De Activo Cautivo a Activo Líquido: Por qué la tokenización de colateral requiere privacidad por sub-transacción.

Análisis del caso Canton Network vs. redes de pago y registros compartidos.

Albert Salvany

Tabla de contenido

De Activo Cautivo a Activo Líquido: Por qué la tokenización de colateral requiere privacidad por sub-transacción. 1
Análisis del caso Canton Network vs. redes de pago y registros compartidos. 1
Resumen Ejecutivo: 4
CAPÍTULO 1: El Problema de Origen: Sistemas Fragmentados y la "Falsa Digitalización" 5
1.1 El paradigma de la fragmentación operativa tradicional 5
1.2 La paradoja de la mensajería asíncrona: SWIFT como parche 6
1.3 El impacto de la asincronía en los procesos de post-trading 7
1.4 Cuantificación macroeconómica de la inmovilización de capital 9
1.5 La trampa de liquidez: Buffers preventivos del 30% 11
1.6 El coste de oportunidad estratégico de los fines de semana (Weekend Downtime) 13
1.7 La Asimetría de Inacción (Competitive Drag): El coste estratégico de postergar la adopción 14
CAPÍTULO 2: Por qué la Blockchain Pública no es Viable para la Operativa Bancaria ... 17
2.1 El obstáculo absoluto de la publicidad de los datos de la Layer 1 17
2.2 El riesgo de contraparte y la ausencia de controles KYC/AML nativos 18
El peligro legal de la validación anónima e incontrolada 18
La penalización prudencial del Comité de Basilea 19
La incompatibilidad con la *Travel Rule* y controles KYC 19
La alternativa síncrona y permisionada de Canton 21
2.3 La ineficiencia estructural de las soluciones de parche 22
CAPÍTULO 3: La Incompatibilidad de las Redes Privadas de Registro Único Compartido 26
3.1 El mito del "Libro Mayor Único Compartido" (Shared Ledger) 26
3.2 El problema de la contención de recursos financieros 27
3.3 Gobernanza rígida y centralizada 28
CAPÍTULO 4: El Modelo Canton: Red de Redes con Privacidad Nativa en Layer 1 31
4.1 Filosofía de "Red de Redes": El Libro Mayor Virtual Global 31
4.2 Separación bicapa del consenso de Canton 32
4.3 Arquitectura y Roles de los Componentes de Red 34
4.4 El Sincronizador Global (Global Synchronizer) y Gobernanza G-SIB 36
CAPÍTULO 5: El Lenguaje Daml y el Motor de Privacidad por Sub-transacción 39
5.1 Fundamentos de Daml como lenguaje funcional para finanzas 39

5.2 El modelo contractual inmutable de Daml..... 41
5.3 Control de accesos y derechos contractuales nativos 43
5.4 Privacidad por sub-transacción mediante Árboles Transaccionales 45
CAPÍTULO 6: Caso de Uso Técnico: Rehipotecación Intradía de un Bono del Estado Español 48
6.1 Sinopsis del Flujo Operativo PoC..... 48
6.2 Desglose Paso a Paso del Ciclo de Vida Daml 50
6.3 Stack Tecnológico e Implementación 53
CAPÍTULO 7: Sincronización e Interoperabilidad: Análisis Comparativo Cosmos vs. Canton 55
7.1 Arquitectura: Soberanía frente a Sincronización Coordinada..... 55
7.2 Privacidad: Aislamiento por cadena frente a Privacidad por sub-transacción..... 57
7.3 Rendimiento, TPS y Latencia Operativa 59
7.4 Dependencia de Plataforma (Vendor Lock-In)..... 60
CAPÍTULO 8: Regulación, Cumplimiento y ESG bajo los Marcos MiCA, GDPR y DORA . 62
8.1 Cumplimiento de Prevención de Blanqueo (AML/CFT) con Privacidad Coexistente 62
8.2 Conexión con Supervisores: El nodo observador 64
8.3 Estatus de Canton Coin (CC) según la Regulación MiCA de la UE 66
8.4 El Euro Tokenizado EURØP como liquidación DvP regulada..... 67
8.5 Análisis del Impacto ESG y de Sostenibilidad 68
CONCLUSIÓN, RETORNO DE INVERSIÓN (ROI) Y HOJA DE RUTA C-LEVEL 70
Redefinición del rol de la custodia bancaria en la era digital 70
Métricas financieras de Retorno de Inversión (ROI) proyectadas 70
Hoja de ruta estratégica de implementación en 3 fases para la alta dirección 71
El Coste de la Inacción y el Nuevo Paradigma de la Liquidez Global..... 73
A. La Realidad Inapelable de los Números 73
B. El FOMO Estructural: El Coste de Oportunidad de Operar en T+2 74

Resumen Ejecutivo

La infraestructura operativa del sistema financiero global padece una ineficiencia estructural de origen: **la fragmentación de la confianza y el aislamiento de los registros contables bilaterales**.

Durante décadas, la digitalización tradicional se ha limitado a automatizar el envío de mensajes asíncronos (como el sistema SWIFT) para dar instrucciones de actualización contable, pero no ha logrado unificar de manera síncrona el estado real de los activos entre las contrapartes.

Este desfase y la latencia post-trading asociada obligan a las instituciones a mantener inmovilizados billones de dólares en capital y colateral de alta calidad de forma puramente preventiva para mitigar riesgos de liquidación.

Al operar bajo un modelo asíncrono e inconexo, solo el 11% de los 255 billones de dólares en activos comercializables aptos para colateral se movilizan activamente en la actualidad, dejando el 89% restante atrapado en buffers de liquidez estériles.

Frente a esta fragmentación contable, la tokenización de activos del mundo real (RWA) sobre la infraestructura de **Canton Network** se presenta como una solución estructural definitiva. Diseñada bajo una arquitectura única de "red de redes", Canton permite que los participantes mantengan la soberanía, control y privacidad absoluta de sus datos a nivel de sub-transacción, mientras interactúan de forma atómica y en tiempo real a través de un sincronizador común.

Actualmente, el ecosistema de Canton Network ya procesa más de **6 billones de dólares (USD 6 Trillion+) en volumen de transacciones on-chain**, consolidándose como la primera red pública-permisionada del mundo diseñada expresamente para dar soporte a la infraestructura del mercado mayorista institucional.

La viabilidad a escala industrial de este paradigma de finanzas sincronizadas está plenamente demostrada a través de casos de éxito líderes en producción.

La plataforma **Distributed Ledger Repo (DLR) de Broadridge**, que opera sobre los rieles de Canton, procesa de manera síncrona más de **8 billones de dólares mensuales (USD 8 Trillion/month)** en transacciones de recompra (repos) de deuda pública norteamericana.

Esta escala de actividad en producción real no solo reduce drásticamente los costes de compensación en un rango de entre el 25% y el 50%, sino que evidencia cómo la sincronización contable instantánea y atómica en T+0 elimina por completo el riesgo de contraparte intradía, liberando el capital cautivo para devolverle una liquidez óptima e inmediata al balance bancario.

CAPÍTULO 1: El Problema de Origen: Sistemas Fragmentados y la "Falsa Digitalización"

1.1 El paradigma de la fragmentación operativa tradicional

El modelo operativo sobre el cual se sustenta la infraestructura financiera global actual adolece de una ineficiencia de origen: **la fragmentación de la confianza y el aislamiento de los registros contables bilaterales**.

A menudo se asume que los mercados financieros están totalmente digitalizados, pero la realidad operativa es que las instituciones siguen registrando la propiedad y el estado de sus activos en bases de datos internas completamente aisladas de sus contrapartes, lo que cronifica la duplicación de datos y la asincronía contable.

Esta situación se asemeja a un escenario en el cual cada entidad bancaria mantiene los registros de su dinero y de sus posiciones de activos en su propio "cuaderno privado". Cuando dos bancos deciden realizar una transacción, se ven obligados a comunicarse, contrastar los datos de sus cuadernos individuales y trabajar lentamente para llegar a un acuerdo mutuo. Este proceso de reconciliación asíncrono no solo es sumamente engorroso y costoso, sino que introduce una latencia que hace que la liquidación de las operaciones requiera días y sea altamente propensa a errores o discrepancias contables de sistemas.

Para automatizar esta interacción, la industria financiera tradicional no ha integrado los estados de sus libros contables, sino que ha automatizado la comunicación mediante sistemas de mensajería asíncrona, notablemente a través de flujos de trabajo basados en el protocolo SWIFT e integraciones bilaterales punto a punto. Este paradigma de "comunicación sobre el estado" en lugar de "sincronización de estado" genera un cuello de botella crítico. Aunque estos flujos basados en mensajería logran escalar de manera organizativa, **tienen grandes dificultades para proporcionar atomicidad entre las firmas, sincronización de estado en tiempo real y privacidad de grano fino sin reintroducir reconciliaciones contables complejas o intervenciones manuales constantes**.

Desde una perspectiva fundamental de auditoría y cumplimiento, una cadena de bloques es en realidad una versión superior de libros y registros electrónicos (books and records) que se sincroniza automáticamente con los libros contables de las contrapartes.

Al carecer de esta sincronización nativa, los sistemas tradicionales operan bajo una asincronía contable constante. Esta desconexión operativa y falta de sincronización se concentra de forma especialmente crítica en :

- **los procesos posteriores a la negociación** (la capa de *post-trade*),
- **la gestión de colaterales**,
- **los ciclos de márgenes de derivados** y

- **El procesamiento de servicios de activos**. Esta es precisamente **la capa de la infraestructura de mercado financiero donde se acumulan y concentran de forma desproporcionada los riesgos operativos, legales y de contraparte**.

Las consecuencias de mantener una infraestructura contable fragmentada y aislada se traducen directamente en una severa inmovilización de capital sistémico.

El colateral de alta calidad (HQLA), como los bonos soberanos, es el motor esencial encargado de asegurar las transacciones en los mercados de recompras (repos), los derivados, el préstamo de valores y la gestión de márgenes.

No obstante, **las ineficiencias en el movimiento de colateral y los cuellos de botella en los flujos de post-trade asíncronos ralentizan notablemente estas operaciones, exacerbando las crisis de liquidez y las dislocaciones de mercado**.

El impacto cuantitativo de este bloqueo de colateral es masivo:

- de acuerdo con los datos del *SIFMA Capital Markets Fact Book 2024*, de un inventario potencial total de **255 billones de dólares** en valores negociables demandados para ser utilizados como colateral en el sistema financiero global, **apenas 28 billones de dólares (un escaso 11%) se están movilizando activamente** en el mercado mayorista tradicional.

El 89% restante permanece inactivo o bloqueado preventivamente en las tesorerías bancarias de forma estéril, debido única y exclusivamente a la incapacidad técnica de los sistemas legados de procesar la transferencia, verificación e inscripción del activo de forma atómica y síncrona en tiempo real.

1.2 La paradoja de la mensajería asíncrona: SWIFT como parche

Durante las últimas cinco décadas, la industria financiera global ha confundido la automatización de las comunicaciones con la verdadera digitalización de los procesos de negocio. El pilar de esta confusión ha sido la adopción masiva de redes de mensajería financiera asíncrona, representadas fundamentalmente por los estándares de **SWIFT (MT y los nuevos formatos XML bajo ISO 20022)**.

Aunque estos rieles han permitido la transmisión rápida y estandarizada de información financiera a escala transnacional, se comportan en la práctica como un **parche tecnológico que perpetúa, en lugar de solucionar, la fragmentación operativa original del mercado mayorista**.

La raíz de esta paradoja reside en la diferencia fundamental entre "comunicar sobre el estado de un activo" y "sincronizar el estado real del activo".

En el modelo contable tradicional, cada entidad financiera (bancos comerciales, custodios globales, depositarios centrales de valores y cámaras de compensación) opera su propio

registro o "libro contable privado". Cuando se ejecuta una transacción bilateral, el activo no se transfiere físicamente de forma digital; en su lugar, la entidad origen utiliza SWIFT para enviar una instrucción o un mensaje con la intención de que la entidad destino actualice su propio "cuaderno".

Esta arquitectura genera un **flujo de conciliación en cascada (Multi-book Reconciliation)** que expone severamente las limitaciones del modelo asíncrono:

- **Fragmentación contable:** Una simple transferencia de colateral o una operación de reporto (*repo*) requiere que al menos cuatro libros contables independientes (el del banco ordenante, su custodio de valores, el custodio de la contraparte y el banco receptor) realicen de forma secuencial y asíncrona verificaciones de cumplimiento, validación de saldos y actualizaciones contables individuales.
- **La latencia del "espejismo instantáneo":** Aunque el mensaje SWIFT viaja en milisegundos de un nodo a otro, el procesamiento, la interpretación y la reconciliación manual o semi-automatizada del contenido del mensaje dentro de los sistemas heredados (*core banking*) de cada intermediario consume entre **2 y 3 horas de tiempo operativo**. Automatizar el envío del sobre (el mensaje) no acelera la inspección ni la actualización del libro contable interno, lo que significa que el mercado simplemente ha automatizado la *notificación* de una transacción, pero no su *liquidación* efectiva.
- **Ausencia estructural de atomicidad (DvP asíncrono):** En los flujos basados en mensajería, la pata de la entrega del colateral (valores) y la pata del pago (efectivo) se procesan a través de redes y carriles de comunicación desconectados. Al no existir una sincronización síncrona nativa, no es posible garantizar que el traspaso del bono y la transferencia de la liquidez ocurran en el mismo instante matemático (Entrega contra Pago o *Delivery-versus-Payment* síncrono). Este desfase temporal introduce un riesgo de liquidación intradía que obliga a la banca a depender de costosas entidades de compensación centralizada (CCPs) y a mantener elevados márgenes de garantía.

Por tanto, el uso de mensajería asíncrona como SWIFT actúa como un paliativo que enmascara un problema estructural: la falta de una **infraestructura de estado compartida** en la que los registros de las contrapartes puedan sincronizarse de manera automática y determinista.

Mientras persista este paradigma de "comunicar para conciliar", los activos líquidos clave del sistema mayorista seguirán comportándose como instrumentos estáticos y cautivos del post-trading, obligando a las entidades a asumir riesgos de contraparte innecesarios, costes de reconciliación duplicados y una inmovilización ineficiente de su balance.

1.3 El impacto de la asincronía en los procesos de post-trading

Los procesos posteriores a la negociación —que engloban la liquidación, la compensación, la custodia, la gestión de márgenes y el procesamiento de servicios de activos (*asset servicing*)— constituyen la capa de la infraestructura de mercado financiero

donde se acumulan de forma desproporcionada **los mayores riesgos operativos, legales y de crédito de contraparte** del sector bancario global . En el modelo asíncrono tradicional, la ejecución de una orden se realiza en milisegundos, pero la verdadera complejidad financiera e institucional comienza en el *post-trading*, donde la desconexión de los sistemas informáticos y la falta de un estado contable compartido imponen un peaje diario masivo sobre el balance de las entidades .

Esta problemática estructural se manifiesta en los siguientes vectores operativos críticos:

A. La desconexión de las patas de entrega y pago (Falta de atomicidad nativa)

En los flujos tradicionales, la pata de la entrega de los valores (los bonos o acciones) y la pata del pago en efectivo transitan por redes y carriles de comunicación completamente independientes y desconectados. Al no existir una sincronización síncrona nativa, es técnicamente imposible asegurar de forma bilateral que el traspaso del colateral y la transferencia de la liquidez ocurran en el mismo instante matemático (Entrega contra Pago síncrona o *Delivery-versus-Payment*) .

Para evitar el riesgo de que una de las partes entregue el activo y nunca reciba el efectivo (riesgo de principal), la industria se ve obligada a interponer **Entidades de Contrapartida Central (CCP) y múltiples custodios globales**, quienes actúan como garantes de la operación . Este diseño asíncrono no solo encarece sustancialmente los costes de liquidación directa entre un 25% y un 50%, sino que fragmenta la liquidez y somete a los participantes a constantes llamadas de margen intradía para cubrir las exposiciones latentes durante el periodo en que las transferencias bilaterales permanecen en tránsito asíncrono .

B. Latencias de ciclo (T+1 y T+2) como secuestro de capital

La asincronía inherente a las bases de datos bilaterales obliga a mantener ciclos de liquidación diferidos, típicamente establecidos en **T+1 o T+2 (dos días hábiles para confirmar y asentar la transacción)** . Durante esta ventana temporal de hasta 48 horas, los activos y la liquidez involucrados en la transacción quedan técnicamente bloqueados y fuera del alcance de la mesa de tesorería, impidiendo su reutilización para otras llamadas de margen inmediatas u operaciones de reporto (*repos*) de financiación síncrona .

Este secuestro temporal de colateral disminuye el coeficiente de utilización de los balances bancarios a escala de mercado global. Solo una fracción mínima del inventario potencial de valores negociables se moviliza activamente, forzando a las tesorerías a operar con buffers preventivos sobredimensionados para cubrir la ineficiencia de liquidación post-trading .

C. El coste de la reconciliación y el riesgo de disputas contables

Dado que cada custodio, depositario central de valores (CSD) y banco comercial mantiene un registro privado e independiente de la transacción, el flujo post-trading exige que estas bases de datos asíncronas se crucen e inspeccionen constantemente . Este proceso se realiza mediante el intercambio de mensajes asíncronos secuenciales que deben ser reconciliados contablemente por cada participante .

Si ocurre una discrepancia en los metadatos de la transacción —por ejemplo, un error en los códigos de activos, diferencias en el cálculo de intereses de repos, o desfases de huso

horario—, la reconciliación asíncrona falla. Las incidencias contables bilaterales pueden demorarse **horas o días en resolverse**, requiriendo la intervención manual de equipos enteros de back-office, incrementando notablemente el riesgo operativo del banco y exponiendo a la entidad a sanciones por fallos de liquidación regulatoria .

D. La inoperatividad de fin de semana (Weekend Downtime)

El riesgo post-trading se exacerba críticamente durante el fin de semana.

Mientras los riesgos financieros y macroeconómicos globales no descansan, la infraestructura contable tradicional de liquidación y los sistemas de mensajería (SWIFT) interrumpen su actividad el viernes por la tarde y permanecen inoperativos hasta el lunes por la mañana.

Durante estas **60 horas de desconexión contable**, cientos de miles de millones de euros en activos de alta calidad (HQLA) quedan inmovilizados en las cuentas de los custodios, atrapando el capital de las tesorerías bancarias de manera improductiva . Si una entidad se enfrenta a un evento de tensión de liquidez o volatilidad extrema de mercado durante un sábado, el sistema tradicional le impide movilizar y liquidar de forma atómica sus bonos del Tesoro contra liquidez inmediata**, incrementando drásticamente el riesgo sistémico global**

1.4 Cuantificación macroeconómica de la inmovilización de capital

Para la alta dirección de cualquier entidad financiera, el verdadero coste de operar bajo una infraestructura asíncrona de post-trading solo se hace evidente al examinar el impacto macroeconómico y de balance que tiene la inmovilización global de garantías.

La escala de esta ineficiencia estructural ha sido cuantificada con precisión matemática en los datos oficiales de la industria recopilados en el **SIFMA Capital Markets Fact Book 2024**, presentados formalmente ante la **U.S. Securities and Exchange Commission (SEC) en febrero de 2025** como parte del análisis estratégico para la modernización de los mercados digitales de capitales.

A. La magnitud del inventario inactivo y el papel de la deuda soberana

A nivel macro, el inventario potencial de valores negociables comercializables aptos y demandados para ser utilizados como colateral en el sistema financiero global asciende a la colosal cifra de **255 billones de dólares**.

