

RootCause Blockchain Security

Vigilar un sistema on-chain sin poder tocarlo: watch-only, local y sin claves.

- Inventario multi-chain, postura de control e incidentes **con causa raíz**.
- 13 controles · 22 detecciones · 15 indicadores de inteligencia.
- Aplicación de escritorio para Windows. **0 dependencias externas**.
- Nunca pide una semilla. Nunca firma. Nunca mueve fondos.

El problema no son las claves

Puedes tener la criptografía perfecta y perderlo todo igual.

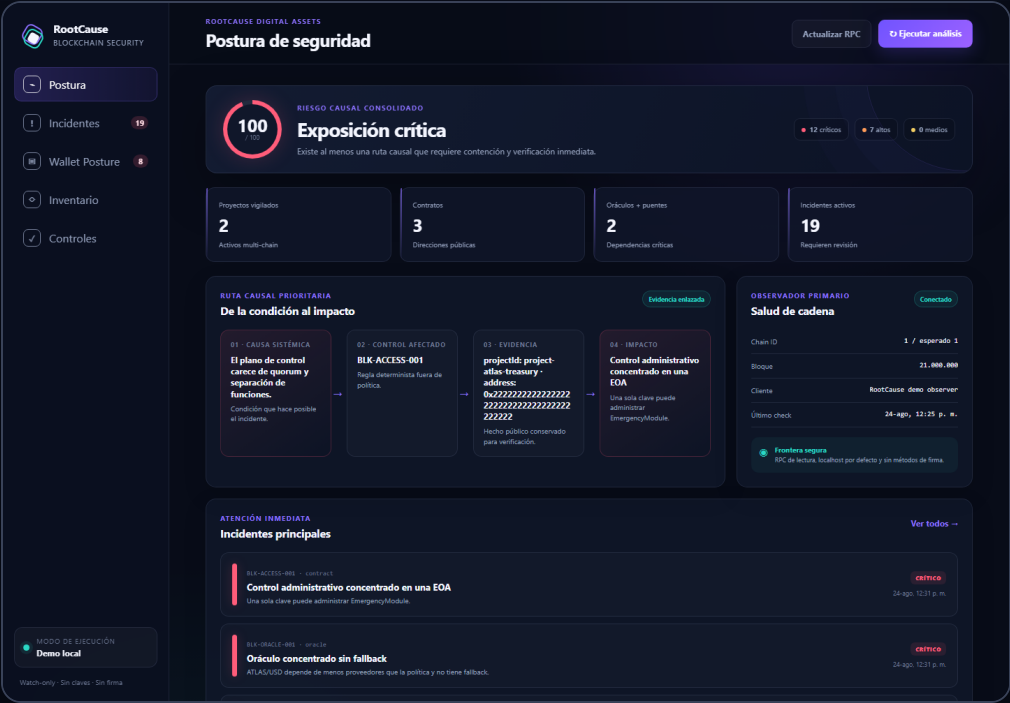
- Una EOA olvidada seguía siendo `owner` del proxy que actualiza el contrato.
- Un oráculo dejó de actualizarse y nadie miró el `heartbeat` hasta la liquidación.
- Un puente con quorum 2-de-3 tenía **los tres firmantes en la misma nube.**

Ninguna de las tres es una falla criptográfica. Las tres son **fallas de control**, y todas eran visibles desde fuera.

Qué es: una consola local, watch-only

Inventario, postura y evidencia. Todo en la máquina del operador.

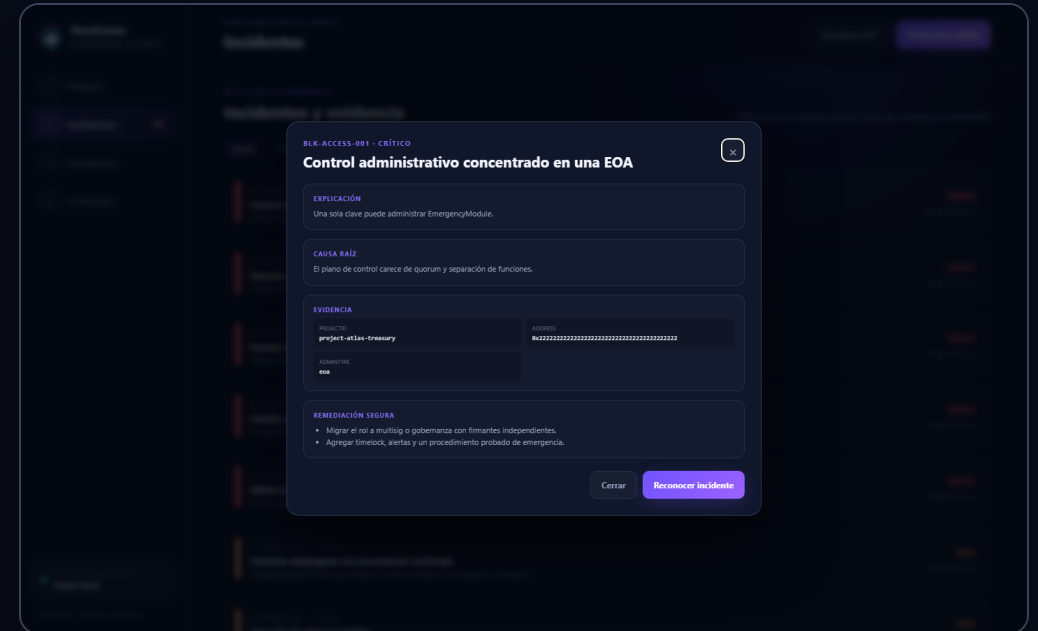
LO QUE TRAE DENTRO	CUÁNTO
Controles de defensa, del bytecode a la actividad de wallets	13
Detecciones deterministas BLK - *	22
Indicadores investigativos INT - *	15
Escenarios sintéticos con su resultado esperado	10
Pruebas automatizadas que CI ejecuta en cada cambio	144
Dependencias externas	0



De la alerta suelta a la causa raíz

Un incidente que no dice qué arreglar es ruido con formato.

