德尔泰
DELTA & CAPITAL

Binance Hot-Wallet Theft

An On-Chain Tracing Research Report

US$6.3 billion and 37 minutes: the attack path, the race to freeze funds, asset movements and subsequent risks

Report ID	DC-RS-20261030-BN
Incident	30 October 2026, from 04:05 Beijing time
Data cutoff	30 October 2026, 20:00 Beijing time (UTC+8)
Coverage	Ethereum, TRON and Arbitrum checked on-chain; Bitcoin, XRP and other chains draw on third-party statistics
Publisher	Delta & Capital
Edition	Complete English translation of the Chinese report

Based on public on-chain records and public information. Figures reflect the stated cutoff; funds may have moved subsequently. This report is not investment advice.

Contents

Executive summary

1. Incident overview: multiple hot wallets compromised within 25 minutes

2. Attack path: from a laptop to EIP-7702 delegation

3. The 37-minute window: three steps before the freezes took effect

4. Arbitrum intervention: chain-level powers move US$30.5 million

5. Fund status: where US$1.34 billion stood at the 20:00 cutoff

6. External responses, attribution and market impact

7. Beyond the announcements: address poisoning, messages and token sell-offs

8. Delta observations

Appendix: key addresses and transactions

Disclosures

Sources

About us

Executive summary

In the early hours of 30 October, Binance hot wallets on XRP Ledger, Ethereum, TRON, Arbitrum, Bitcoin and other chains were drained in succession. Binance estimated the total impact at approximately US$6.3 billion, more than four times the US$1.46 billion Bybit incident in February 2025, setting a new record for a single crypto theft. Its preliminary investigation pointed to a compromised DevOps engineer's laptop, through which the attacker accessed a service container and submitted unauthorized withdrawals.

There were 37 minutes between the hot-wallet compromise and Tether freezing the first attacker address. Subsequent freezes pursued the funds through successive addresses, with the narrowest gap just 36 seconds. Approximately US$3 billion was frozen in total, and the Arbitrum Security Council used chain-level powers to move approximately US$30.5 million from an attacker address. At the 20:00 cutoff, however, the attacker still controlled approximately 505,600 ETH and 631 million TRX, together worth around US$1.34 billion. Neither asset has an issuer capable of freezing it.

US$6.3 billion — estimated total impact reported by Binance	About US$3 billion — total frozen by the parties involved	37 minutes — theft to the first freeze	US$1.34 billion — still controlled by the attacker

Key findings

• Preparations began about 18 hours before the attack. The triggering address 0x7C86…5CA0 was funded from Tornado Cash and deployed its first contract at 10:28 on 29 October, followed by four test calls between 21:51 and 22:24 that evening.

• Only one of 50 pre-signed authorizations took effect. The EIP-7702 transaction at 04:20:59 contained 50 authorizations signed by Binance 14 with consecutive nonces. Only the authorization matching the account nonce took effect. Binance revoked the delegation through Binance 14 itself at 08:10:35.

• 729 million USDT was converted within 37 minutes. Before the freezes, the attacker sold assets at a discount, borrowed 19,762 ETH against collateral on Aave and relayed funds down successive addresses. Several addresses made their final outgoing transfer only 36 to 84 seconds before being frozen.

• Arbitrum used its exceptional chain-level powers. At 08:18:20, a type-0x65 transaction requiring no attacker signature moved 74,559,805 ARB to the Security Council's frozen-funds address.

• Ethereum funds concentrated in six holding addresses. At 20:00, the three largest held a combined 413,477 ETH with no outgoing transfers since receipt. During the afternoon, remaining tokens continued to be sold for ETH and consolidated; 17,260 ETH moved to new address [6].

• TRON funds began moving extensively at 18:15. TSpe5 moved its entire 638 million TRX balance in five transfers between 18:15 and 18:20. Of this, 120 million passed through an intermediary to splitting address TRBd. Since 10:19, TRBd had sent 53.73 million TRX in 145 transfers. Some was swapped for USDT on SunSwap, bridged back to Ethereum through USDT0 and converted to ETH.

1. Incident overview: multiple hot wallets compromised within 25 minutes

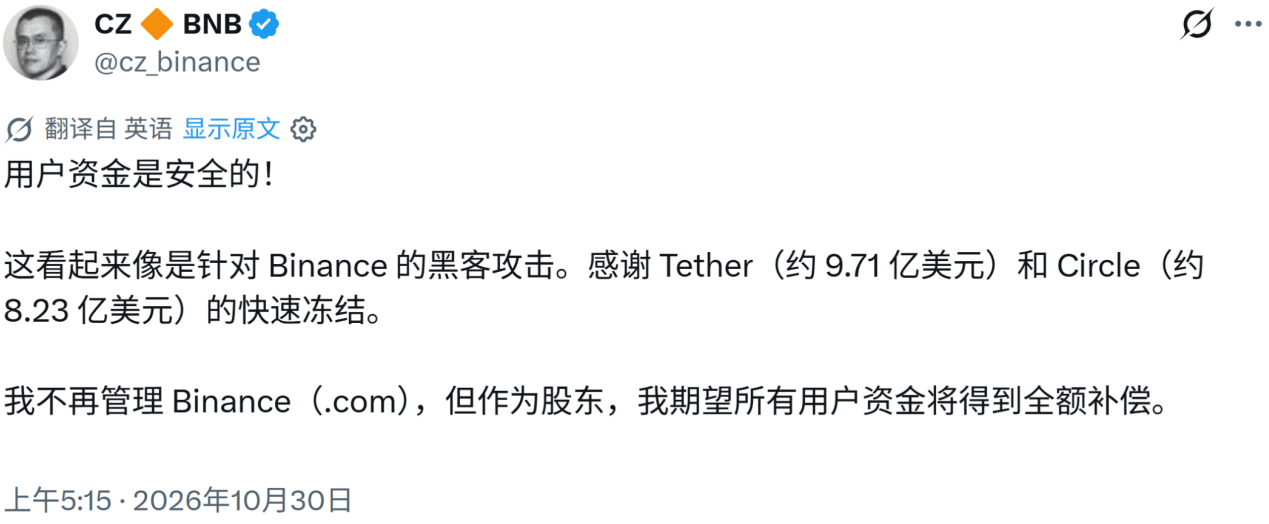


Figure 1. At 05:15, CZ confirmed the Binance hack and thanked Tether and Circle for their rapid freezes. Source: X, @cz_binance.

1.1 What happened

According to TRM Labs and Arkham, the first outflow was approximately US$300 million in XRP on XRP Ledger, between 04:05 and 04:09 on 30 October. All times below are Beijing time. At 04:20:00, Binance's TRON hot wallet sent 10,000 TRX, worth about US$3,500, to a newly created address. Seventy-two seconds later, it sent another 46.38 million TRX to the same address; another 93 seconds later, 613 million USDT followed. The initial 10,000 TRX was a test transfer to confirm the attacker had obtained authority to move funds from the wallet.

At almost the same time, Binance 14 on Ethereum was placed under the control of an attack contract. At 04:24:23, one transaction moved 1.615 billion USDT, 167,000 ETH and more than 60 other tokens to a new address. Twenty-four seconds later, Binance 16 lost 28,005.6 ETH and 55.74 million USDT. At 04:30:34, a suspected Binance hot wallet on Arbitrum transferred 74.56 million ARB. From 04:41, two transfers drained 823 million USDC from a Binance USDC hot wallet. Arkham counted approximately US$6 billion moved through 141 transfers on nine chains excluding XRP; US$4.9 billion arrived within the first 14 minutes, and the largest single transaction was about US$2.53 billion.

At 04:32, on-chain analyst Spreek posted the first alert on X. Binance founder Changpeng Zhao (CZ) confirmed the hack at 05:15. Binance issued an official statement at 05:29 and subsequently suspended withdrawals. At 10:25, it announced preliminary findings: an estimated US$6.3 billion total impact, around US$3 billion frozen, and losses to be covered by the SAFU fund and company funds.

Figure 2. At 04:32, Spreek first warned of a suspected large-scale Binance attack: entire wallet balances were being moved to new addresses, and the triggering transaction was funded from Tornado Cash. Source: X, @spreekaway.

1.2 Loss and freeze measurement bases

The organizations used different observation times, chain coverage and valuation times. Their figures cannot simply be added or subtracted. Subtracting US$3 billion from US$6.3 billion produces US$3.3 billion, but this is only the difference between two approximate figures. It is neither Binance's final net loss nor the attacker's current holdings.

Table 1. Reported losses and frozen amounts

Source	Figure	Measurement basis
Binance official statement, 10:25	Estimated impact of about US$6.3 billion; about US$3 billion frozen	Official estimates; SAFU and company funds to cover losses
TRM Labs	US$6.36 billion at transfer-time exchange rates; later valued at US$6.23 billion	Ten chains; high-confidence attribution to North Korea's TraderTraitor
Arkham	US$6.3 billion: about US$300 million in XRP plus about US$6 billion through 141 transfers on nine chains	Transfers between 04:10 and 07:05; US$4.9 billion arrived in the first 14 minutes

Source	Figure	Measurement basis
Chainalysis, via Reuters	At least US$5.912 billion	As of 08:30
Watcher.Guru, 05:42	More than US$5.6 billion	Early third-party estimate, including US$1.45 billion in BTC
Delta on-chain checks, 11:00	1.759 billion USDT and 823 million USDC frozen on Ethereum and TRON	Tether and Circle contract blacklist events and on-chain balances

Sources: Binance statements, TRM Labs, Arkham, Chainalysis via Reuters, Watcher.Guru, and Delta on-chain checks.

