RESEARCH PAPER · INCIDENT JOURNAL · PROCESS-FLOW CASE STUDY

Anatomy of the Binance Hot-Wallet Breach of 29 October 2026

How roughly US$6.3 billion left the world's largest crypto exchange in twenty minutes, and where the chain could have been broken

Soksamrong VANN

Microsoft Certified Trainer · Cisco Networking Academy Instructor · Phnom Penh, Cambodia
ORCID iD: https://orcid.org/0009-0000-5693-6850 · chamrong@outlook.com

Preprint v1.0 · 30 October 2026 · Status: developing event, all figures preliminary

$6.36B	10	~20 min	$2.7B
moved out of Binance wallets (TRM)	blockchains hit within about 30 minutes	for most funds to leave, from 20:05 UTC	frozen by issuers and networks

ABSTRACT

On 29 October 2026 an attacker moved roughly US$6.3 billion out of wallets belonging to Binance, the world's largest crypto exchange, across ten blockchains. Most of it left within about 20 minutes, starting at 20:05 UTC. It is the largest crypto theft on record, about four times the US$1.5 billion Bybit theft of February 2025. Binance reports that its initial investigation points to a compromised laptop of a DevOps engineer, used to reach a service container and submit unauthorized withdrawals. The blockchain analytics firm TRM Labs concludes that the evidence points to a compromise of Binance's hot-wallet signing infrastructure and attributes the attack, with high confidence, to North Korea's TraderTraitor unit. Stablecoin issuers and one network froze about US$2.7 billion within hours, yet the attacker still controls about US$2.4 billion in assets that no issuer can freeze.

This paper reconstructs the incident as a seven-stage process flow, builds a minute-level incident journal, traces the movement and conversion of funds, and maps defensive controls to the stage each one would interrupt. All facts come from public secondary sources; inferences are labelled as hypotheses.

Keywords: Binance; exchange security; hot wallet; signing infrastructure; EIP-7702; TraderTraitor; stablecoin freeze; crypto incident response; case study

Reading guide. Section 5 holds the main process-flow case study (Figures 1 and 3). Section 4 holds the incident journal and timeline (Figure 2). Sections 6 to 9 cover funds flow, response, control analysis and recommendations (Figures 4 to 6). Facts are cited to the sources in the References; statements marked *hypothesis* are the author's inference.

1 Introduction

Centralized exchanges hold customer assets in two broad layers. **Cold storage** keeps keys offline: slow but hard to attack. **Hot wallets** stay online so that withdrawals can be processed automatically and within seconds. The hot layer is where attackers concentrate, because it has to be able to sign transactions without a person in the loop. Whoever can make that signing system approve a transaction can move the funds, whether or not any private key is ever copied.

The Binance incident of 29 October 2026 deserves close study for three reasons. First, its scale: about US$6.3 billion, the largest crypto theft on record. Second, its breadth: wallets on ten blockchains with different key types and signing schemes produced valid signatures for the attacker within about half an hour, which points to a weakness in shared infrastructure rather than in any single chain. Third, the speed and the limits of the response: stablecoin issuers froze large balances within an hour, yet the assets that cannot be frozen, ETH and BTC, remained in the attacker's hands.

Research questions.

- **RQ1.** What sequence of stages did the attacker follow, and what does public evidence show about each?
- **RQ2.** How did the funds move and how much was recovered or frozen in the first hours?
- **RQ3.** At which stages could the chain have been broken, and by which controls?

2 Method, sources and limitations

This is a secondary-source case study of a developing event. The backbone is the on-chain reconstruction published by TRM Labs on 29 October 2026, which traces transfers across ten chains. It is supplemented by reports of Binance's own announcements, summarized in news coverage, and by Al Jazeera, Engadget, Insurance Journal, InvestingLive and VPNLab. No non-public information is used.

Source type	Used for	Reliability note
TRM Labs on-chain analysis	Timeline, amounts, mechanism, attribution, freezes	Primary on-chain evidence; attribution is an assessment (high confidence)
Binance statements (as reported)	Entry point, user impact, remediation promises	Preliminary; no root-cause post-mortem yet
News and analyst coverage	Market reaction, totals, corroboration	Figures differ by outlet and pricing time
Author analysis	Stage model, control mapping, hypotheses	Inference, labelled as such

Limitations. The event is hours old and figures will change. Loss estimates differ (Binance about US$6.3B, TRM about US$6.36B at time of theft or US$6.23B at current prices, Chainalysis about US$5.9B). The attribution to North Korea has not been commented on by Binance. The author had no access to Binance's internal logs, so every statement about internal control failure is a hypothesis.

3 Background

3.1 Hot wallets and the signing layer

A hot wallet needs a signing service: software or hardware that holds, or can use, keys and applies a policy before approving a transaction. In a mature design the policy checks destination, amount, velocity and approvals. If an attacker can reach the service and make it sign, those checks are the last line of defence.

