

币安热钱包被盗事件

链上追踪研究报告

63 亿美元与 37 分钟：攻击路径、冻结赛跑、资金去向与后续风险

报告编号	DC-RS-20261030-BN
事件时间	2026 年 10 月 30 日 04:05 起 (北京时间)
数据截止	2026 年 10 月 30 日 20:00 (北京时间)
覆盖范围	以太坊、波场、Arbitrum 链上数据；比特币、XRP 等链引用第三方统计
发布机构	德尔泰 DELTA & CAPITAL

本报告依据公开链上数据与公开信息整理，资金仍在持续变动，数字以截止时点为准。不构成任何投资建议。

核心摘要

10月30日凌晨，币安在 XRP Ledger、以太坊、波场、Arbitrum、比特币等多条链上的热钱包相继被转空，官方预计总影响约 63 亿美元，是 2025 年 2 月 Bybit 案（14.6 亿美元）的 4 倍多，刷新加密行业单起被盗纪录。币安初步调查指向一名 DevOps 工程师的笔记本电脑被攻破，攻击者借此访问服务容器并提交了未经授权的提现。

从热钱包失守到 Tether 冻结首个攻击者地址，中间隔了 37 分钟。冻结令此后沿资金链逐级追赶，最惊险的一跳只差 36 秒。各方合计冻结约 30 亿美元，Arbitrum 安全委员会以链级权限从攻击者地址转走约 3,050 万美元资产；但截至 20:00，攻击者仍控制约 50.56 万枚 ETH 与约 6.31 亿枚 TRX，合计约 13.4 亿美元，这部分资产没有任何发行方可以冻结。

63 亿	约 30 亿	37 分钟	13.4 亿
官方预计总影响（美元）	各方合计冻结（美元）	被盗至首次冻结	仍在攻击者手中（美元）

核心发现

- **攻击提前约 18 小时布置。**触发攻击的地址 0x7C86...5CA0 由 Tornado Cash 注资，10月29日 10:28 部署首个合约，当晚 21:51 至 22:24 四次测试调用。
- **50 个预签授权，只有 1 个生效。**04:20:59 的 EIP-7702 授权交易一次塞入 50 个由 Binance 14 签名、nonce 连续的授权，只有与当时账户 nonce 吻合的一个生效；08:10:35，币安从 Binance 14 自身发交易撤销了委托。
- **37 分钟内 7.29 亿 USDT 被换走。**攻击者在冻结前折价抛售、抵押 Aave 借出 19,762 枚 ETH、沿接力链逐级下传，多个地址的最后一笔转出只比冻结早 36 至 84 秒。
- **Arbitrum 罕见动用链级权限。**08:18:20，一笔无需攻击者签名的 0x65 类型交易，把 74,559,805 枚 ARB 转入安全委员会冻结地址。

- **以太坊资金向 6 个存放地址集中。**截至 20:00，前三大存放地址合计 413,477 枚 ETH 自入账起没有任何转出；午后剩余代币继续被卖成 ETH 并入存放地址，17,260 枚 ETH 转入新地址⑥。
- **波场资金 18:15 起全面动身。**存放 6.38 亿枚 TRX 的 TSpe5 地址在 18:15 至 18:20 分 5 笔全部转出，其中 1.2 亿枚经中转进入拆分地址 TRBd；TRBd 自 10:19 起已分 145 笔转出 5,373 万枚 TRX，部分经 SunSwap 换成 USDT 后，通过 USDT0 跨链回到以太坊换成 ETH。

目录

一、事件概览：多链热钱包在 25 分钟内相继失守..... 5

二、攻击路径：从一台笔记本到 EIP-7702 委托..... 9

三、37 分钟窗口期：冻结生效前的三步操作..... 12

四、Arbitrum 罕见出手：链级权限转走 3,050 万美元..... 15

五、资金现状：13.4 亿美元停在哪里（截至 20:00） 17

六、外部响应、归因与市场影响.....24

七、公告之外：投毒、留言与清仓式抛售..... 27

八、德尔泰观察.....28

附录：关键地址与交易、声明、资料来源..... 30

一 事件概览：多链热钱包在 25 分钟内相继失守



翻译自 英语 显示原文

用户资金是安全的！

这看起来像是针对 Binance 的黑客攻击。感谢 Tether（约 9.71 亿美元）和 Circle（约 8.23 亿美元）的快速冻结。

我不再管理 Binance (.com)，但作为股东，我期望所有用户资金将得到全额补偿。

上午5:15 · 2026年10月30日

图 1 05:15, CZ 发帖确认币安遭黑客攻击，并感谢 Tether 与 Circle 的快速冻结（图源：X @cz_binance）

1.1 事件经过

据 TRM Labs 与 Arkham 统计，最早被转走的是 XRP Ledger 上约 3 亿美元的 XRP，时间为 10 月 30 日 04:05 至 04:09（北京时间，下同）。04:20:00，币安波场热钱包向一个新建地址转出 1 万枚 TRX，价值约 3,500 美元；72 秒后，该热钱包向同一地址转出 4,638 万枚 TRX；又过 93 秒，6.13 亿枚 USDT 随之流出。最初那 1 万枚 TRX 是攻击者的试探性转账，用于确认已经取得该钱包的转账权限。

几乎同一时间，以太坊上的币安热钱包 Binance 14 被改为由攻击合约控制。04:24:23，攻击者用一笔交易将 16.15 亿 USDT、16.7 万枚 ETH 及 60 余种代币全部转入新地址；24 秒后，Binance 16 被转走 28,005.6 枚 ETH 和 5,574 万 USDT；04:30:34，Arbitrum 上一个疑似币安热钱包的地址转出 7,456 万枚 ARB；04:41 起，币安 USDC 热钱包分两笔流出 8.23 亿 USDC。Arkham 统计，除 XRP 外，攻击者在 9 条链上通过 141 次转账转移约 60 亿美元，其中 49 亿美元在头 14 分钟内到达，最大一笔单笔交易约 25.3 亿美元。

04:32，链上分析师 Spreek 在 X 上发出首条预警。05:15，币安创始人赵长鹏（CZ）发帖确认遭到黑客攻击；05:29，币安官方发布声明，随后暂停提现。10:25，币安公布初步调查结果，预计总影响约 63 亿美元，已冻结约 30 亿美元，损失由 SAFU 基金和公司资金承担。



上午4:32 · 2026年10月30日

图 2 04:32，Spreek 首发预警：疑似币安遭大规模攻击，钱包资产被整体转入新地址，触发交易的资金来自 Tornado Cash（图源：X @spreekaway）

1.2 损失与冻结口径

各机构统计的时间点、覆盖链和计价时点不同，数字不能直接相加或相减。63 亿减去 30 亿得到的 33 亿美元，只是两个近似值之差，既不等于币安的最终净损失，也不等于攻击者当前持有的资产。

表 1 各方公布的损失与冻结数字

来源	数值	口径说明
币安官方 (10:25)	总影响约 63 亿美元；已冻结约 30 亿美元	官方预计值；SAFU 基金与公司资金承担损失
TRM Labs	63.6 亿美元（按转移时汇率），后续估值 62.3 亿美元	覆盖 10 条链；归因朝鲜 TraderTraitor（高置信度）
Arkham	63 亿美元：约 3 亿 XRP + 9 条链 141 次转账约 60 亿	04:10 至 07:05 完成转移，49 亿美元在头 14 分钟到达
Chainalysis（经路透）	至少 59.12 亿美元	截至 08:30 统计
Watcher.Guru (05:42)	超过 56 亿美元	早期第三方统计，含 14.5 亿美元 BTC
德尔泰链上核对 (11:00)	以太坊、波场冻结 17.59 亿 USDT 与 8.23 亿 USDC	按 Tether、Circle 合约黑名单事件与链上余额统计