Este agregado de colateral potencial de alta calidad (HQLA) representa el cimiento sobre el cual se sustenta la mitigación del riesgo de crédito de contraparte en todo el mundo.

Dentro de este inventario, el mercado de bonos del Tesoro de los EE. UU. (U.S. Treasuries) constituye el componente individual más crítico y el activo de referencia para la financiación mayorista, acumulando un volumen de **27 billones de dólares** de deuda en circulación.

Sin embargo, debido a las limitaciones tecnológicas de los sistemas legados de custodia y liquidación diferida analizados en los apartados anteriores, **este inmenso volumen de activos seguros no puede circular con la velocidad requerida por las necesidades de liquidez intradía, quedando atrapado en los balances como capital improductivo**.

B. La paradoja del 11%: Custody Drag y la inactividad de las garantías

A pesar de la existencia de este colchón potencial de 255 billones de dólares para asegurar transacciones financieras, la realidad operativa global presenta una paradoja insostenible:

- **Colateral Activo:** Únicamente **28 billones de dólares (un escaso 11%)** de este inventario se encuentra realmente activo y movilizándose en los mercados financieros internacionales para respaldar operaciones de repo, derivados, préstamos de valores y gestión de márgenes.
- **Colateral Inactivo (Custody Drag):** El restante **89% (227 billones de dólares)** permanece completamente inactivo, estancado bajo un fenómeno técnico denominado ***custody drag*** **o lastre de custodia**.

Este 89% inactivo no es el resultado de una falta de demanda de garantías por parte de los operadores del mercado, sino de la **incapacidad de la infraestructura tradicional para procesar el traspaso, la verificación y la inscripción registral de los activos de forma síncrona y en tiempo real**. Los activos quedan retenidos preventivamente en las cuentas de custodia únicamente para cubrir los desajustes de tiempo (T+1 o T+2) y los retrasos de conciliación de la mensajería asíncrona bilateral.

C. El coste de oportunidad financiero para el balance bancario

Mantener el 89% del colateral global en estado de inactividad genera un coste de oportunidad financiero que drena directamente el ROA (*Return on Assets*) de las instituciones y limita la eficiencia de los balances:

1. **Deterioro de la liquidez intradía:** Las tesorerías se ven obligadas a inmovilizar capital preventivo estéril (el buffer del 30% analizado en el apartado 1.2) para precaverse de llamadas de margen que no puedan liquidarse antes de las 2 o 3 horas que consume la mensajería tradicional.
2. **Pérdida de eficiencia en el mercado de financiación mayorista:** Si la deuda soberana pudiera movilizarse y pignorarse las 24 horas del día, los 7 días de la semana (24/7) de forma atómica y sin riesgo de puente, la banca global podría desbloquear de inmediato miles de millones en eficiencias operativas.
3. **Cuantificación del ahorro mediante sincronización:** La transición hacia un modelo de colateral síncrono en tiempo real (como el implementado sobre Canton Network) permitiría movilizar una porción sustancial de la deuda soberana. El análisis presentado ante la SEC proyecta que la pignoración en tiempo real y la movilización intradía de colaterales de EE. UU. generaría un **ahorro de capital**

anual superior a los 1.000 millones de dólares para las instituciones de crédito, acompañado de una **reducción de entre el 25% y el 50% en los costes de compensación** transaccional y una disminución drástica del riesgo de contraparte.

1.5 La trampa de liquidez: Buffers preventivos del 30%

A. La mecánica de la ineficiencia intradía: El coste del tiempo en tránsito

La gestión de la liquidez mayorista en la banca tradicional está sujeta a una restricción severa: **la velocidad del colateral no coincide con la velocidad de la volatilidad del mercado**.

Cuando una entidad financiera se enfrenta a una llamada de margen intradía, a un requerimiento de cobertura o a la necesidad de asegurar una operación de financiación a corto plazo, la tesorería se ve obligada a iniciar un proceso que, lejos de ser instantáneo, consume horas de mercado críticas.

La preparación, envío y procesamiento de instrucciones de liquidación y pignoración a través de redes de mensajería asíncrona como SWIFT inicia un flujo de reconciliación en cascada que involucra de forma aislada a los sistemas internos del banco, sus custodios globales y locales, y las cámaras de compensación.

Este desfase operativo consume entre 2 y 3 horas para una transferencia nacional estándar, y puede demorarse considerablemente más en transacciones internacionales. Durante esta ventana temporal, los activos pignorados se encuentran bloqueados en tránsito, en un "limbo contable", imposibilitando su reutilización inmediata (*rehypothecation*) para otras obligaciones de liquidez urgentes. Esta latencia intradía representa una exposición al riesgo de principal y de contraparte que las entidades deben cubrir de forma obligatoria mediante capital improductivo.

B. Ciclos de liquidación diferidos (T+2 / T+1) como secuestradores de capital

La persistencia de ciclos de liquidación diferidos, típicamente de **T+1 o T+2**, es un reflejo de la asincronía de los registros de custodia tradicionales, que actúan como "libros mayores privados aislados". En lugar de unificar el estado del activo de forma síncrona y directa entre las contrapartes, la infraestructura tradicional requiere que cada intermediario actualice secuencialmente su propio libro contable.

Este ciclo diferido secuestra temporalmente el balance de las tesorerías: **los bonos de alta calidad (HQLA) y la liquidez comprometidos en una transacción de colateral quedan técnicamente inmovilizados durante 24 a 48 horas**, limitando sustancialmente su velocidad de circulación sistémica.

Al no existir un mecanismo de liquidación atómica síncrona que ejecute el intercambio del activo contra el efectivo en el mismo instante matemático (Entrega contra Pago o DvP síncrono), las entidades financieras se ven atrapadas en ciclos asíncronos que drenan la eficiencia de su capital.

C. El "Weekend Downtime" y el sobredimensionamiento de los buffers

El impacto financiero de estas limitaciones operativas intradía y de ciclo diferido se agrava críticamente durante el **"Weekend Downtime" (el tiempo muerto de fin de semana)**. Las redes tradicionales de mensajería (SWIFT) y las cámaras de compensación y liquidación interrumpen su actividad el viernes por la tarde y permanecen cerradas durante un periodo de aproximadamente **60 horas** hasta el lunes por la mañana.

Dado que los riesgos geopolíticos, macroeconómicos y de mercado no se detienen durante el fin de semana, **las tesorerías bancarias se ven forzadas a mantener colchones de liquidez y garantías inactivos y sobredimensionados de forma puramente preventiva para sobrevivir a este periodo de inoperatividad de los sistemas tradicionales**. Si ocurre un evento de tensión financiera un sábado, la imposibilidad técnica de movilizar y liquidar de manera síncrona y atómica bonos soberanos contra efectivo para obtener liquidez inmediata expone al banco a un severo riesgo operativo intradía.

D. La trampa del 30%: El coste financiero del capital cautivo

Como consecuencia de la combinación de estos tres factores

1. la latencia intradía de 2 a 3 horas,
2. el secuestro de capital bajo ciclos T+2/T+1 y
3. las 60 horas de inactividad del fin de semana,

las tesorerías bancarias se ven obligadas a mantener inmovilizado de manera preventiva un buffer de hasta un 30% de sus activos líquidos de alta calidad (HQLA).

Este colchón estéril no responde a necesidades estratégicas o de inversión del negocio; su única función es mitigar y absorber la ineficiencia operativa de la infraestructura tradicional para asegurar que el colateral físico llegue a tiempo ante fluctuaciones imprevistas de mercado.

Este buffer del 30% representa una **"trampa de liquidez"** que penaliza directamente la rentabilidad de la institución:

- **Destrucción de rentabilidad (Capital Drag):** Al mantener congelada casi una tercera parte de sus reservas de garantía de alta calidad para cubrir la latencia operativa, la entidad disminuye drásticamente el rendimiento potencial de sus activos, impactando negativamente sobre el ROA (*Return on Assets*).
- **Inmovilización del colateral global:** A nivel macroeconómico, esto explica por qué de los **255 billones de dólares** en valores negociables aptos para colateral en el mundo, **solo el 11% (28 billones) se moviliza activamente**, mientras que el 89% restante permanece inactivo bajo un lastre de custodia preventivo (*custody drag*).
- **Asimetría Competitiva Directa:** Aquellas instituciones que posterguen la transición hacia infraestructuras síncronas operarán con costes de compensación duplicados y una ineficiencia estructural de capital de un tercio de su balance frente a competidores que adopten arquitecturas de sincronización síncrona como **Canton Network**, la cual permite liquidación atómica instantánea T+0, real-time valuation 24/7 y la eliminación de la conciliación bilateral manual.

1.6 El coste de oportunidad estratégico de los fines de semana (Weekend Downtime)

A. El fin de semana como "tiempo muerto" de la infraestructura financiera global

En la economía global interconectada actual, los riesgos financieros, geopolíticos y de mercado operan sin interrupción las 24 horas del día, los 7 días de la semana.

Sin embargo, **la infraestructura contable tradicional y los rieles de post-trading tradicionales cesan su actividad por completo los viernes por la tarde y permanecen cerrados durante aproximadamente 60 horas** hasta la mañana del lunes. Este cierre operativo sistemático responde a las limitaciones de horario de los custodios globales, las cámaras de compensación y los depositarios centrales de valores (CSD).

Durante esta prolongada ventana de inactividad, **el colateral y la liquidez comprometidos en el mercado mayorista tradicional quedan completamente inmovilizados**, atrapados en bases de datos desconectadas que son técnicamente incapaces de procesar transferencias o actualizaciones contables bilaterales. Este fenómeno de "tiempo muerto" (*dead time*) representa una ineficiencia crítica, ya que los balances de las tesorerías bancarias quedan congelados frente a cualquier fluctuación imprevista del mercado o necesidad de cobertura urgente que ocurra fuera de las horas de oficina estándar.

B. El sobredimensionamiento preventivo de las reservas líquidas

Para mitigar el riesgo sistémico de no poder movilizar colateral de alta calidad (HQLA) durante el fin de semana ante variaciones de margen o tensiones de liquidez, **las tesorerías bancarias tradicionales se ven forzadas a sobredimensionar sus reservas de efectivo y sus buffers líquidos de manera puramente preventiva**.

Este colchón de seguridad obligatorio actúa como una costosa póliza de seguro frente a la asincronía de la infraestructura tradicional:

- **Secuestro de capacidad productiva:** En lugar de desplegar estos activos líquidos para generar rendimientos activos o respaldar operaciones de financiación mayorista rentables, las entidades deben mantener capital inactivo para absorber las latencias operativas del fin de semana.
- **Inmovilización agregada:** Esta ineficiencia explica, en gran medida, por qué una proporción tan elevada del inventario global de colateral potencial de alta calidad —que asciende a **255 billones de dólares** a nivel macro— permanece bloqueada e inactiva bajo un lastre de custodia preventivo (*custody drag*), incapaz de circular cuando el mercado más lo necesita.

C. La brecha estratégica de financiamiento síncrono 24/7

La rigidez de mantener sistemas cerrados durante el fin de semana impide que las entidades optimicen su capital regulatorio en tiempo real y apliquen un margen dinámico y adaptativo.

Al carecer de una sincronización continua, **una llamada de margen imprevista en sábado o domingo no puede ser satisfecha movilizando síncronamente bonos soberanos contra liquidez de manera bilateral**, lo que incrementa notablemente la exposición al

riesgo de crédito de contraparte intradía y perpetúa la dependencia de costosos procesos de compensación centralizada al inicio de la semana siguiente.

La sincronización en tiempo real elimina este desfase temporal, permitiendo una **movilidad de colateral 24/7** y la optimización de la liquidez a través de la valoración continua y automatizada de los activos en el mismo instante matemático de su transferencia.

D. La validación empírica: El hito de liquidación en Canton Network

La viabilidad técnica y operativa de eliminar las fricciones del fin de semana ha sido plenamente demostrada en producción mediante hitos líderes dentro del ecosistema de Canton Network.

En **agosto de 2025, un consorcio integrado por Bank of America, Citadel Securities, DTCC, Societe Generale y Tradeweb completó con éxito la primera financiación de bonos del Tesoro de los EE. UU. contra USDC en tiempo real y on-chain un sábado**.

Esta operación histórica puso de manifiesto la capacidad del protocolo para:

1. **Sincronizar de forma atómica la entrega del activo y el pago (DvP síncrono) en fin de semana**, sin riesgo de principal y sin requerir la intervención manual o la apertura de las plataformas de liquidación tradicionales.
2. **Eliminar de forma inmediata los buffers preventivos de liquidez** de fin de semana, devolviendo una flexibilidad total a las tesorerías mediante una capacidad de financiación activa las 24 horas del día, los 7 días de la semana.

Esta demostración síncrona a gran escala se alinea con iniciativas estratégicas del mercado mayorista, como el **piloto de movilidad de colateral de Euroclear**, el cual utiliza Canton para transferir Gilts británicos, Eurobonos y oro físico entre registros y dominios de forma ininterrumpida las 24 horas del día, sentando las bases de una infraestructura de capital global sincronizada e inmune al *weekend downtime*.

1.7 La Asimetría de Inacción (Competitive Drag): El coste estratégico de postergar la adopción

La transformación de los mercados mayoristas de capitales mediante la pignoración y movilización de colateral en tiempo real ha dejado de ser una mera opción de eficiencia tecnológica para convertirse en una **asimetría competitiva de balance insostenible para las entidades tradicionales**.

El mantenimiento de infraestructuras asíncronas basadas en silos de información locales y mensajería de conciliación secuencial no representa una postura prudente de gestión de riesgos, sino la aceptación voluntaria de un **lastre financiero y operativo permanente frente a la competencia sincronizada**.

Las entidades que posterguen o decidan posponer de forma indefinida su migración hacia arquitecturas de sincronización síncrona y privacidad nativa de Layer 1, como la provista

por Canton Network, se verán expuestas a tres vectores de desventaja estratégica destructiva en sus estados financieros:

A. Capital Drag (El lastre de capital sobre el ROA)

En la operativa bancaria tradicional, las latencias derivadas del ciclo diferido T+1 o T+2 y las demoras de 2 a 3 horas requeridas para procesar y reconciliar instrucciones de valores bilaterales obligan a las tesorerías a mantener inmovilizado de manera preventiva un **buffer del 30% de sus activos líquidos de alta calidad (HQLA)**.

Mientras los competidores adaptados a redes de estado unificado logran movilizar el **100% de su balance de garantías en tiempo real y con liquidación instantánea T+0**, el banco tradicional continuará pagando el coste de oportunidad financiero de mantener una tercera parte de su colateral estéril y congelada45.

A escala global, esta ineficiencia se traduce en un fenómeno masivo de **custody drag o lastre de custodia**: de los **255 billones de dólares** en valores negociables demandados para su uso como colateral en el sistema financiero global, **solo el 11% (28 billones) se encuentra realmente activo y movilizado**, mientras que el 89% restante permanece inactivo en las cuentas de los custodios tradicionales. Las instituciones que adopten infraestructuras sincronizadas liberarán de inmediato este capital atrapado, optimizando su rentabilidad sobre activos (ROA) y operando con una flexibilidad de balance inalcanzable para las entidades rezagadas, lo que provocará un desplazamiento inmediato en las cuotas de participación del mercado de financiación mayorista.

B. Diferencial de Costes de Compensación y Ventaja de Precio

La sincronización contable instantánea y la atomicidad intrínseca de la entrega contra pago (DvP) nativa en la infraestructura de Canton eliminan por completo la necesidad de conciliación manual bilateral y reducen la dependencia de los intermediarios de post-trading.

Esta automatización de estado unificado permite a las entidades adaptadas registrar una **reducción de entre el 25% y el 50% en sus costes de compensación y liquidación transaccional intradía**, junto con un **ahorro de entre 3 y 5 millones de dólares en costes de riesgo de contraparte**.

Operar con una estructura de costes operativos que representa la mitad de la tradicional dota a los bancos sincronizados de una **capacidad de fijación de precios extremadamente agresiva**.

Estos competidores podrán estructurar y ofrecer préstamos respaldados, operaciones de recompra (*repos*) y derivados complejos con márgenes de beneficio mucho más competitivos, haciendo que la oferta del banco tradicional resulte financieramente inviable y fuera de mercado para los clientes institucionales regulados

Esta ventaja operativa se apoya además en la robustez matemática del sistema: las garantías de seguridad demostradas formalmente garantizan que la finalidad de estas transacciones sea legalmente indisputable, cerrando cualquier vulnerabilidad operativa intradía.

C. Exclusión de los Canales de Liquidez 24/7 y Riesgo de Volatilidad

Los mercados de colateral tradicionales operan bajo la limitación del horario laboral de los custodios e infraestructuras centrales de compensación, interrumpiendo su actividad durante los fines de semana y generando una ventana de **60 horas de inactividad operativa o Weekend Downtime**. Durante este fin de semana, el colateral y la liquidez tradicionales quedan completamente congelados e inmovilizados, forzando a las entidades a sobredimensionar sus colchones líquidos preventivos para absorber posibles crisis de liquidez fuera de hora.

En contraste, Canton Network rompe esta limitación física al habilitar una **capacidad de financiación activa las 24 horas del día, los 7 días de la semana (24/7)**, permitiendo ejecutar transferencias de garantías y swaps atómicos intradía de forma ininterrumpida.

Un hito definitivo de esta capacidad se demostró en **agosto de 2025, cuando un consorcio de primer nivel compuesto por Bank of America, Citadel Securities, DTCC, Societe Generale y Tradeweb liquidó con éxito la primera operación de financiación real on-chain de bonos del Tesoro de EE. UU. contra USDC un sábado**.

Las entidades tradicionales que pospongan su unión a estas plataformas síncronas quedarán **completamente excluidas de estos nuevos pools de liquidez y swaps interbancarios de fin de semana**.

Al carecer de herramientas de movilización de colateral HQLA durante sábado y domingo, estas tesorerías tradicionales no podrán ajustar sus coberturas ni responder de forma síncrona a eventos imprevistos de volatilidad internacional, quedando expuestas de manera asimétrica a severos choques de mercado y llamadas de margen acumuladas en la apertura del lunes por la mañana, mientras sus competidores sincronizados ya habrán mitigado y neutralizado el riesgo en tiempo real en fin de semana.

CAPÍTULO 2: Por qué la Blockchain Pública no es Viable para la Operativa Bancaria

2.1 El obstáculo absoluto de la publicidad de los datos de la Layer 1

La adopción de la tecnología blockchain en el mercado financiero mayorista se ha enfrentado históricamente a una barrera de diseño insalvable: **la publicidad radical de las arquitecturas de primera generación**.

Redes públicas de estado globalmente replicado como Ethereum, Solana o XRP Ledger (Ripple) fueron concebidas bajo el principio de la transparencia total, donde cada transacción, saldo y dirección es visible para cualquier nodo de la red. Este modelo de visibilidad absoluta es **estructural y legalmente incompatible con los requisitos de confidencialidad comercial, secreto bancario y deber de custodia** que rigen la actividad de las instituciones financieras reguladas.

Desde una perspectiva de control contable y de cumplimiento, un registro distribuido (*ledger*) es la representación definitiva de los libros y registros (*books and records*) del banco.