3.2 EIP-7702 in one paragraph

Introduced in Ethereum's Pectra upgrade in May 2025, EIP-7702 lets an ordinary wallet hand control of its behaviour to a smart contract by signing an authorization. From then on every call to the wallet runs that contract's code until the wallet signs a new authorization. It is a legitimate feature, but it means one validly signed authorization can silently change what a high-value wallet does. Every wallet also keeps a transaction counter (nonce), and an authorization is valid only at the nonce reached when it executes.

3.3 Precedents

Year	Incident	Approx. loss	Relevance
2019	Binance hot-wallet theft	7,000 BTC (about US$40M at the time)	Earlier hot-wallet compromise at the same exchange
2022	Binance BNB Chain bridge exploit	About US$570M	Bridge flaw, not exchange wallets
Feb 2025	Bybit theft	US$1.5B	FBI attributed to TraderTraitor; pre-staged signatures
Apr 2026	KelpDAO hack	Not stated in sources used	TRM links same behavioural pattern
Oct 2026	Binance breach (this paper)	About US$6.3B	Largest on record, about four times Bybit

TRM notes shared features between this attack and earlier North Korea-linked heists: small Tornado Cash withdrawals funding an operator wallet, staging that began well before the theft, and signatures obtained in advance then executed in one burst. The laundering route differs: large swaps through market makers and lending protocols rather than the bridge-heavy pattern seen after Bybit.

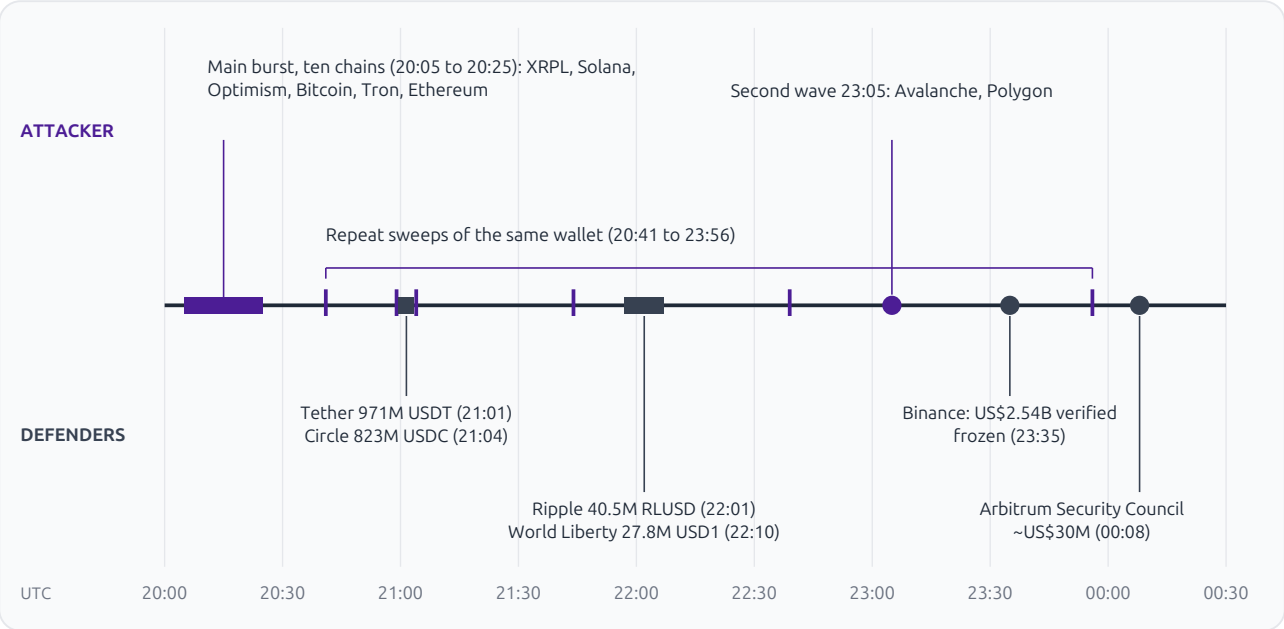
4 Incident journal

Times are UTC from TRM Labs and public statements; Cambodia time (ICT) is UTC+7, so the burst began at 03:05 on 30 October in Phnom Penh. Figure 2 shows the same events on one axis.

UTC	ICT	Event
28 Oct, morning	28 Oct	Operator wallet receives three small Tornado Cash withdrawals. Preparation begins at least 36 hours before the theft.
29 Oct, early	29 Oct	Attack code deployed and tested on two wallets; final version rehearsed on a third wallet, test funds sent back.
29 Oct, about 4 h after rehearsal	29 Oct	Same code installed on a Binance hot wallet.
20:05–20:09	03:05–03:09	Five Binance XRP Ledger wallets send 233.46M XRP to one attacker address, leaving minimum balances.
about 20:10	about 03:10	Binance wallets on Solana and Optimism follow.
20:20	03:20	Bitcoin hot wallet sends 18,270 BTC; attacker begins a peel chain. One Ethereum transaction submits 50 authorizations.
shortly after 20:20	about 03:22	Tron hot wallet sends 612.7M USDT and 46.4M TRX.
3 min 24 s after delegation	about 03:24	Ethereum hot wallet instructed to send its balance: 167,464 ETH and 63 tokens, incl. 1.615B USDT.
20:41, 20:59, 21:04, 21:44, 22:39, 23:56	03:41 onward	Further sweeps as new funds reach the still-delegated wallet.
21:01	04:01	Tether freezes 971.1M USDT in the main receiving wallet, 37 minutes after the main sweep.
21:04	04:04	Circle freezes 823M USDC, in coordination with law enforcement.