Figure 3. At 05:42, Watcher.Guru estimated Binance's stolen assets at more than US$5.6 billion. Different organizations used different scopes and observation times. Source: X, @WatcherGuru.

1.3 Incident timeline

Table 2. Key events, Beijing time, through 20:00

Time	Event
10-29 10:28	Trigger address 0x7C86…5CA0 deployed its first contract; four tests followed between 21:51 and 22:24
04:05–04:09	Approximately US$300 million in XRP moved first on XRP Ledger, according to TRM and Arkham
04:20:00	TRON hot wallet sent a 10,000 TRX test transfer

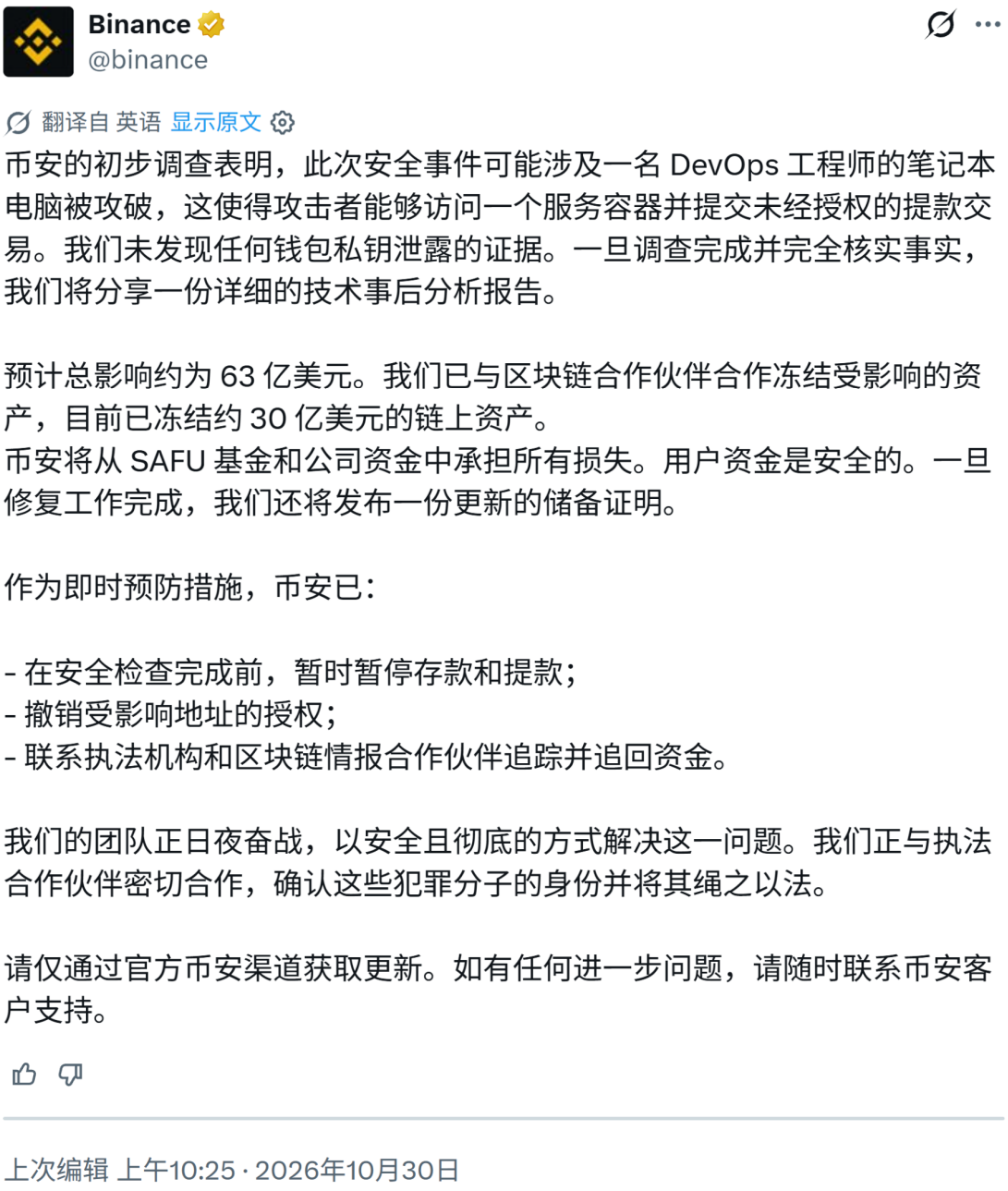
Time	Event
04:20:59	Binance 14 EIP-7702 transaction containing 50 authorizations confirmed
04:22:45	TRON hot wallet sent 613 million USDT
04:24:23	Binance 14 lost 1.615 billion USDT, 167,000 ETH and more than 60 other tokens in one transaction
04:30:34	74.56 million ARB moved to the attacker’s main address
04:34–04:49	325 million USDT sold at a discount for 122,316 ETH
04:38:47	195,460 ETH moved in one transfer to holding address [1]
04:57–05:00	60 million USDT supplied to Aave as collateral; 19,762 ETH borrowed
05:01:35	Tether froze the main address; seven more downstream Ethereum addresses were frozen over the next 17 minutes
05:04:59	Circle froze 823 million USDC at the main address
05:09–05:21	Tether froze three TRON addresses
06:06:23	Tether blacklisted Binance 14 itself
08:10:35	Binance 14 revoked its EIP-7702 delegation through its own transaction
08:18:20	Arbitrum Security Council moved 74,559,805 ARB through a type-0x65 transaction
10:19	TRON address TRBd began splitting TRX
10:25	Binance preliminary investigation identified a compromised DevOps laptop and estimated US$6.3 billion total impact
13:15	Main address sent 17,260 ETH to new holding address [6]
14:02	Binance said the employee device was only the starting point of a more complex attack; no private-key leak had been found
14:36	7,647 ETH from remaining token sales consolidated into holding address [4]
18:15–18:20	TSpe5 sent its entire 638.2 million TRX balance in five transfers
18:27	He Yi said the 60 million USDT collateral on Aave was not fully frozen; the attacker had actually taken about US$46 million in ETH
19:03	Binance disclosed over US$6.34 billion in reserved company funds and began replenishing affected user assets
19:24	Binance support said withdrawals were expected to resume within 45 hours; pending withdrawals had been canceled
19:45	Reuters reported Binance was working with the FBI, US Secret Service and other law-enforcement agencies

Sources: Ethereum, TRON and Arbitrum on-chain records; public information from Binance, TRM Labs, Arkham, Chainalysis and Reuters.

2. Attack path: from a laptop to EIP-7702 delegation

2.1 Official investigation: an engineer’s computer was the entry point

Binance’s preliminary statement at 10:25 said the incident may have begun with a compromised DevOps engineer’s laptop. The attacker used it to access a service container and submit unauthorized withdrawal transactions. No evidence of wallet private-key leakage had been found. At 14:02, Binance clarified that the compromised employee device was only the starting point: compromising one device or abusing one engineer’s permissions alone could not have accomplished the transfers. The process was more complex, and the investigation had not assigned responsibility to any individual. The security team was tracing the full attack path from the compromised computer, with a complete root-cause report to follow.



Binance
@binance

翻译自 英语 显示原文

币安的初步调查表明，此次安全事件可能涉及一名 DevOps 工程师的笔记本电脑被攻破，这使得攻击者能够访问一个服务容器并提交未经授权的提款交易。我们未发现任何钱包私钥泄露的证据。一旦调查完成并完全核实事实，我们将分享一份详细的技术事后分析报告。

预计总影响约为 63 亿美元。我们已与区块链合作伙伴合作冻结受影响的资产，目前已冻结约 30 亿美元的链上资产。
币安将从 SAFU 基金和公司资金中承担所有损失。用户资金是安全的。一旦修复工作完成，我们还将发布一份更新的储备证明。

作为即时预防措施，币安已：

- 在安全检查完成前，暂时暂停存款和提款；
- 撤销受影响地址的授权；
- 联系执法机构和区块链情报合作伙伴追踪并追回资金。

我们的团队正日夜奋战，以安全且彻底的方式解决这一问题。我们正与执法合作伙伴密切合作，确认这些犯罪分子的身份并将其绳之以法。

请仅通过官方币安渠道获取更新。如有任何进一步问题，请随时联系币安客户支持。

上次编辑 上午10:25 · 2026年10月30日

Figure 4. At 10:25, Binance published preliminary findings: a DevOps engineer's laptop had been compromised; estimated total impact was about US$6.3 billion, with about US$3 billion frozen. Source: X, @binance.

2.2 Preparations about 18 hours before the attack

On-chain records show preparation extending beyond a single day. The triggering address 0x7C86…5CA0 was initially funded from Tornado Cash and deployed its first contract at 10:28 on 29 October. Between 21:51 and 22:24 that evening, it made four test calls to two contracts, around 18 hours before the attack.

