



ALDERLUX

THE INSIDER · INVESTIGATIVE · #0024

What the Binance Theft Actually Teaches

30 OCTOBER 2026

Roughly \$6.36 billion left Binance's wallets on the evening of 29 October. The interesting part is not the size of it. It is that nobody appears to have stolen a key — and what that says about the difference between protecting a key and controlling the system allowed to use it.

On the evening of 29 October 2026, approximately **\$6.36 billion** in digital assets left wallets controlled by Binance. Most of the initial movement happened within about twenty minutes; outflows continued for nearly four hours overall. It is the largest reported theft in the industry's history — more than four times the \$1.5 billion taken from Bybit in February 2025.

Around \$2.7 billion has since been frozen or restricted. Most of that was stablecoins frozen by their own issuers — Tether, Circle, Ripple and World Liberty Financial can all blacklist addresses holding their tokens. Arbitrum's Security Council separately froze ETH and ARB on its own network.

The distinction matters. A substantial amount remains under the attacker's control, although the composition has shifted as assets were swapped and freezes landed. Much of what is left is Bitcoin and native Ether, which have no central issuer with the power to freeze anything.

The part worth understanding is that nobody appears to have stolen a key.

Every wallet is controlled by a private key, and the usual assumption after a theft on this scale is that someone obtained one. Binance's account points elsewhere. On the night of the theft it said its initial investigation suggested the incident "may have involved a compromised laptop" — chief executive Richard Teng later specified a DevOps engineer's — which gave an attacker a route into internal infrastructure from which withdrawal transactions could be submitted. It said it had found no evidence that a wallet private key leaked.

The following day Binance went further, saying its "subsequent investigation has uncovered additional points of breach" and describing a complex attack. Teng added that the attacker "did not simply use one engineer's permissions, and this was not a single 'one-click' action."

So the laptop was a starting point rather than the whole story, and the account is still moving. Binance's wording throughout is hedged — "suggested", "may have involved" — and finding no evidence of a leaked key is not the same as proving nobody reached one. The full technical post-mortem has not been published. But the evidence on the blockchain points the same way, for a reason worth following.

What the system was asked to sign

In May 2025 Ethereum introduced a feature called EIP-7702. It lets an ordinary wallet delegate its execution to a smart contract. Once authorised, that contract's code operates through the wallet — and keeps operating until the delegation is replaced or revoked. It does not lapse on its own.

The authorisation that grants this is a strange object. It names the network, the contract being authorised, and a counter value, and that is all. It carries no recipient, no amount and no payment instruction, because it is not a payment.

Think of the difference between signing a cheque and signing a power of attorney. A bank's fraud system is built to examine cheques: who is it payable to, how much, does that look right? Hand that same system a power of attorney and those questions have no answers — there is no payee and no sum.

The information is not absent. The document names the party being appointed, and a system that understood what it was looking at could ask whether that party should be trusted. But checks built to read cheques do not ask that question, because cheques never raise it. That is the gap the attacker used.

There is a further problem beneath that one. A signing service is often handed only a fixed-length fingerprint of the thing it is being asked to approve, rather than the thing itself. Given a fingerprint, it cannot tell an authorisation of this kind from an ordinary payment, because at that point the two are indistinguishable. Whether that was the arrangement at Binance has not been established, but it is one architectural weakness this attack illustrates: the difference between a system that fails to inspect a request properly and one that was never shown the request at all.

At 20:20:59 UTC, fifty such authorisations were recorded against Binance 14, the exchange's busiest Ethereum hot wallet, all naming the same attacker-controlled contract. At 20:24:23 — three minutes and twenty-four seconds later — that contract swept nearly all the wallet's assets in a single contract call: 167,464 ETH and 63 tokens, including roughly \$1.6 billion of Tether.

The delegation stayed attached for nearly four hours, and the attacker returned repeatedly to sweep deposits that arrived in the meantime. Binance revoked the delegation at 00:10:35.

Fifty signatures, and what they imply

An authorisation of this kind takes effect only at one precise moment. It is tied to a counter — a nonce — that increments each time the account sends a transaction, and it is valid only when that number matches exactly. Binance 14 is the busiest wallet the exchange runs, so any single authorisation risked being stale before it could be used.

The answer was fifty of them, covering fifty consecutive counter values. As Bitquery puts it, each authorisation works only when the wallet's transaction count hits one exact value, so fifty were signed, one for each count in a row, and one matched.