En su comunicación oficial ante la SEC en febrero de 2025, se planteaba una analogía fundamental para la alta dirección: de la misma forma que ninguna entidad financiera regulada aceptaría mantener sus registros de cuentas tradicionales en un panel de anuncios de acceso público en internet, **es inviable que la banca deposite el registro de propiedad de sus valores y colaterales en redes donde cualquier actor anónimo puede auditar el balance completo de la institución.**

La transparencia por defecto de los estados contables públicos constituye, por tanto, un obstáculo absoluto e ineludible.

El impacto de esta transparencia no es meramente normativo, sino que afecta de forma directa a la viabilidad de las estrategias comerciales en el mercado mayorista:

Exposición de estrategias y front-running: Si una mesa de tesorería ejecuta operaciones de recompra (*repos*) o pignoración de colaterales en una cadena pública transparente, está **retransmitiendo en vivo sus posiciones de liquidez, coberturas y acuerdos de financiación a sus competidores directos.** Al analizar el volumen y la frecuencia del tráfico de metadatos o direcciones pseudónimas, firmas rivales pueden predecir necesidades de refinanciación inminentes y ejecutar tácticas de arbitraje o *front-running*, destruyendo el margen comercial de la operación.

Fuga de datos de clientes e inteligencia empresarial: El procesamiento de cobros, nóminas corporativas, pagos a proveedores o márgenes de derivados en redes replicadas **desvela relaciones corporativas y flujos de caja estratégicos que deben permanecer bajo estricto secreto comercial.** En entornos altamente competitivos, la inferencia de flujos de repos interbancarios a través del análisis de libros mayores compartidos elimina la asimetría de información necesaria para la negociación de precios bilateral.

El fracaso de la falsa privacidad pseudónima: La creencia de que el pseudonimato (operar con claves públicas en lugar de identidades explícitas) protege a la banca en redes públicas ha quedado desmontada por el avance del análisis de datos en cadena (*blockchain intelligence*). Herramientas sofisticadas de rastreo permiten asociar patrones de comportamiento y agrupamiento de direcciones con identidades institucionales reales en cuestión de minutos, lo que expone a los bancos a severas vulnerabilidades operativas y de ciberseguridad.

Esta incompatibilidad estructural explica por qué, a pesar de que casi todos los bancos de importancia sistémica global (G-SIBs) ejecutaron múltiples pruebas piloto e iniciativas experimentales en blockchains públicas o consorcios de libro único entre 2017 y 2022, **prácticamente ninguna de estas iniciativas logró alcanzar la fase de producción regulatoria.**

La transparencia de los datos y la consiguiente pérdida de control sobre los activos pignorados representaban un riesgo sistémico inaceptable para los departamentos de riesgos y de cumplimiento.

En consecuencia, la replicación global de estados y la visibilidad de extremo a extremo en la Layer 1 pública se consolidaron como un **"non-starter" definitivo para la integración segura del colateral financiero mayorista on-chain.**

2.2 El riesgo de contraparte y la ausencia de controles KYC/AML nativos

El segundo obstáculo estructural que invalida el uso de blockchains públicas tradicionales (basadas en mecanismos de consenso *Proof-of-Work* o *Proof-of-Stake*) en el mercado financiero mayorista no es de índole criptográfica, sino de **arquitectura legal y prudencial**.

Para una entidad financiera regulada, la adopción de una tecnología de registro distribuido implica, en última instancia, utilizar la cadena de bloques como el sistema definitivo de **libros y registros contables (*books and records*)** de sus activos y valores.

Bajo esta premisa, la actualización de estos registros no puede ser delegada a una red abierta de validadores anónimos.

El peligro legal de la validación anónima e incontrolada

En redes como Ethereum o Solana, la validación de las transacciones y la actualización del estado global de la red dependen de un conjunto dinámico de nodos validadores distribuidos globalmente, donde literalmente cualquier sujeto puede operar un nodo sin identificación previa.

Para un banco que gestiona activos de alta calidad (HQLA), como un bono del Estado Español o bonos del Tesoro de EE. UU., **permitir que el registro contable de la propiedad de estos valores sea actualizado por validadores anónimos —que podrían estar ubicados en jurisdicciones sancionadas o no sometidas a supervisión bancaria—**

representa una quiebra inadmisible del deber de control interno, de la finalidad de la liquidación y de las obligaciones de prevención del blanqueo de capitales (AML/CFT).

La banca regulada exige de forma ineludible interactuar con **contrapartes conocidas y legalmente responsables**, eliminando la incertidumbre de un consenso gestionado por desconocidos.

La penalización prudencial del Comité de Basilea

Este riesgo operativo y legal ha sido firmemente sancionado por las autoridades regulatorias globales. En sus normas prudenciales sobre la exposición a criptoactivos (*Prudential Standards for the Treatment of Cryptoasset Exposures*), el **Comité de Basilea de Supervisión Bancaria (BCBS)** dictaminó que cuando un activo del mundo real (como un bono tradicional) es tokenizado sobre una blockchain pública y sin permisos (*permissionless*), este **pierde su consideración de valor tradicional pignorable y recibe el mismo tratamiento de alto riesgo y penalización de capital que un criptoactivo nativo (como Bitcoin o Ether)**.

El Comité justifica esta severa clasificación debido a que el uso de redes públicas introduce riesgos únicos que no se pueden mitigar en la actualidad, destacando de forma explícita la dependencia de terceros no identificados para realizar operaciones básicas, la falta de gobernanza, los problemas de privacidad, la incertidumbre en la finalidad de la liquidación (*settlement finality*) y la ausencia de controles AML/CFT en la capa de protocolo.

La incompatibilidad con la Travel Rule y controles KYC

Los deudores y entidades financieras tradicionales están obligados por mandatos del GAFI a verificar la identidad de los ordenantes y beneficiarios de cualquier transferencia de valor (KYC/AML) y a transmitir esta información de forma segura junto con la transacción (Travel Rule).

En una blockchain pública convencional, la transparencia radical y la falta de soporte nativo para identidades autenticadas impiden cumplir de manera complementaria con la privacidad de los datos personales (conforme a regulaciones como **GDPR**) y los controles de cumplimiento de prevención del blanqueo.

Intentar implementar estos controles mediante segundas capas (Layer 2) o parches externos de conocimiento cero (ZKP) no resuelve la ecuación, ya que **rompe la composibilidad transaccional, fragmenta la liquidez en nuevos silos y añade riesgos severos de seguridad por la opacidad total de los datos de balance.**

Esta frase sintetiza los tres grandes problemas técnicos y financieros que ocurren cuando las instituciones intentan "parchear" la falta de privacidad de las blockchains públicas (como Ethereum o Solana)

A continuación, se desglosa el significado profundo de cada uno de los tres componentes de la afirmación:

1. "Rompe la composibilidad transaccional"

La **composibilidad transaccional** es la capacidad de que múltiples aplicaciones, contratos inteligentes y activos interactúen entre sí de manera directa y se liquiden de

forma **atómica** (es decir, en un único instante matemático bajo el principio de "todo o nada").

- **El problema en redes públicas:** Para evitar que todo el mundo vea sus operaciones en la Capa 1 (L1) pública, los bancos se ven obligados a mover sus activos a redes de Segunda Capa (L2) o canales laterales.
- **La ruptura:** Al hacer esto, las transacciones quedan confinadas a esa L2 específica. Si un banco quiere realizar una entrega contra pago (DvP) donde el activo está en la "L2 de bonos" y el efectivo está en la "L2 de depósitos", **los contratos ya no se pueden ejecutar en una sola transacción unificada y atómica a nivel de L1**. Para conectarlas se requiere el uso de "puentes" (*bridges*) o protocolos complejos de mensajería que **añaden latencia, rompen la sincronización instantánea y destruyen la composibilidad nativa** del sistema.

2. "Fragmenta la liquidez en nuevos silos"

En el sistema financiero tradicional, la fragmentación de la liquidez en silos contables es una de las mayores causas de ineficiencia. Paradójicamente, las soluciones L2 replican este problema en el entorno digital.

- **El aislamiento de los activos:** En lugar de operar en un mercado unificado y fluido, cada solución de privacidad L2 o canal privado funciona como una **isla tecnológica independiente**. Al mover los valores a una L2 para proteger la confidencialidad, **se desconecta a los participantes de la liquidez del resto de la red**.
- **La paradoja de la privacidad en L2:** Además, dentro de una misma L2, la privacidad individual suele desaparecer: todos los participantes autorizados en esa L2 en particular pueden ver las transacciones y posiciones de los demás (un problema real que se detectó, por ejemplo, en pilotos de bancos centrales como el proyecto Drex de Brasil). Por tanto, la liquidez se divide en decenas de pequeños silos ineficientes que no se comunican entre sí.

3. "Añade riesgos severos de seguridad por la opacidad total de los datos de balance"

Para proteger la privacidad sin salirse de la L1 pública, muchos proyectos proponen usar **Pruebas de Conocimiento Cero (ZKPs)**. Las ZKPs permiten demostrar criptográficamente que una transacción es válida (por ejemplo, que el emisor tiene fondos suficientes) sin revelar el saldo real de la cuenta ni las identidades implicadas. Sin embargo, en el mercado institucional regulado, esto introduce un riesgo de seguridad crítico.

- **Vulnerabilidades de código e "inflación infinita":** Las implementaciones de ZKP son matemáticamente complejas y difíciles de auditar, lo que las hace vulnerables a fallos de software ocultos. Si el código de un circuito ZKP tiene un error, un atacante podría falsificar las pruebas criptográficas y **crear activos de la nada (un riesgo de falsificación o duplicación infinita de activos)**, tal como ocurrió históricamente en redes de privacidad nativa como Zcash.
- **Incertidumbre del colateral pignorado:** Debido a la opacidad total que imponen las ZKPs, una mesa de tesorería que acepte bonos del Tesoro como colateral para una operación de repo **no tiene forma de verificar con total certeza si la**

contraparte posee realmente el activo físico de respaldo. Si el sistema falla y el repo debe deshacerse bajo condiciones de estrés, la imposibilidad de auditar directamente la existencia del activo subyacente puede desencadenar un **colapso sistémico y una pérdida total de confianza en el mercado**.

La Solución de Canton Network frente a este escenario

Canton Network fue diseñada específicamente para resolver esta encrucijada mediante su **privacidad nativa en la Layer 1 basada en "necesidad de saber"**.

En lugar de aislar los activos en L2s o cegar los balances por completo con ZKPs, Canton segmenta los datos utilizando el lenguaje **Daml**. Solo las contrapartes implicadas en una transacción concreta ven e inscriben el cambio de estado (que se valida de forma bilateral P2P), mientras que un **Global Synchronizer** descentralizado ordena los mensajes cifrados para evitar el doble gasto de colateral sin llegar a ver el contenido de los balances.

Esto permite que la red mantenga la **composibilidad atómica y la liquidez global** de todas las dApps financieras integradas en la L1, proporcionando al mismo tiempo una **pista de auditoría criptográfica auditable** (incluso mediante nodos especiales para reguladores) que elimina de raíz los riesgos de opacidad de las ZKPs tradicionales.

La alternativa síncrona y permisionada de Canton

Canton Network supera esta limitación mediante su estructura **público-permisionada**, donde se produce una estricta separación entre la validación del smart contract (ejecutado únicamente de forma P2P por las partes directamente involucradas mediante el protocolo *Proof of Stakeholder*) y la ordenación secuencial de las transacciones (delegada de forma cifrada al *Global Synchronizer*). Esto garantiza que:

1. **Gobernanza de Identidad:** Todos los validadores e instituciones participantes de la red son entidades conocidas, supervisadas y previamente identificadas criptográficamente dentro del directorio topológico administrado de forma federada por la *Canton Network Foundation*.
2. **Cumplimiento AML/KYC Integrado:** El uso del lenguaje funcional **Daml** permite codificar reglas de cumplimiento y verificación de credenciales directamente en el núcleo de los contratos inteligentes. De este modo, la privacidad por defecto coexiste nativamente con la auditabilidad reguladora, permitiendo configurar roles específicos de observador (*Observer*) para que los reguladores o supervisores puedan monitorizar transacciones sospechosas en tiempo real sin revelar las posiciones comerciales al resto del mercado.
3. **Inteligencia de Cumplimiento en Entornos Privados:** Mediante la integración de herramientas avanzadas de *blockchain intelligence* como las provistas por **TRM Labs**, la red permite aplicar un modelo de **divulgación basada en el riesgo (*risk-based disclosure*)**. En este entorno, las transacciones legítimas se mantienen totalmente encriptadas y privadas por defecto, pero ante señales de alto riesgo o alertas del sistema de cumplimiento, se pueden desencadenar revelaciones de datos controladas y auditables hacia los oficiales de cumplimiento (*Guardians* de los activos) o autoridades de supervisión competentes.

Con esto, Canton unifica la robustez de los controles de cumplimiento de las instituciones con la agilidad y finalidad determinista intradía de la tecnología de registro distribuido,

pavimentando un camino seguro y compatible para la movilización de colaterales de alta calidad sin incurrir en las vulnerabilidades de cumplimiento e insolvencia operativa de las blockchains públicas.

2.3 La ineficiencia estructural de las soluciones de parche

La incapacidad intrínseca de las redes descentralizadas públicas de Layer 1 tradicionales para ofrecer confidencialidad nativa ha impulsado el desarrollo de tecnologías accesorias diseñadas para mitigar estas deficiencias. Sin embargo, la implementación de segundas capas (Layer 2) y de Pruebas de Conocimiento Cero (ZKP) se comporta en la práctica como una colección de parches tecnológicos que, lejos de resolver los problemas de origen de la infraestructura de mercado, introducen nuevas ineficiencias estructurales, vulnerabilidades críticas de seguridad y una fragmentación severa del balance y la liquidez.

2.3.1 Limitaciones de las Pruebas de Conocimiento Cero (ZKP)

Las Pruebas de Conocimiento Cero (ZKP) se presentan frecuentemente ante la junta directiva como la solución definitiva a la privacidad en entornos descentralizados, pero su aplicación práctica en las finanzas mayoristas reguladas adolece de limitaciones conceptuales y técnicas de gravedad extrema.

- **La falacia del blindaje total frente a la "necesidad de saber":** Las soluciones basadas en ZKP imponen un modelo de privacidad binario y rígido: u ocultan los datos por completo mediante un blindaje total o los exponen públicamente en la Layer 1. Este enfoque de "todo o nada" carece de la flexibilidad nativa necesaria para la operativa financiera real, donde la confidencialidad no debe traducirse en un bloqueo absoluto de información, sino en una gobernanza dinámica basada en la **"necesidad de saber" (*need-to-know*)**. En Canton Network, la privacidad por sub-transacción permite que cada parte registre y visualice únicamente la porción del contrato inteligente que le compete (por ejemplo, el banco liquidador ve la pata de efectivo y el registrador ve la pata de valores en una Entrega contra Pago), manteniendo una composibilidad completa. Las ZKPs no pueden replicar este comportamiento estructurado y multifacético sin destruir su eficiencia matemática o requerir complejos esquemas de revelación que devalúan su propósito original.
- **Ruptura de la auditabilidad en tiempo real:** Al encriptar y cegar por completo el estado del libro contable mayor, las ZKPs rompen la auditabilidad directa y en tiempo real que exigen las autoridades de supervisión y los departamentos de control de riesgos. Un banco regulado debe estar en condiciones de proporcionar a sus supervisores y reguladores un acceso transparente e inmediato a sus registros transaccionales para cumplir con normativas de prevención del blanqueo de capitales (AML) y reporte sistémico. Canton Network resuelve esta tensión de manera nativa al permitir la asignación de nodos observadores (*Observers*) específicos para los reguladores, quienes pueden auditar transacciones en tiempo real sin que estas dejen de ser visibles o privadas para el resto de los participantes del mercado. Bajo un esquema ZKP, la opacidad matemática impide que el regulador actúe como un validador pasivo integrado, forzando la creación de

engorrosos canales de descifrado fuera de banda que reintroducen latencias y fallos operativos.

- **Vulnerabilidades de software e inflación infinita:** Las matemáticas detrás de los circuitos de ZKP son de una complejidad extrema, lo que las hace altamente vulnerables a fallos de codificación, exploits y errores de implementación que escapan a las pruebas convencionales de software. Un error de diseño en un algoritmo ZKP puede permitir que un atacante genere pruebas criptográficas falsas pero válidas, lo que abre la puerta a la **falsificación o duplicación infinita de activos sin que la red lo detecte**. Esta amenaza no es teórica; la historia de las redes de privacidad nativa registra incidentes críticos, como el histórico bug de Zcash que habría permitido la falsificación ilimitada de tokens. Un riesgo de esta naturaleza es absoluto e inaceptable para la infraestructura contable de instrumentos sistémicos como la deuda soberana.
- **Incertidumbre del colateral y riesgo de liquidación catastrófico:** La opacidad de las ZKPs introduce un riesgo moral y operativo insostenible en el mercado de financiación mayorista. Si una entidad financiera acepta bonos del Tesoro de EE. UU. tokenizados como colateral para un repo mediante un sistema protegido por ZKP, **la seguridad del balance dependerá enteramente de la infalibilidad matemática del algoritmo de prueba, no de la existencia verificable del activo**. Debido a fallos latentes en el software, las tenencias reales de la contraparte podrían diferir drásticamente de lo que afirma su prueba criptográfica, incluso después de que tales fallos hayan sido descubiertos y parchados. Si el repo requiere ser deshecho bajo condiciones de estrés de mercado y se descubre que el colateral subyacente es inexistente o insuficiente, las consecuencias de liquidez para la entidad acreedora y para el sistema financiero global serían catastróficas.

2.3.2 Fragmentación de liquidez en Layer 2

Para solventar las limitaciones de rendimiento y privacidad de las Layer 1 públicas, la industria ha recurrido de forma sistemática al despliegue de redes de Segunda Capa (Layer 2 o L2) y rollups. Sin embargo, trasladar la operativa de colateral a estas redes accesorias fragmenta el mercado y reproduce las mismas ineficiencias de silos de datos que la tecnología blockchain pretendía eliminar originalmente.