2.3 EIP-7702: only one of 50 pre-signed authorizations took effect

On Ethereum, the attacker used EIP-7702, introduced in the Pectra upgrade in May 2025. It lets an ordinary wallet authorize, by signature, a smart contract to supply its execution logic. Subsequent calls to the address execute the delegated code. The mechanism was designed for uses such as transaction batching and sponsored gas fees.

At 04:20:59, trigger address 0x7C86 submitted a type-4 transaction to Binance 14 containing 50 authorizations. All delegated to contract 0x63e8…6fAe; every signature recovered to Binance 14. The nonces descended consecutively from 18,914,824 to 18,914,775. Under protocol rules, only an authorization matching the account's current nonce can take effect. Binance 14 had just used nonce 18,914,808 in the same block, so only the authorization for 18,914,809 became effective. Three minutes and 24 seconds later, the attack contract called sweep and began draining the hot wallet.

The authorization bundle shows that the attacker had obtained signatures from Binance 14 for a range of future nonces, accommodating nonce drift from the hot wallet's frequent transactions. A valid signature establishes only that the corresponding key participated in signing. On-chain data cannot distinguish a leaked private key from abuse of a signing service or manipulation of an approval process; Binance's internal logs are needed to resolve that question. SlowMist founder Cos also noted that EIP-7702 merely made it easier to sweep hot-wallet tokens in batches; the mechanism itself was not faulty.

At 08:10:35, Binance 14 sent its own type-4 transaction setting the delegation target to the zero address, revoking the attack contract's control three hours and 49 minutes after the authorization took effect. Revocation prevents subsequent delegated calls; it does not restore transferred assets or reverse prior token approvals.

Table 3. Binance 14 delegation and revocation

Time	Transaction	Details
04:20:59	0xad99…298b	0x7C86 submitted a type-4 transaction with 50 authorizations delegating to 0x63e8…6fAe; only one took effect
04:24:23	0x53bd…e2f3	Attack contract called sweep; balances from 64 token contract addresses plus ETH moved to the main address
08:10:35	0xafbf…7209	Binance 14 sent a type-4 transaction with the zero address as delegation target, revoking delegation

Source: Ethereum on-chain records, Blockscout. Full transaction hashes appear in the appendix.

2.4 Sixty-four tokens moved in one transaction

The sweep call at 04:24:23 listed 64 token contract addresses. It moved Binance 14's 1.615 billion USDT, 62.6 million RLUSD, 29,934 WBETH, 11,372 XAUT (Tether Gold), 6.19 million UNI, 27.76 million USD1, 198 million ENA, 7.175 trillion PEPE, 2.26 million LINK and 128,000 AAVE, among other assets, together with 167,000 ETH, to the attacker's main address 0x5227…2f8c. That address had no prior transaction history.

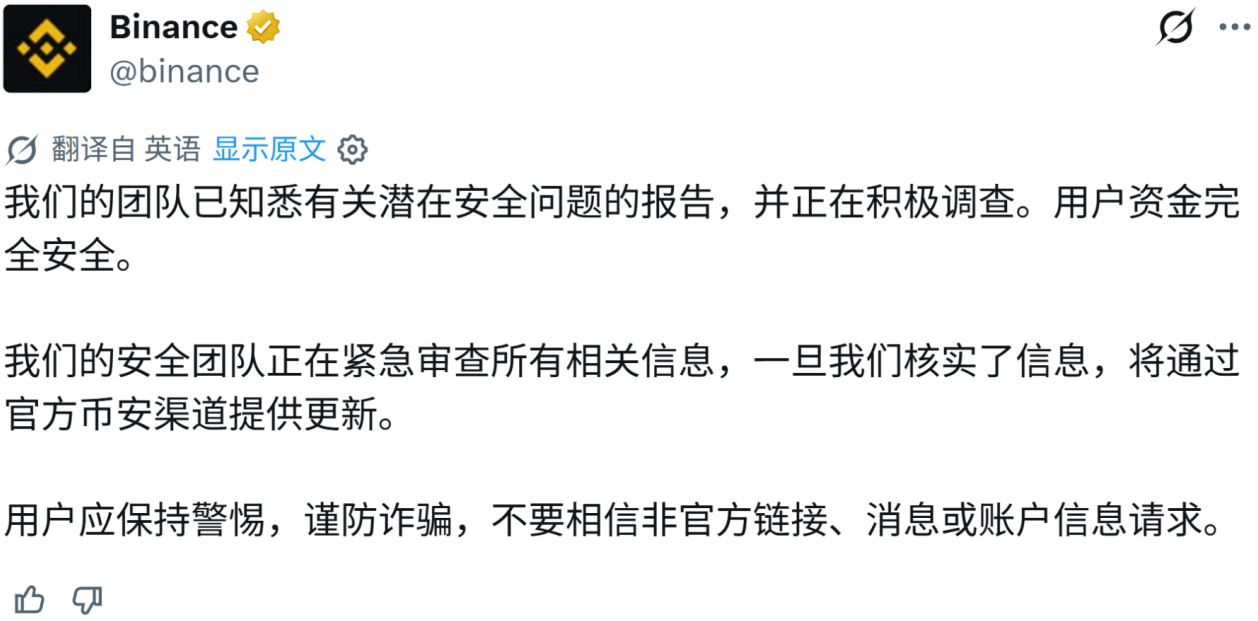


Figure 5. At 05:29, Binance's first official response said the team was actively investigating, user funds were safe, and users should beware of scams. Source: X, @binance.

2.5 Deposit consolidation continued; the attacker returned twice

Binance 14 was not completely isolated for more than an hour after the attack. At 05:55, researcher Conor Grogan noted that Binance's deposit consolidation was still running: newly deposited assets continued to enter the hot wallet and were promptly taken again. At 05:04:23, another 3.92 million USDT and 1,699.9 ETH left Binance 14. At 05:44:11, a further 200.4 million USDT and 369.8 ETH were transferred. All went to the attacker's main address.

When the 200 million USDT arrived, Tether had already blacklisted the main address at 05:01:35, so the funds were locked immediately on receipt. At 06:06:23, Tether also blacklisted Binance 14 itself. Binance's own hot wallet joined the attacker addresses on the freeze list.

Figure 6. At 05:55, Conor Grogan noted that deposit consolidation was still replenishing the hot wallet, which the attacker subsequently drained again. Source: X, @jconorgrogan.

3. The 37-minute window: three steps before the freezes took effect

Funds were stolen at 04:24. Tether froze the main address at 05:01:35, and Circle froze its USDC at 05:04:59. Within those 37 minutes, 729 million USDT was sold at discounts, pledged as loan collateral or relayed onward, becoming ETH and TRX without issuers capable of freezing them. Chainalysis's 18:27 investigation supported this account: in about 20 minutes the attacker converted US$325 million in stolen stablecoins into US$285 million worth of ETH, then sent another US$175 million in stablecoins through intermediary wallets in an attempt to outrun freezes.

Step 1: selling 325 million USDT at a discount

At 04:30:11, the main address sent 500 million USDT to selling address A, 0x9749…C762. Four minutes later it began selling in batches. Nine USDT transfers entered five execution contracts; the corresponding ETH was paid in installments by the UniswapX V2DutchOrderReactor settlement contract and another order settlement contract. Between 04:34 and 04:49, all 325 million USDT was sold for 122,316 ETH.

The attacker accepted a substantial discount. At the then ETH price of US$2,315, 325 million USDT could theoretically have bought about 140,000 ETH; actual proceeds were about 18,000 ETH lower. Including two other batches sold directly into Uniswap and other pools, about 435 million USDT was sold before freezes for around 160,000 ETH, roughly 27,000 ETH below market value—a difference of about US$60 million. Some batches effectively cost more than US$3,000 per ETH. At 04:59:11, selling address A sent its

remaining 175 million USDT to the next intermediary. It was frozen two minutes and 24 seconds later.

Step 2: borrowing 19,762 ETH from Aave against stolen collateral

At 04:33:23, the main address sent 200 million USDT to selling address B, 0x0Ddf…697E. That address sold 10 million USDT in Uniswap and other pools for 3,552 ETH, then sent the remaining 190 million USDT and that ETH to 0x8d53…639A.

Delta found that 0x8d53 did not continue selling. At 04:57:59 and 05:00:11, it supplied a combined 60 million USDT as collateral to Aave v3. At 04:59:11 and 05:00:59, it used Aave's WETH borrowing gateway to borrow 3,271 and 16,491 ETH, totaling 19,762 ETH. About 19,762.5 WETH of variable-rate debt remained outstanding. At 05:01:59, 0x8d53 sent its remaining 130 million USDT onward and was frozen by Tether 48 seconds later. Twelve seconds before that USDT transfer, 23,314.5 ETH had already left.