UTC	ICT	Event
22:01	05:01	Ripple freezes 40.5M RLUSD; also freezes RLUSD in the compromised wallet so new deposits cannot be swept.
22:10 and 22:26	05:10, 05:26	World Liberty Financial freezes 27.8M USD1, then USD1 in the compromised wallet.
23:05	06:05	Second wave: Binance wallets on Avalanche and Polygon.
23:35	06:35	Binance says verified frozen funds total US$2.54B.
30 Oct, 00:08	07:08	Arbitrum Security Council forces out 8,426 ETH and 74.6M ARB (about US$30M) from the attacker's wallet.
30 Oct		Binance estimates about US$6.3B impact, about US$3B frozen; will cover losses from SAFU and own funds; hopes to restore withdrawals in about 48 h. Bitcoin falls 4–5% below US$77,000.

Figure 2 **Attack and response on one time axis**

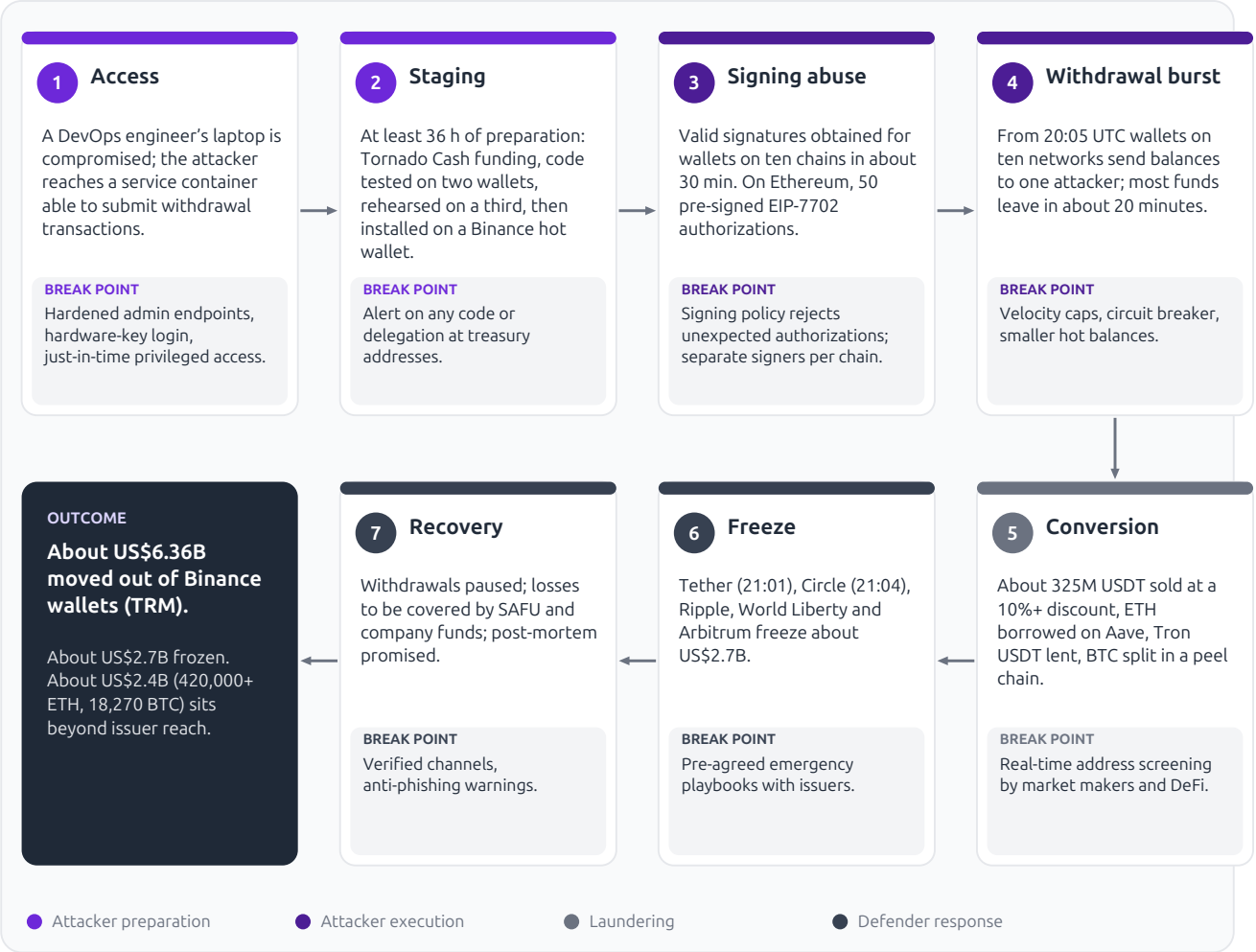


Deep purple marks attacker activity; dark gray marks defender actions. Source: TRM Labs on-chain reconstruction and Binance statements as reported. Times are UTC (Cambodia time is UTC+7). Events 3 to 9 minutes apart are drawn together.