数据来源：币安官方公告、TRM Labs、Arkham、Chainalysis（经路透社）、Watcher.Guru、德尔泰链上核对。



图 3 05:42，Watcher.Guru 统计币安被盗资产超过 56 亿美元，各机构口径与时间点不同（图源：X @WatcherGuru）

1.3 事件时间线

表 2 事件关键节点（北京时间，截至 20:00）

时间	事件
10-29 10:28	攻击触发地址 0x7C86...5CA0 部署首个合约；21:51 至 22:24 四次测试调用

时间	事件
04:05–04:09	XRP Ledger 上约 3 亿美元 XRP 最先被转走 (TRM、Arkham)
04:20:00	波场热钱包转出 1 万 TRX 试探
04:20:59	Binance 14 的 EIP-7702 授权交易上链, 含 50 个授权
04:22:45	波场热钱包转出 6.13 亿 USDT
04:24:23	Binance 14 一次性被转走 16.15 亿 USDT、16.7 万 ETH 及 60 余种代币
04:30:34	Arbitrum 上 7,456 万 ARB 转入攻击者主地址
04:34–04:49	3.25 亿 USDT 折价卖出, 换回 122,316 枚 ETH
04:38:47	195,460 枚 ETH 整笔转入存放地址①
04:57–05:00	6,000 万 USDT 存入 Aave 作抵押, 借出 19,762 枚 ETH
05:01:35	Tether 冻结攻击者主地址, 此后 17 分钟内在以太坊上又冻结 7 个下游地址
05:04:59	Circle 冻结主地址上的 8.23 亿 USDC
05:09–05:21	Tether 在波场冻结 3 个地址
06:06:23	Tether 将 Binance 14 本身列入黑名单
08:10:35	Binance 14 自发交易撤销 EIP-7702 委托
08:18:20	Arbitrum 安全委员会以 0x65 交易转走 74,559,805 枚 ARB
10:19	波场地址 TRBd 开始拆分 TRX
10:25	币安公布初步调查: DevOps 工程师笔记本被攻破, 预计总影响约 63 亿美元
13:15	攻击者主地址将 17,260 枚 ETH 转入新地址⑥
14:02	币安表示员工电脑只是攻击起点, 实际过程更复杂, 未发现私钥泄露
14:36	剩余代币卖出所得 7,647 枚 ETH 并入存放地址④
18:15–18:20	波场存放地址 TSp5 分 5 笔转出全部 6.382 亿枚 TRX
18:27	何一: Aave 抵押的 6,000 万 USDT 不在完全冻结范围, 攻击者实际拿走约 4,600 万美元 ETH
19:03	币安披露已预留超过 63.4 亿美元公司资金, 开始为用户回填被盗资产
19:24	币安客服: 提现预计在 45 小时内恢复, 待处理提现已取消
19:45	路透社: 币安正与 FBI、美国特勤局等执法机构合作

数据来源：以太坊、波场、Arbitrum 链上记录；币安、TRM Labs、Arkham、Chainalysis、路透社公开信息。

二 攻击路径：从一台笔记本到 EIP-7702 委托

2.1 官方调查：入口是一台工程师电脑

币安 10:25 的初步说明称，事件可能源于一名 DevOps 工程师的笔记本电脑被攻破，攻击者借此访问了一个服务容器，并提交了未经授权的提款交易；目前未发现钱包私钥泄露的证据。14:02，币安进一步表示，员工电脑遭入侵只是攻击起点，单凭攻破一台设备或利用某位工程师的权限无法完成资金转移，实际涉及更复杂的攻击过程，调查尚未将责任归于任何个人；安全团队正在沿被入侵的电脑追查完整攻击路径，完整的根因报告将随后发布。

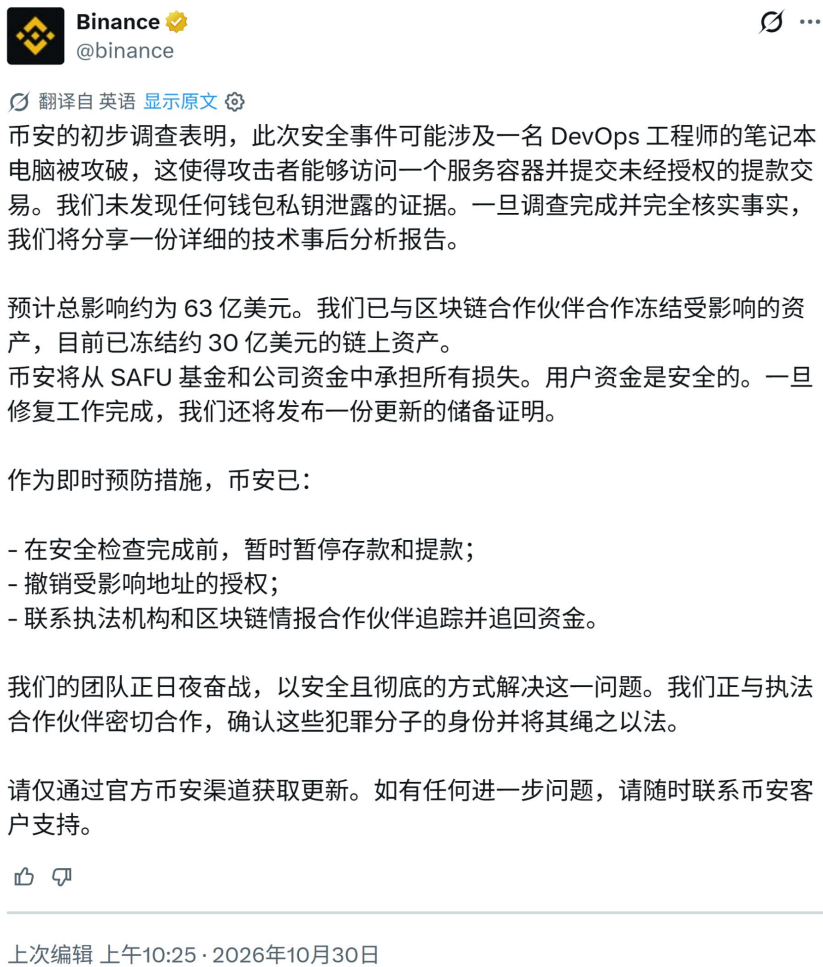


图 4 10:25，币安公布初步调查结果：一名 DevOps 工程师的笔记本电脑被攻破，预计总影响约 63 亿美元，已冻结约 30 亿美元（图源：X @binance）

2.2 提前约 18 小时的布置

链上记录显示，攻击者为此准备了不止一天。攻击触发地址 0x7C86...5CA0 的启动资金来自混币器 Tornado Cash，10 月 29 日 10:28 就已部署第一个合约，当晚 21:51 至 22:24 又对两个合约做了四次调用测试，距离正式动手提前约 18 小时。

2.3 EIP-7702：50 个预签授权，只有 1 个生效

在以太坊上，攻击者用到了 2025 年 5 月 Pectra 升级引入的 EIP-7702 机制。该机制允许普通钱包地址通过签名授权，把账户执行逻辑指向一个智能合约，此后对该地址的调用都按合约代码执行，原本用于批量交易、代付手续费等场景。

04:20:59，攻击触发地址 0x7C86 向 Binance 14 提交了一笔 type-4 交易，交易内塞入 50 个授权，委托目标都是合约 0x63e8...6fAe，签名均可还原为 Binance 14，nonce 从 18,914,824 依次递减至 18,914,775。按协议规则，只有 nonce 与账户当时 nonce 一致的授权才会生效。同一区块里 Binance 14 刚用掉 nonce 18,914,808，因此只有 nonce 为 18,914,809 的那一个授权生效。3 分 24 秒后，攻击合约调用 sweep 函数，开始清扫热钱包。

这组授权说明攻击者在动手前拿到了 Binance 14 对一整段未来 nonce 的签名，用来应对热钱包高频交易造成的 nonce 漂移。签名有效只能说明对应密钥参与了签名，无法从链上区分私钥泄露、签名服务被滥用还是审批流程被操纵，这一点需要币安内部日志才能闭合。慢雾创始人余弦（Cos）也指出，EIP-7702 只是方便攻击者批量清扫热钱包上的代币，机制本身没有问题。

08:10:35，Binance 14 以自身地址发出一笔 type-4 交易，将委托目标改为零地址，撤销了攻击合约的控制权，距授权生效 3 小时 49 分。撤销委托只能阻止后续调用，已经转走的资产和此前的代币授权不会因此恢复。

表 3 Binance 14 的委托与撤销

时间	交易	内容
04:20:59	0xad99...298b	0x7C86 提交 type-4 交易，50 个授权，委托目标 0x63e8...6fAe，仅 1 个生效
04:24:23	0x53bd...e2f3	攻击合约调用 sweep，64 个代币合约地址 + ETH 一次转入主地址
08:10:35	0xafbf...7209	Binance 14 自发 type-4 交易，委托目标改为零地址，撤销委托

数据来源：以太坊链上记录（Blockscout）。完整交易哈希见附录。

2.4 一笔交易转走 64 种代币

04:24:23 的 sweep 调用中列明 64 个代币合约地址。这笔交易将 Binance 14 上的 16.15 亿 USDT、6,260 万 RLUSD、29,934 枚 WBETH、11,372 枚 XAUT（Tether 黄金）、619 万 UNI、2,776 万 USD1、1.98 亿 ENA、7.175 万亿 PEPE、226 万 LINK、12.8 万 AAVE 等资产，连同 16.7 万枚 ETH，一次性转入攻击者主地址 0x5227...2f8c。该主地址此前没有任何交易记录。

