

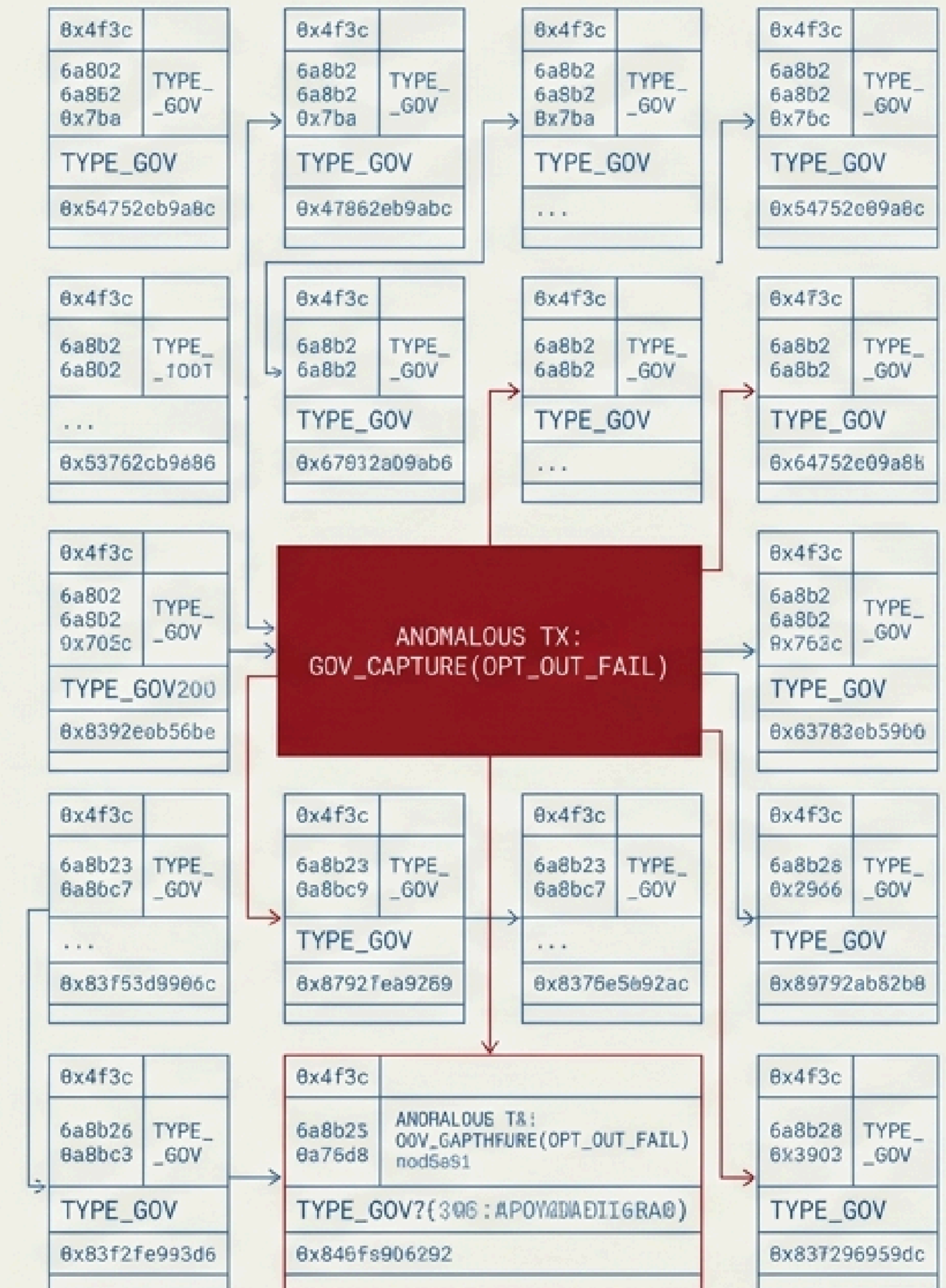


El Ingenio y la Inacción

La captura de gobernanza de Term Finance: cuando la inacción se convierte en el vector de ataque

El Hackeo que no fue un Hackeo: La Captura de Term Finance

Cómo un diseño de gobernanza 'Opt-Out' costó \$8.5 Millones sin romper un solo contrato inteligente.