- Cada hallazgo abre con **explicación, causa raíz, evidencia y remediación**.
- Las reglas son **deterministas**: el mismo estado produce el mismo veredicto.
- Cada código **BLK-*** pertenece a un control del catálogo. Un gate lo obliga.
- La remediación es un **runbook para una persona**, no un botón.



Wallets e inteligencia: señalar no es acusar

Dos catálogos separados a propósito, y no se mezclan nunca.

	POSTURA BLK - *	INTELIGENCIA INT - *
Qué afirma	Un control está mal puesto	Hay algo que conviene revisar
Cómo se decide	Regla determinista contra política	Indicador con umbral calibrable
Qué produce	Un incidente con remediación	Una señal con su explicación
Lo que nunca hace	—	Atribuir identidad, inferir intención, bloquear fondos

RootCause
BLOCKCHAIN SECURITY

Postura

Incidentes 19

Wallet Posture 8

Inteligencia 7

Inventario

Controles

ROOTCAUSE DIGITAL ASSETS

Blockchain Intelligence

Actualizar RPC Ejecutar análisis

ANÁLISIS ON-CHAIN PÚBLICO

Blockchain Intelligence

Indicadores investigables, puntaje explicable y seguimiento de fondos sobre datos públicos. Nada de esto acusa a nadie son señales que una persona debe revisar.

Transacciones analizadas
31
Redes: bitcoin, ethereum

Indicadores activos
7
Señales investigables

Alertas abiertas
7
0 falsos positivos registrados

Casos
0
0 abiertos

Grafo
38
34 aristas

Direcciones marcadas
2
Registro local del operador

Reorganizaciones
0
0 transacciones huérfanas

Evidencia
0
Huérfana e inmutable

RIESGO EXPLICABLE

Consultar una dirección

Nunca un número sin explicación

Ethereum 0xc8c800

EVALUAR

77
/ 100

ETHEREUM:0xc8c800

Crítico · confianza medium

Puntaje 77/100 (crítico) a partir de 2 indicador(es) distintos y 1 factor(es) atenuante(s).

Modelo inteligencia-1.0.0 - 31 transacciones analizadas

FACTORES QUE AUMENTAN EL PUNTAJE

+34

Coincidencia con un drainer del conjunto local

una ocurrencia (evidencia de 0 días)

INDICADOR

+26

Aprobación de gasto limitada

una ocurrencia (evidencia de 0 días)

INDICADOR

+18

Cercanía en el grafo a una dirección marcada localmente

A 1 salto(s) de ethereum:0xc8c800 por transferencias observadas.
La proximidad en el grafo no implica relación ni participación: una dirección puede recibir fondos sin conocer su origen.

INFERENCIA

FACTORES QUE LO REDUCEN

-1

Fiabilidad limitada de la fuente de datos

Los indicadores se apoyan en fuentes cuya fiabilidad declarada es 0.9.

INFERENCIA

v0.3.0 · 13 controles · 22 detecciones · 15 indicadores · 0 dependencias

vladimiracunadev-create.github.io/rootcause-blockchain-security

Seis principios que se comprueban solos

Una promesa de seguridad que nadie verifica es material de marketing.

1. Nunca pide ni guarda semillas, claves, keystores ni transacciones sin publicar.
2. No firma, no construye y no transmite transacciones.
3. El JSON-RPC usa una **allowlist estricta de métodos de lectura**.
4. Acepta `localhost`; un destino remoto exige habilitación explícita.
5. Las reglas son deterministas. **La IA es opcional y no tiene autoridad**.
6. Toda acción privilegiada exige runbook y aprobación humana separada.

Los seis se verifican **arrancando la aplicación real** y atacándola: **51 invariantes** en `scripts/check-security-claims.js`.

Demo en vivo: 90 segundos de terminal

Dos comandos. Sin red, sin instalar nada, sin datos reales.

COMANDO	LO QUE IMPRIME
<code>pnpm check:local-only</code>	Claim solo-local verificado: cero dependencias, cero orígenes remotos, cero proveedores alojados.
<code>pnpm check:security</code>	Invariantes de seguridad verificados: 51 comprobaciones.

Esta tabla se rellena **ejecutando los dos comandos** al generar las diapositivas. Si la terminal falla delante del público, señalala y sigue.

Lo que nunca hará, y cómo se adopta

La lista de lo que no hace es parte del producto, no una nota al pie.

NUNCA	SÍ, HOY
Custodiar claves ni firmar	Vigilar controles y explicar por qué fallan
Sustituir una auditoría o una verificación formal	Detectar controles mal puestos, en continuo
Atribuir identidad ni bloquear fondos	Señalar lo que conviene investigar, con evidencia
Prometer soporte de toda cadena	EVM implementado; el resto, por eventos normalizados

- **Empezar:** descargar el instalador de Windows, o `pnpm start` para el modo demo.
- **Antes de datos reales:** la lista de comprobación de seguridad. En ese orden.
- **Licencia MIT.** Versión 0.3.0. Sin telemetría, sin cuenta, sin nube.