

Criptoactivos y Finanzas Descentralizadas (DeFi): evaluación de riesgos y exposición institucional

8vo Seminario Latinoamericano en Gestión del Riesgo Operacional

Fidel Gómez

Jueves 20 de agosto de 2026

Objetivos de la sesión



Identificar los riesgos clave

Riesgos asociados a criptoactivos, exchanges, stablecoins, wallets digitales y plataformas DeFi.



Entender el giro estructural

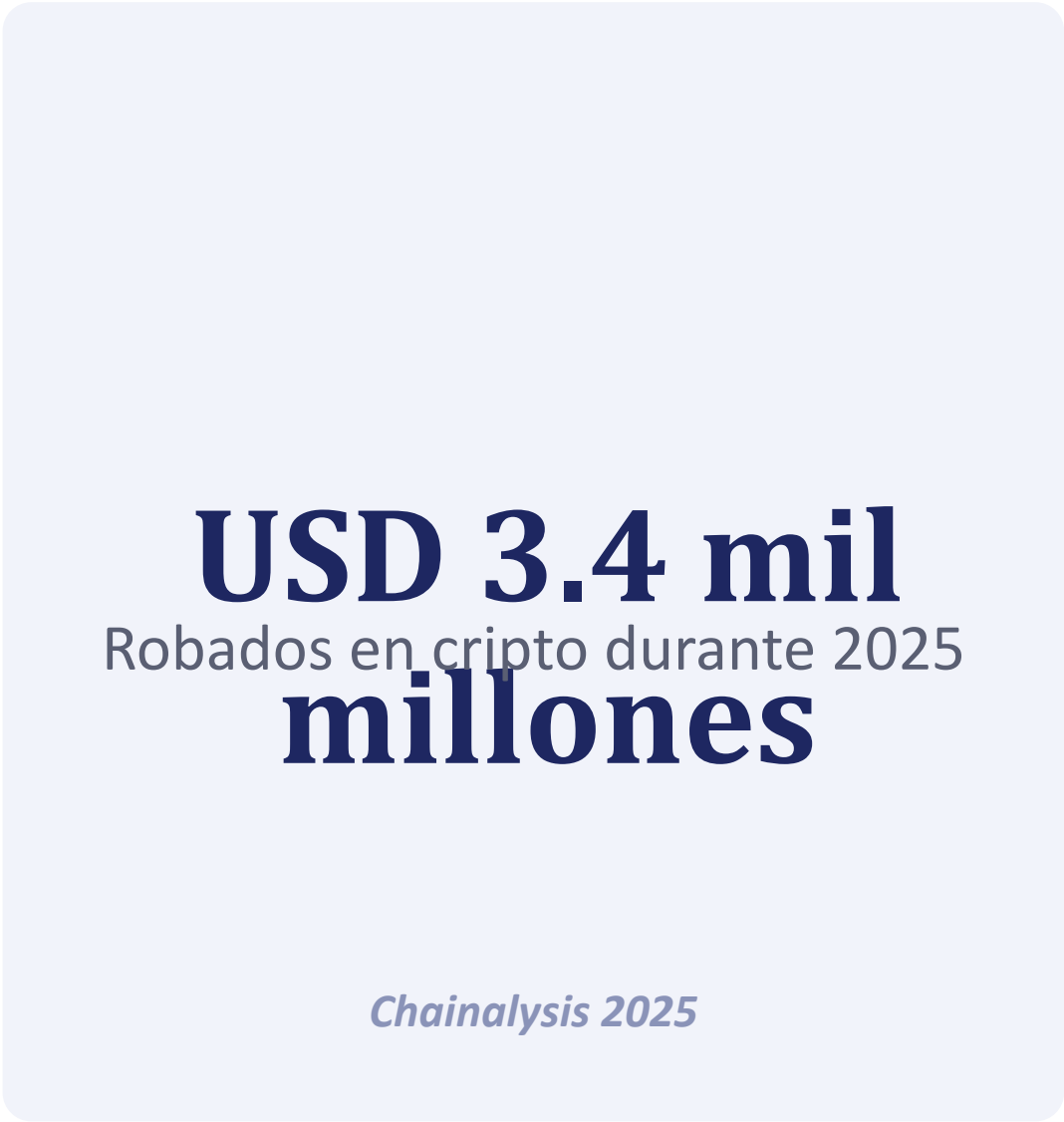
Cómo los modelos descentralizados modifican los enfoques tradicionales de gestión de riesgos, supervisión y control financiero.