USDT can be frozen by its issuer; ETH has no issuer that can freeze it. Pledging USDT expected to be frozen allowed the attacker to extract ETH that could not be issuer-frozen. Even if the collateral was subsequently locked, the borrowed ETH was already in the attacker's hands. At 18:27, Binance co-founder He Yi said the 60 million USDT deposited with Aave was not within the fully frozen amount; the attacker had actually taken about US$46 million in ETH. Unlocking the collateral through law-enforcement procedures could recover approximately US$14 million more. Following disclosures by Aave risk provider LlamaRisk, Aave froze new borrowing in the relevant markets.

Step 3: relaying funds seconds ahead of freeze orders

From 05:01:35, Tether froze downstream addresses one after another. Delta's comparison of Tether contract blacklist events showed that several addresses made their last outgoing transfer only tens of seconds before their freeze:

Table 4. Last outgoing transfers compared with Tether freeze times

Address	USDT received	Last outgoing transfer	Frozen at	Outcome
Main address 0x5227…2f8c	1.875 billion	04:33:23 — 200 million sent	05:01:35	1.175 billion frozen
Selling address A 0x9749…C762	500 million	04:59:11 — 175 million sent	05:01:35 — gap 2 min 24 sec	Emptied
Selling address B 0x0Ddf…697E	200 million	04:52:59 — 190 million sent	05:01:47 — gap 8 min 48 sec	Emptied
Aave borrower 0x8d53…639A	190 million	05:01:59 — 130 million sent	05:02:47 — gap 48 sec	60 million pledged on Aave
Relay selling address 2, 0x7Aa4…BFd1	80 million	05:11:11 — 30 million sent	05:12:35 — gap 84 sec	Emptied
Downstream intermediary 0xAa24…54a0	175 million	—	05:14:59	175 million frozen
Relay intermediary 3, 0xCcBE…A263	30 million	05:16:11 — 30 million sent	05:16:47 — gap 36 sec	Emptied

Address	USDT received	Last outgoing transfer	Frozen at	Outcome
Terminal address 0xb171…c8c3	30 million	—	05:18:59	30 million frozen

Source: Ethereum on-chain records and Tether AddedBlackList contract events, Blockscout.

Along this relay, selling addresses 1 (0x77ED…c3eb) and 2 each sold approximately 50 million USDT in Uniswap and other pools. The ETH proceeds traveled downstream alongside USDT. At terminal address 0xb171, 30 million USDT was not transferred in time and was frozen. However, 57,891.8 ETH from the same batch moved to a new holding address at 05:35:59.

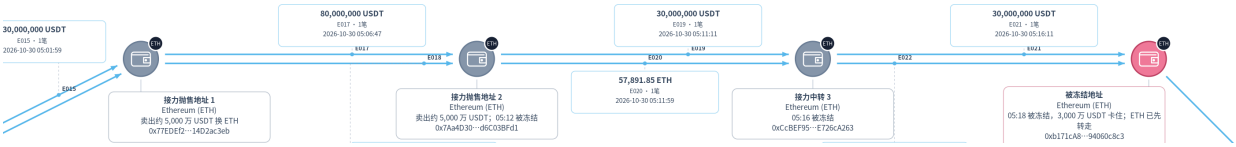


Figure 7. USDT and ETH moved together down the relay chain. The red node is the terminal address that still held 30 million USDT when frozen. Data cutoff: 11:00.

Differences among published freeze figures largely reflect different observation times. CZ cited 971 million USDT at 05:15; Paolo announced 1.567 billion USDT at 05:25. On-chain balances showed 1.380 billion USDT frozen across three Ethereum addresses and 379 million across two TRON addresses, totaling 1.759 billion USDT. This includes the 200 million USDT sent to the already-frozen main address at 05:44.

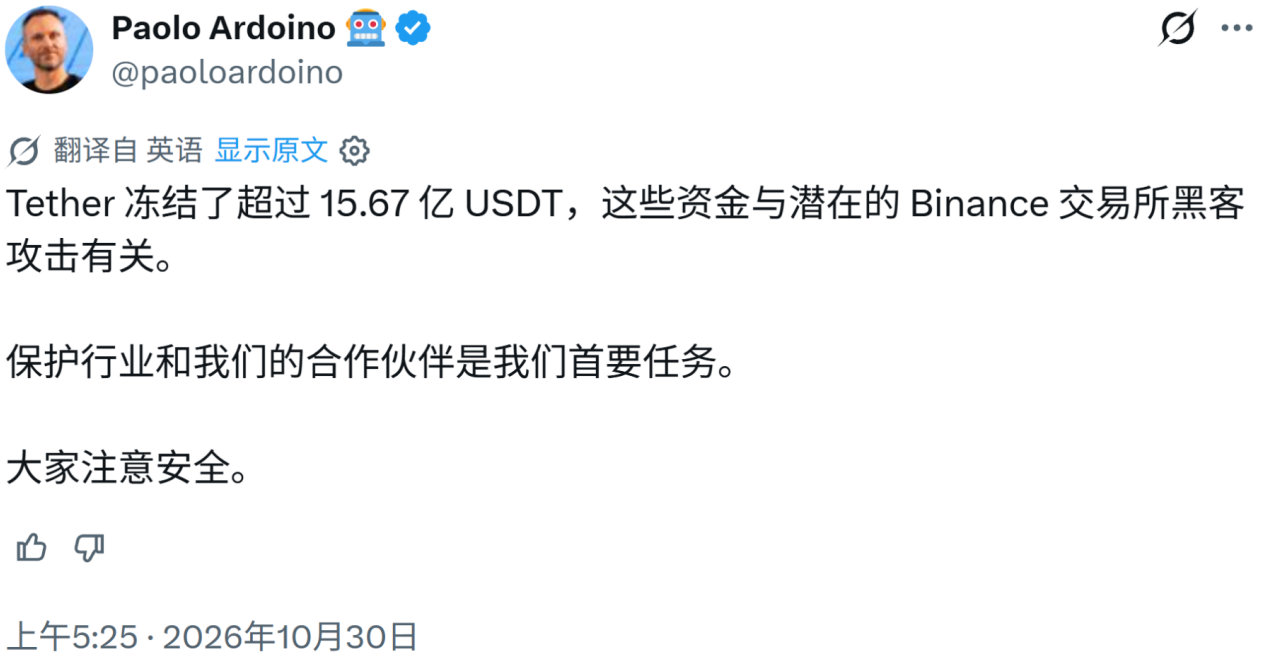


Figure 8. At 05:25, Tether CEO Paolo Ardoino announced more than 1.567 billion USDT frozen. Source: X, @paoloardoino.

Figure 9. At 05:18, Circle CEO Jeremy Allaire said more than 800 million USDC had been frozen in coordination with law enforcement. Source: X, @jerallaire.

4. Arbitrum intervention: chain-level powers move US$30.5 million

Neither ARB nor ETH on Arbitrum has an issuer capable of freezing it. Moving these approximately US$30.5 million in assets depended on the Arbitrum Security Council's chain-level authority.

At 04:30:34, Arbitrum address 0xB38e…891D, which had sent more than 8.5 million transactions in total, transferred 74,559,805 ARB to the attacker's main address, 0x5227…2f8c. The attacker used exactly the same main address on Arbitrum as on Ethereum. At 05:29, the main address sent 0.5 ETH on Ethereum to 0x3E2b…32d5. Two minutes later, that address bridged through MetaBridge to obtain gas funds on Arbitrum. At 05:36:30, 74.56 million ARB moved to 0x3E2b.

At 08:18:20, the ARB moved from 0x3E2b to the frozen-funds address designated by the Arbitrum Security Council. On-chain records showed the attacker address itself as sender, but the transaction was Arbitrum-specific type 0x65, which does not require that address's private-key signature. The attacker had not signed this transfer, yet the assets left its wallet. At 08:19, Arbitrum confirmed that the Security Council had moved 74,559,805 ARB and 8,425 ETH. These assets could be used only following further Security Council action or an Arbitrum DAO vote. Their combined value was about US$30.5 million.

Figure 10. The path of 74.56 million ARB on Arbitrum. The red node is the Security Council's frozen-funds address.