The researcher who first decoded the raw transaction, writing as 808bits, reconstructed which one. By the time the batch was submitted the wallet had already moved past thirty-three of the fifty; sixteen were spare, and the sixteenth in the list was the one that took effect.

That is the most informative detail in the incident. An attacker with direct, unrestricted use of the private key could have signed a single authorisation against the wallet's current nonce and submitted it immediately. Preparing fifty consecutive authorisations instead suggests someone who could request signatures but could not reliably control when they would come back.

TRM Labs arrives at the same conclusion from a different direction: it describes signatures obtained in advance and executed in a single burst, and notes that transfers across the other networks were signed inside the same window — which points to a compromise of Binance's signing infrastructure rather than the theft of a key.

It is strong evidence about how the attack was conducted. It is not proof about who had access to the key. The blockchain cannot settle that on its own, and Binance has not yet published the post-mortem that could.

The other networks

Bitcoin, the XRP Ledger and Solana have no equivalent of EIP-7702, and there the attacker did not need one. The same signing path simply approved ordinary transfers to addresses the wallets had never used before.

On Bitcoin, 18,270 BTC left in a single block. On the XRP Ledger, five Binance accounts sent approximately 233.5 million XRP to one new receiving account, beginning at around 20:04 — a quarter of an hour before the Ethereum delegation was even recorded. The Solana drain began at 20:10.

The method differed by network. The failure did not: a signing system approved transactions that its controls should have questioned.

Who did it

TRM Labs has attributed the attack to TraderTraitor, a North Korean hacking unit, with high confidence, drawing on both blockchain evidence and intelligence gathered off-chain. It links the same group to the 2025 Bybit theft and reports a matching preparation pattern.

That is TRM's assessment rather than an independently established fact. Binance has not publicly confirmed who was responsible.

What this means for anyone holding digital assets

The lesson usually drawn from these events — protect your keys — is incomplete here. Binance's preliminary findings suggest the keys were not stolen at all. What failed was the process around them: a system willing to approve a request it could not read, and safeguards built to inspect a kind of instruction the attacker never used.

For a private holder the useful question is therefore not *could someone steal my key? It is what is my signing process willing to approve without understanding it?*

That question applies in three places most people never examine:

- A **hardware wallet** is not automatically exposed to this failure. But a confirmation screen showing a contract address is not the same as explaining what that contract will do with the authority you are granting. Its protection depends on what the device can interpret, what it shows you, and whether you understand what you are approving.

- A **multi-signature arrangement** protects you only if the other signers examine what arrives. Several people approving the same unread request is one point of failure wearing a disguise.
- A **custodian** will describe its controls. Whether those controls have ever been tested against a request they were not designed to recognise is a different question, and one worth asking directly.

Custody risk is not only about where a key is stored. It is about who, or what, has the authority to use it, and how that authority is checked. For anyone relying on an institutional custodian, that distinction is the whole question: a guarantee that private keys are protected is not, by itself, evidence that the systems permitted to use them are.

Method and sources. This note draws on four published sources, which establish different things:

SOURCE	WHAT IT ESTABLISHES
808bits	The original decoding of the raw transaction: the twenty-nine byte signed message, the recovery of the signing authority behind all fifty authorisations, the nonce sequence, and which authorisation took effect. Ethereum only. Anonymous. Link
Bitquery	Independent transaction tracing: the delegation, the fifty authorisations and why fifty were needed, the timings and the asset movements
TRM Labs	The multi-chain investigation, the totals and freezes, and the attribution
Binance	Its own preliminary account of how the attacker got in

The 808bits analysis is published without a byline. Its reconstruction of which authorisation took effect is the only claim in this note resting on a single source, and it is attributed in the text rather than asserted. Readers should note that an expanded version of that article has circulated on social media containing material the original does not include, and at least one altered timestamp; nothing from that version is used here.

Figures are as reported on 30 October 2026 and may be revised: totals quoted by different analysts over the first twenty-four hours ranged from \$3.3 billion to \$6.36 billion as the scope became clear. The two principal investigations also differ on how many networks were affected — Bitquery counts nine, TRM ten — so no count is given here. Binance's technical post-mortem has not been published.

No figure in this note is an Alderlux calculation, and no claim rests on a source Alderlux could not verify.

Alderlux provides education and information only. We do not provide regulated financial advice, investment recommendations, legal or tax advice. Alderlux is not authorised by the Financial Conduct Authority.