Analizar riesgos emergentes

Volatilidad, fraude, lavado de activos, ciberseguridad y concentración tecnológica.

Por qué esto importa ahora



Categorías de exposición



Criptoactivos

Activos altamente volátiles que pueden entrar al balance de la organización vía tesorería, clientes o proveedores.



Exchanges (CEX/DEX)

Puntos de conversión y custodia — el riesgo de contraparte depende de si hay o no supervisión regulatoria real detrás.



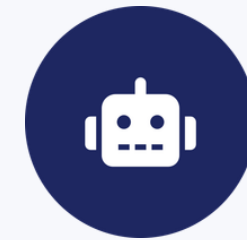
Stablecoins

Se usan como "efectivo digital", pero su estabilidad depende enteramente de la calidad y transparencia de su respaldo.



Wallets digitales

La posesión de la llave privada equivale a la posesión del activo — no hay reversión de transacciones ni "llamar al banco" si se pierde o se roba.



Plataformas DeFi

Servicios financieros (préstamo, trading, rendimiento) operados por código, sin una entidad regulada claramente responsable.

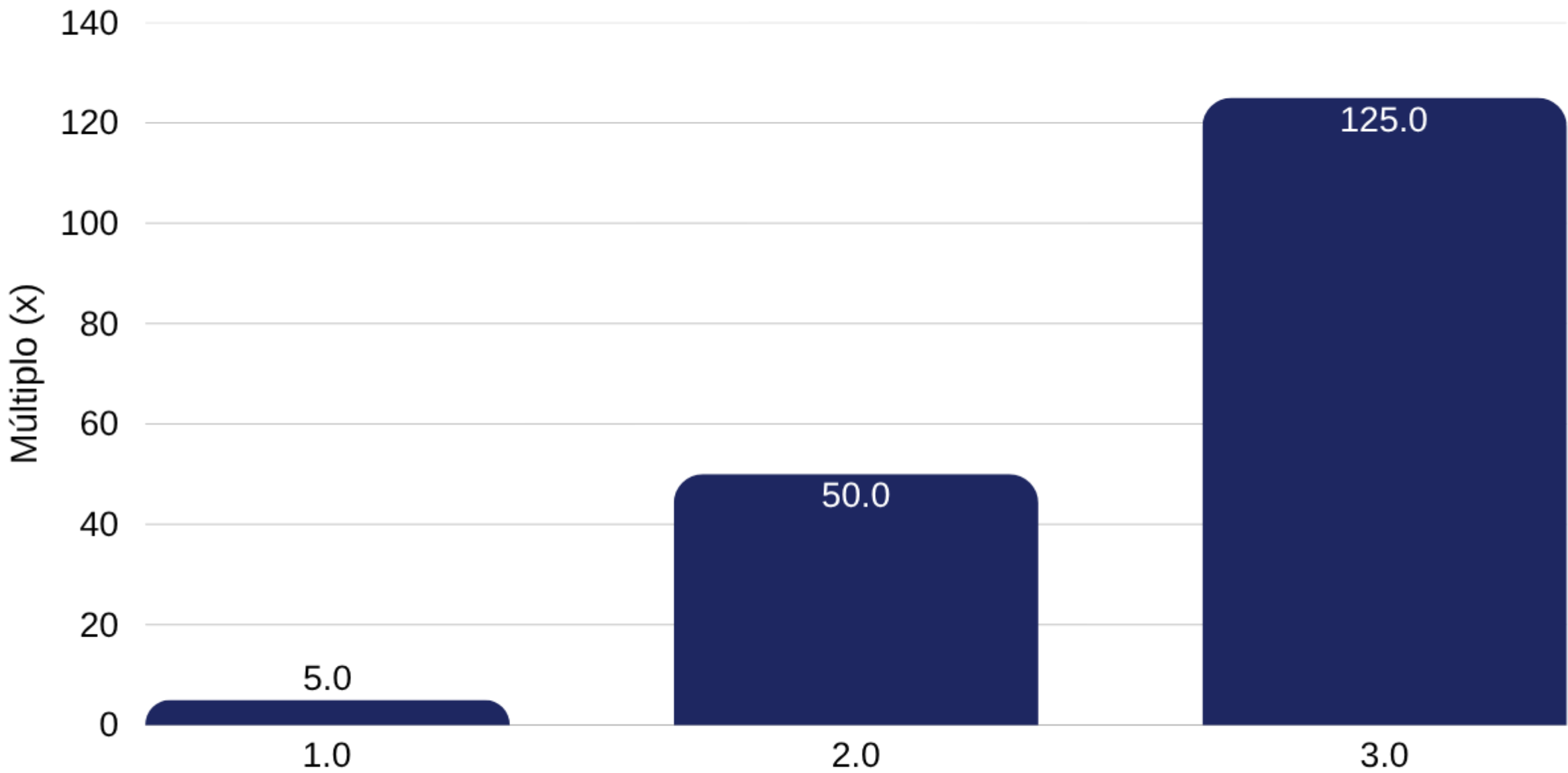
Cómo evaluamos estos riesgos



En crypto, la prevención pesa más que en otros activos:

muchas de estas pérdidas no tienen mecanismo de reversión ni fondo de garantía que las respalde después del hecho.

Apalancamiento máximo permitido



125x

el apalancamiento máximo permitido en algunos DEX crypto, hasta 25 veces más que en derivados regulados como CME.

A mayor apalancamiento permitido, mayor probabilidad de que muchas posiciones se liquiden al mismo tiempo, de forma correlacionada.

Fuente: BIS, 2021

Las liquidaciones en plataformas crypto son automáticas y sin intervención humana —sin llamada de margen, sin período de gracia— lo que amplifica la volatilidad y puede generar pérdidas súbitas en el balance de quien tiene exposición directa o indirecta. La prevención aquí son límites de exposición y colateral conservador definidos antes de tomar la posición, no una reacción después de la caída.

Patrones de fraude y señales de alerta



Salida abrupta de liquidez

Los promotores del proyecto retiran liquidez o fondos de forma abrupta y sin previo aviso a los inversionistas.