Impacto Financiero	Vector del Incidente
~\$8.5 Millones 68% del TVL (Total Value Locked) de los vaults afectados volatilizado.	Exploit de Gobernanza Abuso malicioso de reglas "Veto/Opt-out" legítimas del sistema.
Integridad del Código	Estado de Respuesta
0 Vulnerabilidades Contratos operaron según diseño. Auditorías intactas. Cero ataques de reentrancy.	Cierre Irreversible Term Meta Vaults clausurados. Protocolo base 100% seguro; retiros habilitados.

El Cambio de Paradigma: Anatomía de la Amenaza

	Exploits Clásicos	El Caso Term Finance
Mecánica de Ejecución	Bugs de código (Reentrancy, manipulación de precios de oráculos).	Reglas legítimas de los contratos usadas con intención maliciosa.
Ventana de Visibilidad	Transacciones atómicas/instantáneas en un solo bloque.	Propuesta pública on-chain, visible e inactiva durante días.
Línea de Defensa Crítica	Auditorías de código y validación formal.	Participación activa de la comunidad (que falló por apatía).

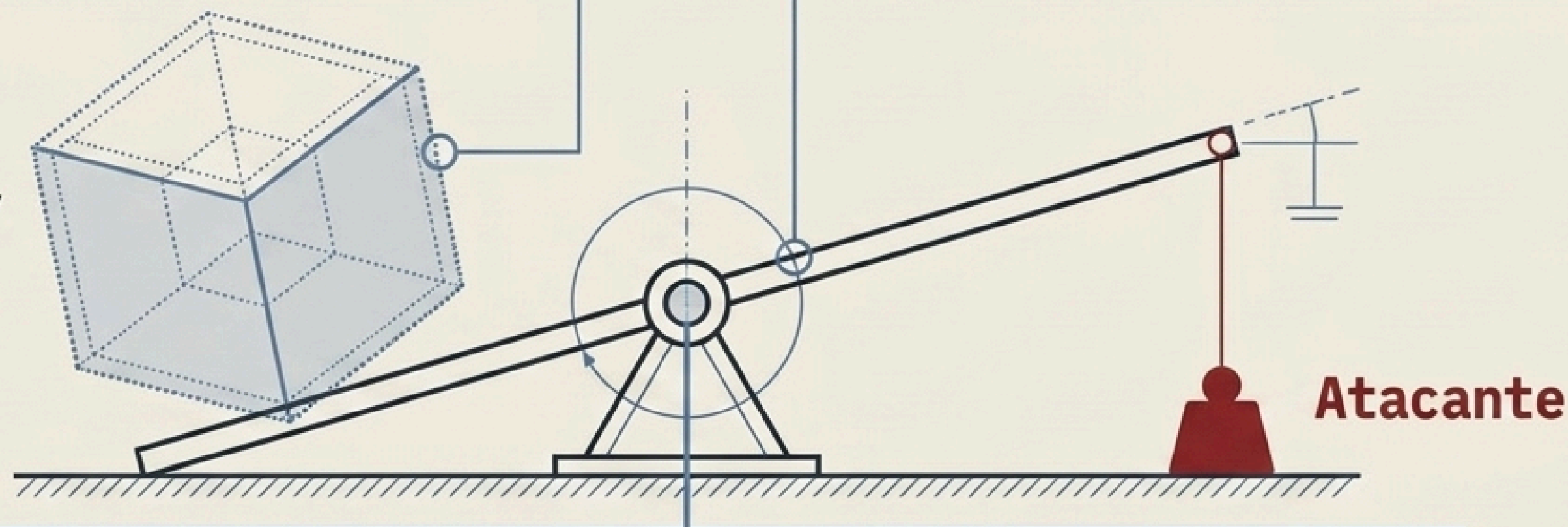
TAKEAWAY: Las auditorías de contratos inteligentes no ofrecen ninguna **protección contra la apatía** de los votantes en la gobernanza on-

El Eje del Fallo: Gobernanza "Opt-Out"

El Diseño Original: Pensado para "curators" que requerían cambiar parámetros rápidamente.
Regla fundamental: **La inacción equivale a la aprobación.**

El Defecto Sistémico: Los umbrales mínimos para proponer eran críticamente bajos (fracciones de centavo en USDC vaults).