- **Creación de nuevos silos de datos inconexos:** Al mover los activos del mundo real (RWA) a canales L2 independientes para proteger su privacidad, las tesorerías bancarias aíslan sus activos en infraestructuras cerradas. Cada rollup o canal de segunda capa funciona como un compartimento estanco técnico y contable que carece de interoperabilidad nativa con los demás. Este diseño obliga a los participantes a dispersar sus reservas de colateral en múltiples redes separadas, reduciendo severamente la velocidad de circulación de las garantías y obligando a mantener buffers de capital inactivos aún mayores para cubrir las posiciones de cada canal individual.
- **Ruptura de la atomicidad y la composibilidad transaccional:** La ventaja primordial de la digitalización síncrona es la **composibilidad atómica**, es decir, la capacidad de ejecutar transacciones multifirma bajo el principio de "todo o nada" en un único instante matemático. En un proceso de post-trading tradicional o en un DvP, el traspaso del activo (colateral) y la liquidación del pago (efectivo) deben ser completamente síncronos. Sin embargo, las Layer 2 carecen de composibilidad transaccional a nivel de Layer 1. Si la pata del efectivo reside en una L2 y la pata del activo en otra L2 o en la capa principal, la liquidación atómica bilateral es técnicamente inviable sin recurrir a intermediarios o a complejos esquemas de coordinación que reintroducen el riesgo de principal.
- **Ausencia de privacidad real dentro de la propia Layer 2:** Mover la operativa a una Capa 2 solo protege la información frente a los observadores externos de la Layer 1 pública, pero **dentro de la propia Layer 2 la privacidad es inexistente**. Todos los participantes autorizados que operan dentro de un mismo canal L2 o rollup tienen acceso directo a la información transaccional, saldos e identidades del resto de las instituciones integradas en esa misma capa. Un ejemplo empírico de esta limitación fue el programa piloto del banco central de Brasil (para su CBDC, Drex), donde quedó demostrado que las soluciones de Layer 2 no eran viables para la banca regulada porque cualquier entidad participante del canal podía ver e incluso poseer los registros transaccionales completos del resto de sus competidores.
- **El riesgo sistémico de los puentes (*bridges*) de Layer 2:** Para lograr que los activos de diferentes Layer 2 interactúen entre sí, las arquitecturas públicas tradicionales dependen críticamente de puentes criptográficos de terceros (*cross-chain bridges*). Estos puentes funcionan bloqueando el activo original en un contrato inteligente de origen y emitiendo una representación respaldada ("wrapped") en la red de destino. Desde el punto de vista de la seguridad de la infraestructura mayorista, esta arquitectura es un vector de vulnerabilidad inaceptable: **si el contrato inteligente del puente o su custodio es hackeado o comprometido, el activo wrapped en la red de destino pierde instantáneamente todo su valor y**

respaldo real. La escala del riesgo es masiva; los exploits históricos en puentes de criptoactivos (como Ronin, Binance, Wormhole o Nomad) han acumulado pérdidas por miles de millones de dólares, demostrando que la dependencia de estas pasarelas accesorias constituye el punto de fallo más vulnerable del ecosistema mayorista on-chain.

CAPÍTULO 3: La Incompatibilidad de las Redes Privadas de Registro Único Compartido

3.1 El mito del "Libro Mayor Único Compartido" (Shared Ledger)

La primera ola de experimentación con tecnologías de registro distribuido (DLT) en el sector financiero —llevada a cabo fundamentalmente entre 2017 y 2022— se concentró en el despliegue de **blockchains privadas consorciadas y permisionadas**. Bajo plataformas tradicionales como Hyperledger Fabric o Corda, la industria intentó resolver el problema de la confianza mediante la creación de subredes o canales cerrados. Sin embargo, estas arquitecturas heredaron un vicio de diseño fundamental de las redes descentralizadas primitivas: **la dependencia de un registro contable único y compartido, cuyo estado completo es replicado de forma redundante entre múltiples participantes**.

Esta replicación global de estado dentro de la subred consorciada desmorona cualquier expectativa de confidencialidad comercial y secreto profesional en el mercado financiero mayorista:

- **Visibilidad redundante y replicación forzada:** En las blockchains consorciadas tradicionales, todos los participantes admitidos en un canal o subred deben almacenar y validar una copia idéntica del libro contable mayor para mantener el consenso. Esto implica que, aunque se restrinja el acceso a actores externos, **cualquier entidad perteneciente al consorcio puede ver todos los cambios de estado, saldos y detalles transaccionales de los demás miembros de la subred**. Intentar mitigar esta visibilidad mediante el aislamiento en múltiples "canales bilaterales" independientes solo fragmenta la liquidez de colateral en silos rígidos que impiden la interoperabilidad y rompen la composibilidad transaccional síncrona.
- **La quiebra del secreto bancario y la exposición estratégica:** Obligar a entidades financieras competidoras a compartir la misma base de datos contable expone de forma directa sus estrategias comerciales bilaterales, sus necesidades intradía de colateralización y sus acuerdos de liquidez a los demás miembros del consorcio. Al supervisar el volumen, la frecuencia y los patrones de actualización del registro compartido, una entidad rival puede deducir posiciones de tesorería críticas y realizar prácticas de arbitraje o *front-running*, destruyendo la neutralidad comercial del mercado. El modelo de "un solo libro mayor compartido" es, por tanto, una contradicción técnica insalvable para la banca mayorista: exige que los competidores elijan entre cooperar sobre una infraestructura común que les expone comercialmente o aislarse en silos contables ineficientes que perpetúan las latencias de conciliación tradicionales.

Esta limitación estructural de las blockchains privadas tradicionales se evidenció de forma empírica en iniciativas gubernamentales recientes. Durante las pruebas del programa piloto del banco central de Brasil para su moneda digital (Drex), se intentó emplear una infraestructura de segunda capa sobre un libro compartido para proteger la privacidad de los flujos interbancarios. Sin embargo, el piloto demostró que **cualquier banco participante del canal o subred compartida seguía teniendo visibilidad técnica sobre**

la totalidad de los datos transaccionales de sus competidores, haciendo imposible el cumplimiento del secreto bancario y las normas de protección de datos personales. La persistencia en arquitecturas de estado globalmente replicado anula la posibilidad de estructurar flujos de colateral síncronos con privacidad de "necesidad de saber" (*need-to-know*), consolidando al registro compartido consorciado como un callejón sin salida estratégico para la banca mayorista regulada.

3.2 El problema de la contención de recursos financieros

El segundo defecto estructural de los sistemas basados en un registro compartido único es la **contención de recursos globales**. En las arquitecturas blockchain tradicionales de primera y segunda generación, todas las aplicaciones, contratos inteligentes y participantes de la red compiten de forma directa por el mismo rendimiento de transacciones y por la capacidad de procesamiento del procesador de red. Esta centralización forzada del procesamiento repliega de manera exacta las congestiones, la volatilidad de las tarifas y los cuellos de botella característicos de las redes públicas sin permisos.

Para las tesorerías e infraestructuras del mercado financiero mayorista, la contención de recursos representa una vulnerabilidad operativa y financiera inasumible bajo tres dimensiones críticas:

- **Vulnerabilidad operativa por congestión ajena (el "Efecto CryptoKitties"):** En un registro compartido único, el rendimiento y la latencia de procesamiento de una transacción financiera sistémica están directamente condicionados por la actividad de aplicaciones completamente ajenas e irrelevantes para el negocio institucional. La historia de las blockchains públicas ofrece precedentes ilustrativos: en 2017, el lanzamiento masivo del juego digital *CryptoKitties* en la red Ethereum llegó a consumir más del 12% de la capacidad transaccional de la Layer 1, colapsando el sistema y disparando las tarifas de gas de forma generalizada para todos los usuarios. Trasladado al ámbito institucional, **un banco que intente liquidar de urgencia una operación de reporto (repo) de 500 millones de dólares para cumplir con una llamada de margen regulatoria no puede verse sometido a retrasos operativos ni competir en el mismo "mempool" global de transacciones con emisiones de tokens especulativos, robots de arbitraje o juegos minoristas**.
- **Impredictibilidad y encarecimiento de los costes de transacciones (Tarifas Interconectadas):** En las redes con recursos de procesamiento global compartidos, el coste por transacción (gas) es altamente dinámico e impredecible. Debido a la interconexión de las comisiones, un incremento repentino en el volumen de uso de una sola dApp popular de la red eleva mecánicamente los costes de transacción para todos los participantes de la plataforma. Para una tesorería bancaria, la imposibilidad de presupuestar de forma precisa y predecible sus costes de post-trading intradía introduce una volatilidad de balance inasumible que erosiona el margen comercial de las operaciones de financiación y de cobertura de riesgos.

- **Límites verticales de escalabilidad y "off-chain drift":** Las limitaciones verticales de rendimiento de los registros únicos compartidos obligan a los desarrolladores a construir la mayor parte de la lógica compleja de negocio "fuera de la cadena" (*off-chain*), utilizando proveedores centralizados. Al hacer esto, la red blockchain queda reducida a un mero registro de saldos simplificado, mientras que los flujos de trabajo, las validaciones y el control de cumplimiento vuelven a confinarse en servidores tradicionales aislados. Este diseño asíncrono no solo anula la verificabilidad independiente que los participantes esperan de un registro distribuido, sino que recrea la necesidad de reconciliación bilateral contable que la tecnología blockchain debía erradicar.

La Solución mediante la Partición de Estado de Canton Network

Canton Network elimina de raíz el problema de la contención de recursos al sustituir la replicación de estado global por una **arquitectura horizontal descentralizada de "red de redes"**. Al separar la validación de contratos del ordenamiento de transacciones, Canton permite que los participantes y las aplicaciones se organicen en dominios de sincronización específicos para cada caso de uso.

De este modo:

1. **Paralelismo transaccional absoluto:** Un dominio que procesa flujos de repo intradía (como Broadridge DLR) opera de forma totalmente aislada e independiente de los dominios de depósitos tokenizados o de activos digitales de consumo, evitando cualquier tipo de interferencia mutua en el rendimiento transaccional.
2. **Rendimiento y capacidad altamente escalables:** Dado que cada participante solo almacena, procesa y valida los contratos en los que tiene un rol de parte autorizada (*Active Contract Set* o ACS), el rendimiento del sistema no tiene un límite superior técnico global, sino que escala de forma horizontal y lineal con cada nuevo participante o dominio que se incorpora al ecosistema.
3. **Costes transaccionales fijos y predecibles:** Al operar sobre dominios específicos, Canton independiza las comisiones de la actividad general de la red. El uso de comisiones fijas en dólares para el acceso al *Global Synchronizer* otorga a las instituciones la predictibilidad de costes que requiere la planificación financiera a largo plazo, desactivando de forma definitiva la trampa operativa de los registros compartidos únicos.

3.3 Gobernanza rígida y centralizada

La tercera gran limitación de las redes blockchain consorciadas convencionales radica en su **inflexibilidad y centralización a nivel de gobernanza institucional**. Los consorcios privados tradicionales de base de datos compartida sufren de una gobernanza rígida, donde un único operador de infraestructura o un subcomité central de control decide de manera unilateral todas las actualizaciones del sistema, retiene las llaves criptográficas de seguridad y administra de forma exclusiva los permisos de membresía de la red.

Esta centralización de facto anula los principios de soberanía bancaria e introduce barreras críticas:

- **El obstáculo de la gobernanza heredada u homogénea:** En los esquemas consorciados tradicionales, todas las aplicaciones y participantes del consorcio están obligados a heredar la misma estructura de gobernanza, políticas de acceso y reglas de privacidad del libro compartido subyacente. Esto impide que un emisor de colaterales configure políticas de control, acceso y tarifas personalizadas según los requerimientos regulatorios locales de su jurisdicción, forzándolo a una operativa de "todo o nada" que es inviable en el sector financiero altamente diversificado.
- **Riesgo de bloqueo y veto operativo (Vendor Lock-in):** Si el comité de control central decide postergar o denegar una actualización crítica para los procesos de post-trading de un participante, este último se encuentra completamente atado a la hoja de ruta de la fundación o empresa proveedora de la tecnología, asumiendo costes de migración insostenibles.

La respuesta de Canton: Soberanía de Gobernanza y Federación Democrática

Canton Network rompe con este modelo rígido de gobernanza centralizada al implementar una **arquitectura descentralizada de "red de redes"**, estructurando la gobernanza sobre dos pilares fundamentales:

1. **Soberanía absoluta de las aplicaciones (Sistemas Federados Libres):** En Canton, el uso del lenguaje de contratos inteligentes Daml y la separación de la lógica contractual respecto a la ordenación física de las transacciones garantizan que cada participante retenga la autonomía absoluta sobre sus activos. **Cada emisor y proveedor de aplicaciones decide de forma soberana sus propias políticas de privacidad, tarifas, escalabilidad, permisos y gobernanza particular sin depender de un administrador global con control omnímodo ("God Mode") o de un subcomité de control de consorcio**.
2. **Gobernanza federada basada en identidad ("1 Institución = 1 Voto"):** Para transacciones atómicas que deben cruzar dominios y aplicaciones interbancarias, Canton proporciona el **Global Synchronizer**. No obstante, este sincronizador global no está administrado por una sola corporación tecnológica, sino que está gobernado de forma independiente y neutral por la **Canton Network Foundation (CNF)**. La junta directiva de esta fundación, establecida como entidad sin fines de lucro bajo el paraguas de la *Linux Foundation*, está compuesta por representantes elegidos de las propias instituciones bancarias globales (como bancos sistémicos G-SIBs) y operadores de infraestructuras financieras.
3. **Prevención de la cartelización plutocrática:** A diferencia de las segundas capas (Layer 2) o redes públicas basadas en pesos financieros donde se impone el principio de "1 token = 1 voto" (lo que facilita la cartelización transaccional por acumulación de capital), **la gobernanza de Canton se basa estrictamente en la identidad institucional y corporativa verificada bajo el lema de "1 institución = 1 voto"**. Esto asegura una gobernanza robusta, predecible y democrática, alineada

por completo con los estándares de control, resiliencia y cumplimiento de riesgos que exigen los reguladores internacionales.

CAPÍTULO 4: El Modelo Canton: Red de Redes con Privacidad Nativa en Layer 1

4.1 Filosofía de "Red de Redes": El Libro Mayor Virtual Global

El núcleo de la innovación arquitectónica de Canton Network radica en una ruptura radical con el dogma de la tecnología blockchain convencional: **la eliminación de la replicación global de estados y la superación del paradigma del registro compartido único.**

Mientras que las redes blockchain de primera y segunda generación obligan a todos los participantes a almacenar, validar e inscribir la totalidad de las transacciones y contratos de la red (generando problemas insalvables de privacidad, escalabilidad y contención de recursos), **Canton introduce una filosofía descentralizada de "Red de Redes" estructurada sobre un Libro Mayor Virtual Global sin necesidad de un estado global replicado.**

Bajo esta concepción virtual y distribuida, la arquitectura de Canton opera de la siguiente manera:

- **Segmentación de datos y soberanía local:** En lugar de replicar el libro de contabilidad de forma redundante y masiva entre todos los nodos, el registro se segmenta estrictamente de acuerdo con reglas de visibilidad y autorización de grano fino. **Cada institución financiera participante opera su propio nodo (Participant Node), el cual actúa como su portal exclusivo de lectura y escritura al ecosistema, alojando única y exclusivamente el fragmento o "porción" (*slice*) del registro global de la que es legalmente dueña, firmante o parte interesada autorizada.**
- **El Active Contract Set (ACS) local:** Este fragmento privado de información se traduce en el *Active Contract Set* (ACS) de cada participante, que representa el conjunto de contratos inteligentes activos y saldos vigentes que la entidad tiene permitido conocer y modificar. Un nodo participante de Canton solo se activa, almacena y procesa cómputos en aquellas transacciones bilaterales o multilaterales en las que tiene un rol explícito. Si un banco no es parte o beneficiario de una operación de colateral o repo, los payloads de datos de dicha operación **físicamente nunca viajan ni llegan a almacenarse en su servidor, eliminando de raíz el riesgo de ingeniería social o análisis de tráfico competitivo.**
- **La ilusión síncrona del Libro Mayor Virtual Global:** A pesar de que los datos de propiedad y balance están fragmentados y distribuidos físicamente en multitud de bases de datos locales e independientes, **el protocolo Canton garantiza de forma matemática que la vista de cada participante se comporte conceptualmente como un subconjunto consistente de un único libro contable global y virtual.** Las partes que participan en una transacción de colateral o en un intercambio atómico multilateral perciben una sincronización absoluta del estado de sus activos, con la seguridad jurídica y técnica de que la contraparte realmente posee la titularidad del activo de respaldo, y que este no puede sufrir de doble gasto, a pesar de que ningún tercero centralizado ni ningún validador anónimo tenga la base de datos completa de saldos.

- **Interoperabilidad nativa libre de puentes (*bridges*):** Esta segmentación preserva la privacidad por defecto en reposo y en tránsito, pero no bloquea la composibilidad. Los nodos participantes de Canton pueden conectarse y sincronizarse de manera simultánea a múltiples dominios de sincronización (*sync domains*), lo que les permite coordinar flujos de trabajo multipartidistas complejos (como un DvP síncrono que cruce una pata de efectivo y una pata de valores) de forma atómica y en tiempo real sin requerir de puentes criptográficos de terceros o activos envueltos (*wrapped assets*), eliminando el principal vector de hackeo de la Web3 tradicional.

De este modo, Canton redefine el concepto de libro mayor distribuido: la verdad ya no reside en una gigantesca base de datos pública compartida, sino en la **coordinación de múltiples silos privados de información que interactúan síncronamente sobre una infraestructura descentralizada de mensajería cifrada.** Al operar bajo este modelo de "Red de Redes", la banca mayorista regulada puede finalmente beneficiarse de la velocidad, la atomicidad y la eliminación del riesgo de contraparte intradía sin sacrificar la confidencialidad estratégica de sus posiciones ni ceder el control de sus activos a validadores externos

4.2 Separación bicapa del consenso de Canton

A diferencia de las arquitecturas blockchain tradicionales donde un único conjunto global de validadores reejecuta cada contrato y ordena las transacciones de forma centralizada, el protocolo Canton **separa conceptual y operativamente dos funciones críticas: la validación de los contratos inteligentes y la secuenciación de las transacciones**.

Esta arquitectura desacoplada de consenso bicapa permite optimizar de forma independiente la privacidad y el rendimiento de la red, evitando que los validadores de infraestructura tengan acceso a la información confidencial de negocio.

4.2.1 Smart Contract Consensus (Capa de Validación Local)

La validez del negocio, la conformidad de la lógica de los contratos inteligentes y la legitimidad de las firmas criptográficas se procesan exclusivamente en la **capa de consenso de contratos inteligentes**. Esta capa opera bajo las siguientes reglas técnicas de diseño:

- **El Protocolo "Proof of Stakeholder":** Canton delega la validación de la transacción únicamente a los nodos participantes (*Participant Nodes*) que representan a las partes directamente involucradas en el contrato (los *stakeholders*, definidos como firmantes y observadores). Esto significa que **solo las contrapartes de una transacción ejecutan el código de Daml y validan el cambio de estado**, eliminando la necesidad de delegar la validación a un pool de terceros o validadores de infraestructura anónimos. Además, bajo este modelo no existe un requisito de *staking* financiero para validar las transacciones locales.
- **Validación de Sub-transacciones Peer-to-Peer:** Los nodos participantes reciben de forma encriptada únicamente las vistas de la transacción que tienen derecho a ver. Por ejemplo, en una transacción de Entrega contra Pago (DvP), el nodo del banco comercial solo valida y registra la pata de efectivo, mientras que el nodo del

registrador de valores solo procesa la pata de activos, preservando la confidencialidad mutua mientras se ejecuta un cambio de estado atómico de extremo a extremo.

- **Coordinación de Compromiso en Dos Fases (2PC) y el Mediador:** Para asegurar que los cambios de estado multilaterales se apliquen bajo el principio de "todo o nada", el protocolo implementa un modelo de compromiso en dos fases mediado por un componente lógico llamado **Mediador**. Cada nodo participante valida de manera independiente su vista local de la transacción y envía su voto (Aprobación o Rechazo) cifrado al Mediador. El Mediador agrega los votos y, **únicamente tras recibir la aprobación unánime (100%) de todos los nodos participantes requeridos, emite un veredicto definitivo de confirmación ("Commit Verdict")**. Si existe una discrepancia, un fallo de lógica o una firma ausente, el Mediador emite un veredicto de reversión ("Rollback Verdict"), revirtiendo el borrador de la transacción y liberando cualquier bloqueo sobre los activos.