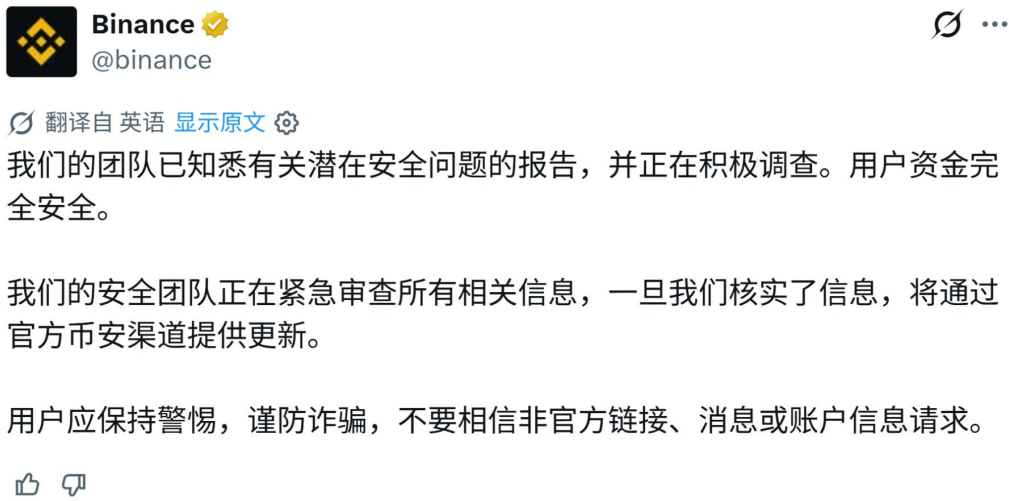


图 5 05:29，币安官方首次发声：团队正在积极调查，用户资金安全，并提醒用户谨防诈骗（图源：X @binance）

2.5 归集仍在运行，攻击者两度返场

攻击发生后一个多小时内，Binance 14 并未被完全切断。05:55，链上研究员 Conor Grogan 指出，币安的充值归集仍在运行，新充值的资产会被持续归集到热钱包，攻击者随即再次转走。05:04:23，

Binance 14 再被转走 392 万 USDT 和 1,699.9 枚 ETH；05:44:11，又被转走 2.004 亿 USDT 和 369.8 枚 ETH，均进入攻击者主地址。

其中 2 亿 USDT 到账时，攻击者主地址已于 05:01:35 被 Tether 列入黑名单，这笔资金入账即被锁定。06:06:23，Tether 将 Binance 14 本身也列入黑名单，币安自己的热钱包与攻击者地址一同进入冻结名单。



图 6 05:55，Conor Grogan：充值归集仍在向热钱包补充资金，攻击者随后再次清空热钱包（图源：X @jconorgrogan）

三 37 分钟窗口期：冻结生效前的三步操作

04:24 资金被转走，05:01:35 Tether 冻结攻击者主地址，05:04:59 Circle 冻结同一地址的 USDC。37 分钟里，7.29 亿 USDT 被折价抛售、抵押借贷和接力转移，换成了没有发行方可以冻结的 ETH 与 TRX。Chainalysis 18:27 发布的调查也印证了这一点：攻击者在约 20 分钟内把 3.25 亿美元被盗稳定币换成价值 2.85 亿美元的 ETH，随后将另外 1.75 亿美元稳定币转往中转钱包，试图赶在冻结前完成转移。

第一步：折价抛售 3.25 亿 USDT

04:30:11，主地址将 5 亿 USDT 转给抛售地址 A (0x9749...C762)。4 分钟后，该地址开始分批出货，9 笔 USDT 分别进入 5 个成交合约，对应的 ETH 由 UniswapX 订单结算合约 (V2DutchOrderReactor) 和另一个订单结算合约分批支付。04:34 至 04:49 的 15 分钟内，3.25 亿 USDT 全部卖出，换回 122,316 枚 ETH。

攻击者在大幅让价出货。按当时 2,315 美元的 ETH 价格计算，3.25 亿 USDT 理论上可换得约 14 万枚 ETH，实际少换约 1.8 万枚。加上另外两批直接在 Uniswap 等资金池砸盘的 USDT，攻击者在冻结前共卖出约 4.35 亿 USDT，换回约 16 万枚 ETH，较市价少换约 2.7 万枚，差价约 6,000 万美元，部分批次的实际成交成本超过每枚 3,000 美元。剩余的 1.75 亿 USDT 于 04:59:11 由抛售地址 A 转给下一个中转地址，2 分 24 秒后，抛售地址 A 被冻结。

第二步：以赃款作抵押，从 Aave 借出 19,762 枚 ETH

04:33:23，主地址将 2 亿 USDT 转给抛售地址 B (0x0Ddf...697E)，该地址先在 Uniswap 等资金池卖出 1,000 万 USDT，换得 3,552 枚 ETH，随后将剩余 1.9 亿 USDT 与这批 ETH 一并转给 0x8d53...639A。

德尔泰追踪发现，0x8d53 并未继续卖币。04:57:59 和 05:00:11，该地址分两笔将 6,000 万 USDT 存入借贷协议 Aave v3 作为抵押，并于 04:59:11 和 05:00:59 通过 Aave 的 WETH 借款网关先后借出 3,271 枚和 16,491 枚 ETH，合计 19,762 枚，目前仍有约 19,762.5 枚 WETH 的浮动利率借款未偿还。05:01:59，0x8d53 将剩余 1.3 亿 USDT 转给下一个地址，48 秒后被 Tether 冻结，此前 12 秒，23,314.5 枚 ETH 已经先行转出。

USDT 可以被发行方冻结，ETH 没有发行方可以冻结。把注定会被冻结的 USDT 抵押出去，换出一笔无法冻结的 ETH，即使抵押品事后被锁定，借出的 ETH 也已转到攻击者手中。币安联合创始人何一 18:27 表示，Aave 中抵押的 6,000 万 USDT 不在完全冻结范围内，攻击者实际拿走约 4,600 万美元的

ETH，这部分抵押物通过执法程序解锁后，还能多追回约 1,400 万美元。Aave 的风险服务商 LlamaRisk 披露后，Aave 也冻结了相关市场的新增借款。

第三步：与冻结令逐秒赛跑的资金接力

05:01:35 起，Tether 沿资金链逐级冻结下游地址。德尔泰比对 Tether 合约的黑名单事件发现，多个地址的最后一笔转出只比冻结早几十秒：

表 4 最后一笔转出与被 Tether 冻结的时间对照

地址	收到 USDT	最后一笔转出	被冻结	结果
主地址 0x5227...2f8c	18.75 亿	04:33:23 转出 2 亿	05:01:35	11.75 亿被冻结
抛售地址 A 0x9749...C762	5 亿	04:59:11 转出 1.75 亿	05:01:35 (差 2 分 24 秒)	已转空
抛售地址 B 0x0Ddf...697E	2 亿	04:52:59 转出 1.9 亿	05:01:47 (差 8 分 48 秒)	已转空
Aave 借款地址 0x8d53...639A	1.9 亿	05:01:59 转出 1.3 亿	05:02:47 (差 48 秒)	6,000 万抵押在 Aave
接力抛售地址 2 0x7Aa4...BFd1	8,000 万	05:11:11 转出 3,000 万	05:12:35 (差 84 秒)	已转空
中转下游 0xAa24...54a0	1.75 亿	—	05:14:59	1.75 亿被冻结
接力中转 3 0xCcBE...A263	3,000 万	05:16:11 转出 3,000 万	05:16:47 (差 36 秒)	已转空
末端地址 0xb171...c8c3	3,000 万	—	05:18:59	3,000 万被冻结

数据来源：以太坊链上记录，Tether 合约 AddedBlackList 事件（Blockscout）。

在这条接力链上，接力抛售地址 1（0x77ED...c3eb）和接力抛售地址 2 又各自在 Uniswap 等资金池卖出约 5,000 万 USDT，所得 ETH 随 USDT 一路向下传递。到末端地址 0xb171 时，3,000 万 USDT 未能及时转出而被冻结，但同一批次的 57,891.8 枚 ETH 已在 05:35:59 转入新的存放地址。