5 Process-flow case study

The incident is modelled as seven stages. The stage boundaries are the author's; the facts inside each stage come from the sources. Figure 1 shows the whole chain with the point at which each stage could have been broken.

Figure 1 End-to-end process flow of the breach



Cards 1 to 4 are the attack; 5 is laundering; 6 and 7 are response. Break points are defensive controls proposed in this paper, not statements about what Binance had in place.

5.1 Stage-by-stage detail

Stage 1 · Access	
What happened	Binance reports that its initial investigation points to a compromised laptop of a DevOps engineer. From it the attacker reached a service container and used it to submit unauthorized withdrawal transactions. Binance found no evidence that wallet private keys leaked.
Evidence	Binance official update as reported by VPNLab and others. Preliminary; the root cause is promised in a post-mortem.
Indicators	Privileged sessions into production from a developer endpoint; unusual calls from a container to the withdrawal path.
Break points	Phishing-resistant authentication, hardware keys, dedicated admin workstations, just-in-time privileged access, no standing path from laptops to signing-adjacent services.

Stage 2 · Staging and testing	
What happened	From the morning of 28 October the operator wallet received three small Tornado Cash withdrawals. Early on 29 October the attack code was deployed and tested on two wallets; the final version was rehearsed on a third wallet and the test funds routed back. About four hours after that rehearsal the same code was installed on a Binance hot wallet.
Evidence	TRM on-chain analysis (strong).
Indicators	Mixer-funded wallet deploying contracts; code present at an exchange address that should have none.
Break points	Alert on any code or delegation at treasury addresses; ingest threat-intelligence blocklists of operator wallets; require a pre-approved method to revoke.

Stage 3 · Signing-layer abuse	
What happened	Wallets on different chains, key types and signing schemes all produced valid signatures for the attacker within about half an hour. On Ethereum, 50 pre-signed EIP-7702 authorizations covered consecutive nonces, so that one would be valid when the transaction executed (Figure 3). TRM concludes the most likely explanation is that the attacker could make Binance's hot-wallet signing system sign transactions of its choosing.
Evidence	TRM assessment based on cross-chain pattern. Early indicators suggested the Ethereum authorizations might have been phished; that does not explain the other nine chains.
Indicators	Requests for many authorizations across a range of nonces; signing across ten chains inside half an hour; destinations outside normal patterns.
Break points	Reject EIP-7702 authorizations unless expected; destination allow-lists; separate signing infrastructure and approval paths by chain and wallet tier; out-of-band approval above a threshold.

Stage 4 · Multi-chain withdrawal burst	
What happened	From 20:05 UTC wallets on ten networks sent their balances to addresses controlled by one attacker: XRPL (233.46M XRP), Solana and Optimism, Bitcoin (18,270 BTC at 20:20), Tron within two minutes, and one Ethereum transaction 3 min 24 s after delegation (167,464 ETH, 63 tokens). A second wave at 23:05 reached Avalanche and Polygon. Another Ethereum hot wallet sent 28,006 ETH, 55.7M USDT and 25.9M RLUSD through ordinary signed transfers.
Evidence	TRM on-chain tracing (strong).
Indicators	Balances falling to protocol minimums; outflow many times above daily baseline; all destinations tied to one controller.
Break points	Velocity and per-wallet caps, circuit breaker that halts signing on abnormal outflow, delayed release of very large withdrawals, lower hot-wallet balances.

Stage 5 · Conversion and laundering	
What happened	The attacker raced the freezes. About 325M USDT was sold to professional fillers through UniswapX and similar contracts for about 122,300 ETH, implying roughly US$2,650 per ETH when ETH traded near US$2,300 to 2,350, a discount above 10%. A second wallet supplied 60M USDT to Aave and borrowed about 19,760 ETH, after which Aave froze the affected markets. 300M USDT on Tron went into JustLend; 200M USDT moved through hop wallets to Uniswap (30M frozen); 48M of 88.5M RLUSD was sold before Ripple's freeze. The Bitcoin was split into 1,000 and 100 BTC pieces in a peel chain.
Evidence	TRM on-chain tracing (strong).
Indicators	Large sales by a wallet that received the funds minutes earlier; borrowing against freshly received stablecoin.
Break points	Real-time address screening by market makers and solvers; protocol-level market freezes; blocklists shared with exchanges and OTC desks.