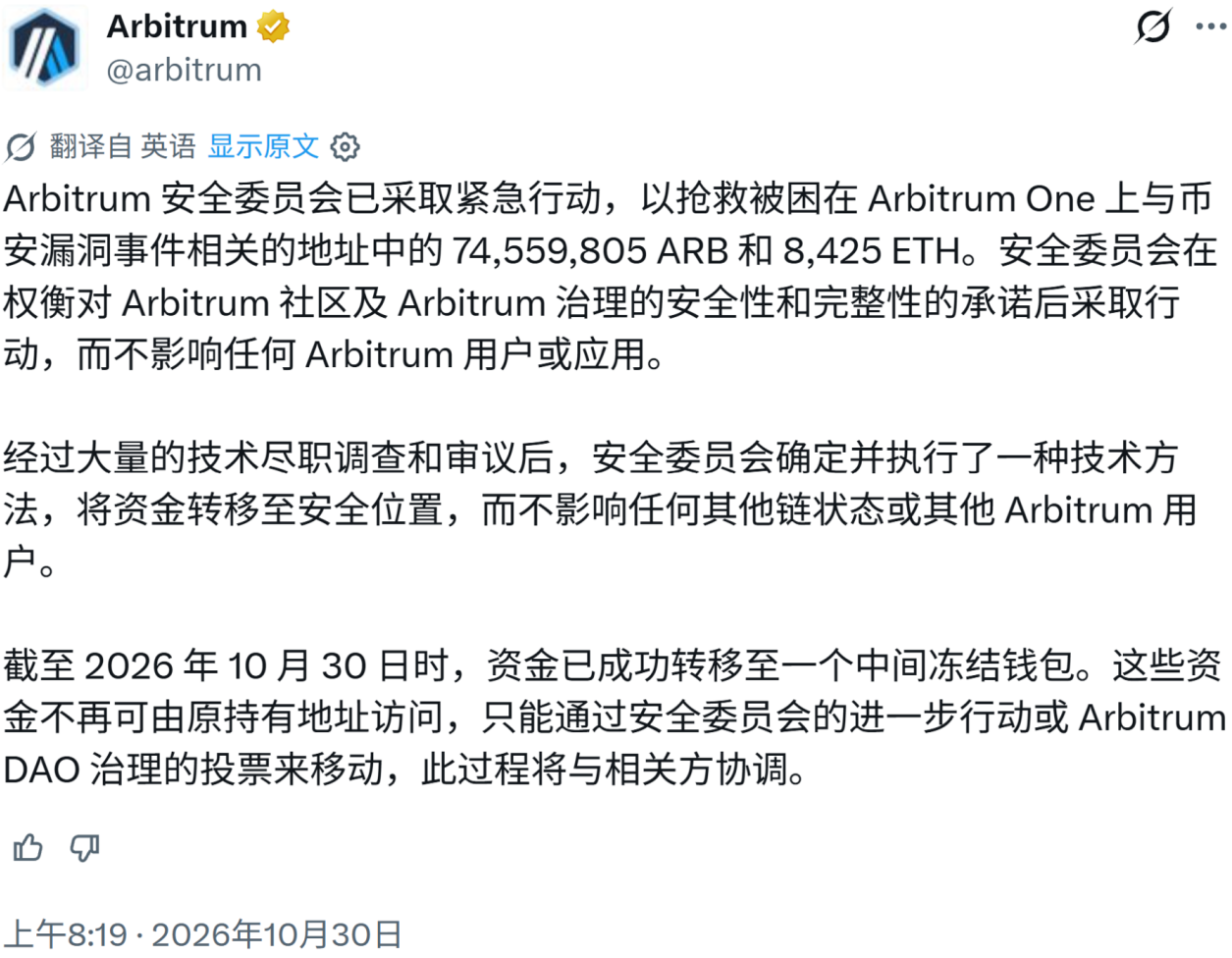


Figure 11. At 08:19, Arbitrum said the Security Council had taken emergency action to move 74,559,805 ARB and 8,425 ETH to a frozen-funds wallet. Source: X, @arbitrum.

Ethereum mainnet has no equivalent mechanism. Intercepting the attacker's mainnet ETH therefore depends on tracing it to exchanges and over-the-counter channels. This precedent of on-chain governance directly handling assets in a user address will also continue to prompt discussion.

5. Fund status: where US$1.34 billion stood at the 20:00 cutoff

Table 5. Main assets still controlled by the attacker

Asset	Quantity	Value, US dollars	Status
ETH — six holding addresses plus the main address	About 505,622 ETH	About 1.129 billion	No issuer freeze; no outgoing transfers from the three largest addresses since receipt
TRX — four new holding addresses plus splitting address TRBd	About 631 million TRX	About 215 million	No issuer freeze; extensive movement began at 18:15 and splitting continued
Total	—	About 1.34 billion	Excludes TRX already split among dozens of new addresses and assets on Bitcoin

Prices: ETH US$2,233; TRX US$0.3405, using CoinGecko quotes around 20:00. The main address also held approximately 27.82 million USD1, 12,600 XAUT, 1,907 PAXG and 3.45 million FDUSD, worth about US$61 million combined. These were excluded because their issuers have freeze capabilities.

5.1 Ethereum: funds concentrate in six holding addresses

Table 6. Ethereum holding-address balances at 20:00

Address	ETH balance	Origin and activity
Holding address [1] 0x8532…43D4	197,460	195,460 ETH received from the main address at 04:38 and another 2,000 at 09:14; no outgoing transfers
Holding address [2] 0xc887…286A	137,602	122,310 ETH from selling address A plus 15,292 from ENA sales; no outgoing transfers
Holding address [3] 0x897C…8DF3	78,415.25	57,891.77 ETH from the end of the relay chain plus UNI and other sales; no outgoing transfers
Holding address [4] 0x5440…C942	40,600.67	Proceeds from AAVE, RLUSD, WLD, RSR, MORPHO and other sales; another 7,647 ETH consolidated at 14:36
Holding address [5] 0x79e7…544A	34,279.69	Proceeds from USDe, WBTC and PEPE; 14,529 ETH consolidated from LINK and USDe selling addresses at 13:31–13:35
New holding address [6] 0x03b0…20ea	17,260.1	Single transfer from the main address at 13:15; no outgoing transfers or entry into Tornado Cash
Main address 0x5227…2f8c	About 4.5	More than 30 tokens sold on Uniswap from 08:08; 1.175 billion USDT and 823 million USDC frozen

Source: Ethereum on-chain records, Blockscout.

After 11:00, Ethereum funds continued consolidating into holding addresses. At 13:15, the main address sent 17,260 ETH, worth about US$38.82 million, to new address 0x03b0…20ea. Arkham suggested at the time that it might head to Tornado Cash, but by 20:00 none of that ETH had moved out. From 13:28 to 13:35, the former LINK selling address, holding 11,560.82 ETH, the USDe/WBTC selling address, holding 2,856.9 ETH, and the PEPE selling address moved their ETH into holding address [5]. From 14:17 to 14:20, 0xA97b…8d10 sold remaining tokens on Uniswap; at 14:36, the resulting 7,647 ETH consolidated into holding address [4].

Holding addresses [1], [2] and [3] held a combined 413,477 ETH with no outgoing transfers since receipt. During the afternoon, they received many zero-value and very small transfers: third-party on-chain messages and address poisoning. Cashing out large ETH holdings generally involves mixers, bridges or OTC channels. The first outgoing transfer from these addresses will be an important signal for assessing recovery difficulty.

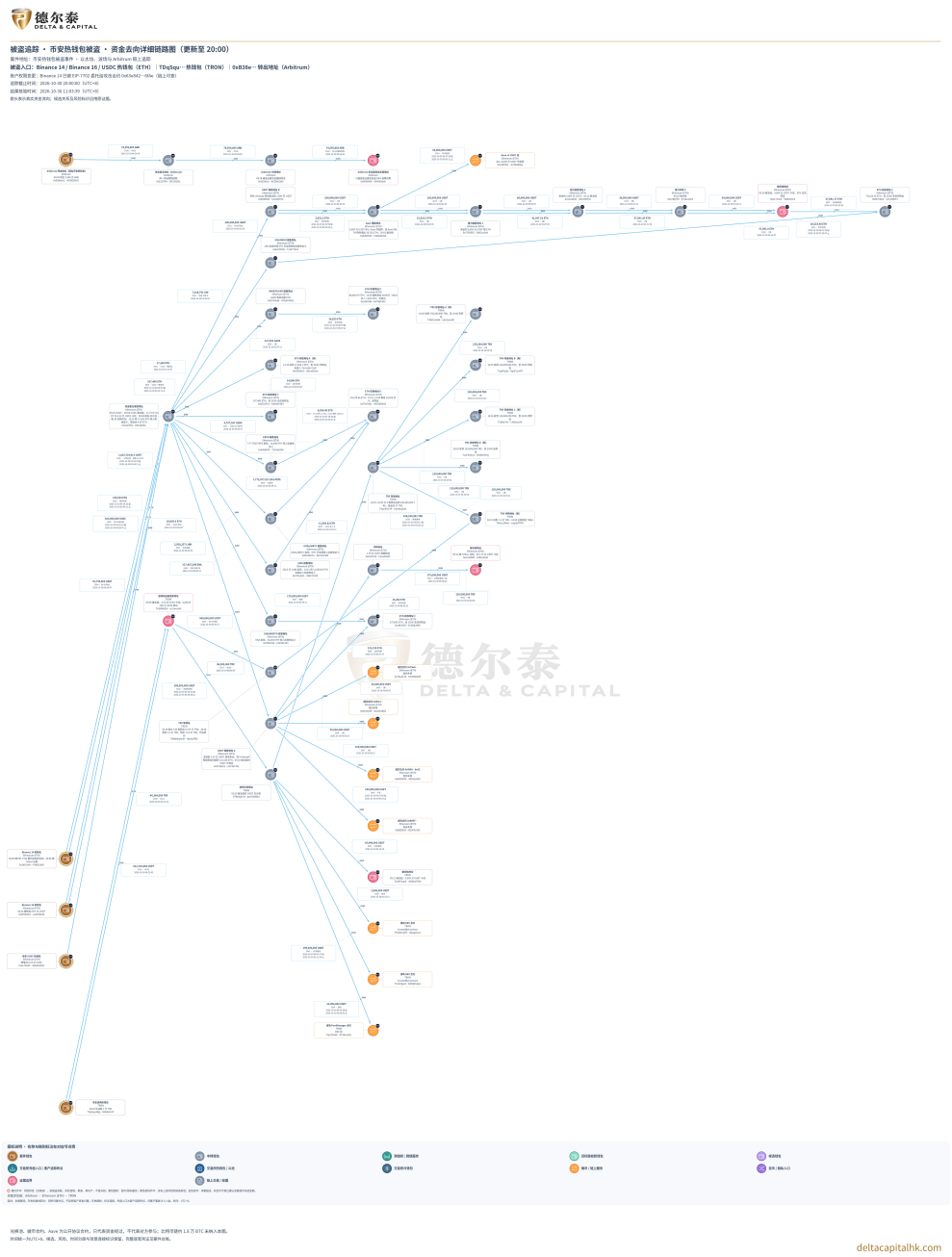


Figure 12. Detailed flow of the stolen Binance hot-wallet funds: Ethereum holding addresses and the full TRON and Arbitrum paths. Data cutoff: 30 October, 20:00.