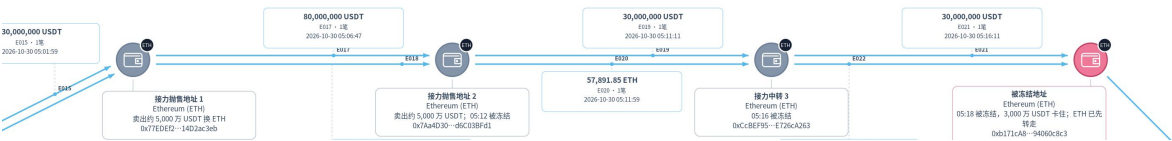


图 7 USDT 与 ETH 沿接力链同步下传，红色节点为被冻结时仍留有 3,000 万 USDT 的末端地址（数据截至 11:00）

各方公布的冻结金额不一致，主要源于统计时间不同：05:15 赵长鹏引用的是 9.71 亿 USDT，05:25 Paolo 公布的是 15.67 亿 USDT。按链上余额统计，以太坊 3 个地址合计冻结 13.80 亿 USDT，波场 2 个地址合计 3.79 亿 USDT，共 17.59 亿 USDT，其中包括 05:44 转入已冻结主地址的 2 亿 USDT。

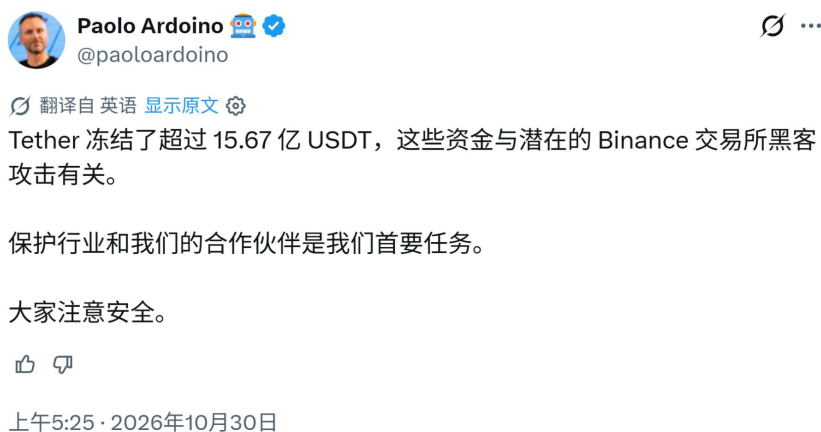


图 8 05:25, Tether CEO Paolo Ardoino: 已冻结超过 15.67 亿 USDT (图源: X @paoloardoino)



图 9 05:18, Circle CEO Jeremy Allaire: 与执法部门协调，已冻结超过 8 亿 USDC (图源: X @jerallaire)

四 Arbitrum 罕见出手：链级权限转走 3,050 万美元

ARB 和 Arbitrum 上的 ETH 都没有发行方可以冻结，这 3,050 万美元被转走，靠的是 Arbitrum 安全委员会的链级权限。

04:30:34，Arbitrum 上一个累计发出超过 850 万笔交易的地址 0xB38e...891D，向攻击者主地址 0x5227...2f8c 转出 74,559,805 枚 ARB。攻击者在 Arbitrum 上使用的是与以太坊完全相同的主地址。

05:29, 主地址在以太坊上给 0x3E2b...32d5 转去 0.5 枚 ETH, 后者两分钟后通过 MetaBridge 跨链, 在 Arbitrum 上备好了手续费; 05:36:30, 7,456 万枚 ARB 被转入 0x3E2b。

08:18:20, 这 7,456 万枚 ARB 从 0x3E2b 转入 Arbitrum 安全委员会指定的冻结地址。Arbitrum 链上记录显示, 这笔交易的发送方是攻击者地址本身, 交易类型却是 Arbitrum 特有的 0x65, 即无需该地址私钥签名的交易类型。攻击者没有签过这笔转账, 资产已经离开了他的钱包。08:19, Arbitrum 官方确认, 安全委员会已转移该地址上的 74,559,805 枚 ARB 和 8,425 枚 ETH, 这些资金只能经安全委员会进一步行动或 Arbitrum DAO 投票才能动用, 两者合计约 3,050 万美元。



图 10 7,456 万枚 ARB 在 Arbitrum 上的流转, 红色节点为安全委员会冻结地址



翻译自 英语 显示原文

Arbitrum 安全委员会已采取紧急行动, 以抢救被困在 Arbitrum One 上与币安漏洞事件相关的地址中的 74,559,805 ARB 和 8,425 ETH。安全委员会在权衡对 Arbitrum 社区及 Arbitrum 治理的安全性和完整性的承诺后采取行动, 而不影响任何 Arbitrum 用户或应用。

经过大量的技术尽职调查和审议后, 安全委员会确定并执行了一种技术方法, 将资金转移至安全位置, 而不影响任何其他链状态或其他 Arbitrum 用户。

截至 2026 年 10 月 30 日时, 资金已成功转移至一个中间冻结钱包。这些资金不再可由原持有地址访问, 只能通过安全委员会的进一步行动或 Arbitrum DAO 治理的投票来移动, 此过程将与相关方协调。



上午8:19 · 2026年10月30日

图 11 08:19, Arbitrum 官方: 安全委员会已采取紧急行动, 转移 74,559,805 枚 ARB 和 8,425 枚 ETH 至冻结钱包 (图源: X @arbitrum)

以太坊主网没有类似机制，攻击者在主网上的 ETH 只能靠追踪资金最终流向的交易所和场外渠道去拦截。链上治理直接处置用户地址中的资产，这一先例此后也会持续引发讨论。

五 资金现状：13.4 亿美元停在哪里（截至 20:00）

表 5 攻击者仍控制的主要资产

资产	数量	估值（美元）	状态
ETH（6 个存放地址 + 主地址）	约 505,622 枚	约 11.29 亿	无发行方可冻结；前三大地址自入账起无转出
TRX（4 个新存放地址 + 拆分地址 TRBd）	约 6.31 亿枚	约 2.15 亿	无发行方可冻结；18:15 起全面移动，持续拆分
合计	—	约 13.4 亿	不含已拆分到数十个新地址的 TRX 与比特币链资产

价格：ETH 2,233 美元、TRX 0.3405 美元（CoinGecko，20:00 前后）。主地址另有约 2,782 万 USD1、1.26 万 XAUT、1,907 PAXG、345 万 FDUSD（合计约 6,100 万美元），发行方具备冻结能力，未计入。