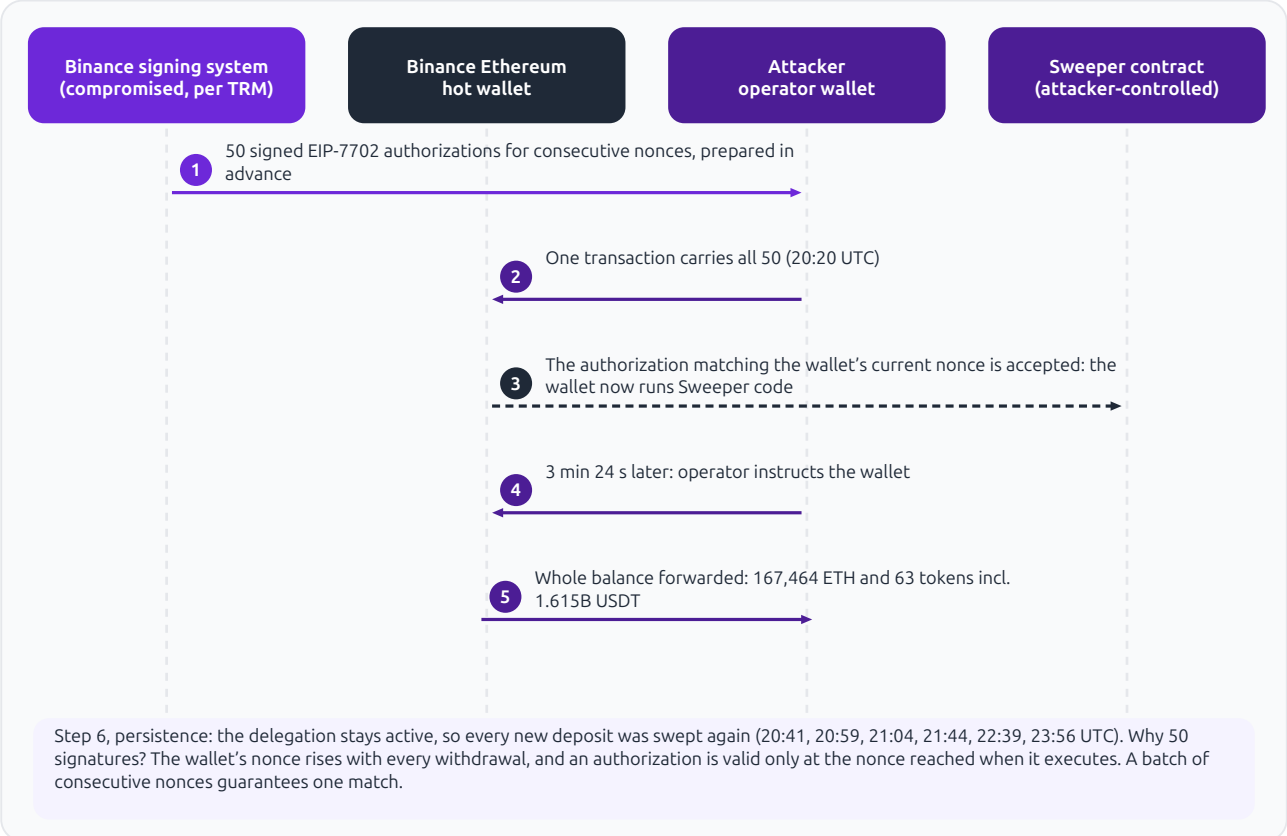
Stage 6 · Detection and freezing	
What happened	Tether froze 971.1M USDT at 21:01 and later more, for about US$1.77B in total; Circle froze about US$825M USDC from 21:04; Ripple 40.5M RLUSD; World Liberty Financial 27.8M USD1; Arbitrum's Security Council about US$30M. Binance reported US$2.54B verified frozen at 23:35; TRM counts about US$2.7B as of 00:30 UTC on 30 October.
Evidence	Multiple sources, consistent.
Break points	Pre-agreed emergency contacts and playbooks so that freezes start in minutes, not about an hour.

Stage 7 · Recovery and disclosure	
What happened	Binance paused deposits and withdrawals, said user funds are safe, said it will cover losses from its SAFU fund and its own resources, hoped to restore withdrawals in about 48 hours after rebuilding the withdrawal service, and promised a detailed post-mortem and updated reserves. The next regular proof-of-reserves snapshot is due on 1 November. Binance.US and Coinbase said they were not affected.
Evidence	Binance statements as reported; CoinDesk review of the 1 October proof of reserves, as summarized by VPNLab.
Break points	Verified-channel communication, rapid anti-phishing warnings, transparent reserve reporting.

5.2 The Ethereum mechanism

Figure 3 shows the Ethereum step as TRM describes it. The point for defenders is that a single validly signed authorization, once accepted, turned a well-known hot wallet into a contract only the attacker could command, and the arrangement stayed in place until replaced.