Funciones ocultas de control

Funciones administrativas que solo controla el equipo, sin ninguna revelación previa a los inversionistas.



Venta oculta del equipo fundador

Venta gradual y no revelada de las tenencias del equipo, equivalente a operar con información privilegiada, sin marco de revelación de posiciones.

No existe un prospecto verificado, un custodio regulado ni KYC del emisor. Si el equipo detrás del proyecto es anónimo, no hay a quién exigirle cuentas después del hecho, la debida diligencia previa es la prevención, no un paso más del proceso.

Rastrear el flujo vs. atribuir identidad



Rastrear el flujo

Casi siempre posible en cadenas públicas y transparentes. Bitcoin y Ethereum son, en este sentido, más transparentes que el efectivo.



Atribuir identidad

Mucho más difícil, ahí están los verdaderos puntos ciegos: monedas de privacidad, mezcladores y salidas por exchanges sin KYC. La prevención es elegir contrapartes y exchanges con controles KYC/AML robustos, no confiar en que el flujo se pueda rastrear después.

40% → 15%

Flujo directo a exchanges congelables, de 2021-22 a Q2 2025 (Chainalysis).

3.8%

Recuperado de los USD 1.46 mil millones robados a Bybit (FATF 2025).

Ciberseguridad: la magnitud del problema

Robados en cripto en 2025

USD 3.4B

Hackeo a Bybit, feb. 2025, el mayor robo cripto registrado (Corea del Norte)

USD 1.5B

De las pérdidas del Q1 2025 ocurrieron en exchanges centralizados

88%

Incidentes en wallets personales en 2025, el triple que en 2022

158,000

Nota positiva: los robos en DeFi se mantuvieron contenidos pese al crecimiento del TVL (Total Value Locked), señal de mejoras reales en auditoría de smart contracts.

La prevención aquí es capacitación del personal, custodia multisig y segregación de llaves, no solo respuesta a incidentes.

Riesgo tecnológico y de concentración



Los contratos no se pueden "corregir" fácilmente

Una falla de diseño queda expuesta hasta que alguien la explota. Una auditoría de código reduce el riesgo, pero no lo elimina.