Inacción de LPs /
Cero Votos



El Resultado Matemático: Ante la ausencia total de vetos, una posición de capital estadísticamente igual a \$0.00 controló el **100% del poder de decisión** en los vaults afectados.

Fase 1: Preparación e Infiltración

El Fondeo

Posicionamiento Inicial

Origen: 2 ETH extraídos de Tornado Cash.

División: 1 ETH por cada wallet operada por el atacante.

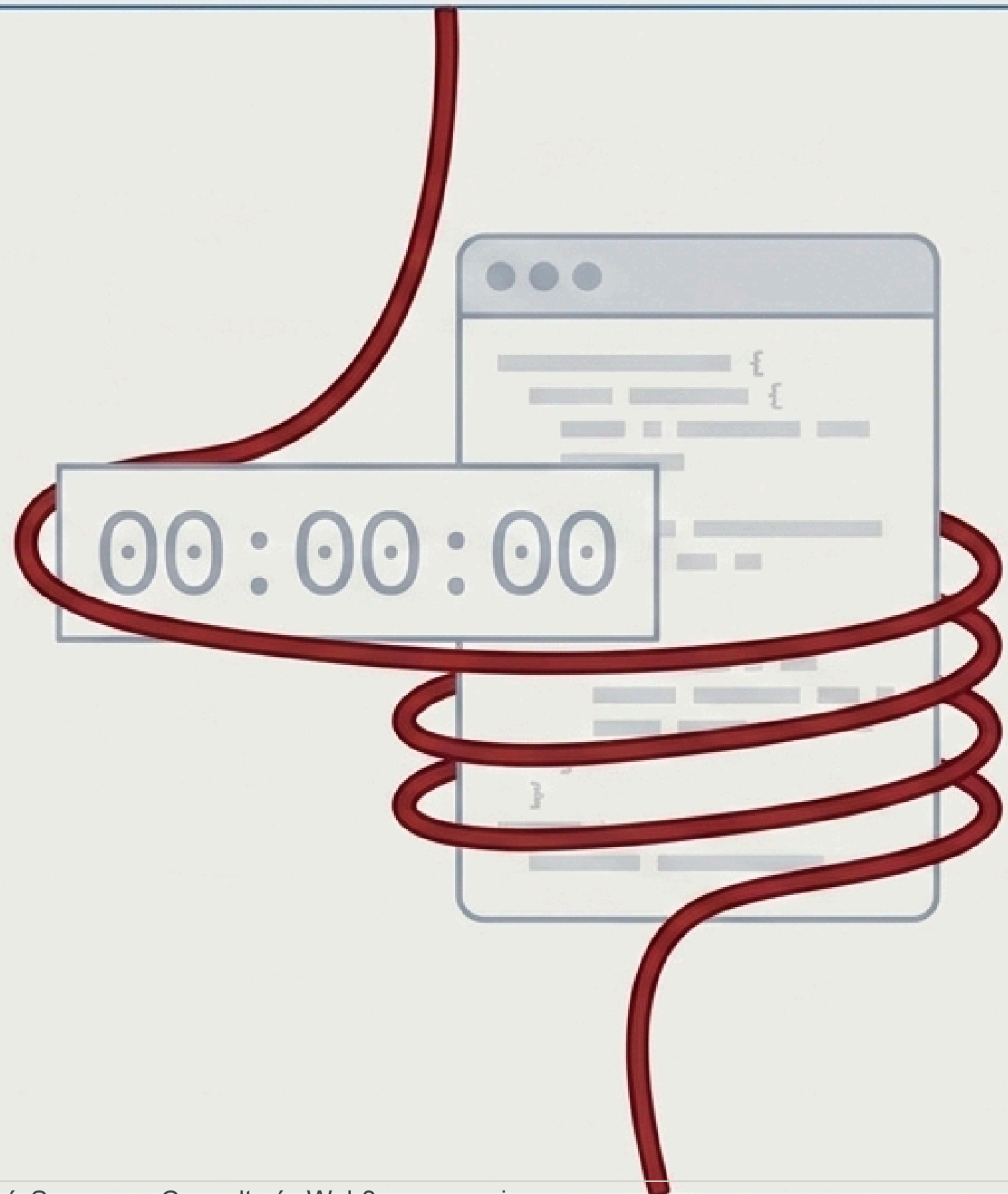
A. ETH Meta Vault:
Depósito de ~0.5 ETH.