Figure 3 EIP-7702 delegation and sweep on the Ethereum hot wallet



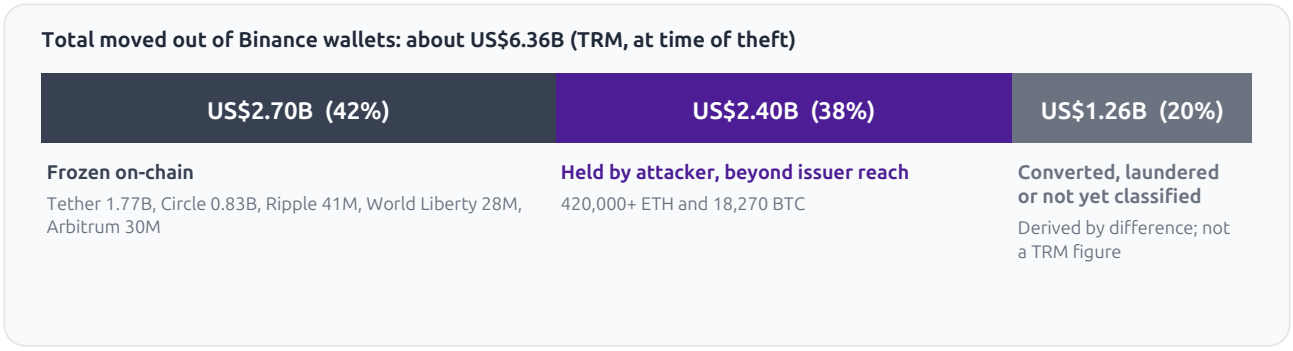
Based on TRM Labs' description. Whether the signing system itself was compromised is TRM's assessment; Binance has not yet published a root cause.

5.3 Why ten chains mattered

On Ethereum alone, phishing of authorizations was a plausible reading. But Binance wallets on the XRP Ledger, Arbitrum, Avalanche, Optimism, Base, Bitcoin, Tron and Solana also sent funds through standard signed transfers, and another Ethereum hot wallet did so without any delegation. Different chains, key types and signing schemes all yielded valid signatures inside half an hour. TRM therefore judges that the attacker gained the ability to make the signing system itself approve transactions. This is compatible with Binance's account of an engineer laptop reaching a service container. *Hypothesis:* the laptop was the entry point and the signing service the pivot. Only the post-mortem can confirm it.

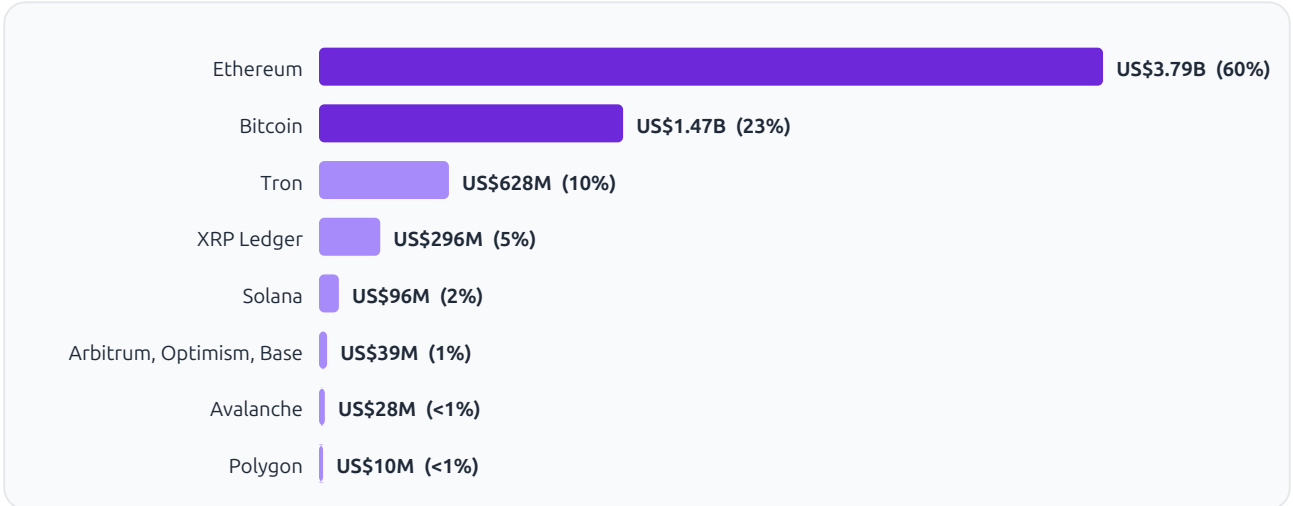
6 Funds flow and impact

Figure 4 Where the US$6.36B stood about five hours after the first outflow



Frozen and held figures are TRM's at 00:30 UTC on 30 October; the third segment is derived by subtraction and combines funds already converted, laundered or not yet classified. Segments may overlap in practice.

Figure 5 Approximate loss by chain



US$ at time of theft (TRM). Ethereum carries 3.79B including 200,630 ETH and 185 other tokens; shares add to about 100%.

Freezer	Asset and amount	Time (UTC)	Delay after main sweep (about 20:24)
Tether	About 1.77B USDT (971.1M first)	21:01 onward	about 37 min
Circle	About 825M USDC	21:04 onward	about 40 min
Ripple	40.5M RLUSD	22:01	about 1 h 37 min
World Liberty Financial	27.8M USD1	22:10	about 1 h 46 min
Arbitrum Security Council	8,426 ETH and 74.6M ARB (about US$30M)	00:08 (30 Oct)	about 3 h 44 min

Reserves and markets. A CoinDesk review of Binance's 1 October proof of reserves, as summarized by VPNLab, found that the drained wallets were among those backing customer balances; until losses are replaced, Binance's ETH backing is likely about 94% rather than 100%. Bitcoin fell 4 to 5% to below US$77,000 on the news. Totals differ by source because of pricing at different moments: TRM US$6.36B at theft or US$6.23B at current prices; Binance about US$6.3B; Chainalysis about US$5.9B.