La infraestructura está más concentrada de lo que sugiere "descentralizado"

Custodios, validadores, emisores de stablecoin y puentes entre redes: ahí es donde ocurren las mayores pérdidas del ecosistema.

83%

Del mercado de stablecoins concentrado en solo 2 emisores

USD 625M

Ronin Bridge, 2022 - punto único de infraestructura comprometido

USD 325M

Wormhole, 2022 - mismo patrón: un solo punto de falla

El eslabón más débil de este ecosistema suele ser el menos descentralizado. La prevención es límite de concentración por proveedor o custodio y debida diligencia de auditorías — no confiar en que "es descentralizado".

Tres colapsos, tres lecciones



FTX

Noviembre 2022

Falla de gobernanza y custodia

Uso indebido de fondos de clientes, sin segregación de activos.

Prevención: segregación estricta de los activos de clientes frente a los activos propios del exchange.



Terra / Luna

Mayo 2022

Falla de diseño de producto e incentivos

- Un rendimiento del 19.5% insosteniblemente subsidiado generó demanda artificial.
- Al romperse la confianza, el mecanismo de estabilización no tenía respaldo real y colapsó en días. Pérdida total: USD 40–60 mil millones.
- Lección de gobernanza: Alameda Research (firma hermana de FTX) tuvo acceso preferencial y salió con pérdidas menores que el resto — asimetría de información sin marco de revelación.

Prevención: límite a rendimientos insosteniblemente subsidiados y debida diligencia del diseño de producto.



Bybit

Febrero 2025

Falla de seguridad y concentración de custodia

USD 1.5 mil millones robados — el mayor robo cripto registrado, atribuido a actores vinculados a Corea del Norte.

Prevención: segregación y límites de custodia, con controles de acceso reforzados.

Cuatro capas de regulación



Prudencial (Basilea)
Capital por exposición cripto. Group 1 vs Group 2; tope agregado Group 2: 1% del capital Tier 1.



Estabilidad sistémica (FSB)
"Same activity, same risk, same regulation."



AML/CFT (GAFI/FATF)
Travel Rule en 99 jurisdicciones (2025). La mayoría de la actividad ilícita on-chain ahora usa stablecoins, no Bitcoin.



Licenciamiento local
Cada país avanza a ritmo distinto, ver comparación abajo.

País	Estado regulatorio
Brasil	Más avanzado — Banco Central, Resoluciones 519/520/521 (nov. 2025), nueva figura SPSVA, autorización obligatoria desde feb. 2026, límite de USD 100,000 por transacción con contrapartes no autorizadas.
México	Ley Fintech en actualización; sin regulación específica para DeFi, NFTs o stablecoins.
Colombia	Proyecto de Ley 510/2025 archivado — solo obligaciones tributarias DIAN/UIAF; sin licencia de operación ni reglas de custodia, reservas o segregación de activos.

Tres países vecinos, tres etapas regulatorias distintas: arbitraje regulatorio dentro de la propia región LatAm, no solo frente a paraísos lejanos.

Preguntas para su organización

	¿Exposición directa o indirecta?	Vía proveedores, clientes o tesorería propia.
	Debida diligencia de contrapartes	Y de emisores de stablecoin utilizados.
	KRIs específicos	Concentración de custodia, exposición a protocolos no auditados, dependencia de un solo oráculo o bridge.
	Gobernanza de custodia	Esquemas multisig y distribución de llaves.
	Capacitación del personal	Especialmente en ingeniería social.

***Este es su marco de prevención:** las preguntas que su organización debe poder responder antes de que el riesgo se materialice, no después.*

Conclusiones y mensajes clave

- 1 La ausencia de un intermediario regulado no elimina el riesgo**
Lo traslada a la organización que decide exponerse y ahí es donde debe actuar la prevención.
- 2 Los marcos tradicionales siguen siendo el lenguaje correcto**
Pero hay que remapear sus supuestos.
- 3 La trazabilidad ya no es el problema técnico principal**
El problema es la atribución de identidad y la brecha regulatoria entre jurisdicciones.
- 4 La regulación ya está definida a nivel de principios**
El riesgo real hoy es la brecha de implementación.

Preguntas

Gracias — Fidel