Obteniendo apenas el 0.017% del supply total de tmvETH.

B. USDC Vaults:
Depósitos minúsculos minúsculos (orden de centavos), logrando el 100% del poder de voto efectivo.

Insight: El atacante compró los “derechos de administrador” del protocolo por menos del costo de un café.

Fase 2: La Trampa a Plena Vista



El Cebo (Propuesta Maliciosa)

Mecánica de Engaño: Estilo de veto negativo. "Vota SÍ para vetar el cambio. Si no hay votos, el cambio se ejecuta automáticamente."

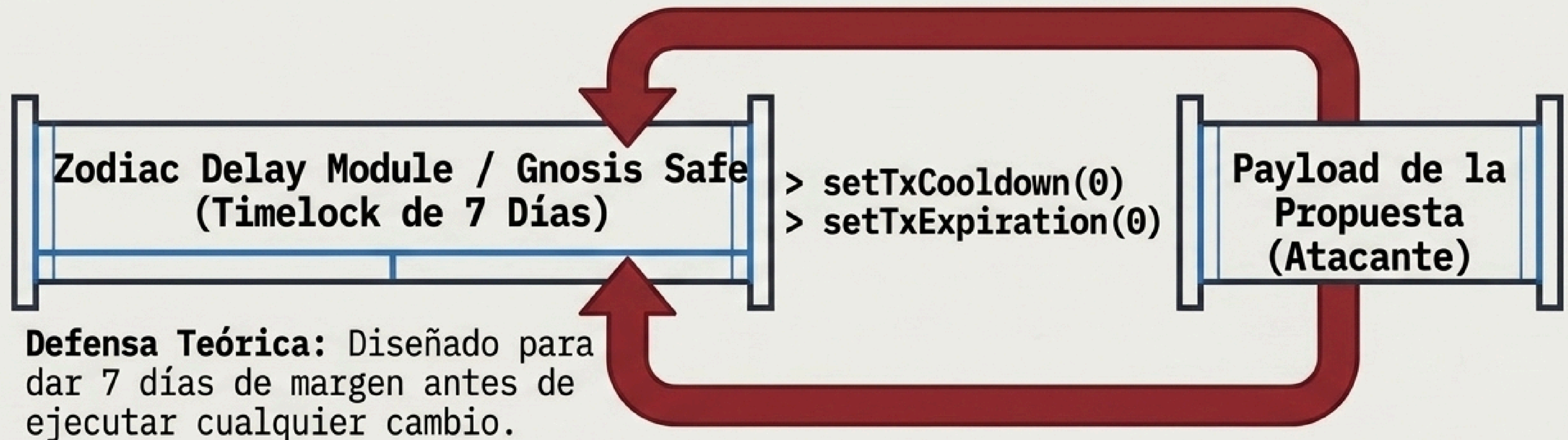
El Factor Tiempo

Estado: Las propuestas permanecieron públicas on-chain durante varios días sin interrupción.

0.00% de Participación

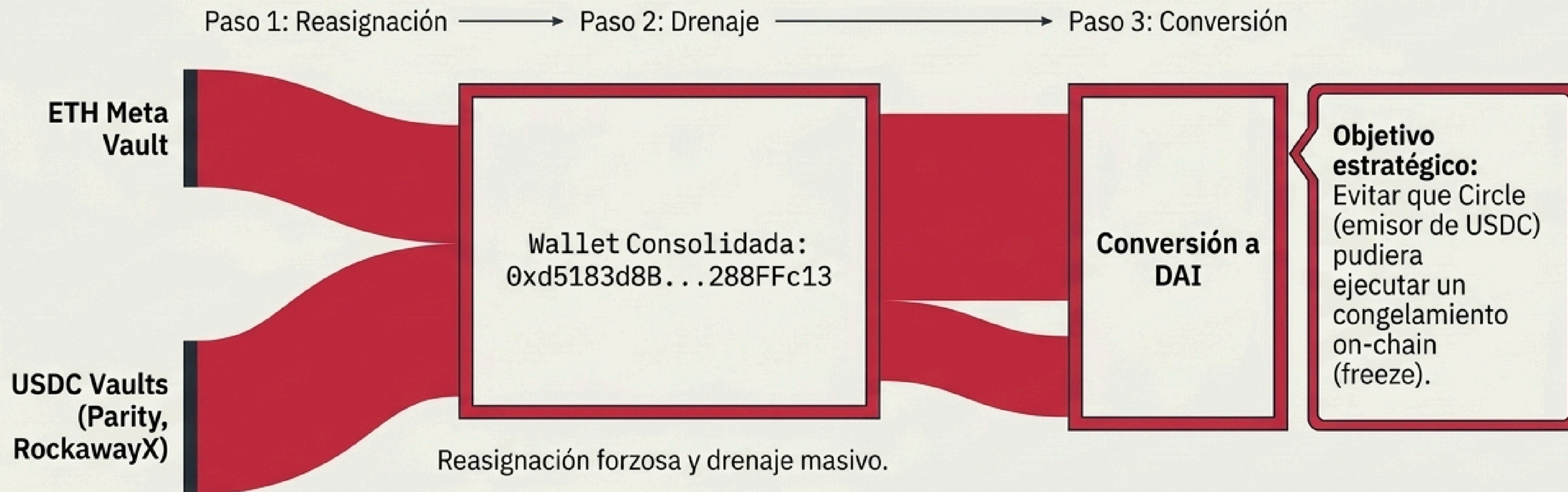
Ningún usuario, curator, o sistema de monitoreo vetó la transacción. Los proveedores de liquidez (LPs) ignoraron la propuesta.