7 Analysis of the response

7.1 What worked

- **Issuer speed.** Tether froze within about 37 minutes of the main sweep and Circle within about 40, in coordination with law enforcement.
- **Freezing inside the compromised wallet.** Ripple and World Liberty froze balances inside the compromised hot wallet, so new deposits could not be swept.
- **Network-level action.** Arbitrum's Security Council used emergency powers to force two transfers out of the attacker's wallet.
- **Protocol response.** Aave froze affected markets after the attacker borrowed ETH against USDT.

7.2 What did not

- **Freezing reaches only centrally issued assets.** About 42% of the loss was frozen (2.7 of 6.36, derived); ETH and BTC cannot be frozen.
- **Market liquidity helped the attacker.** Market makers and solvers bought about 325M USDT minutes after it was stolen, at a steep discount the attacker accepted.
- **Detection lag.** About 36 hours of on-chain staging preceded the theft, and the first public freeze came about 56 minutes after the first outflow.

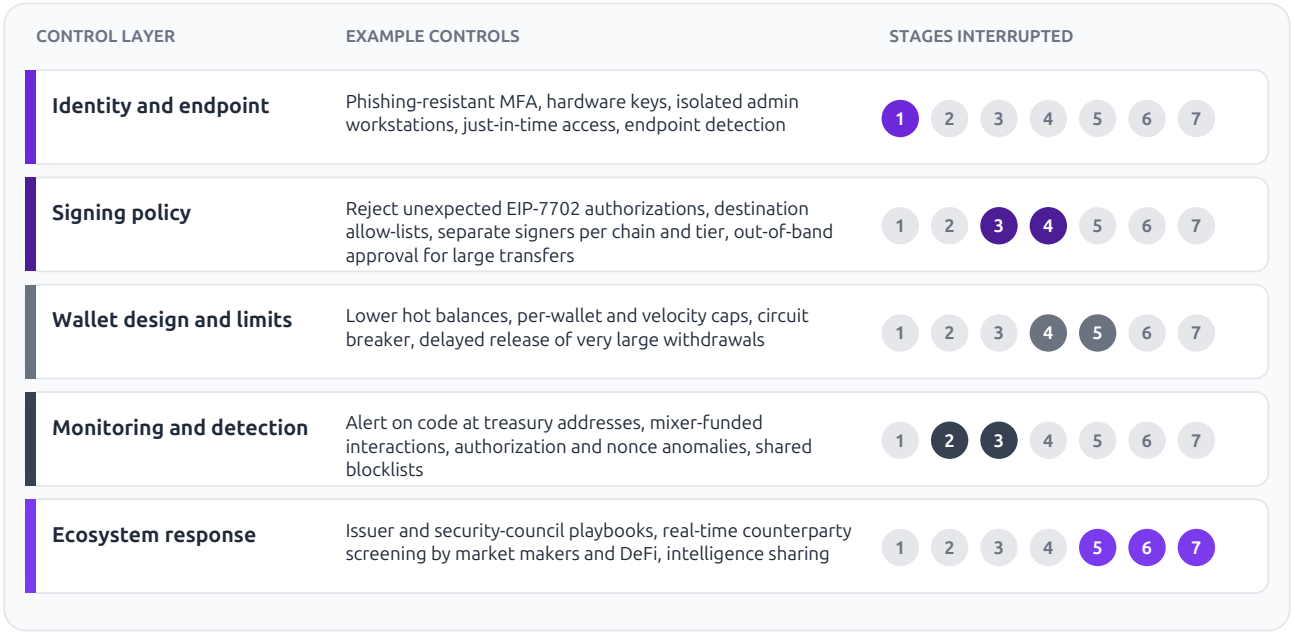
7.3 Hypotheses on control gaps

Hypothesis (pending post-mortem)	Observation that fits it	What would confirm or refute it
H1. One access path reached signing capability across many chains	Valid signatures on ten chains within about 30 min	Binance architecture report: how many signers share one trust boundary
H2. Signing policy did not flag a batch of 50 authorizations	A batch across consecutive nonces was accepted	Policy logs showing whether the requests were evaluated or bypassed
H3. Outflow limits were absent or too high for hot balances	Balances were drained to minimums within minutes	Configured per-wallet caps and circuit-breaker settings
H4. Pre-theft staging was not monitored	36 hours of staging, including code on a Binance address	Whether alerts fired on code or delegation at that address

8 Control map and recommendations

Figure 6 groups defences into five layers and shows which of the seven stages each layer would interrupt. The strongest designs overlap: a failure in one layer is caught by another.

Figure 6 **Defensive control layers mapped to attack stages**



Numbers 1 to 7 refer to the stages in Figure 1. Proposed by the author; not a statement about Binance's actual controls.