5.1 以太坊：资金向 6 个存放地址集中

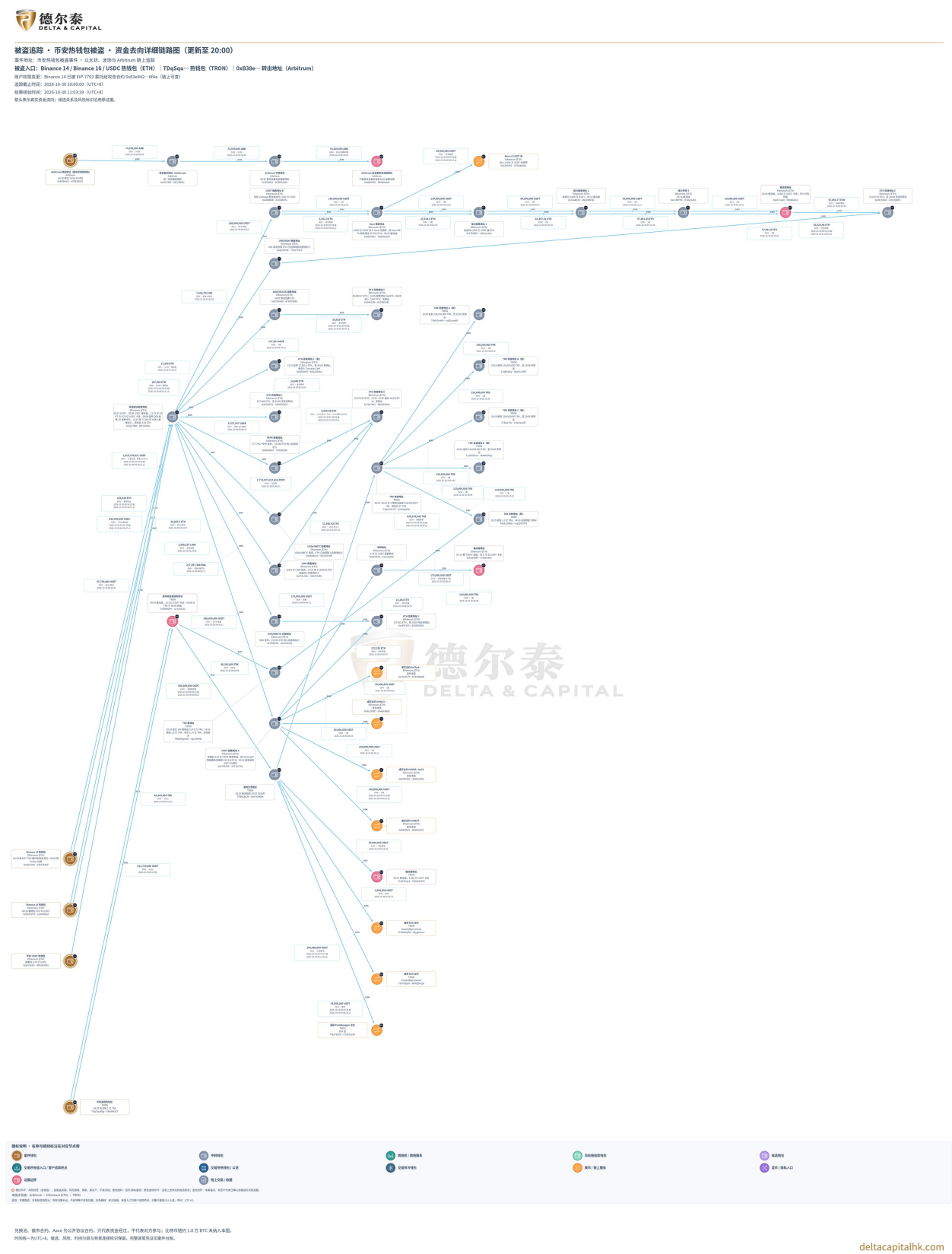
表 6 以太坊存放地址余额（截至 20:00）

地址	ETH 余额	来源与动态
存放地址① 0x8532...43D4	197,460	04:38 主地址转入 195,460 枚，09:14 再转入 2,000 枚；无转出
存放地址② 0xc887...286A	137,602	抛售地址 A 卖币所得 122,310 枚 + ENA 卖出所得 15,292 枚；无转出
存放地址③ 0x897C...8DF3	78,415.25	接力链末端 57,891.77 枚 + UNI 等卖出所得；无转出
存放地址④ 0x5440...C942	40,600.67	AAVE、RLUSD、WLD、RSR、MORPHO 等卖出所得；14:36 再并入 7,647 枚
存放地址⑤ 0x79e7...544A	34,279.69	USDe、WBTC、PEPE 卖出所得；13:31–13:35 并入 LINK、USDe 抛售地址的 14,529 枚
存放地址⑥ 0x03b0...20ea（新）	17,260.1	13:15 由主地址一次转入；无转出，未进入 Tornado Cash
主地址 0x5227...2f8c	约 4.5	08:08 起在 Uniswap 抛售 30 余种代币；11.75 亿 USDT、8.23 亿 USDC 被冻结

数据来源：以太坊链上记录 (Blockscout)。

11:00 之后，以太坊上的资金继续向存放地址归集。13:15，攻击者主地址把 17,260 枚 ETH (约 3,882 万美元) 一次转入新地址 0x03b0...20ea，Arkham 当时提示其可能流向 Tornado Cash，截至 20:00 这笔 ETH 没有任何转出。13:28 至 13:35，原 LINK 抛售地址 (11,560.82 枚)、USDe/WBTC 抛售地址 (2,856.9 枚) 和 PEPE 抛售地址把 ETH 全部并入存放地址⑤；14:17 至 14:20，地址 0xA97b...8d10 在 Uniswap 上连续抛售剩余代币，14:36 把换得的 7,647 枚 ETH 并入存放地址④。

存放地址①②③合计 413,477 枚 ETH，自入账起没有一笔转出。午后这几个地址持续收到大量零额和极小额转账，属于第三方的链上留言与地址投毒。大额 ETH 变现通常要经过混币器、跨链桥或场外渠道，这几个地址的第一笔转出，将是判断追回难度的关键信号。



5.2 波场：冻结前 2.34 亿 USDT 换成 6.38 亿枚 TRX

04:22:45, 6.13 亿 USDT 从币安波场热钱包转入攻击者收款地址 TG5i...zsGi。04:45 和 04:56, 该地址分两笔将 3 亿 USDT 转给分流地址 TPBk...KN4。分流地址随后在 24 分钟内, 将 1.99 亿 USDT 分 13 笔转入一个波场去中心化交易所合约, 另将 3,300 万和 200 万 USDT 转入两个兑换合约, 换得的 TRX 于 04:56:12 和 05:42:42 两次转入新地址 TSpe5...yZ8A, 合计 638,190,941 枚。

Tether 在波场的冻结同样慢了一步。05:09:12 冻结收款地址时, 地址内仍有 3.13 亿 USDT; 05:16:18, 分流地址将最后 6,599 万 USDT 转给 TCzB...Y62, 5 分钟后该地址被冻结; 05:20:57 分流地址本身被冻结时, 账上的 USDT 已经全部转出。08:06:09, 收款地址上剩余的 4,638 万枚 TRX 被整笔转入一个 3 秒前才激活的新地址 TRBd...PRki。

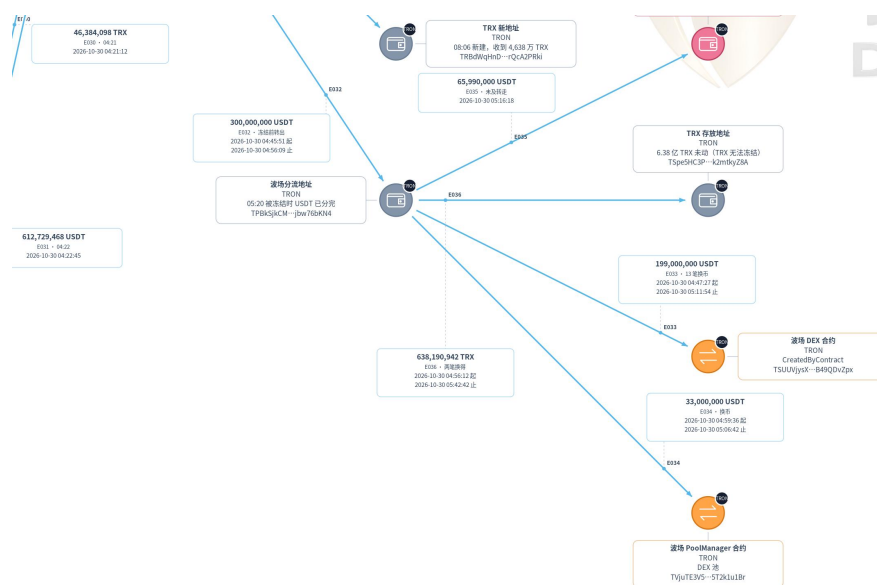


图 13 波场部分：6.13 亿 USDT 中 3.79 亿被冻结，2.34 亿换成 TRX 后转入 TSpe5（数据截至 11:00）

5.3 18:15 之后：6.38 亿枚 TRX 全部离开存放地址

德尔泰追踪发现, 持有 6.38 亿枚 TRX、此前一直未动的 TSpe5 地址, 在 18:15 至 18:20 的 5 分钟内分 5 笔转出全部余额, 现仅剩约 37 枚 TRX。其中 1.2 亿枚先进入一个中转地址, 18:20:48 再转入拆分地址 TRBd; 其余 4 笔共 5.182 亿枚分别停在 4 个新地址, 截至 20:00 没有继续转出。

表 7 TSPe5 的 5 笔转出 (北京时间)

时间	接收地址	TRX 数量	后续
18:15:21	TAk1...UFYP5 (中转)	120,000,000	18:20:48 全部转入 TRBd
18:18:09	TL2F...NcfVwj	120,000,000	未动
18:18:42	TCBA...63ao1fk	120,000,000	未动
18:19:24	TJaj...FaLLHKT	120,000,000	未动
18:20:18	TKkH...vdd1xvw6K	158,200,900	未动