Fase 3: El Bypass del Timelock

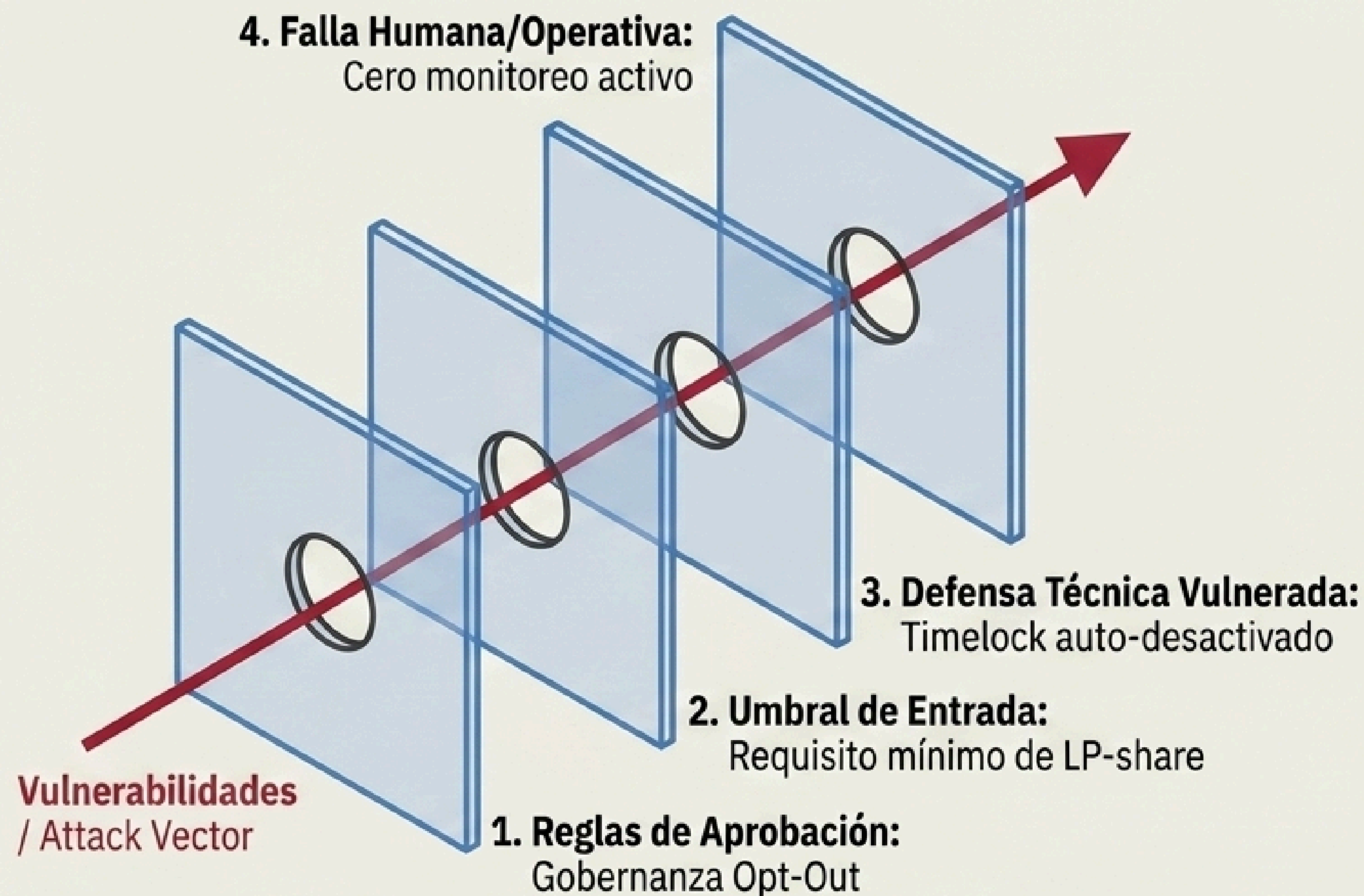


- **El Error Fatal de Arquitectura:** El propio payload (el código ejecutable) tenía permisos del sistema para modificar su propio Timelock.
- **El Efecto:** El muro defensivo de 7 días se redujo instantáneamente a 0 segundos, permitiendo la ejecución atómica.

Fase 4: La Extracción y Evasión



Síntesis del Fallo: El Modelo del Queso Suizo



- 1. Reglas de Aprobación:** Gobernanza Opt-Out (Inacción = Aprobación automática).
- 2. Umbral de Entrada:** Requisito mínimo de LP-share extremadamente bajo (centavos de dólar).
- 3. Defensa Técnica Vulnerada:** Timelock auto-desactivado por el propio payload de la propuesta.
- 4. Falla Humana/Operativa:** Cero monitoreo activo durante los días de exposición pública.

Radiografía del Impacto Financiero



Pérdida Total: ~\$8.5 Millones

ETH Meta Vault:

~\$6.87M – \$7.1M
(2.843 ETH drenados).

USDC Vaults:

~\$1.68M
(Múltiples vaults afectados).

Contexto de Red y Verificación:

- El ataque consumió el ~68% del TVL pre-ataque (\$12.45M).
- Concentrado casi en su totalidad sobre la red Ethereum.
- Cifras y rastreo on-chain verificados de forma independiente por PeckShield y CertiK.

Radio de Impacto: Comprometido vs. Seguro