4.2.2 Ordering Consensus (Capa de Secuenciación Cifrada)

Una vez garantizada la validez de la lógica del contrato inteligente por las partes interesadas, la red debe asegurar la consistencia cronológica de los registros contables para evitar el riesgo de doble gasto. Esta función corresponde a la **capa de consenso de secuenciación y ordenamiento**:

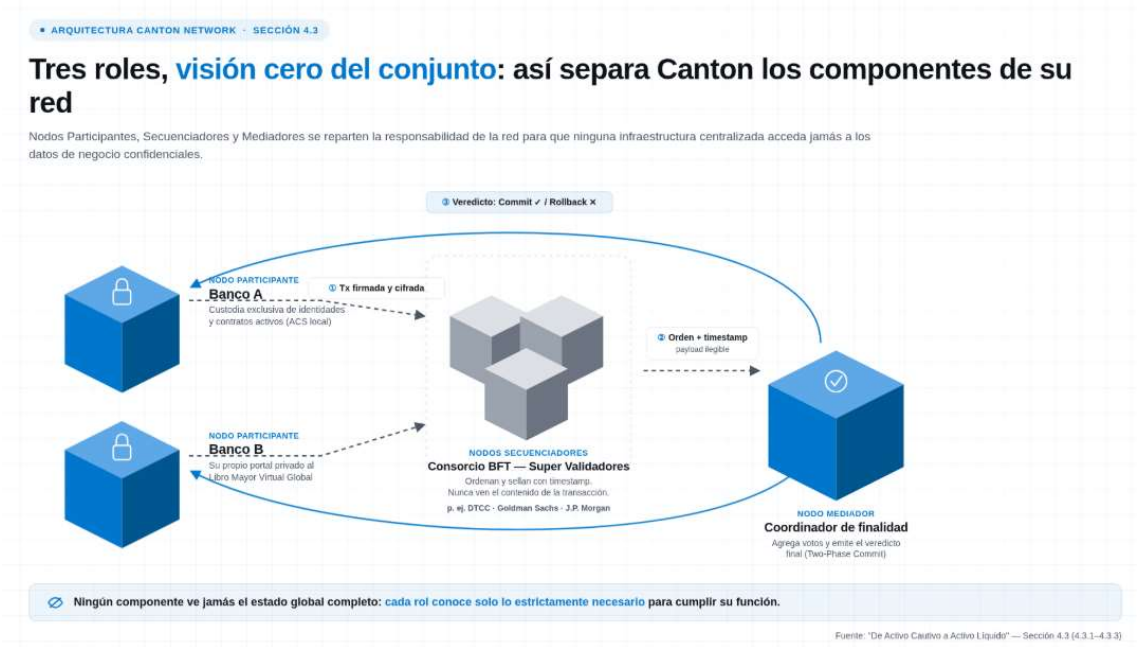
- **El Rol de los Nodos Secuenciadores (Domains):** Los secuenciadores actúan como pasarelas de mensajería de alta disponibilidad y tolerancia a fallos. Su única responsabilidad es recibir los paquetes cifrados de las transacciones, **asignarles un número de secuencia lineal y único, y estamparles un marcador temporal (*timestamp*) consistente**. Este orden secuencial determinista permite que los nodos participantes resuelvan cualquier conflicto de concurrencia o de doble gasto exactamente de la misma manera.

- **Secuenciación Cifrada de Extremo a Extremo (Blinded View):** Para proteger la neutralidad de la red y la privacidad del mercado mayorista, **todos los payloads de datos de las transacciones viajan completamente encriptados de extremo a extremo**. Los nodos secuenciadores y los operadores de los dominios físicos de sincronización son completamente incapaces de descifrar el contenido de los contratos inteligentes, el tipo o valor de los activos movilizados, o las identidades comerciales reales detrás de las transacciones. El secuenciador solo procesa metadatos técnicos cifrados (como el tamaño del mensaje y la lista de destinatarios) necesarios para enrutar el tráfico.

- **Consenso Tolerante a Fallos Bizantinos (BFT):** Cuando las transacciones cruzan múltiples dominios o utilizan el canal público de interoperabilidad de Canton, se recurre al **Global Synchronizer**. Este sincronizador global está operado por un consorcio descentralizado de **Super Validadores** bajo un protocolo de consenso tolerante a fallos bizantinos (BFT) inspirado en esquemas ISS. Los Super Validadores secuencian los mensajes cifrados y garantizan la unicidad del estado sin necesidad de ejecutar o conocer la lógica de negocio subyacente. El orden establecido es legal y técnicamente definitivo una vez secuenciado el veredicto del

Mediador, lo que descarta cualquier posibilidad de bifurcaciones de la cadena o reorganizaciones de estado (*chain reorgs*)

4.3 Arquitectura y Roles de los Componentes de Red



La viabilidad operativa y la seguridad de la arquitectura de "Red de Redes" de Canton Network se sustentan en una división clara y especializada de responsabilidades entre tres componentes lógicos y físicos independientes. Esta segregación estructural garantiza que ninguna entidad de infraestructura centralizada tenga acceso a los datos confidenciales de negocio, al mismo tiempo que preserva la atomicidad de las transacciones interbancarias y elimina de manera determinista el riesgo de doble gasto.

4.3.1 Participant Nodes (Nodos Participantes)

Los **Nodos Participantes** constituyen la frontera de soberanía y propiedad de datos para las instituciones financieras dentro del ecosistema de Canton Network. A diferencia de los modelos blockchain tradicionales, donde las entidades dependen de servidores externos compartidos, en Canton **cada institución opera y controla de manera exclusiva su propio Nodo Participante, el cual funciona como su portal de acceso privado al Libro Mayor Virtual Global**.

- **Alojamiento de Identidades Criptográficas (*Parties*):** El nodo participante aloja las claves privadas y las identidades criptográficas (*Parties*) del banco o de sus clientes. Estas identidades se utilizan para firmar digitalmente transacciones de Daml y autorizar de forma exclusiva los movimientos de colaterales o activos, actuando como la base de la gobernanza de identidad regulada.
- **Custodia y Segmentación del *Active Contract Set* (ACS) Local:** En lugar de replicar todo el estado de la red, cada nodo almacena únicamente el **Active Contract Set (ACS)** local, que representa la porción específica (*slice*) de contratos

activos, saldos de efectivo y registros de propiedad de valores que la institución tiene derecho legal a conocer y gestionar. Si el banco no participa en una operación bilateral de repo, los payloads de datos correspondientes nunca tocan físicamente su base de datos local, resolviendo estructuralmente el riesgo de fuga de datos comerciales ante competidores directos.

- **Ejecución de la *Ledger API* y Validación Local:** Los nodos participantes exponen la *Ledger API*, que sirve como pasarela estandarizada para que las aplicaciones de back-office y los sistemas empresariales del banco interactúen de forma segura con la red. Asimismo, el nodo es el encargado de ejecutar el intérprete de Daml para realizar de forma local la validación lógica, matemática y de autorización de cada transacción antes de ser enviada para su secuenciación cifrada.

4.3.2 Sequencer Nodes (Nodos Secuenciadores)

Los **Nodos Secuenciadores** actúan como la infraestructura de mensajería y ordenamiento cronológico para los dominios de sincronización de la red. Su función principal es proporcionar un secuenciamiento lineal y determinista a los flujos de transacciones para impedir la concurrencia conflictiva y el doble gasto de activos digitales.

- **Ordenación Cronológica y Asignación de *Timestamps*:** El secuenciador recibe de los nodos participantes paquetes de transacciones encriptadas y les asigna un **número de secuencia progresivo y una marca de tiempo (*timestamp*) exacta y única**. Este orden cronológico es absoluto y vinculante para todos los participantes del dominio, sirviendo como la fuente de verdad temporal que define qué transacción llegó primero ante un intento de doble gasto.
- **Garantía de Confidencialidad mediante *Blinded Views*:** Para asegurar el cumplimiento del secreto comercial, **la comunicación a través de los secuenciadores se realiza bajo un modelo de cifrado de extremo a extremo**. El secuenciador solo procesa metadatos técnicos cifrados (como hashes de estado e indicaciones de destinatarios) necesarios para enrutar el tráfico. El payload, los saldos, los términos de los repos y las identidades comerciales subyacentes permanecen completamente opacos (*blinded*) e ilegibles para el operador del secuenciador o del dominio.
- **Consenso de Secuenciación Descentralizado (BFT):** En entornos institucionales multiaplicación, los secuenciadores están operados de manera federada por un consorcio de **Super Validadores** (que incluye a instituciones de la talla de DTCC, Goldman Sachs y J.P. Morgan). Estos supervalidadores utilizan un protocolo tolerante a fallos bizantinos (BFT) inspirado en esquemas ISS para ordenar los mensajes y asegurar la disponibilidad de la red sin necesidad de conocer ni revelar la lógica de negocio que están secuenciando.

4.3.3 Mediator Nodes (Nodos Mediadores)

Los **Nodos Mediadores** son los componentes de infraestructura encargados de coordinar y decretar la finalidad definitiva (*settlement finality*) de las transacciones multilaterales. Actúan como coordinadores neutrales de consenso aplicando el protocolo clásico de **compromiso en dos fases (Two-Phase Commit o 2PC)** de forma totalmente compatible con la descentralización.

- **Coordinación del Compromiso en Dos Fases (2PC):** En la fase de preparación, tras la ordenación del secuenciador, los nodos participantes validan localmente la lógica de la transacción y envían sus firmas de aprobación o rechazo (votos) de forma encriptada al Mediador. El Mediador actúa como el punto de agregación de estos votos.
- **Emisión de Veredictos Deterministas (Commit / Rollback):** Si el Mediador recibe de forma unánime los votos de aprobación de todos los participantes y firmantes requeridos por el contrato, emite de forma automática e irrevocable un **Veredicto de Confirmación (*Commit Verdict*)**, el cual se distribuye a través del secuenciador para aplicar los cambios de estado en los balances locales de manera síncrona y en tiempo real. Si se detecta un doble gasto, un error lógico o la falta de una firma requerida, el Mediador emite un **Veredicto de Reversión (*Rollback Verdict*)**, descartando el borrador de la transacción, liberando los bloqueos temporales sobre los activos y preservando la inalterabilidad de los registros contables.
- **Gobernanza de Seguridad y Prueba de Malicia:** Para evitar que un Mediador corrupto o comprometido declare unilateralmente un estado como confirmado sin contar con los votos reales de los participantes, el protocolo exige que cada veredicto contenga el **registro completo y firmado de los votos de los stakeholders**. Un veredicto de confirmación emitido por un Mediador que carezca de la totalidad de las firmas válidas de los participantes constituye de inmediato una **Prueba Criptográfica de Malfamiento (*Proof of Malfeasance*)**, permitiendo a los nodos participantes detectar la anomalía al instante y desencadenar penalizaciones (*slashing*) de gobernanza a través de la *Canton Network Foundation*.

4.4 El Sincronizador Global (Global Synchronizer) y Gobernanza G-SIB

Como espina dorsal de la interoperabilidad interbancaria descentralizada, **Canton Network opera un dominio de sincronización compartido que sirve como el tejido común de interconexión para todas las aplicaciones y subredes independientes de la red, denominado Sincronizador Global (*Global Synchronizer*)**.

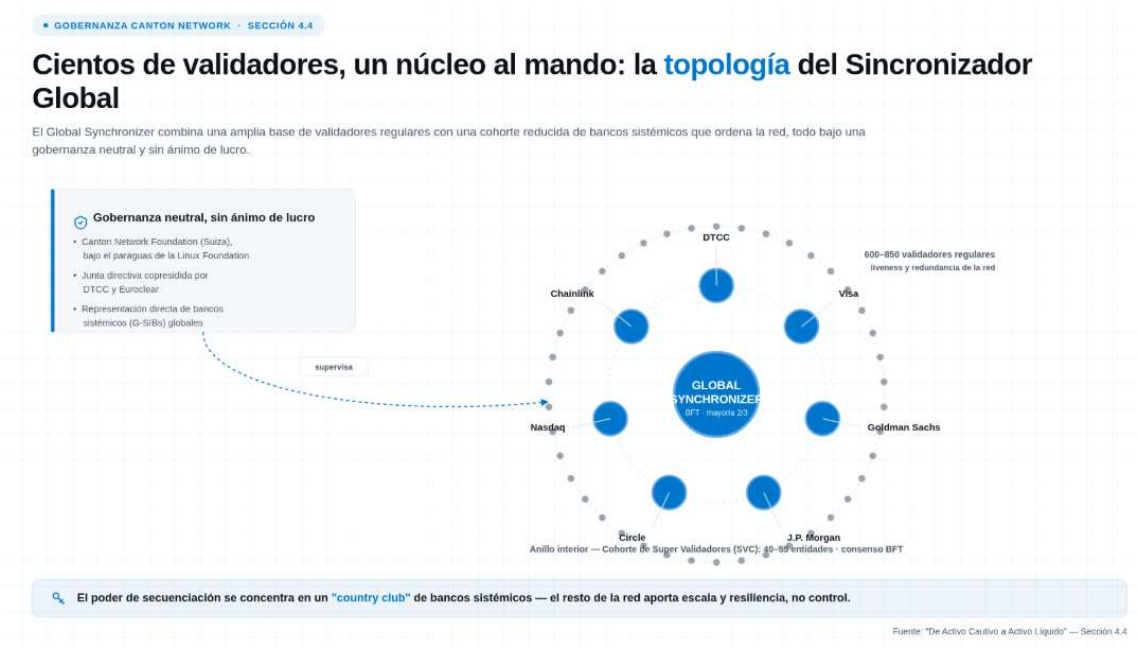
El Sincronizador Global, que **se lanzó formalmente en producción el 1 de julio de 2024 tras casi un año de pruebas piloto y diez años de desarrollo tecnológico general**, resuelve el desafío de coordinar transacciones atómicas multidominio (como un intercambio instantáneo de activos pignorados en un dominio por depósitos bancarios representados en otro) conservando intactas las fronteras de privacidad de cada participante.

Para asegurar la neutralidad operativa y evitar que la infraestructura caiga bajo el control de un único operador o proveedor comercial, la gobernanza y la independencia del Sincronizador Global están estrictamente blindadas bajo un esquema institucional transparente:

- **La Global Synchronizer Foundation (o Canton Network Foundation):** El Sincronizador Global está administrado y supervisado de manera neutral por la

Canton Network Foundation (o Global Synchronizer Foundation). Esta entidad sin fines de lucro, establecida en Suiza, opera de forma afiliada **bajo el paraguas de la prestigiosa Linux Foundation**. Esta vinculación garantiza que el desarrollo del protocolo, las especificaciones de interoperabilidad y las reglas de participación sigan estándares de gobernanza abiertos, rigurosos y democráticos.

- **Junta Directiva con Representación G-SIB:** El órgano de gobierno supremo de la Fundación (el "Senado" del ecosistema) está integrado directamente por directivos y tecnólogos de **los principales bancos de importancia sistémica global (G-SIBs) y operadores de infraestructuras de mercado clave**. Entidades de la talla de **DTCC y Euroclear**—las cuales custodian y liquidan colectivamente la gran mayoría de los valores negociables del planeta— copresiden activamente la Fundación, asegurando que la evolución de la red responda de manera fidedigna a las exigencias de resiliencia y cumplimiento normativo del mercado mayorista internacional.
- **La Estructura Jerárquica de la Red (Validadores y Super Validadores):**
    - **Validadores Regulares (alrededor de 600-850 nodos activos):** La base operativa de la red está constituida por una amplia red descentralizada de **entre 600 y 850 validadores regulares** operados de forma independiente por bancos, gestores de activos, custodios y empresas tecnológicas. Estos nodos validan localmente sus propias transacciones de Daml, mantienen el estado segmentado de sus representaciones de colaterales (*Active Contract Sets*) y proporcionan una capa robusta de redundancia, descentralización y *liveness* al ecosistema general.
    - **La Cohorte Exclusiva de Super Validadores (SVC):** El núcleo de procesamiento, secuenciación y ordenamiento temporal del Sincronizador Global está restringido a un grupo VIP y altamente regulado de **entre 40 y 55 entidades financieras de primer nivel (Super Validators)**. Esta cohorte de Super Validadores opera de forma distribuida los nodos secuenciadores centrales del Sincronizador Global mediante un protocolo de consenso tolerante a fallos bizantinos (BFT) con un umbral de mayoría de 2/3 para las confirmaciones de estado. Este "country club" de infraestructura de mercado mayorista está integrado exclusivamente por las firmas más creíbles del panorama financiero global, incluyendo a **DTCC, Visa, Goldman Sachs, J.P. Morgan, Circle, Nasdaq, Chainlink y Nasdaq**. Estos Super Validadores tienen la responsabilidad compartida de secuenciar cronológicamente las transacciones cifradas, evitar colisiones o doble gasto de garantías de manera síncrona, gestionar la emisión del token de utilidad Canton Coin (CC) y votar de manera unificada las actualizaciones del protocolo de red y las decisiones críticas de membresía y tarifas de uso.



Mediante esta arquitectura, **Canton unifica la agilidad operativa y la finalidad atómica instantánea de los registros compartidos con la rigurosidad, la identidad auditada y el control democrático institucional que exige el ordenamiento bancario internacional**, consolidando al Sincronizador Global como la infraestructura por excelencia para la futura red de movilidad de colaterales globales.

CAPÍTULO 5: El Lenguaje Daml y el Motor de Privacidad por Sub-transacción

5.1 Fundamentos de Daml como lenguaje funcional para finanzas

Para que un registro distribuido (*ledger*) actúe como el sistema definitivo de libros y registros (*books and records*) de una entidad financiera mayorista, el lenguaje de programación subyacente no solo debe ser expresivo, sino estructuralmente seguro. Las blockchains tradicionales han dependido de lenguajes imperativos y orientados a objetos (como Solidity en Ethereum), los cuales exponen a las tesorerías a vulnerabilidades críticas de ejecución. Para resolver esta debilidad, la arquitectura de Canton Network se sustenta sobre **Daml, un lenguaje de contratos inteligentes de paradigma funcional y tipado estático**, diseñado específicamente para modelar acuerdos multipartidistas con garantías matemáticas de corrección.

A. La inspiración funcional (Haskell) y el tipado estático

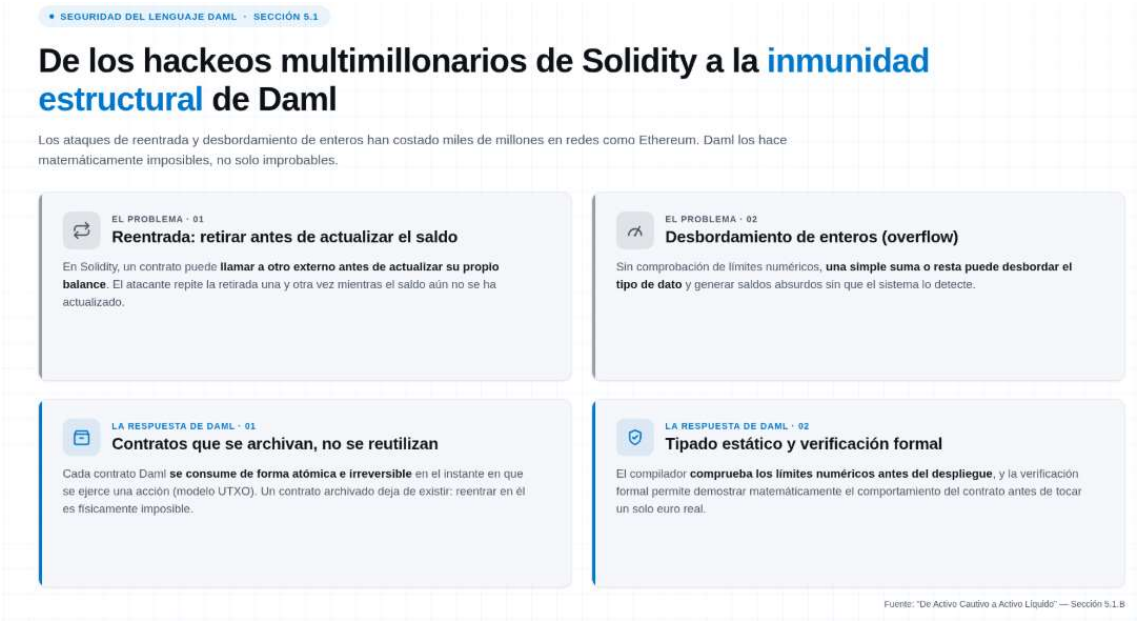
Daml está fuertemente inspirado en la sintaxis y los principios del lenguaje funcional puro **Haskell**. El uso de un **sistema de tipado estático fuerte** permite que el compilador descarte de raíz múltiples clases de fallos lógicos y errores de consistencia en el momento de la compilación, antes de que cualquier línea de código sea desplegada en el entorno de pruebas o en el Sincronizador Global.