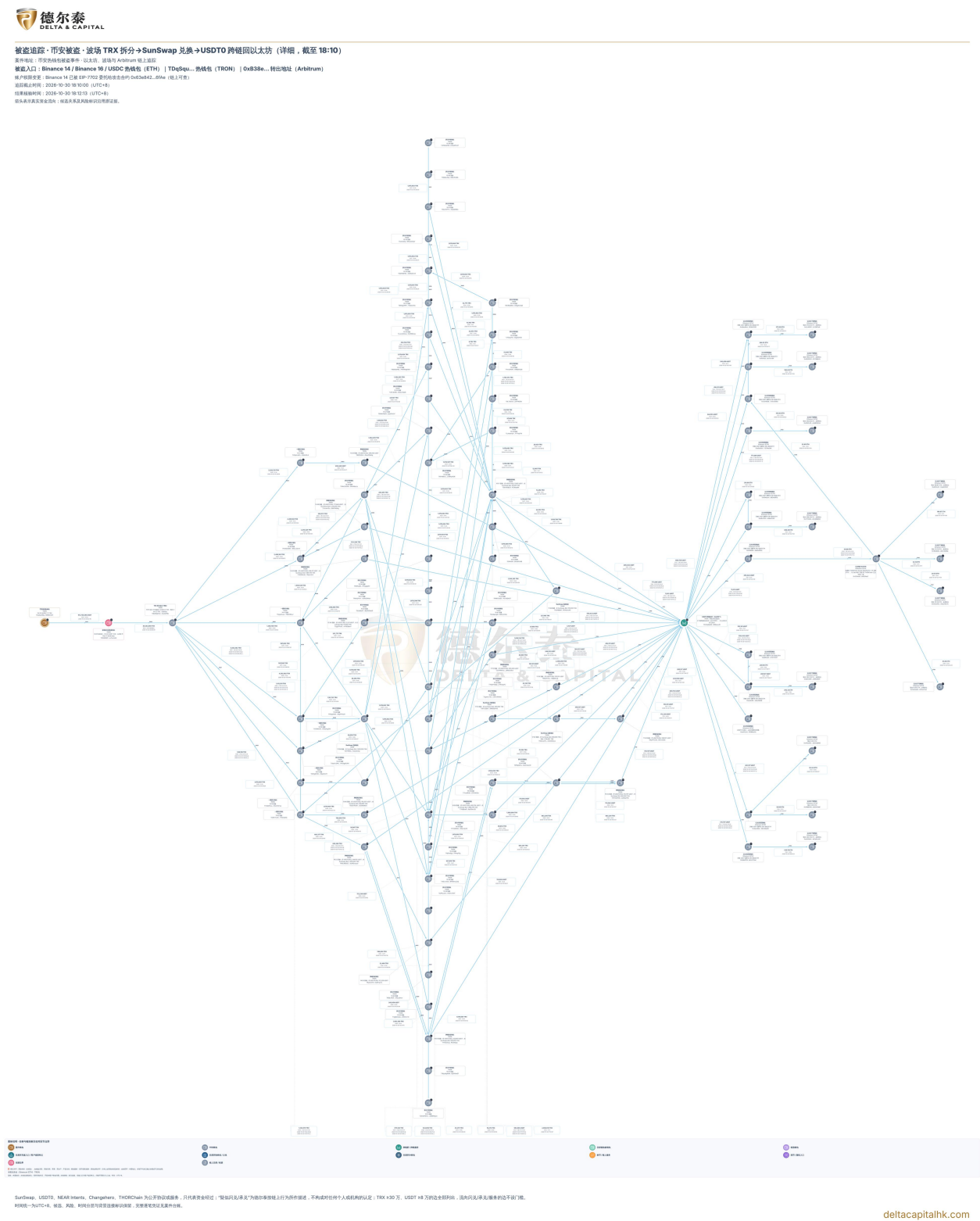
数据来源：波场链上记录 (TronGrid)。完整地址与交易哈希见附录。

5.4 TRBd：拆分、SunSwap 兑换与 USDT0 跨链回流

TRBd 自 10:19 起持续拆分，截至 20:00 已分 145 笔转出 5,373 万枚 TRX，18:20 收到 1.2 亿枚后余额回升至约 1.13 亿枚，拆分仍在进行。被拆出的 TRX 先进入 13 个一级拆分地址和 41 个拆分中转地址，这些地址大多在 10:19 之后才新建。

截至 18:10，其中约 1,174 万枚 TRX 在 SunSwap 上换成 USDT，再由 14 个跨链发起地址通过 USDT0 的跨链合约分 27 笔转回以太坊，合计 4,043,953 USDT；到达以太坊的 9 个回流地址收到 USDT 后随即在 DEX 换成 ETH。另有少量 TRX 和 USDT 流向疑似闪兑、场外承兑与兑换服务：5 个疑似 TRX→USDT 闪兑地址在 10 月 12 日同一分钟内激活，其中 1 个在 17 天内向币安充值约 371 万美元；疑似场外承兑地址 TZG47 现持约 692 万 USDT，311 天内向 Bitget 充值约 4,887 万美元；此外还有 Changehero (混合 KYC 兑换服务) 和 NEAR Intents 跨链热钱包。

这条路径对冻结方并非全无机会：经 USDT0 跨链的是 Tether 可冻结的 USDT，闪兑与承兑地址又与币安、Bitget 等交易所存在充值往来。Chainalysis 18:09 也观察到，攻击者正在用自动化手段在短时间内执行数千笔交易，反复在地址之间循环资金，常常把资金送回序列中较早出现的地址。慢雾 MistTrack 则发现，被盗 TRX 在转移中经 Bitget Wallet 跨链兑换流入一个曾被 Phemex 黑客使用过的地址，Bitget Wallet 随后表示已将识别出的涉案地址列入黑名单并限制相关服务。



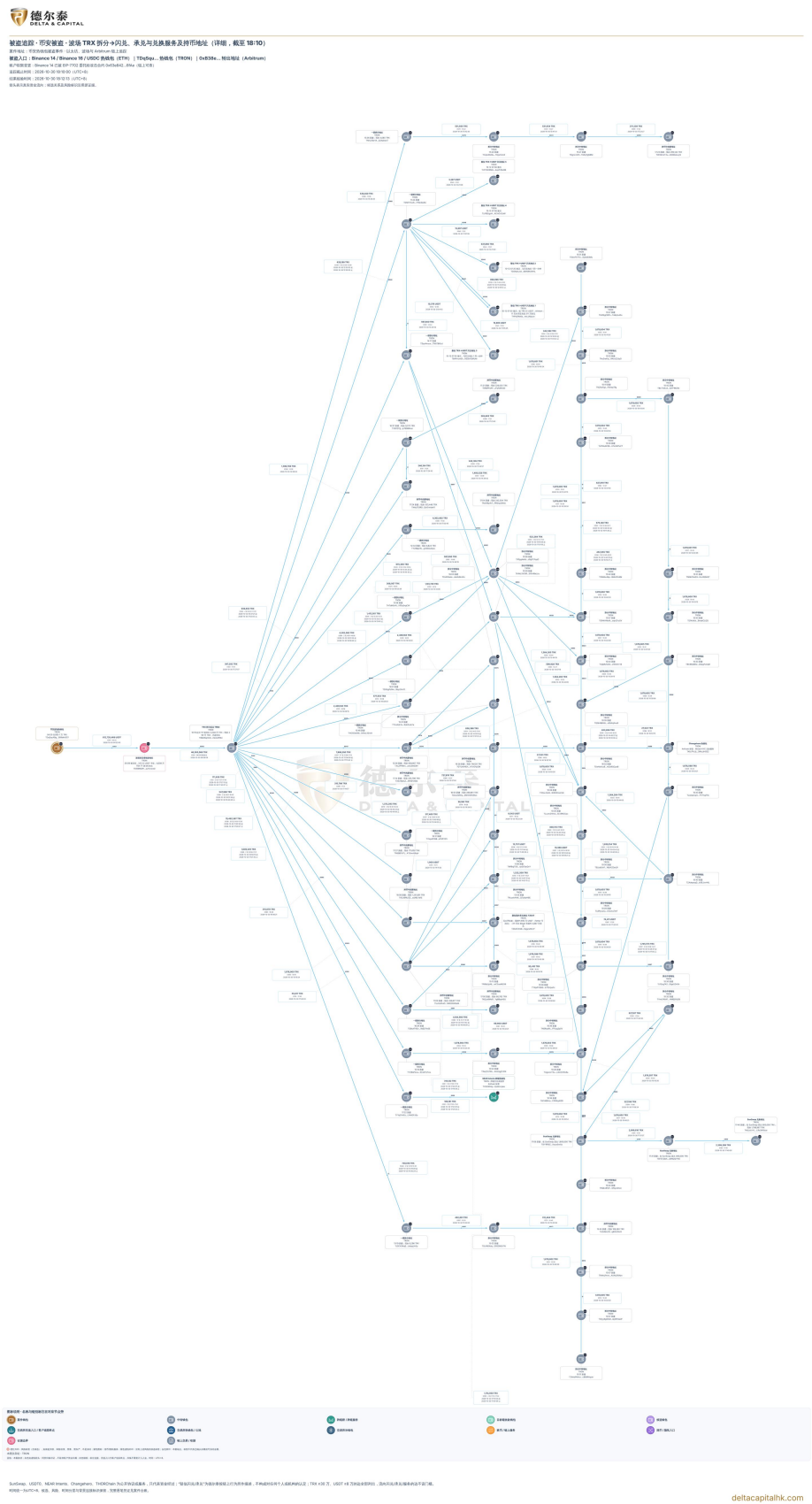


图 15 波场 TRX 拆分后的闪兑、场外承兑与兑换服务及持币地址（数据截至 10 月 30 日 18:10）

六 外部响应、归因与市场影响

6.1 冻结与协同处置

表 8 各方冻结与处置情况

参与方	已公开的处置	说明
Tether	冻结超过 15.67 亿 USDT (05:25)	链上合计 17.59 亿 USDT 被锁在以太坊、波场 5 个地址
Circle	冻结超过 8 亿 USDC (05:18)	主地址 8.23 亿 USDC 于 05:04:59 被冻结
Arbitrum 安全委员会	74,559,805 ARB 与 8,425 ETH 转入冻结地址	约 3,050 万美元；动用需委员会或 DAO 投票
World Liberty Financial / BitGo	据何一，冻结约 2,700 万 USD1 与约 200 万美元 WLF1	主地址持有约 2,782 万 USD1
Ripple	正在冻结攻击者持有的 RLUSD (06:08)	攻击者曾持有 6,260 万 RLUSD，部分已卖出
Syntheticx	通过 DAO 追回约 841 万枚 SNX，存放于协议多签	已通知币安，可按要求返还
USDT0	一度暂停以太坊与波场之间的跨链转账，已恢复	防止赃款经跨链转移
Bitget Wallet	将识别出的涉案地址列入黑名单，限制相关服务	与币安安全团队协作追踪
Aave	冻结相关市场的新增借款	还款、提取与清算照常