ZONA COMPROMETIDA

Term Meta Vaults

Impacto total. Bóvedas de estrategia avanzada.

Estas bóvedas operaban sobre infraestructura customizada customizada basada en Yearn V3.

Yearn aclaró públicamente que el vector de ataque fue exclusivamente la capa de gobernanza personalizada de Term, NO los contratos estándar de los vaults de Yearn.

ZONA SEGURA

Protocolo Base de Term

Totalmente seguro e intacto.

Los mercados de lending/borrowing a tasa fija directos de Term Finance no se vieron afectados.

No hubo contagio a la capa base de préstamos del protocolo.

Registro de Incidentes: Contención de Term Labs

01 | RECONOCIMIENTO

Confirmación inmediata del 'governance exploit' on-chain el mismo día del evento.

02 | CIERRE IRREVERSIBLE

Cierre total y definitivo de los Term Meta Vaults afectados. Revocación de roles de la DAO para bloquear instantáneamente cualquier nuevo depósito.

03 | LIQUIDEZ DE USUARIOS

Los retiros (withdrawals) se mantuvieron explícitamente abiertos para permitir a los usuarios rescatar fondos de bóvedas no afectadas.

04 | MITIGACIÓN ACTIVA

Trabajo continuo con firmas de seguridad externas. Exploración de soluciones y mecanismos de recuperación para cubrir el déficit (shortfall) de los usuarios afectados.