En la práctica financiera, esta robustez formal se traduce en:

- **Ausencia de variables mutables:** En Daml no existen variables mutables ni estados globales modificables a nivel de aplicación. **Cada asignación de valor (*binding*) es estrictamente inmutable** y fija durante todo su ámbito de ejecución (*scope*). Esto impide que un atacante altere dinámicamente parámetros clave (como tipos de interés o identidades de destino) durante el ciclo de vida de la transacción.
- **Estructura de datos frente a herencia:** A diferencia de la programación orientada a objetos (OOP), Daml **carece de herencia, subclases, campos protegidos o llamadas a métodos basados en punteros virtuales (this)**. Los tipos de datos se definen mediante registros inmutables (*records*) y tipos suma (*sum types*), mientras que el comportamiento se expresa a través de funciones puras e independientes organizadas mediante clases de tipos (*type classes*). Esta separación total de datos y comportamiento elimina los riesgos de sobreescritura accidental de métodos críticos de cumplimiento normativo.

B. Erradicación estructural de exploits de ejecución (Re-entrancy e Integer Overflow)

En entornos como la Ethereum Virtual Machine (EVM), los hackeos multimillonarios ocurren con frecuencia debido a fallos de reentrada (*re-entrancy*) o desbordamiento de enteros (*integer overflows*). Daml neutraliza estas dos categorías de exploits mediante principios de diseño de su máquina de ejecución:



1. **Inmunidad a la Reentrada por Modelo UTXO:** El modelo de cuentas mutable de Solidity permite que un contrato llame a otro contrato externo antes de actualizar su propio balance local, facilitando ataques de reentrada (donde el atacante retira fondos repetidamente antes de que el saldo se actualice). En Daml, los contratos son **objetos inmutables que se asemejan al modelo UTXO de Bitcoin**. Un contrato inteligente Daml activo en el *Active Contract Set* (ACS) **se consume de forma atómica e irreversible (se archiva) en el mismo instante matemático en que se ejerce una acción (*choice*)**. Dado que un contrato archivado deja de existir para el validador, es físicamente imposible volver a entrar en él para duplicar una retirada de colateral.

2. **Mitigación de desbordamientos e indeterminismo:** El tipado estático restrictivo y la comprobación de límites numéricos en tiempo de compilación impiden los desbordamientos de enteros (*overflows* y *underflows*). Además, como el lenguaje cuenta con soporte de **verificación formal parametrizable**, los desarrolladores pueden demostrar matemáticamente el comportamiento esperado y las invariants del colateral de manera previa al despliegue, asegurando que un contrato solo pueda comportarse de la forma estrictamente predefinida por las reglas de negocio.

C. Control de flujo sin nulos ni excepciones descontroladas

Daml impone un modelo riguroso de manejo de datos y errores, alineado con las demandas de control operacional de la banca mayorista:

- **Eliminación del puntero nulo (NullPointerException):** En Daml **no existe el valor nulo**. Las ausencias de datos o los resultados opcionales se modelan obligatoriamente mediante el tipo algebraico Optional a, el cual exige de forma explícita al programador tratar los constructores Some a y None mediante

coincidencia de patrones (*pattern matching*), evitando fallos fatales e inesperados en tiempo de ejecución.

- **Manejo de errores por aborto atómico:** El lenguaje no implementa capturas de excepciones dinámicas para errores comerciales. En su lugar, si una condición financiera no se cumple (por ejemplo, saldo de colateral insuficiente para un repo), el comando assertMsg interrumpe de inmediato la ejecución y **aborta la totalidad de la transacción de forma atómica**. Al cancelarse la transacción, el ledger permanece intacto, libre de estados intermedios parcialmente aplicados o saldos inconsistentes en tránsito.

A través de esta arquitectura funcional, Daml desplaza el peso de la seguridad desde las revisiones manuales de código de back-office hacia la propia estructura del lenguaje, proporcionando una base determinista e inalterable sobre la cual estructurar flujos financieros de alta criticidad reguladora.

5.2 El modelo contractual inmutable de Daml

El diseño del modelo de ejecución de Daml para Canton Network se aparta de manera radical del modelo tradicional de "cuentas mutables" empleado por entornos basados en Ethereum (EVM).

En lugar de modificar directamente el estado de los saldos o las variables dentro de un único registro de cuenta global, **Daml implementa un modelo de contratos inmutables en el que cualquier cambio de estado se ejecuta de forma estrictamente atómica, consumiendo (archivando) el contrato existente y creando uno nuevo modificado de forma inmutable**.

Este principio operativo se articula a través de las siguientes especificaciones técnicas y ventajas operativas:

A. Inmutabilidad transaccional y el ciclo de vida del contrato

En Daml, un contrato es un objeto inalterable que reside en el libro mayor de los participantes autorizados. Cuando una contraparte ejerce una acción (*choice*) con el fin de alterar los términos o la propiedad de un activo (por ejemplo, retirar fondos de una cuenta o pignorar un colateral), el motor de ejecución de Canton no edita el registro existente. En su lugar, el proceso se descompone de forma transparente bajo las siguientes fases atómicas:

1. **Consumo (Archivado):** Al ejecutarse una elección de tipo consumidora (*consuming choice*), el contrato inteligente de origen es marcado de forma inmediata como **archivado**, quedando inhabilitado permanentemente para cualquier interacción posterior.
2. **Re-creación (Creación de Outputs):** De forma síncrona y dentro del mismo árbol transaccional, se instancia un **nuevo contrato inmutable** que incorpora las variables modificadas (como el nuevo propietario o el saldo remanente).

3. **Atomicidad Absoluta ("Todo o Nada"):** Ambos eventos —el archivado del contrato original y la creación del contrato resultante— se registran en una sola transacción. Si cualquier paso o validación posterior de la transacción falla (como un saldo insuficiente o una firma ausente), la operación completa se aborta, impidiendo que el balance de la institución quede expuesto a estados intermedios inconsistentes.

B. El Active Contract Set (ACS) como el equivalente del modelo UTXO

El agregado dinámico de todos los contratos que permanecen en estado inalterado y listos para ser operados en la red constituye el **Active Contract Set (ACS) o Conjunto de Contratos Activos**.

El ACS representa el **análogo técnico directo del modelo de Salidas de Transacciones No Gastadas (UTXO)** popularizado por Bitcoin. Al igual que en la arquitectura UTXO, donde el saldo de una clave pública se calcula sumando las transacciones no gastadas, la verdad contable de una institución en Canton se deriva de la suma de sus contratos vigentes en el ACS, mapeados a través de un grafo de transacciones acíclico y determinista.

C. Ventajas en la mitigación del doble gasto y control de concurrencia

La adopción de este modelo basado en UTXO/ACS dota a Canton de una resistencia estructural contra las incidencias de **doble gasto de colateral**, sin requerir que las aplicaciones asuman la sobrecarga de implementar bloqueos optimistas o dinámicas de sincronización manual de bases de datos:

- **Detección determinista:** Si un participante intenta pignorar un mismo bono del Tesoro de manera simultánea en dos transacciones de repo concurrentes, ambas se procesarán de manera aislada. No obstante, una vez que la primera transacción es secuenciada e inscrita por el secuenciador BFT, el contrato del bono de origen queda formalmente **archivado**.
- **Invalidación inmediata:** En el instante en que la segunda transacción es distribuida a los nodos participantes para su validación, el motor del intérprete de

Daml detecta que el identificador del contrato de origen (*ContractId*) hace referencia a un elemento que ya ha sido consumido (un estado archivado). Como consecuencia, la validación del segundo repo falla instantáneamente y es descartada por el Mediador mediante un veredicto de reversión (*Rollback Verdict*), anulando cualquier posibilidad de fraude o duplicidad de garantías.

D. Las dos innovaciones de Canton sobre el modelo UTXO clásico

A pesar de su paralelismo con la contabilidad de Bitcoin, Canton y Daml refinan la tecnología UTXO mediante dos aportaciones de diseño críticas para las finanzas de importancia sistémica:

1. **Visibilidad Fraccionada y Sharding de Privacidad:** En las blockchains UTXO públicas tradicionales (como Bitcoin o Cardano), la integridad del sistema exige que cada nodo almacene y verifique el grafo transaccional completo, eliminando cualquier vestigio de privacidad para el balance institucional. En Canton, **el grafo se segmenta de forma que cada participante solo almacena y visualiza el fragmento del ACS del cual es firmante u observador autorizado (su vista local del ledger)**. Ningún tercero ajeno a la transacción tiene la capacidad física de auditar o inferir los movimientos del balance general, combinando la finalidad UTXO con la confidencialidad absoluta del secreto comercial.
2. **Soporte de Acciones No Consumidoras (*Non-consuming Choices*):** En el UTXO clásico, cualquier consulta o referencia a un dato inscribe necesariamente su gasto y destrucción. Daml supera esta ineficiencia al permitir definir acciones de tipo no consumidor (*non-consuming choices*). Esta funcionalidad permite que una transacción consulte, verifique o firme digitalmente un contrato activo (como un registro de credenciales KYC, un límite de crédito corporativo o un índice de tasas de interés diarias) **sin necesidad de archivarlo o destruirlo**, reduciendo radicalmente los problemas de congestión y colisiones de red que sufren otros registros distribuidos ante procesos de alta concurrencia

5.3 Control de accesos y derechos contractuales nativos

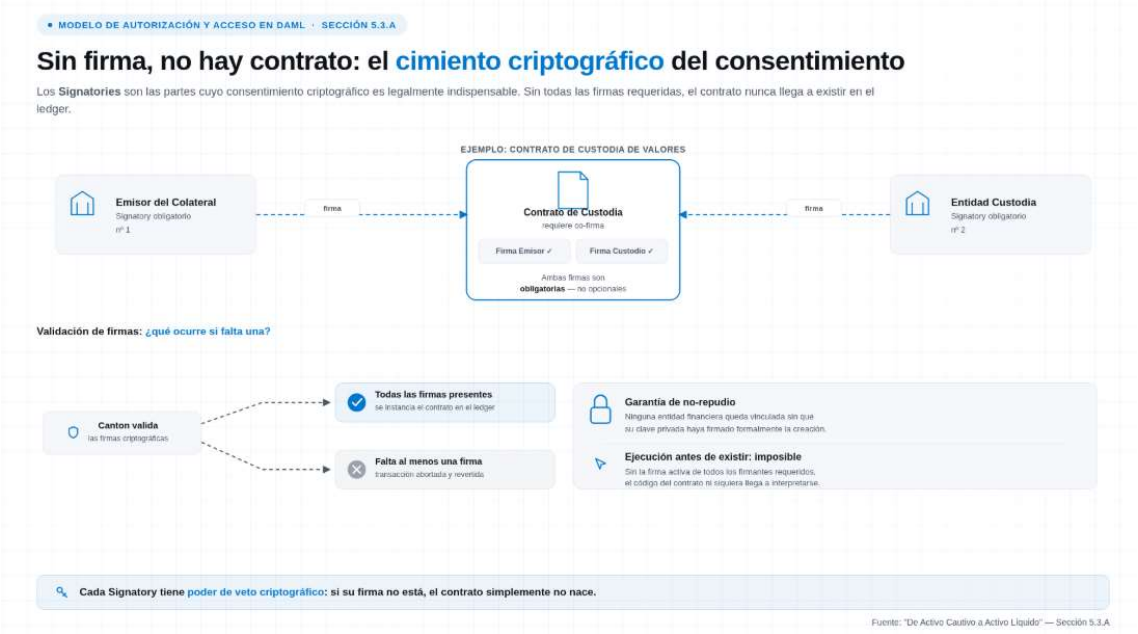
En los sistemas tradicionales, la lógica de negocio y las políticas de acceso (*access control lists* o ACL) se gestionan como capas de software independientes de la base de datos. Esto genera una vulnerabilidad operativa crítica: un fallo o exploit en el servidor de aplicaciones puede eludir las reglas de control de acceso y exponer datos confidenciales directamente desde la base de datos subyacente. El lenguaje **Daml solventa esta brecha integrando las reglas de autorización, control de accesos y derechos de visibilidad directamente en la capa de definición del propio modelo de datos (en el contract template)**.

Esta gobernanza de accesos nativa a nivel de Layer 1 se articula a través de tres primitivas de seguridad declarativas que el protocolo Canton hace cumplir de manera rigurosa:

A. Signatories (Firmantes): El cimiento criptográfico del consentimiento

En Daml, los **Signatories (Firmantes)** representan a las partes u organizaciones cuyo consentimiento explícito y firma criptográfica son legalmente indispensables para la existencia, creación o archivado de un contrato en el ledger.

- **Garantía de No-Repudio:** No es posible crear un contrato inteligente que obligue o vincule a una entidad financiera sin que su clave privada haya firmado formalmente la transacción de creación. Por ejemplo, en un contrato de custodia de valores, tanto el emisor del colateral como la entidad custodia deben ser definidos como co-firmantes (*co-signatories*).
- **Validación de Firmas:** El ledger Canton realiza una comprobación de firmas criptográficas durante la fase de validación. Si una transacción intenta instanciar un contrato sin contar con la firma activa de todos los firmantes requeridos, **la transacción es abortada y revertida de forma atómica antes de que tenga cualquier efecto sobre el ledger**.



B. Observers (Observadores): Divulgación selectiva regulada (Need-to-Know)

Los **Observers (Observadores)** son las partes expresamente autorizadas en el código del contrato para tener acceso de lectura a sus campos de datos, pero que **carecen por completo de derechos de firma o de la capacidad de ejecutar acciones unilaterales para modificar el estado del contrato**.

- **Privacidad física y Sharding de datos:** Si un nodo participante no está registrado explícitamente como firmante (*Signatory*) u observador (*Observer*) en un contrato inteligente, **los datos encriptados del contrato físicamente nunca se transmitirán ni se almacenarán en su base de datos local (Participant Node)**. Esto evita que firmas rivales o intermediarios de infraestructura puedan analizar el tráfico o deducir saldos de balance.
- **Supervisión y cumplimiento regulatorio:** Esta primitiva permite añadir a un **regulador financiero, supervisor o auditor como "Observer"** directamente en la

capa del contrato inteligente. El regulador obtiene una vía de auditoría y visibilidad read-only y en tiempo real sobre transacciones que alcancen ciertos umbrales de cumplimiento (como transacciones superiores a 10.000 dólares) sin exponer dichos flujos comerciales al resto del mercado, permitiendo el cumplimiento simultáneo de normativas de protección de datos personales y obligaciones contra el blanqueo de capitales (*Travel Rule*).

C. Controllers and Choices (Controladores y Acciones): Lógica funcional restringida

Las interacciones que alteran el estado del ledger se gestionan en Daml mediante **Choices (Acciones)**, las cuales representan funciones o métodos de negocio equivalentes a procedimientos almacenados. Cada Choice debe declarar explícitamente a su **Controller (Controlador)**: la parte autorizada que tiene el derecho exclusivo de llamar y ejecutar dicha función.

- **Comprobación previa de autorización:** Cuando un nodo envía un comando para ejecutar una acción (por ejemplo, ejercer la Choice de Withdraw sobre una cuenta de garantía), **la Ledger API y el motor de Canton verifican en primer lugar si el emisor de la instrucción coincide criptográficamente con el Controller definido**. Si la verificación de autorización falla, el comando es rechazado de inmediato y el código interno de la Choice nunca se interpreta ni se ejecuta.
- **Acciones y operaciones fundamentales del Ledger:** El ciclo de vida y los cambios de estado en Daml se limitan a cuatro acciones básicas protegidas que manipulan el *Active Contract Set* (ACS) de forma inmutable:
    1. create: Instancia un nuevo contrato inmutable en el ledger, requiriendo de forma obligatoria la autorización de todos sus firmantes.
    2. exercise: Desencadena y ejecuta una Choice específica sobre un contrato activo (es la herramienta principal para la lógica de negocio y liquidación).
    3. fetch: Recupera los datos de un contrato activo directamente del ledger, operación que solo se permite si el nodo solicitante es un stakeholder autorizado (firmante u observador).
    4. archive: Consume y archiva permanentemente el contrato para que no pueda volver a ser referenciado (ejecutado por defecto en elecciones de tipo consumidor para prevenir de manera nativa el doble gasto de activos)

5.4 Privacidad por sub-transacción mediante Árboles Transaccionales

Las transacciones financieras complejas en los mercados de capitales (como los canjes de colateral, préstamos sindicados o compensaciones de derivados) involucran de manera habitual a múltiples partes que requieren coordinar flujos de trabajo interdependientes.

Sin embargo, la regulación prudencial prohíbe que estas instituciones expongan la totalidad de sus posiciones y términos comerciales a entidades que no forman parte de la transacción. Para resolver este dilema sin recurrir a silos inconexos, el protocolo de Canton y el lenguaje Daml implementan una innovadora arquitectura de **Privacidad por Sub-transacción mediante Árboles Transaccionales (*Transaction Trees*)**.

A. Descomposición Jerárquica: El Árbol Transaccional (Transaction Tree)

En lugar de estructurar las transacciones como una lista plana de operaciones secuenciales (el modelo EVM tradicional), **Canton organiza y representa cada transacción en forma de un árbol de acciones (*Transaction Tree*)**. Cada nodo de este árbol representa una acción contractual específica en Daml (como la creación de un contrato, el archivado de un activo, o la ejecución de una Choice de negocio).

Esta arquitectura jerárquica dota al sistema de dos ventajas primordiales:

1. **Composibilidad de Workflows:** Los árboles transaccionales de procesos independientes desarrollados sobre diferentes dApps (por ejemplo, el traslado de un bono del tesoro en una app de liquidación y la emisión de una stablecoin en una app de pagos) pueden unirse de forma nativa para formar los subárboles de una transacción unificada más amplia.

2. **Validación y Atomicidad Localizada:** Cada participante de la transacción tiene la capacidad técnica de **validar localmente su propio subárbol (o vista de la transacción)** sin tener que reejecutar o almacenar el árbol transaccional completo de la red, garantizando que el commit sea estrictamente de tipo "todo o nada" sin riesgo de principal.

B. El Mecanismo de Vistas Cegadas (Blinded Views)

La visibilidad fraccionada dentro del árbol transaccional se materializa criptográficamente a través de las **Vistas Cegadas (*Blinded Views*)**. Cuando un nodo participante de origen somete una transacción estructurada al ledger, **el protocolo Canton segmenta el árbol transaccional y genera vistas individuales encriptadas de extremo a extremo, destinadas únicamente a los participantes autorizados de cada sub-acción**.