数据来源：各方 X 官方账号、吴说、路透社公开信息。



翻译自 英语 显示原文

Ripple 正在密切关注涉及 Binance 及其攻击者 RLUSD 持仓的潜在漏洞报告，我们正在积极冻结受影响的资金。我们正在与相关方协调，并随时准备支持任何调查和适当行动，以保护用户安全。



上午6:08 · 2026年10月30日

图 16 06:08, Ripple 高管 Jack McDonald: 正在积极冻结攻击者持有的 RLUSD (图源: X @_JackMcDonald_)

6.2 攻击者归因

TRM Labs 以较高置信度将此次攻击归于与朝鲜相关的 TraderTraitor。链上侦探 ZachXBT 判断攻击者为朝鲜 Lazarus 旗下的 TraderTraitor，并发现当日中午，本次被盗资金与上月 Bitget 3.88 亿美元被盗赃款经 THORChain 汇入同一地址后发生混合，两起事件很可能由同一攻击者实施。Lookonchain 也认为，币安、Bybit 与 Bitget 三起被盗背后可能都与 Lazarus 有关。上述均为研究机构与链上分析人士的判断，尚无执法机构的正式认定。据路透社 19:45 报道，币安正与包括 FBI 和美国特勤局在内的全球执法机构合作。



翻译自 英语 显示原文

突发: Arbitrum 安全委员会已执行一笔交易，冻结了来自 Binance 漏洞的约 3050 万美元。

感谢所有其他参与的签名者。

攻击者地址

0x3E2bf1ac6bf0934BBba6456C341c2EcbCED632d5

交易哈希:

0xb69c81774f507d46ce776aeaed8b4d31df96dd66ce6fd05073481011835355d6



上午8:14 · 2026年10月30日

图 17 08:14, ZachXBT: Arbitrum 安全委员会已执行交易，冻结约 3,050 万美元，并公布攻击者地址与交易哈希 (图

源: X @zachxbt)

6.3 币安的应对与用户安排

币安在 06:33 暂停提现，08:13 一度暂停存款。12:36，币安宣布充值已恢复正常，提现预计在 48 小时内恢复；19:24，币安客服更新为预计在 45 小时内恢复，并表示待处理的提现已被取消，用户可通过 P2P、法币提现或交易处理资金。

赔付方面，CZ 10:23 表示用户资金安全无虞，何一 11:51 回应称会追到底。19:03，币安披露已预留超过 63.4 亿美元公司资金用于弥补损失，其中约 50 亿美元已以受影响的相同代币形式持有，其余正通过公开市场和场外交易买入；何一 19:07 表示，正在通过场外和场内交易买入完全匹配数量的被盗山寨币。18:55，币安宣布已开始为用户回填受影响的资产。修复完成后，币安将发布更新的储备证明。



图 18 06:23，CZ 回应：损失可能比这个数字稍高，但会覆盖（图源：X @cz_binance）

6.4 市场影响

事件发生后，加密市场明显回撤。截至 20:00，BTC 报 77,394 美元，24 小时下跌 3.5%，盘中一度跌至 7.7 万美元附近；ETH 报 2,233 美元，下跌 4.0%，一度跌破 2,200 美元；BNB 报 699 美元，下跌 5.4%。印度交易所 CoinDCX 以一家全球流动性提供商受影响为由，将期货业务临时调整为只减仓模式。Ballet 创始人 Bobby Lee 接受彭博社采访时表示，被盗的比特币大概率已无法追回。CZ 则提到，当日传统金融市场同样大幅下跌，市场波动不应全部归因于此次攻击。

价格数据来源：CoinGecko，20:00 前后报价，仅反映截止时点。

七 公告之外：投毒、留言与清仓式抛售

7.1 攻击者地址同样遭遇地址投毒

Spreek 首发预警附带的截图中，攻击者主地址的交易记录里出现了一笔来自 0x9749F766...C762 的转账。真正的抛售地址 A 是 0x9749292D...C762，两者开头和结尾完全相同，只有中间字符不同。攻击者 04:29 向抛售地址 A 转入 0.5 枚 ETH 作为手续费，不到一分钟，仿冒地址的转账就已出现。链上还出现了一个显示名称为 USDT 的假代币，伪造出主地址向另一个仿冒的 0x9749...c762 地址转出 5 亿枚 USDT 的记录，数额与真实转账完全一致。

7.2 二十余条链上留言

被盗后的几个小时内，攻击者主地址陆续收到约二十条链上留言，内容包括直接索要 5 万美元、引用圣经经文、推广各类代币，也有人留下 Funds are UNSAFU 一句，调侃币安过去常用的 Funds are SAFU 口号。截至 20:00，币安尚未在链上向攻击者喊话或公布白帽赏金。

7.3 山寨币清仓式抛售

06:48，Lookonchain 提醒攻击者正在链上卖出 PEPE、UNI、LINK 等代币换取 ETH。两个多小时后，这些代币已全部卖完，7.77 万亿枚 PEPE 换得约 14,049 枚 ETH，PEPE 价格随之下跌 12.33%；33.8 亿枚 RSR 在 08:53 至 09:08 间全部兑换为 1,856 枚 ETH。08:08 起，主地址又在 Uniswap 上抛售 ZAMA、FET、PENDLE、CRV、SHIB、EIGEN、LDO 等 30 余种长尾代币，午后剩余代币继续由 0xA97b 等地址卖出并归集到存放地址。



图 19 06:48, Lookonchain: 币安黑客正在链上抛售 PEPE、UNI、LINK 等代币换取 ETH (图源: X @lookonchain)

八 德尔泰观察

本次各方的响应速度已经相当快：Tether 37 分钟内出手，17 分钟内在以太坊上连续冻结 8 个地址；Arbitrum 安全委员会在 4 小时内从攻击者地址转走 3,050 万美元，合计冻结约 30 亿美元。即便如此，仍有 7.29 亿 USDT 在冻结生效前被换成 ETH 和 TRX，截至 20:00 仍有约 13.4 亿美元资产没有任何机构能够冻结，且波场一侧已在 18:15 后全面动身。币安用户、提现暂停期间急于转移资产的投资者，以及自行保管资产的持币人，需要注意以下几点。

1. 提现恢复前后，警惕各类钓鱼诈骗

交易所遭攻击、提现暂停、官方承诺赔付，这三个条件叠加，正是诈骗团伙最常利用的时机。未来几天，以币安赔付登记、SAFU 补偿领取、资产迁移验证为名的链接、短信和私信可能大量出现，部分还会冒充币安客服或安全团队主动联系用户。任何要求连接钱包、输入助记词、签名授权或先行转账验证的信息，均应视为诈骗。

2. 每次转账前，逐位核对完整地址

坐拥数十亿美元赃款的攻击者，在被盗后几分钟内同样成为地址投毒的目标。提现恢复后，用户集中转出资产时，交易记录中同样可能混入首尾相同的仿冒地址。转账前应逐位核对完整地址，避免直接从历史记录中复制；大额转账先做小额测试，确认到账后再转出余额。

3. 冻结要抢在兑换之前，追踪要盯住回流节点

USDT、USDC 被盗后存在冻结机会，但窗口期以分钟计算；一旦被换成 ETH、TRX、BTC 等没有发行方的资产，冻结途径基本失效。本案波场资金在拆分后又经 SunSwap 换回 USDT、通过 USDT0 跨回以太坊，并流向与交易所有充值往来的闪兑和承兑地址，这些节点重新出现了可冻结资产和可协查的交易所账户。个人用户遭遇被盗后，应第一时间保存交易哈希和相关钱包地址，委托专业机构并报案，尽快启动链上追踪，在资金被兑换、混币或跨链之前，以规范的调查报告向稳定币发行方和相关交易所申请冻结。德尔泰可提供链上追踪、资金流向分析与证据报告等服务。