Actor	Recommendation	Priority
Exchanges and custodians	Separate signing infrastructure and approval paths by chain and wallet tier so one compromise cannot sign everywhere.	Critical
Exchanges and custodians	Alert on any EIP-7702 delegation at treasury wallets, reject authorizations unless expected, treat a batch across a range of nonces as an indicator of compromise, and keep a tested pre-approved method to sign a revocation.	Critical
Exchanges and custodians	Enforce velocity limits, per-wallet caps and an automatic circuit breaker; keep hot-wallet balances as low as operations allow.	High
Exchanges and custodians	Treat DevOps and admin workstations as top-tier assets: hardware-key authentication, isolation, strict least privilege.	High
Exchanges and issuers	Maintain pre-agreed emergency contacts and playbooks with stablecoin issuers and chain security councils, and rehearse them.	High
Market makers, solvers, DeFi	Screen counterparties in real time before filling large orders; honour shared blocklists.	High
Users	Follow only binance.com and Binance's verified accounts; ignore messages offering compensation, refunds or wallet verification (no real refund needs your password, 2FA code or seed phrase); do not install recovery tools; enable 2FA and the withdrawal-address whitelist; remember funds on any exchange carry that exchange's risk.	Immediate
Regulators and researchers	Require post-incident root-cause reports and publish comparable reserve snapshots so users can see the effect on backing.	Medium

9 Open questions

- What is Binance's confirmed root cause, and how did the attacker obtain signing capability on ten chains?
- Was the access time-limited, and why were 50 pre-signed authorizations needed?
- How much of the remaining US$2.4 billion will be traced or recovered, and by what route will it be laundered?
- What will the 1 November proof-of-reserves snapshot show, and how quickly will withdrawals be restored?
- Will regulators and law enforcement publish formal attribution?

10 Conclusion

The Binance breach shows that the weakest layer of a large exchange is often not the blockchain but the operational system that decides what gets signed. The attack followed a now-familiar pattern: long, quiet preparation; a short burst of withdrawals across many chains; and rapid conversion into assets that cannot be frozen. Issuer freezes saved about 42% of the loss, a strong result for a response measured in minutes, but not enough. The durable defences are architectural: separated signers, strict signing policy, outflow limits and well-rehearsed coordination. This paper will be updated when Binance publishes its post-mortem and when TRM and other analysts revise their figures.

A Glossary

Term	Meaning in this paper
Hot wallet	An online wallet used by an exchange to process customer withdrawals automatically.
Signing infrastructure	The systems that hold or use keys and apply policy before a transaction is signed.
EIP-7702	Ethereum feature (Pectra, May 2025) letting a wallet delegate its behaviour to a smart contract via a signed authorization.
Nonce	A wallet's running transaction count; an authorization is valid only at the nonce reached when it executes.
Sweeper contract	A contract that forwards a wallet's whole balance to a chosen address on command.
Peel chain	Repeatedly splitting a large balance into smaller outputs to make tracing harder.
Tornado Cash	A mixing service that obscures where crypto comes from.
SAFU	Binance's emergency fund, which it says will help cover the losses.
Proof of reserves	A published snapshot showing wallets that back customer balances.
TraderTraitor	North Korea-linked hacking unit named by the FBI for the Bybit theft and by TRM for this attack.
Stablecoin freeze	An issuer disabling transfers of its token from specified addresses.

B References

1. TRM Labs (2026, 29 October). North Korea Steals USD 6.36 Billion From Binance in the Largest Hack in History. https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history
2. VPNLab.io editorial team (2026, 30 October). Binance loses $6.3 billion in the largest crypto theft on record (summarizes Binance's official update, TRM, Chainalysis and CoinDesk). https://vpnlab.io/en/binance-6-3-billion-hack-largest-crypto-theft-2026-3127
3. Al Jazeera (2026, 30 October). Binance says $2.54bn in crypto funds frozen amid potential security issue. https://www.aljazeera.com/economy/2026/10/30/binance-says-2-54bn-in-crypto-funds-frozen-amid-potential-security-issue
4. Engadget (2026, 30 October). Binance hacked for an estimated $6.3 billion in record crypto theft. https://www.engadget.com/2301941/binance-hacked-for-estimated-6-3-billion-in-record-crypto-theft/
5. Insurance Journal (2026, 30 October). Binance Estimates $6.3 Billion Hacked in Crypto's Biggest-Ever Heist. https://www.insurancejournal.com/news/international/2026/10/30/890894.htm
6. InvestingLive (2026, 29 October). Binance appears hacked, CZ says, as Tether and Circle freeze $1.79B in stablecoins. https://investinglive.com/cryptocurrency/binance-appears-hacked-cz-says-as-tether-and-circle-freeze-1-79b-in-stablecoins/

Suggested citation. Vann, Soksamrong (2026). Anatomy of the Binance hot-wallet breach of 29 October 2026: a process-flow case study (Preprint v1.0). ORCID: 0009-0000-5693-6850. **Data availability.** All data come from the public sources listed above; no private or leaked material was used. **Disclaimer.** Educational case study of a developing event, not investment, legal or security advice; verify current facts against Binance's official announcements.