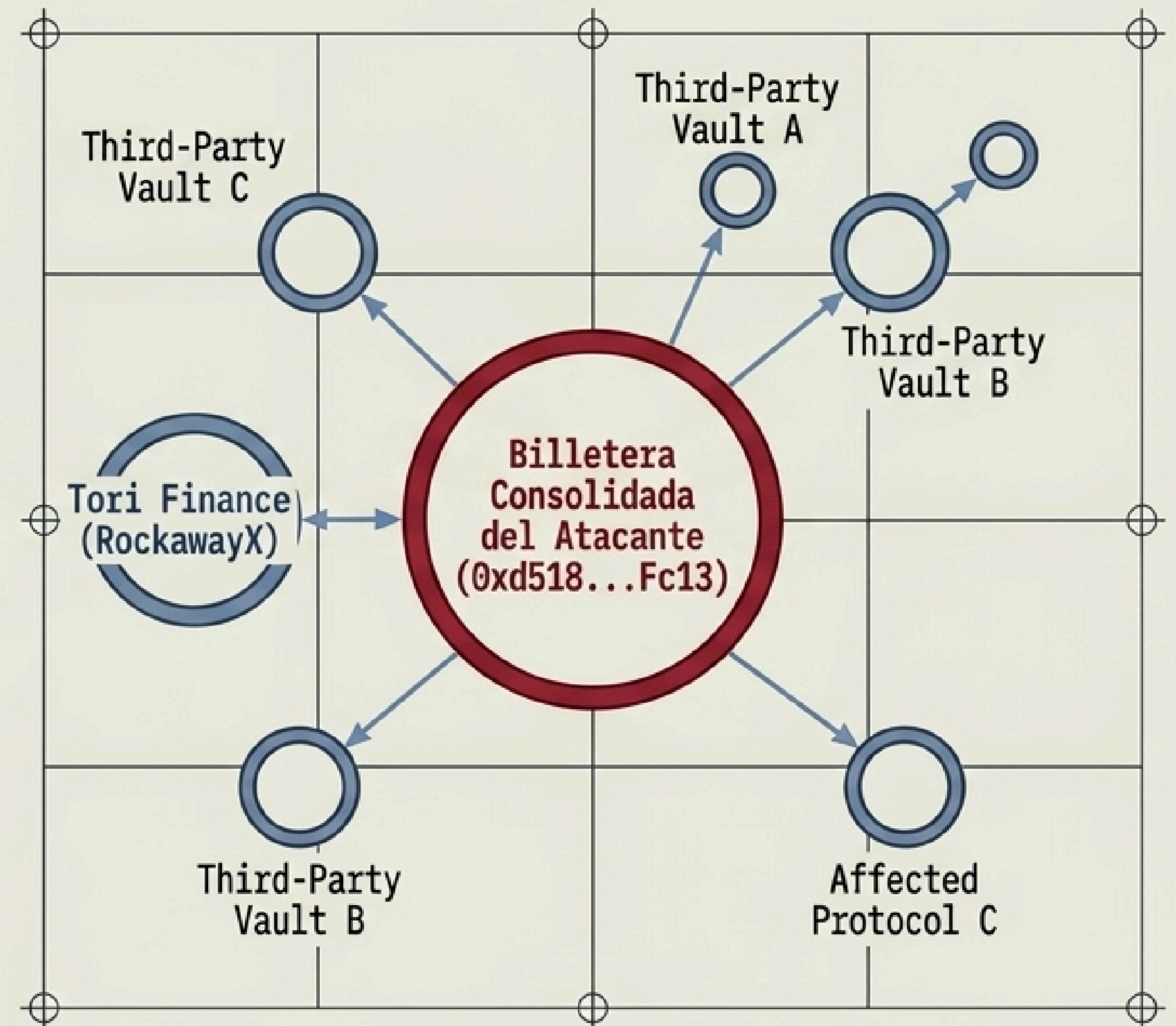
Daño Colateral y Estado Actual (Al 24 de Agosto)

Estado de los Fondos

Los \$8.5 Millones permanecen inmóviles ('dormant') en la billetera consolidada del atacante (**0xd518...Fc13**).
A la espera de un Post-mortem técnico profundo por parte de Term Labs.

Efecto Dominó (Contagio a Terceros)

Impacto en vaults de terceros que asignaban liquidez a las estrategias de Term.
Caso Destacado: **Tori Finance (RockawayX)** reportó exposición directa, asumiendo públicamente la cobertura de las pérdidas para proteger a sus depositantes.



EL PATRÓN MACRO: Este marca el tercer gran ataque a DAOs registrado este año. El panorama de amenazas ha evolucionado.

“No es un hackeo; es una captura legítima ejecutada según las reglas del sistema. En DeFi, si el diseño de gobernanza no requiere participación activa para proteger los fondos, la inacción se convierte en el vector de ataque más letal.”