Este modelo de seguridad garantiza de manera absoluta el principio de **"necesidad de saber" (*need-to-know*)** a nivel de protocolo de red:

- **Ofuscación Criptográfica:** Aquellas porciones del árbol transaccional que detallan operaciones en las que una contraparte no tiene un rol legítimo (como firmante u observador) **quedan completamente ofuscadas (*blinded*) e invisibles para ella**. El nodo participante solo recibe y descifra la vista correspondiente al subárbol que le compete validar y firmar.

- **Cegado de Infraestructura:** Esta ofuscación se extiende de manera rigurosa a los operadores de infraestructura. Tanto los **nodos secuenciadores** de los dominios como los **Super Validadores** del Sincronizador Global son completamente incapaces de descifrar el contenido del payload de la transacción, operando exclusivamente sobre metadatos e inputs encriptados (*blinded envelopes*) para resolver de forma síncrona el orden de las transacciones y prevenir el doble gasto.

C. Aplicación Práctica: Un Flujo DvP Síncrono y Privado

La potencia operativa de las Blinded Views y los Transaction Trees se aprecia con total claridad al modelar una operación estándar de **Entrega contra Pago (DvP)**, donde una cantidad de efectivo se liquida de forma atómica contra la entrega de un colateral o valor:

1. **Envío del Comando:** La aplicación de mercado inicia una transacción atómica unificada para intercambiar un lote de bonos por un valor de $10,000 en depósitos tokenizados. El árbol transaccional resultante se compone de dos subárboles interconectados: el subárbol de transferencia de efectivo y el subárbol de entrega de valores.
2. **Distribución y Descifrado Selectivo:** El secuenciador enruta las vistas encriptadas de manera diferenciada a los participantes autorizados:
    - El **Banco Comercial de Liquidación** (operador del efectivo) solo recibe, descifra e inspecciona la porción que detalla el movimiento de los $10,000. El subárbol correspondiente a la entrega de los bonos soberanos permanece completamente cegado e ilegible para sus servidores.
    - El **Registrador de Valores** (custodio del colateral) solo recibe y valida la pata de transferencia de los bonos, permaneciendo ciego ante la cuenta de efectivo y la identidad monetaria de origen.
    - El **Comprador y el Vendedor**, que actúan como contrapartes directas de ambas patas, tienen acceso de descifrado completo para visualizar tanto el efectivo como los activos.
3. **Votación Unánime del Mediador:** Todos los validadores confirman criptográficamente la validez lógica de sus respectivas vistas y envían sus firmas cifradas al Mediador. Únicamente tras registrar el 100% de los votos favorables de los participantes requeridos, el Mediador expide un veredicto definitivo de confirmación (*Commit Verdict*), aplicando los balances correspondientes de forma síncrona, atómica e irreversible.

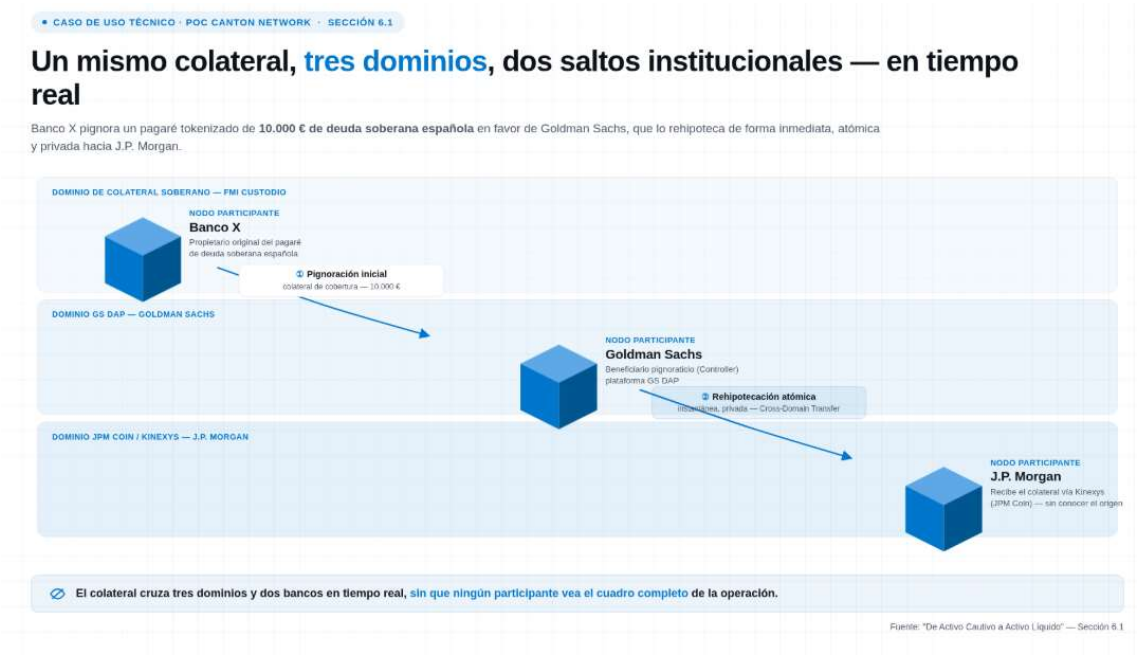
A través de esta sofisticada arquitectura de seguridad nativa, Canton demuestra que la privacidad de nivel institucional y la interoperabilidad de mercado no son características excluyentes. La banca mayorista regulada puede desplegar colaterales y movilizar balances en tiempo real, con la certeza absoluta de que sus competidores e intermediarios jamás podrán reconstruir o interceptar sus flujos de tesorería y estrategias comerciales bilaterales.

CAPÍTULO 6: Caso de Uso Técnico: Rehipotecación Intradía de un Bono del Estado Español

6.1 Sinopsis del Flujo Operativo PoC

La movilización ininterrumpida de colaterales y la optimización del balance de tesorería intradía encuentran su máxima expresión práctica en la capacidad de ejecutar rehipotecaciones complejas en tiempo real, sin riesgo de principal y bajo estrictos criterios de confidencialidad comercial.

Este caso de uso técnico detalla la simulación de una Prueba de Concepto (PoC) basada en la infraestructura de Canton Network. En ella, un banco comercial europeo (**Banco X**) pignora un pagaré tokenizado representativo de **10.000 € de deuda soberana española** en favor de **Goldman Sachs** como colateral de cobertura, activo que posteriormente es rehipotecado de manera inmediata, atómica y privada hacia **J.P. Morgan**.



A. Arquitectura de Nodos y Estructura Topológica del Caso de Uso

Para llevar a cabo este flujo operativo transfronterizo e interinstitucional, cada uno de los tres participantes principales opera su propio entorno tecnológico conectado de forma síncrona a la red:

1. **Nodos Participantes de Canton (Participant Nodes):** Banco X, Goldman Sachs y J.P. Morgan gestionan sus respectivas identidades criptográficas (*Parties*) e inventarios de colateral en sus propios servidores soberanos. El nodo de Goldman Sachs interactúa de forma nativa con la plataforma de activos digitales **GS DAP**, mientras que el nodo de J.P. Morgan se comunica con su división blockchain Kinexys (que administra el depósito digital **JPM Coin**).

2. **Sincronización Multidominio sin Puentes (*Bridges*):** A diferencia de las arquitecturas tradicionales que fragmentan la liquidez y exigen el uso de puentes de tercera parte vulnerables a hackeos, **los nodos de Canton se conectan**

simultáneamente a múltiples dominios de sincronización (*sync domains*). En esta PoC, la operación involucra tres dominios diferenciados:

- **Dominio de Colateral Soberano (FMI Custodio):** Registra el pagaré de deuda española tokenizado bajo la gobernanza del emisor o depositario central correspondiente.
- **Dominio de GS DAP (Goldman Sachs):** Entorno permisionado donde se estructuran los contratos de cobertura y pignoración bilateral.
- **Dominio de JPM Coin / Kinexys (J.P. Morgan):** Red de liquidación y efectivo institucional que gestiona la liquidez en euros y dólares.

B. Mecánica de la Pignoración Inicial (Banco X a Goldman Sachs)

El flujo se inicia cuando el Banco X requiere constituir una garantía de cobertura en favor de Goldman Sachs. La operación se ejecuta on-chain mediante las siguientes fases criptográficas:

- **Creación del Contrato de Colateral en Daml:** Utilizando el lenguaje funcional Daml, se instancia un contrato de tipo SovereignCollateral en el ledger. Este contrato inteligente define de forma inmutable al **Banco X como propietario original**, a la **entidad pública emisora como firmante del activo (*Signatory*)**, y a **Goldman Sachs como beneficiario pignoraticio con rol de controlador (*Controller*)** para el ejercicio de opciones de liquidación.
- **Consumo y archivado atómico del pagaré libre:** Para pignorar el pagaré de 10k€, el nodo del Banco X ejerce la acción (*Choice*) de transferir el control. El protocolo Canton archiva de inmediato el pagaré libre original en el *Active Contract Set* (ACS) de Banco X y crea, en el mismo instante matemático, el contrato de colateral bloqueado en favor de Goldman Sachs, eliminando nativamente cualquier posibilidad de doble pignoración intradía.

C. Mecánica de la Rehipotecación Atómica Intradía hacia J.P. Morgan

Una vez que Goldman Sachs tiene el control del pagaré de deuda española pignorado, decide rehipotecar dicho colateral en tiempo real hacia J.P. Morgan a cambio de financiación intradía en efectivo (euros representados a través de depósitos JPM Coin o tokens EURØP de Schuman Financial). Esta segunda fase constituye el núcleo de la composibilidad de Canton:

1. **La Transacción Cruzada entre Dominios (*Cross-Domain Transfer*):** El activo (el pagaré pignorado de 10k€) debe trasladar su residencia contable desde el Dominio de Goldman Sachs (GS DAP) hacia el Dominio de J.P. Morgan.
2. **Transfer-Out (Extinción en el Origen):** El participante inicia una solicitud de salida en el dominio GS DAP. El nodo de Goldman Sachs extingue y archiva el colateral localmente, y el secuenciador del dominio de origen emite un **recibo criptográfico firmado y con marca de tiempo (*Signed Sequencing Proof*)** que certifica que el activo ha sido inmovilizado irreversiblemente.
3. **Transfer-In (Rematerialización en el Destino):** El nodo participante presenta dicha prueba firmada ante el secuenciador del dominio de J.P. Morgan. Tras validar

criptográficamente la procedencia y firma de la prueba, **el dominio de destino rematerializa el colateral en el balance de J.P. Morgan de forma instantánea y determinista**, completando el traspaso de residencia sin que el activo haya estado expuesto en ningún momento a los riesgos de custodia propios de los puentes de terceros tradicionales.

D. Preservación Absoluta de la Privacidad por Sub-transacción (Blinded Views)

El aspecto más disruptivo de esta rehipotecación es la confidencialidad estratégica de la transacción global. A pesar de que los activos se mueven de forma atómica cruzando múltiples fronteras institucionales y dominios, **ningún participante ajeno a cada sub-acción de negocio obtiene visibilidad sobre el balance general o las estrategias de cobertura de las contrapartes**:

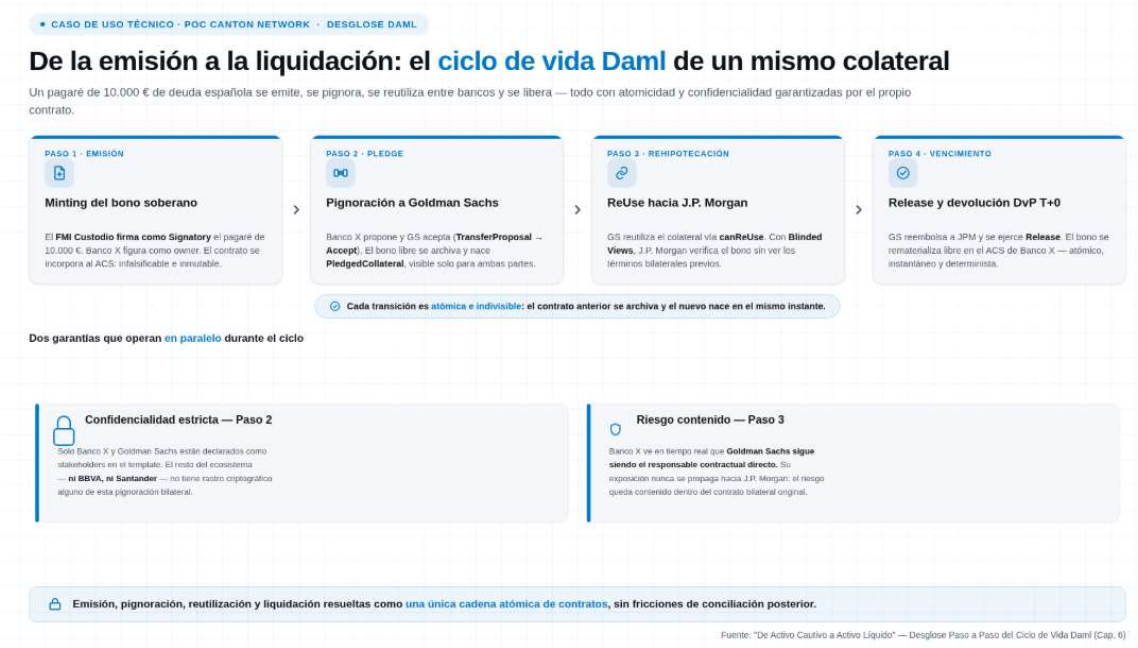
- **Banco X permanece ciego ante la rehipotecación:** El Banco X solo ve que su pagaré de 10k€ de deuda española está bloqueado en favor de Goldman Sachs en el ledger de origen. Banco X **no tiene constancia física ni visibilidad criptográfica alguna en su nodo participante de que Goldman Sachs ha rehipotecado posteriormente ese mismo colateral hacia J.P. Morgan**, protegiendo la estrategia de refinanciación de Goldman Sachs.
- **J.P. Morgan no conoce el origen comercial:** J.P. Morgan recibe el pagaré de 10k€ de deuda soberana española de manos de Goldman Sachs como contraparte directa. Su nodo participante y sus oficiales de cumplimiento verifican la validez criptográfica del activo subyacente y la legitimidad del traspaso, pero **no tienen acceso a los balances históricos de Banco X ni conocen los términos del acuerdo de cobertura bilateral previo firmado entre Banco X y Goldman Sachs**.
- **La infraestructura opera en la opacidad total:** Los nodos secuenciadores de los dominios y los Super Validadores del Sincronizador Global procesan y ordenan las transacciones de *Transfer-Out* y *Transfer-In* en formato de sobres encriptados (*Blinded Views*). Ordenan cronológicamente las marcas de tiempo para evitar el doble gasto de la deuda española, pero **son físicamente incapaces de descifrar que se trata de deuda española, que el monto es de 10.000 € o que las identidades involucradas corresponden a Banco X, Goldman Sachs o J.P. Morgan**.

De este modo, Canton demuestra en producción que es viable alcanzar una movilidad global del colateral las 24 horas del día, los 7 días de la semana, eliminando de raíz el lastre por inactividad (*weekend downtime*) y los buffers de capital preventivos, mientras se garantiza un cumplimiento riguroso de la confidencialidad mayorista y las normativas prudenciales de Basilea.

6.2 Desglose Paso a Paso del Ciclo de Vida Daml

El ciclo de vida del colateral de deuda soberana española tokenizado en Canton se instrumenta a través de la ejecución determinista de contratos inteligentes en Daml. Cada una de las transiciones de estado descritas en el caso de uso PoC se desglosa

técnicamente a continuación, vinculando el comportamiento del Active Contract Set (ACS) local de los participantes con la inmutabilidad matemática del protocolo



Paso 1: Emisión (Minting)

- **Mecánica en el Ledger:** El emisor central o depositario de valores regulado (FMI Custodio) actúa como el **Signatory** indispensable del contrato, avalando de forma criptográfica e indisputable la existencia del activo subyacente (el pagaré físico de deuda de 10.000 €). El Banco X figura en los campos de datos como el owner inicial.
- **Estado del ACS:** El Nodo Participante del Banco X ejecuta un comando create a través de la Ledger API para instanciar el contrato inteligente inmutable SovereignBond. El identificador único resultante (ContractId SovereignBond) se incorpora de inmediato al **Active Contract Set (ACS)** de Banco X como un activo libre y listo para transaccionar. Debido a la inmutabilidad contractual, este registro es matemáticamente infalsificable y resistente a manipulaciones de código.

Paso 2: Pledge (Pignoración)

- **Mecánica en el Ledger:** Banco X inicia una transacción bilateral estructurada de tipo propuesta-aceptación (TransferProposal) para constituir la garantía a favor de Goldman Sachs. Banco X firma como proponente (fromOwner) y autoriza la entrega del colateral. Al recibir el mensaje cifrado a través del secuenciador, Goldman Sachs ejecuta de forma local la elección Accept.
- **Consumo y Archivamiento Atómico:** De manera instantánea e indivisible en una única transacción de estado, **el contrato del bono libre original de Banco X es consumido (archivado) y se genera un nuevo contrato PledgedCollateral en estado activo en el ACS de Goldman Sachs y Banco X**.
- **Garantía Estricta de Confidencialidad:** Dado que solo Banco X y Goldman Sachs están declarados como stakeholders legítimos (firmantes u observadores) en el template de Daml, **los metadatos y payloads de esta pignoración físicamente**

nunca son distribuidos a los nodos de competidores directos de la red (como BBVA o Santander). El resto del ecosistema de Canton carece de cualquier rastro criptográfico o hash referente a la existencia de esta operación bilateral, protegiendo al banco de arbitrajes agresivos de precios o fuga de datos de balance.

Paso 3: Rehipotecación (ReUse síncrono interbancario)

- **Mecánica en el Ledger:** Goldman Sachs, con el fin de optimizar sus flujos de liquidez intradía, decide rehipotecar el colateral de 10k€ de deuda española hacia J.P. Morgan. Esta operación está previamente autorizada en el template de Daml mediante la opción delegativa **canReUse** que actúa como un derecho de disposición contractual otorgado por el Banco X al pignorarlo.

- **Verificación Criptográfica Ciega para J.P. Morgan:** Mediante la composición jerárquica de **Transaction Trees** y el uso de **Blinded Views (Vistas Cegadas)**, el nodo participante de J.P. Morgan recibe de forma segura el ContractId del colateral rehipotecado. El motor de Daml de J.P. Morgan verifica criptográficamente la integridad y autenticidad del bono soberano emitido en el Paso 1 por el custodio del Estado Español, **sin necesidad de ver ni descifrar los términos comerciales bilaterales privados del primer préstamo de cobertura pautado entre el Banco X y Goldman Sachs**. J.P. Morgan tiene la plena certidumbre matemática de que el colateral subyacente es legalmente válido y no ha sufrido doble gasto.

- **Contención del Riesgo en Tiempo Real para Banco X:** A través de su Nodo Participante, el Banco X (emisor inicial del colateral) observa en tiempo real que Goldman Sachs continúa figurando en los registros contables como el **responsable contractual directo del activo bloqueado**. La rehipotecación hacia J.P. Morgan se gestiona como una sub-transacción delegada: J.P. Morgan adquiere la potestad de ejecutar y liquidar el pagaré en caso de un incumplimiento por parte de Goldman, pero la soberanía de los datos de Banco X permanece blindada y su riesgo de contraparte se mantiene estrictamente contenido dentro de las fronteras del contrato bilateral original con Goldman Sachs, evitando la propagación de riesgos sistémicos no controlados.