5.2 TRON: 234 million USDT converted to 638 million TRX before freezing

At 04:22:45, 613 million USDT moved from Binance's TRON hot wallet to attacker receiving address TG5i…zsGi. At 04:45 and 04:56, it sent a combined 300 million USDT to distribution address TPBk…KN4. Over 24 minutes, TPBk sent 199 million USDT through 13 transfers to a TRON DEX contract, plus 33 million and 2 million USDT to two other swap contracts. The resulting TRX arrived at new address TSpe5…yZ8A at 04:56:12 and 05:42:42, totaling 638,190,941 TRX.

Tether's TRON freezes were also a step behind. At 05:09:12, the receiving address was frozen while still holding 313 million USDT. At 05:16:18, the distribution address sent its last 65.99 million USDT to TCzB…Y62, which was frozen five minutes later. By the time the distribution address itself was frozen at 05:20:57, all its USDT had left. At 08:06:09, the receiving address's remaining 46.38 million TRX moved in

one transfer to TRBd…PRki, activated only three seconds earlier.

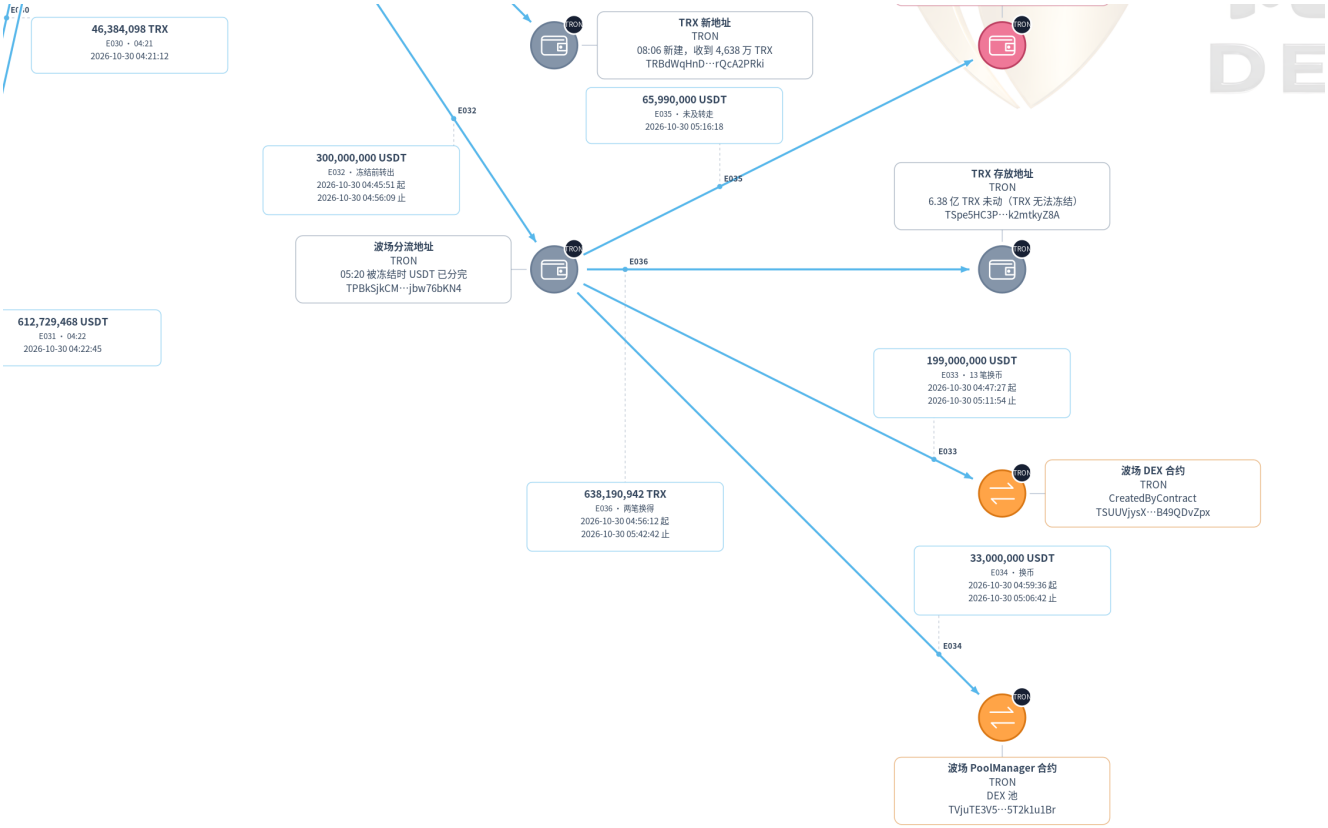


Figure 13. TRON: of 613 million USDT, 379 million was frozen and 234 million was converted to TRX and sent to TSpe5. Data cutoff: 11:00.

5.3 After 18:15: all 638 million TRX leaves the holding address

Delta found that previously inactive TSpe5, holding 638 million TRX, sent its entire balance in five transfers between 18:15 and 18:20. Only about 37 TRX remained. Of the outflow, 120 million TRX first went to an intermediary and then to splitting address TRBd at 18:20:48. The other four transfers, totaling 518.2 million TRX, remained in four new addresses with no further outgoing transfers by 20:00.

Table 7. TSpe5's five outgoing transfers, Beijing time

Time	Recipient	TRX quantity	Subsequent activity
18:15:21	TAk1…UFYP5 — intermediary	120,000,000	Entire amount sent to TRBd at 18:20:48
18:18:09	TL2F…NcfVwj	120,000,000	No further movement
18:18:42	TCBA…63ao1fk	120,000,000	No further movement
18:19:24	TJaj…FaLLHKT	120,000,000	No further movement
18:20:18	TKkH…vdd1xvw6K	158,200,900	No further movement

Source: TRON on-chain records, TronGrid. Full addresses and transaction hashes appear in the appendix.

5.4 TRBd: splitting, SunSwap conversion and return to Ethereum through USDT0

TRBd began splitting funds at 10:19. By 20:00, it had sent 53.73 million TRX in 145 transfers. Receipt of 120 million TRX at 18:20 raised its balance back to approximately 113 million, and splitting continued. The funds initially passed through 13 first-level splitting addresses and 41 relay addresses, most newly created after 10:19.

As of 18:10, about 11.74 million of this TRX had been converted to USDT on SunSwap. Fourteen bridge-originating addresses then returned a combined 4,043,953 USDT to Ethereum through 27 transactions using USDT0's bridge contracts. Nine receiving addresses on Ethereum immediately swapped the USDT for ETH on DEXs. Smaller amounts of TRX and USDT also reached suspected instant-swap services, OTC settlement services and other conversion providers. Five suspected TRX-to-USDT instant-swap addresses were activated in the same minute on 12 October; one deposited about US$3.71 million to Binance over 17 days. Suspected OTC settlement address TZG47 held about 6.92 million USDT and had deposited approximately US$48.87 million to Bitget over 311 days. Other destinations included Changehero, a conversion service with mixed KYC practices, and a NEAR Intents cross-chain hot wallet.

This route still presented opportunities for freezing parties: USDT bridged through USDT0 remained freezeable by Tether, while the swap and settlement addresses had deposit relationships with Binance and Bitget. At 18:09, Chainalysis also observed automation executing thousands of transactions quickly, cycling funds repeatedly between addresses and often returning them to earlier addresses in the sequence. SlowMist's MistTrack found stolen TRX passing through a Bitget Wallet cross-chain swap into an address previously used by the Phemex hacker. Bitget Wallet subsequently said it had blacklisted identified incident-related addresses and restricted the relevant services.

Figure 14. TRON splitting, SunSwap swaps and return to Ethereum through USDT0. Data cutoff: 30 October, 18:10.

