, WHAT IS ASSESSED

Signing system compromise	PROVEN ON-CHAIN
50 signing requests in one batch	PROVEN ON-CHAIN
Attacker wallets were new	PROVEN ON-CHAIN
No exchange deposit from the spreading wallets	PROVEN ON-CHAIN
TraderTraitor attribution	EXTERNAL ASSESSMENT

Last on-chain verification: 30 October 2026, 13:06 UTC. The ETH storage wallet was re-checked at that time and held 197,460 ETH, unchanged.

Full report. The complete investigation, including methods and every traced wallet, is available first to students of the CCI and CCA batch. A detailed report will be released to the public later.

Live case. This is a snapshot of a live investigation based on public blockchain data as of 30 October 2026. Details may change as new activity appears. For information only. This is not legal, financial or investment advice and creates no liability for the author. Please check every address and figure yourself. Corrections: contact withkeshav.com.