冻结键按得再快，也快不过一个提前演练了 18 小时的攻击者；能把损失追回来的，是盯住每一个回流节点的耐心。

如需案件咨询或合作沟通，可通过官方 X 账号 @delta_team_hk、官网 deltacapitalhk.com 或公众号后台留言联系我们。

附录 关键地址与交易

表 9 关键地址（完整）

角色	链	地址
Binance 14 热钱包	ETH	0x28C6c06298d514Db089934071355E5743bf21d60
攻击触发与授权提交地址	ETH	0x7C8601d4645B93CEA45F71e118a729332e6b5Ca0
EIP-7702 委托合约	ETH	0x63e842B054bd624a465454D533c33F573e9C6fAe
攻击者主地址（ETH / Arbitrum）	ETH	0x5227f603C1eE34CE3C06eFe6477003BDfCCB2f8c
存放地址①	ETH	0x8532FA14ACAf483729C449b8458aedDb900543D4
存放地址②	ETH	0xc887aF690E0301CD4edBbCe8F8d31b4EC65B286A
存放地址③	ETH	0x897C80d1a9729E94460e2Bd93178bD5215158DF3
存放地址④	ETH	0x54401f80Da97893a15D43566184635B6674BC942
存放地址⑤	ETH	0x79e70d139fC05AA75F75611fDF2680E9952B544A
存放地址⑥（新）	ETH	0x03b0eE5d82990cFF1bDa48651AC3e436d1a020ea
Aave 借款地址	ETH	0x8d53903625b8e839b9DF4bd28B0EFb1CD6b8639A
Arbitrum 中转地址	ARB	0x3e2bf1ac6bf0934bbba6456c341c2ecbcd632d5
原 TRX 存放地址	TRON	TSpe5HC3PRD2svJcr1YoGszhHk2mtkyZ8A
TRX 拆分地址	TRON	TRBdWqHnDVSZCVGfgHdKFLQPirQcA2PRki
TRX 新存放地址 A	TRON	TKkH2vH6kyi2QKcMbqym53WMuvdd1xvw6K
TRX 新存放地址 B	TRON	TJajtPqDqUGh1SrIj8ugHoSXBVpaFLLHKT
TRX 新存放地址 C	TRON	TCBAz7itvtX5CjBzVMPQdrbwQLN63ao1fk
TRX 新存放地址 D	TRON	TL2F4GhnaFVZBZPncHYjwfYZFW44NefVwj
TRX 中转地址	TRON	TAk1xJNWuBYvJHLsUiBFLeuK6xvpQUFYp5

表 10 关键交易

时间	链	交易哈希	内容
04:20:59	ETH	0xad99264d5532ae0dd04b2004eebda05f25657e70dacb764f7ac8d4ccd051298b	EIP-7702 授权 (50 个)
04:24:23	ETH	0x53bd38b816c23e74134786c29a8c18d792777998a3b9326047b583100e88e2f3	sweep, 64 种代币 + ETH
08:10:35	ETH	0xafbf94c92a8d749988411669fa14d4f8866d9b4420b4ebd299f28e958dac7209	撤销委托
04:30:34	ARB	0xa18e57027dae90de066ac093bbb4ac3d63598accbe5175cdf4195c686462edff	7,456 万 ARB 转入主地址
08:18:20	ARB	0x75e81a231a86e26a61e22dd2e6521504873a71a7ac1b2143c06e52796ceeedb6	0x65 交易, ARB 转入冻结地址
18:15:21	TRON	9d0904db84e640d37e9fee8badef0883043db77f5bf9c87ca76e220e0c35c487	TSpe5 → Tak1, 1.2 亿 TRX
18:18:09	TRON	16585e9664a0e7e74d67cae2ecdc9869ec9a84a287dc078a12d34ca078c0d1	TSpe5 → TL2F, 1.2 亿 TRX
18:18:42	TRON	037428516b343a326157ae75495ad3227b43e4a4cb0c8c3837e849d7a18d556e	TSpe5 → TCBA, 1.2 亿 TRX
18:19:24	TRON	3db47d891cc211c300f9ba1aec264bfca8f9c32fbe220c411f30789a31ac8370	TSpe5 → TJaj, 1.2 亿 TRX
18:20:18	TRON	aff887c4be7cd52eb8905899fc9596eaa9c49dea59129519ce25d7c69762334	TSpe5 → TKkH, 1.582 亿 TRX
18:20:48	TRON	0ae2b5a4e1c8849d09e16db5a4dd9d90f7224c3b996a80ccad113bd5b81acd39	Tak1 → TRBd, 1.2 亿 TRX

声明

本文为 [德尔泰 Delta] 原创或编译。未经授权，禁止转载或摘编。如需转载，请后台留言联系我们。

本报告根据公开信息和链上数据整理，链上数据截至 2026 年 10 月 30 日 20:00（北京时间），此后资金可能继续变动；以太坊、波场与 Arbitrum 为德尔泰逐笔核对范围，比特币网络约 1.8 万枚 BTC 及 XRP 等其他链的资金去向引用第三方统计，未纳入 13.4 亿美元的统计；波场拆分、兑换与跨链回流的详细路径数据截至 18:10；资产价格按 20:00 前后 CoinGecko 报价计算；Arbitrum 转出地址 0xB38e...891D 的身份为德尔泰根据链上行为所作判断；攻击者身份为 TRM Labs、ZachXBT 等机构与分析人士的判断，尚无执法机构认定；兑换池、成交合约、Aave、SunSwap、USDT0 及各类兑换服务为公开协议或服务，仅表示资金经过，不代表相关方参与；EIP-7702 授权的链上分析只能说明签名与执行情况，无法据此认定私钥是否泄露；事件原因、损失金额与赔付安排以币安及相关方正式披露为准；文中地址标签为德尔泰根据链上行为所作的描述，不构成对任何个人或机构的认定；本报告不构成任何投资建议、交易建议或收益承诺。

资料来源

Binance 官方 X (@binance、@binancezh、@BinanceHelpDesk)、CZ (@cz_binance)、何一 (@heyibinance)、Tether CEO Paolo Ardoino (@paoloardoino)、Circle CEO Jeremy Allaire (@jerallaire)、Ripple 高管 Jack McDonald

(@_JackMcDonald_)、Arbitrum 官方 (@arbitrum)、ZachXBT (@zachxbt)、余弦 (@evilcos)、Arkham (@arkham)、Chainalysis (@chainalysis)、Lookonchain (@lookonchain)、Spreek (@spreekaway)、Conor Grogan (@jconorgrogan)、Watcher.Guru (@WatcherGuru)、吴说 (@wublockchain12)、Ai 姨 (@ai_9684xtpa)、慢雾 MistTrack、TRM Labs 事件分析；路透社、彭博社报道；Aave 治理论坛 LlamaRisk 披露；GCSA 全球网络安全联盟独立取证报告；以太坊链上数据 (Blockscout, 含 Tether、Circle 合约黑名单事件)、波场链上数据 (TronGrid)、Arbitrum 链上数据 (Arbitrum One RPC)；价格数据 (CoinGecko)。

关于我们

德尔泰是一家专注于区块链法证分析、链上追踪、SOW/SOF/KYT 分析以及合规咨询沟通的安全专业机构。

团队由持证法律专家与资深链上数据工程师组成，为全球有需求的客户提供平台账户解限支持、被盗被骗资产追踪与追回、链上调查与证据报告、案件材料与跨境协作、钱包恢复与安全支持（后台留言获取专业支持）。

Delta&Capital: Restoring Liquidity, Preserving Value.

德尔泰：修复流动性，保全资产价值。



德尔泰

DELTA & CAPITAL

平台解限 · 资产追踪 · 链上法证 · 资产追回

1000+

成功结案

37+

覆盖司法辖区

\$85M+

恢复资产规模

24h

最快解决记录

区块链安全服务

BLOCKCHAIN SECURITY SERVICES



平台账户解限支持
PLATFORM ACCOUNT
UNLOCK SUPPORT



被盗被骗资产追踪
与追回
ASSET TRACING
& RECOVERY



链上调查与证据报告
ON-CHAIN INVESTIGATIONS
& EVIDENCE REPORTS



案件材料与跨境协作
CASE DOCUMENTATION
& CROSS-BORDER
COORDINATION



钱包恢复与安全支持
WALLET RECOVERY
& SECURITY SUPPORT

 deltacapitalhk.com