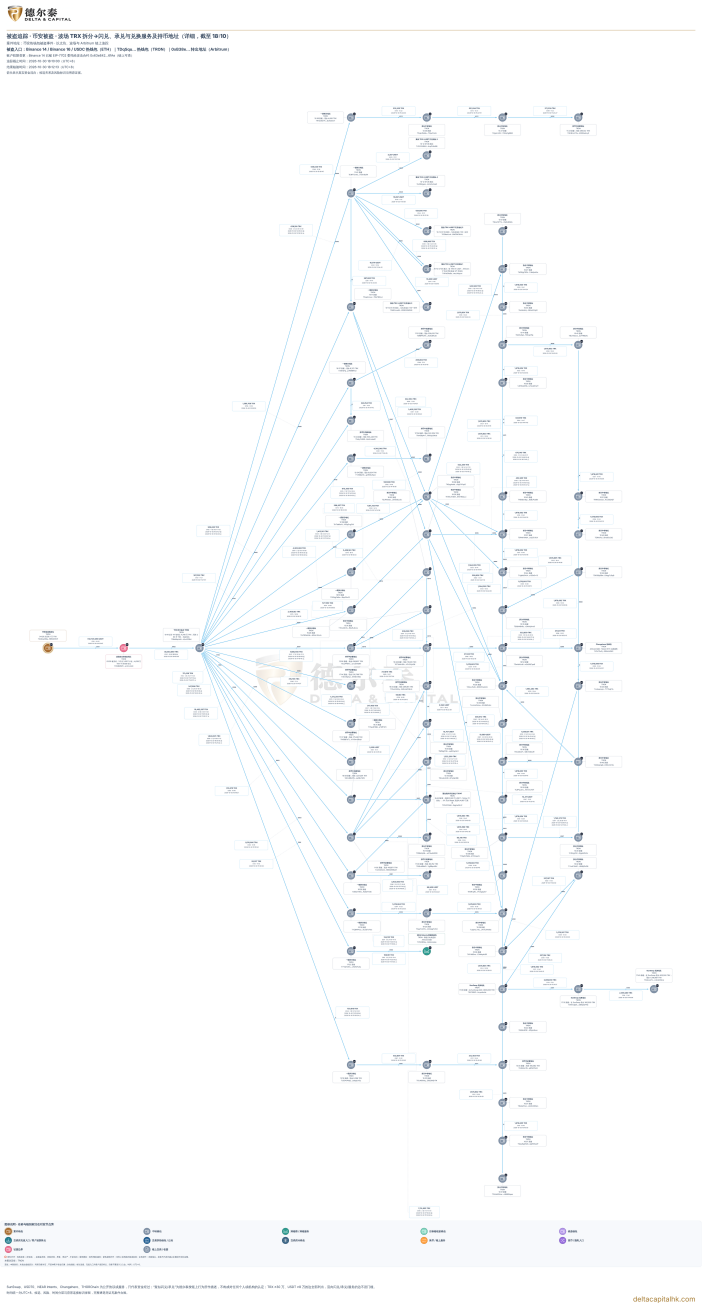


Figure 15. Suspected instant-swap, OTC settlement and conversion services, and holding addresses reached after TRX splitting. Data cutoff: 30 October, 18:10.

6. External responses, attribution and market impact

6.1 Freezing and coordinated action

Table 8. Published freezes and other responses

Party	Published action	Notes
Tether	More than 1.567 billion USDT frozen, announced at 05:25	On-chain total of 1.759 billion USDT locked across five Ethereum and TRON addresses

Party	Published action	Notes
Circle	More than 800 million USDC frozen, announced at 05:18	823 million USDC at the main address frozen at 05:04:59
Arbitrum Security Council	74,559,805 ARB and 8,425 ETH moved to a frozen-funds address	About US$30.5 million; further use requires Council action or a DAO vote
World Liberty Financial / BitGo	According to He Yi, about 27 million USD1 and US$2 million worth of WLFI frozen	The main address held approximately 27.82 million USD1
Ripple	Freezing the attacker's RLUSD holdings, announced at 06:08	The attacker had held 62.6 million RLUSD; some had already been sold
Synthetix	About 8.41 million SNX recovered through the DAO and held in the protocol multisig	Binance notified; tokens available for return on request
USDT0	Ethereum–TRON cross-chain transfers temporarily suspended, subsequently resumed	To prevent cross-chain movement of stolen funds
Bitget Wallet	Identified incident-related addresses blacklisted and services restricted	Tracing in cooperation with Binance's security team
Aave	New borrowing in the relevant markets frozen	Repayment, withdrawal and liquidation remained available

Sources: the parties' official X accounts, Wu Blockchain and Reuters public reporting.

Figure 16. At 06:08, Ripple executive Jack McDonald said active steps were being taken to freeze the attacker's RLUSD holdings. Source: X, @_JackMcDonald_.

6.2 Attribution

TRM Labs attributed the attack with high confidence to North Korea-linked TraderTraitor. On-chain investigator ZachXBT assessed the attacker as TraderTraitor within North Korea's Lazarus group. Around midday, he found funds from this incident mixing at the same address with proceeds from the previous month's US$388 million Bitget theft after passing through THORChain, suggesting both incidents were likely carried out by the same attacker. Lookonchain also considered Lazarus a possible link among the Binance, Bybit and Bitget thefts. These remain assessments by research firms and on-chain analysts, not formal law-enforcement determinations. Reuters reported at 19:45 that Binance was cooperating with law-enforcement agencies worldwide, including the FBI and US Secret Service.

Figure 17. At 08:14, ZachXBT reported that the Arbitrum Security Council had executed a transaction freezing about US$30.5 million, and published the attacker address and transaction hash. Source: X, @zachxbt.

6.3 Binance's response and arrangements for users

Binance suspended withdrawals at 06:33 and temporarily suspended deposits at 08:13. At 12:36, it announced that deposits had returned to normal and withdrawals were expected to resume within 48 hours. At 19:24, support updated the estimate to 45 hours and said pending withdrawal requests had been canceled. Users could manage funds through P2P, fiat withdrawals or trading.

Regarding compensation, CZ said at 10:23 that user funds were safe, and He Yi said at 11:51 that the matter would be pursued to the end. At 19:03, Binance disclosed more than US$6.34 billion in company funds reserved to cover losses. Approximately US$5 billion was already held in the same tokens as the affected assets; the rest was being purchased on public markets and OTC. At 19:07, He Yi said matching

quantities of the stolen altcoins were being bought both on and off exchange. At 18:55, Binance announced that replenishment of affected user assets had begun. Updated proof of reserves would be published after remediation.

Figure 18. At 06:23, CZ said the loss might be slightly above that figure, but would be covered. Source: X, @cz_binance.

6.4 Market impact

Crypto markets fell significantly after the incident. At 20:00, BTC traded at US$77,394, down 3.5% over 24 hours, after briefly approaching US$77,000. ETH was US$2,233, down 4.0%, and had briefly fallen below US$2,200. BNB was US$699, down 5.4%. Indian exchange CoinDCX temporarily put futures into reduce-only mode, citing disruption affecting a global liquidity provider. In a Bloomberg interview, Ballet founder Bobby Lee said the stolen Bitcoin was likely unrecoverable. CZ noted that traditional financial markets had also fallen sharply that day and that not all market volatility should be attributed to this attack.

Price source: CoinGecko quotes around 20:00. These reflect the stated cutoff only.

7. Beyond the announcements: address poisoning, messages and token sell-offs

7.1 The attacker's address was also targeted by address poisoning

The screenshot accompanying Spreek's first alert showed a transfer from 0x9749F766…C762 in the main address's transaction history. The real selling address A was 0x9749292D…C762: the beginning and end matched exactly, while the middle differed. At 04:29, the attacker sent 0.5 ETH to selling address A for gas; a transfer from the lookalike appeared less than a minute later. A fake token displayed as USDT also fabricated a record showing the main address sending 500 million tokens to another imitation 0x9749…c762 address, matching the real transfer amount.

7.2 More than twenty on-chain messages

During the hours following the theft, the main address received around twenty on-chain messages. They included a direct request for US$50,000, Bible quotations and token promotions. One sender wrote "Funds are UNSAFU," mocking Binance's familiar "Funds are SAFU" slogan. As of 20:00, Binance had not sent an on-chain message to the attacker or announced a white-hat bounty.

7.3 Liquidating altcoin holdings

At 06:48, Lookonchain warned that the attacker was selling PEPE, UNI, LINK and other tokens for ETH. Just over two hours later, those tokens had been sold. Some 7.77 trillion PEPE produced approximately 14,049 ETH, while PEPE's price fell 12.33%. Between 08:53 and 09:08, all 3.38 billion RSR was exchanged for 1,856 ETH. From 08:08, the main address also sold more than 30 long-tail tokens on Uniswap, including ZAMA, FET, PENDLE, CRV, SHIB, EIGEN and LDO. Remaining tokens continued to be sold during the afternoon by addresses including 0xA97b, with proceeds consolidated into holding addresses.

Figure 19. At 06:48, Lookonchain reported that the Binance hacker was selling PEPE, UNI, LINK and other tokens for ETH. Source: X, @lookonchain.

8. Delta observations

The parties responded quickly: Tether acted within 37 minutes and froze eight Ethereum addresses over 17 minutes. Within four hours, the Arbitrum Security Council moved US$30.5 million from an attacker address. Approximately US$3 billion was frozen in total. Nevertheless, 729 million USDT had already become ETH and TRX before freezes took effect. At 20:00, about US$1.34 billion in assets remained beyond issuer-freeze capabilities, and extensive TRON movement had begun after 18:15. Binance users, investors seeking to move assets during the withdrawal suspension, and self-custody holders should note the following.

1. Watch for phishing before and after withdrawals resume

An exchange hack, suspended withdrawals and official compensation promises together create conditions that scammers frequently exploit. Over the following days, links, text messages and private messages claiming to offer Binance compensation registration, SAFU payouts or asset-migration verification may proliferate. Some may impersonate Binance support or security staff and contact users first. Any message demanding a wallet connection, seed phrase, authorization signature or advance verification transfer should be treated as a scam.

2. Verify the entire address, character by character, before every transfer

Even an attacker holding billions of dollars in stolen funds became a target of address poisoning within minutes. When users transfer assets after withdrawals resume, their histories may also contain lookalike addresses with matching beginnings and endings. Verify every character of the full recipient address and avoid copying directly from transaction history. For large transfers, test with a small amount and confirm receipt before sending the balance.

3. Freeze before conversion; trace the return points

Stolen USDT and USDC may be freezeable, but the window is measured in minutes. Once converted into issuerless assets such as ETH, TRX or BTC, issuer-freeze routes largely cease to work. Here, split TRON funds were converted back into USDT on SunSwap, bridged to Ethereum through USDT0, and sent to swap and settlement addresses with exchange-deposit relationships. These points reintroduced freezeable assets and exchange accounts that could be subject to information requests. Individual theft victims should immediately preserve transaction hashes and wallet addresses, engage professional assistance, report the incident and begin tracing promptly. Before funds are swapped, mixed or bridged, a properly documented investigative report can support freeze requests to stablecoin issuers and relevant exchanges. Delta provides on-chain tracing, fund-flow analysis and evidence reports.

Even the fastest freeze button cannot outrun an attacker who rehearsed 18 hours in advance. Recovering losses requires the patience to watch every point where funds return to reachable channels.

For case consultations or cooperation, contact our official X account @delta_team_hk, visit deltacapitalhk.com or leave a message through our WeChat official account.

Appendix: key addresses and transactions

Table 9. Key addresses in full

Role	Chain	Address
Binance 14 hot wallet	ETH	0x28C6c06298d514Db089934071355E5743bf21d60
Trigger and authorization-submission address	ETH	0x7C8601d4645B93CEA45F71e118a729332e6b5Ca0
EIP-7702 delegated contract	ETH	0x63e842B054bd624a465454D533c33F573e9C6fAe
Attacker main address, ETH / Arbitrum	ETH	0x5227f603C1eE34CE3C06eFe6477003BDfCCB2f8c

Role	Chain	Address
Holding address [1]	ETH	0x8532FA14ACAf483729C449b8458aedDb900543D4
Holding address [2]	ETH	0xc887aF690E0301CD4edBbCe8F8d31b4EC65B286A
Holding address [3]	ETH	0x897C80d1a9729E94460e2Bd93178bD5215158DF3
Holding address [4]	ETH	0x54401f80Da97893a15D43566184635B6674BC942
Holding address [5]	ETH	0x79e70d139fC05AA75F75611fDF2680E9952B544A
New holding address [6]	ETH	0x03b0eE5d82990cFF1bDa48651AC3e436d1a020ea
Aave borrowing address	ETH	0x8d53903625b8e839b9DF4bd28B0EFb1CD6b8639A
Arbitrum intermediary	ARB	0x3e2bf1ac6bf0934bbba6456c341c2ecbced632d5
Former TRX holding address	TRON	TSpe5HC3PRD2svJcr1YoGszhHk2mtkyZ8A
TRX splitting address	TRON	TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki
New TRX holding address A	TRON	TKkH2vH6kyi2QKcMbqym53WMuvdd1xvw6K
New TRX holding address B	TRON	TJajtPqDqUGh1Sr1j8ugHoSXBVpaFLLHKT
New TRX holding address C	TRON	TCBAz7itvtX5CjBzVMPQdrbwQLN63ao1fk
New TRX holding address D	TRON	TL2F4GhnaFVZBZPncHYjwfYZFW44NcfVwj
TRX intermediary	TRON	TAk1xJNWuBYvJHLsUiBFLeuK6xvpQUFYP5

Table 10. Key transactions

Time	Chain	Transaction hash	Details
04:20:59	ETH	0xad99264d5532ae0dd04b2004eebda05f25657e70dacb764f7ac8d4ccd051298b	EIP-7702 authorization, 50 entries
04:24:23	ETH	0x53bd38b816c23e74134786c29a8c18d792777998a3b9326047b583100e88e2f3	sweep: 64 tokens plus ETH
08:10:35	ETH	0xafbf94c92a8d749988411669fa14d4f8866d9b4420b4ebd299f28e958dac7209	Delegation revoked
04:30:34	ARB	0xa18e57027dae90de066ac093bbb4ae3d63598accbe5175cdf4195c686462edff	74.56 million ARB sent to the main address
08:18:20	ARB	0x75e81a231a86e26a61e22dd2e6521504873a71a7ac1b2143c06e52796ceeedb6	Type-0x65 transaction; ARB moved to the frozen-funds address
18:15:21	TRON	9d0904db84e640d37e9fee8badef0883043db77f5bf9c87ca76e220e0c35c487	TSpe5 → TAk1, 120 million TRX

Time	Chain	Transaction hash	Details
18:18:09	TRON	16585e9664a0e7e74d67caeba2ecdc9869ec9a84a287dc078a12d34ca078c0d1	TSpe5 → TL2F, 120 million TRX
18:18:42	TRON	037428516b343a326157ae75495ad3227b43e4a4cb0c8c3837e849d7a18d556e	TSpe5 → TCBA, 120 million TRX
18:19:24	TRON	3db47d891cc211c300f9ba1aec264bfca8f9e32fbe220c411f30789a31ac8370	TSpe5 → TJaj, 120 million TRX
18:20:18	TRON	aff887c4be7cd52eb8905899fc9596eaaf9c49dea59129519ce25d7c69762334	TSpe5 → TKkH, 158.2 million TRX
18:20:48	TRON	0ae2b5a4e1c8849d09e16db5a4dd9d90f7224c3b996a80ccad113bd5b81acd39	TAk1 → TRBd, 120 million TRX

Disclosures

This article is original or compiled work by Delta. Reproduction or excerpting without authorization is prohibited. To request permission, contact us through our official-account messaging channel.

This report was compiled from public information and on-chain data as of 20:00 Beijing time on 30 October 2026. Funds may have moved subsequently. Delta's transaction-by-transaction checks cover Ethereum, TRON and Arbitrum; movements of approximately 18,000 BTC on Bitcoin and funds on XRP and other chains draw on third-party statistics and are excluded from the US$1.34 billion calculation. Detailed TRON splitting, conversion and cross-chain return paths are cut off at 18:10. Asset values use CoinGecko prices around 20:00. The identity of Arbitrum sender 0xB38e…891D is Delta's assessment based on on-chain behavior. Attacker attribution reflects assessments by TRM Labs, ZachXBT and other researchers, not a law-enforcement determination. Swap pools, execution contracts, Aave, SunSwap, USDT0 and conversion services are public protocols or services; a fund passing through them does not imply their involvement in wrongdoing. EIP-7702 analysis establishes signatures and execution only, not whether a private key leaked. Incident causes, losses and compensation arrangements are subject to formal disclosures by Binance and the relevant parties. Address labels are Delta's behavioral descriptions, not determinations concerning any person or organization. This report is not investment or trading advice and makes no promise of returns.

Sources

Binance's official X accounts (@binance, @binancezh, @BinanceHelpDesk); CZ (@cz_binance); He Yi (@heyibinance); Tether CEO Paolo Ardoino (@paoloardoino); Circle CEO Jeremy Allaire (@jerallaire); Ripple executive Jack McDonald (@_JackMcDonald_); Arbitrum (@arbitrum); ZachXBT (@zachxbt); Cos (@evilcos); Arkham (@arkham); Chainalysis (@chainalysis); Lookonchain (@lookonchain); Spreek (@spreekaway); Conor Grogan (@jconorgrogan); Watcher.Guru (@WatcherGuru); Wu Blockchain (@wublockchain12); Ai Auntie (@ai_9684xtpa); SlowMist MistTrack; TRM Labs incident analysis; Reuters and Bloomberg reporting; LlamaRisk disclosures on the Aave governance forum; an independent forensic report by the Global Cyber Security Alliance (GCSA); Ethereum records via Blockscout, including Tether and Circle blacklist events; TRON records via TronGrid; Arbitrum records via Arbitrum One RPC; and CoinGecko price data.

About us

Delta is a security specialist focused on blockchain forensics, on-chain tracing, SOW/SOF/KYT analysis and compliance consultation and communication.

Our team combines credentialed legal specialists and experienced on-chain data engineers. We assist clients worldwide with platform-account restriction reviews, tracing and recovery support for stolen or fraudulently obtained assets, on-chain investigations and evidence reports, case materials and cross-border cooperation, and wallet recovery and security support. Contact us through our official-account messaging channel for professional assistance.

Delta & Capital: Restoring Liquidity, Preserving Value.

Delta: restoring liquidity, preserving asset value.