Paso 4: Vencimiento (Release / Devolución)

- **Mecánica en el Ledger:** Al completarse el ciclo de financiación intradía, Goldman Sachs reembolsa el efectivo correspondiente a J.P. Morgan en el dominio de liquidación, lo que extingue de forma indivisible la rehipotecación y libera los gravámenes sobre el colateral.

- **Finalidad DvP T+0 Indivisible:** Una vez canceladas las obligaciones de Banco X frente a Goldman Sachs, se ejerce la Choice de Release en el contrato de colateral. El protocolo Canton procesa de forma síncrona el archivado final de PledgedCollateral en el ACS de Goldman Sachs y, de manera atómica e indivisible, **devuelve y rematerializa el pagaré de deuda soberana española de 10.000 € en estado libre en el ACS local de la tesorería de Banco X (DvP T+0 instantáneo)**. El ciclo se cierra de manera determinista y con inalterabilidad garantizada en el ledger descentralizado, eliminando los riesgos de conciliación y la latencia operativa del post-trading tradicional.

6.3 Stack Tecnológico e Implementación

Para materializar la Prueba de Concepto (PoC) de rehipotecación de deuda soberana de forma segura, privada y automatizada, se define un stack tecnológico moderno y optimizado para la integración con sistemas core bancarios heredados (*legacy*).

La arquitectura técnica se divide en la lógica de contratos inteligentes, la capa de cliente/integración API, la topología de infraestructura de red y las herramientas de orquestación ágil.

- **Lógica Contractual (Daml):** La lógica de negocio y las transiciones de estado del colateral (como la emisión, pignoración, reuso y devolución) se implementan en su totalidad mediante el lenguaje funcional **Daml**. Al utilizar Daml, las reglas de autorización criptográfica, las condiciones de visibilidad (*signatories* y *observers*) y los derechos de disposición (*choices*) se codifican directamente dentro del contrato inmutable, asegurando que la privacidad del "need-to-know" se ejecute de forma nativa a nivel de protocolo.

- **Cliente y API (Python** dazl **client):** Para automatizar el ciclo de vida de los repos y las pignoraciones desde interfaces bancarias tradicionales y sistemas heredados (*legacy back-office*), se utiliza el cliente **Python** dazl . Este cliente de Python actúa como un puente de integración robusto, conectándose de forma segura a la *Ledger API* expuesta por los nodos participantes. Mediante dazl, el sistema legacy del banco puede emitir de forma programática comandos de ejercicio de Choices (como Accept o canReUse), leer flujos de eventos del ledger en tiempo real, e integrar reconciliaciones automatizadas sin alterar la infraestructura existente de la entidad.

- **Infraestructura de Pruebas (Canton DevNet de 3 Nodos):** La topología física de la PoC se despliega sobre un entorno **Canton DevNet**, diseñado como el paso previo obligatorio a las fases de TestNet y MainNet. Este DevNet local está configurado por **3 nodos participantes locales interconectados** [283], los cuales representan respectivamente al Banco X, Goldman Sachs y J.P. Morgan. Cada uno de estos nodos mantiene su propio *Active Contract Set* (ACS) local y se conecta a un secuenciador privado local para recibir marcas de tiempo y asegurar un ordenamiento libre de doble gasto.

- **Orquestación y Despliegue (Docker /** docker-compose**):** Con el fin de garantizar la portabilidad, la repetibilidad de las pruebas y la rapidez en el despliegue, la infraestructura completa de la DevNet (los 3 nodos participantes y el sincronizador/secuenciador local) se orquesta utilizando **contenedores Docker** . A través de una receta de orquestación lista en docker-compose.yml, los desarrolladores e ingenieros de DevOps bancarios pueden levantar la red de pruebas con un simple comando (docker-compose up), logrando un entorno operativo y completamente funcional en **menos de dos minutos**. Esta abstracción de contenedores minimiza la complejidad operativa y elimina las fricciones de instalación de software en infraestructuras locales on-premises o en la nube.


CASO DE USO TÉCNICO · POC CANTON NETWORK · SECCIÓN 6.2
Cuatro capas, un comando: el stack tecnológico de la PoC de rehipotecación
Un stack moderno pensado para integrarse con el core bancario heredado — de la lógica de negocio inmutable hasta un entorno de pruebas que se levanta en menos de dos minutos.
01 · LÓGICA CONTRACTUAL
Daml
signatories · observers · choices
Emisión, pignoración, reuso y devolución se codifican como reglas inmutables dentro del propio contrato. La privacidad "need-to-know" se ejecuta de forma nativa a nivel de protocolo, no como una capa externa.
02 · CLIENTE E INTEGRACIÓN
Python — dazl client
Ledger API
Puente entre el back-office legacy del banco y la Ledger API: emite comandos (Accept, canReUse), lee eventos del ledger en tiempo real y automatiza conciliaciones sin tocar la infraestructura existente.
03 · INFRAESTRUCTURA DE PRUEBAS
Canton DevNet
paso previo a TestNet / MainNet
3 nodos participantes locales interconectados, cada uno con su propio ACS y su secuenciador privado para un ordenamiento libre de doble gasto.
Banco X
Goldman Sachs
J.P. Morgan
04 · ORQUESTACIÓN Y DESPLIEGUE
Docker / docker-compose
docker-compose up
Toda la DevNet —los 3 nodos y el secuenciador local— se levanta con un solo comando en menos de 2 minutos: portátil, repetible y sin fricciones de instalación on-premise o en la nube.
De la lógica de negocio al entorno operativo: un stack completo, reproducible en menos de dos minutos.
Fuente: "De Activo Cautivo a Activo Líquido" — Sección 6.2, Stack Tecnológico e Implementación

CAPÍTULO 7: Sincronización e Interoperabilidad: Análisis Comparativo Cosmos vs. Canton

El diseño de la interoperabilidad en los sistemas de registro distribuido (DLT) define la forma en que los activos y los datos se movilizan entre diferentes aplicaciones e instituciones. Para las entidades financieras reguladas, la elección de la infraestructura depende de cómo se equilibren la **soberanía operativa**, la **finalidad de la transacción** y la **privacidad de los datos de negocio**.

Este capítulo realiza un análisis comparativo profundo entre dos de los paradigmas descentralizados más avanzados: el ecosistema de cadenas soberanas de **Cosmos** y la arquitectura de nodos coordinados de **Canton Network**

7.1 Arquitectura: Soberanía frente a Sincronización Coordinada

La diferencia fundamental entre Cosmos y Canton radica en sus modelos de estado y en la topología de sus componentes de red, lo que determina cómo se gestiona la confianza y la consistencia de la información.

COMPARATIVA DE TOPOLOGÍAS DE INTEROPERABILIDAD (COSMOS VS. CANTON)

7.1.1 Cosmos: El modelo de Cadenas Soberanas (App-Chains)

El ecosistema de Cosmos se fundamenta en un modelo de **cadenas de bloques Layer 1 totalmente soberanas e independientes**. Bajo este esquema, cada organización o consorcio que despliega un libro mayor (*ledger*) mantiene el control absoluto sobre las siguientes variables críticas:

- **Soberanía de Infraestructura y Gobernanza:** Cada red o *App-Chain* construida sobre el stack de Cosmos controla de extremo a extremo su estructura interna, su modelo de seguridad de datos, su propio conjunto de operadores de nodos validadores y sus garantías de rendimiento y finalidad transaccional. Esto otorga a la organización una autonomía operativa total, **sin ningún tipo de dependencia de terceros o de redes externas** para el procesamiento y validación de sus transacciones.
- **Mensajería Asíncrona Punto a Punto (Protocolo IBC):** Para que estas cadenas independientes interactúen, Cosmos utiliza el protocolo **Inter-Blockchain Communication (IBC)**. IBC actúa como un protocolo de comunicación general capaz de transmitir instrucciones, datos y activos de manera asíncrona entre redes soberanas, conectando tanto registros públicos como privados y bases de datos tradicionales de instituciones financieras. Al operar como un modelo asíncrono, cada cadena mantiene su propio estado cerrado y procesa las llamadas externas como eventos diferidos, lo que permite un aislamiento operativo pero introduce latencias de confirmación transaccional entre cadenas.

7.1.2 Canton Network: El modelo de Nodos Participantes Coordinados

Canton Network rechaza la creación de cadenas independientes y soberanas que actúen como silos de datos, sustituyéndolas por un modelo de **nodos participantes privados coordinados sobre un único "Libro Mayor Virtual Global"**.

- **Ausencia de Estado Global Replicado:** En Canton, **ningún participante de la infraestructura (ni siquiera los validadores de red) opera un nodo que almacene la totalidad del estado o de los datos del ledger**. El estado contable global es virtual y se encuentra fragmentado de forma física en los servidores locales de cada banco.
- **Custodia del Estado según "Necesidad de Saber":** El nodo participante de cada banco almacena única y exclusivamente los datos e históricos de transacciones que son directamente relevantes para los contratos inteligentes en los que tiene un rol de parte autorizada (*signatory* u *observer*). Las transacciones se encriptan de extremo a extremo y se transmiten de manera segura a nivel de sub-transacción utilizando el modelo de permisos declarativos del lenguaje de contratos inteligentes Daml.
- **Sincronización Cifrada Multidominio:** Para lograr la composibilidad (la capacidad de ejecutar transacciones que crucen múltiples aplicaciones bancarias de forma simultánea y atómica), Canton separa de manera estricta la lógica de negocio respecto al ordenamiento de mensajes. Los nodos participantes de los bancos conectan sus interfaces a **dominios de sincronización específicos** y al **Sincronizador Global (*Global Synchronizer*)**. Estos sincronizadores ordenan de forma secuencial y cronológica los paquetes de transacciones encriptados (*Blinded Views*), garantizando la consistencia temporal de la red y evitando de forma determinista el doble gasto de activos de colateral, sin que los operadores de infraestructura tengan acceso visual a las identidades o balances de los bancos.

7.1.3 Matriz de Síntesis Comparativa: Cosmos vs. Canton Network

Para facilitar la evaluación de la infraestructura por parte de equipos ejecutivos de tecnología y riesgos (C-Level), se presenta a continuación un análisis de los parámetros de diseño más relevantes de ambos entornos:

Dimensión de Evaluación	Cosmos (App-Chains)	Canton Network ("Red de Redes")
Modelo de Estado	**Estado replicado localmente** en cada cadena Layer 1 soberana. Cada cadena tiene su propia base de datos completa.	**Libro Mayor Virtual Global**. El estado real está fragmentado físicamente solo en los nodos que "necesitan saber".
Gobernanza de Red	**Soberana y absoluta.** El emisor controla por completo sus validadores, reglas de acceso e inmutabilidad.	**Gobernanza Federada.** El Sincronizador Global es administrado de manera neutral por la Global Synchronizer Foundation.

Privacidad de Datos	**Privacidad por red.** Las transacciones dentro de una App-Chain privada son visibles para todos los validadores de esa subred.	**Privacidad por sub-transacción.** Cifrado de extremo a extremo nativo. Nadie ve el balance a menos que esté declarado en Daml.
Interoperabilidad	**Asíncrona y P2P (IBC).** Mensajería general para conectar registros públicos, privados e internos.	**Síncrona y Atómica.** Ejecución de workflows multidominio unificados sin puentes criptográficos de terceros.
Rendimiento y Escalabilidad	**Rendimiento predecible y optimizado.** 1.900+ TPS en condiciones estándar, escalable a más de 10.000 TPS.	**Dependiente de la topología del flujo.** El rendimiento varía según el número de participantes en un dominio y la complejidad del contrato.
Ecosistema de Desarrollo	**Ecosistema abierto global.** Stack tecnológico maduro (Cosmos SDK) enfocado en soberanía de múltiples lenguajes.	**Ecosistema institucional consolidado.** Enfoque exclusivo en flujos financieros regulados (Broadridge, Goldman Sachs, J.P. Morgan).
Dependencia del Proveedor	**Ninguna.** El código es de código abierto y no depende de ninguna fundación para su operación o seguridad.	**Dependencia de plataforma.** El protocolo y el compilador del lenguaje Daml son gobernados por Digital Asset y la Fundación

7.2 Privacidad: Aislamiento por cadena frente a Privacidad por sub-transacción

El modelo de confidencialidad y control sobre la visibilidad de los datos comerciales es la dimensión más sensible para la operación de los mercados de capitales regulados. Cosmos y Canton abordan esta exigencia desde fundamentos criptográficos y filosofías de diseño de red contrapuestas:

COSMOS	**CANTON NETWORK**
(Aislamiento de L1)	(Privacidad Sub-tx L1)

A. Cosmos: Privacidad por Aislamiento de Cadena (Chain-Level Isolation)

En el ecosistema de Cosmos, la confidencialidad no se gestiona de manera nativa a nivel de contrato inteligente o de registro individual en una infraestructura común, sino mediante la separación física y lógica de las redes:

- **Aislamiento de Estado por Red Cerrada:** El enfoque por defecto para proteger la información confidencial en Cosmos consiste en desplegar una **cadena Layer 1 privada o permisionada independiente** para cada consorcio, mercado u

organización. Dado que los datos residen exclusivamente en el conjunto de validadores autorizados de esa blockchain específica, no hay riesgo de filtraciones de datos contables hacia competidores ajenos al consorcio.

- **Divulgación Mínima de Interoperabilidad:** Cuando una cadena privada en Cosmos necesita interactuar con otra red (ya sea pública, privada o una base de datos bancaria), el protocolo **IBC (Inter-Blockchain Communication)** se encarga de transferir de forma asíncrona únicamente los metadatos y la información estrictamente necesaria para validar la validez del estado del activo o la instrucción enviada. El resto de los balances, cuentas e historiales internos de la cadena privada de origen permanecen totalmente invisibles y protegidos contra auditorías externas.
- **Primitivas Criptográficas Ad-hoc:** Para aquellos casos de uso que requieran confidencialidad transaccional de grano más fino dentro de una misma red, Cosmos no ofrece una solución integrada en su base. En su lugar, el ecosistema se apoya en desarrollos de blockchains especializadas en privacidad (como *Secret Network*, *Penumbra* o *Fairblock*) que implementan criptografía de umbral (*threshold cryptography*) y entornos de ejecución seguros.

B. Canton Network: Privacidad Nativa por Sub-transacción a Nivel de Layer 1

Canton Network elimina la necesidad de fragmentar la infraestructura en subredes aisladas para obtener confidencialidad, integrando un modelo de **privacidad selectiva y programable en la capa base de su protocolo (Layer 1)**:

- **Reglas de Visibilidad en el Lenguaje Contractual (Daml):** El lenguaje Daml define de manera explícita en su propio código los roles de **Signatories (Firmantes)** y **Observers (Observadores)** para cada contrato. El motor de ejecución de Canton utiliza estas definiciones a nivel de protocolo para garantizar que, si una entidad no es parte interesada o autorizada en una transacción, **los datos encriptados de la transacción físicamente nunca son transmitidos ni almacenados en su nodo participante**, mitigando de raíz el riesgo de ingeniería social o análisis competitivo.
- **Árboles Transaccionales y Vistas Cegadas (*Blinded Views*):** Las transacciones complejas en Canton se descomponen jerárquicamente en forma de árboles de transacciones (*Transaction Trees*). A través de las **Vistas Cegadas (*Blinded Views*)**, los datos se encriptan de extremo a extremo y se distribuyen selectivamente bajo el principio estricto de la "necesidad de saber" (*need-to-know*). Esto permite que diferentes dApps independientes colaboren de forma atómica sobre la misma infraestructura común: por ejemplo, en una liquidación DvP, el nodo del banco de efectivo solo recibe y valida la pata del pago, mientras que el nodo del registrador de colaterales procesa exclusivamente la pata del activo, permaneciendo ambos ciegos respecto a la información comercial confidencial del otro.
- **Auditoría Regulada Coexistente:** Este modelo de divulgación selectiva simplifica el cumplimiento normativo. Es posible añadir a un supervisor financiero (como el Banco de España o la CNMV) con un rol de **Observer (Observador)** a nivel de contrato inteligente Daml. Esto permite al regulador auditar operaciones en tiempo

real y de forma pasiva mediante un nodo dedicado sin necesidad de exponer dichos datos comerciales de forma pública a los competidores del mercado.

7.3 Rendimiento, TPS y Latencia Operativa

El rendimiento de una red financiera y su velocidad de liquidación definitiva (*settlement finality*) determinan su idoneidad para procesar operaciones de alta frecuencia o liquidaciones masivas en mercados secundarios. **Las arquitecturas de Cosmos y Canton Network divergen sustancialmente en cómo balancean el volumen de transacciones por segundo (TPS), el tiempo de finalización y el coste de la consistencia transaccional.**

COSMOS	CANTON NETWORK
(Consenso de Bloque Global)	(Commit en Dos Fases)

A. Cosmos: Alto Rendimiento y Finalidad en Sub-segundos

La pila tecnológica de Cosmos, a través de su motor de consenso **CometBFT**, prioriza la alta capacidad de procesamiento y la minimización de la latencia operativa para entornos financieros de alta transaccionalidad:

- **Rendimiento Sostenido:** Las cadenas de bloques desarrolladas con el SDK de Cosmos logran de manera consistente un rendimiento de **más de 1.900 transacciones por segundo (TPS)** bajo condiciones operativas estándar de producción. En entornos altamente optimizados y con infraestructuras dedicadas, como el ledger de Cronos de Crypto.com, el rendimiento puede **superar las 10.000 TPS**.
- **Latencia de Finalización Inmediata:** Gracias al protocolo de consenso de CometBFT, Cosmos ofrece una finalidad determinista de forma síncrona en **menos de 500 milisegundos (medio segundo)** en configuraciones estándar. Esto significa que, una vez que una transacción de colateral o transferencia es incluida en un bloque, es legal y técnicamente definitiva, eliminando cualquier posibilidad de bifurcación de la cadena (*chain forks*) o reorganización de bloques.
- **Roadmap Técnico:** El mapa de ruta técnico de Cosmos proyecta alcanzar un rendimiento sostenido de **5.000 TPS** en configuraciones de producción estándar para finales de año, lo que consolida su posición para flujos transaccionales masivos y procesamiento de liquidaciones en tiempo real.

B. Canton Network: Latencia Acotada para Preservar la Privacidad Multilateral

A diferencia del enfoque de procesamiento global y plano de Cosmos, Canton Network no está diseñada para optimizar la velocidad pura a expensas de la visibilidad, sino para garantizar la confidencialidad absoluta a nivel de sub-transacción:

- **Ausencia de Benchmarks Estandarizados:** Debido a la naturaleza fragmentada de su arquitectura de "red de redes" (donde cada subred o dominio de sincronización puede operar bajo diferentes tecnologías, reglas de acceso y configuraciones de red), **el protocolo de Canton no publica benchmarks estandarizados de TPS**.

Esto hace complejo comparar su rendimiento de manera lineal con registros tradicionales o blockchains públicas.

- **El Coste Operativo del Compromiso en Dos Fases (2PC):** Para ejecutar un cambio de estado multilateral de forma consistente, Canton depende del protocolo de **Compromiso en Dos Fases (Two-Phase Commit)** coordinado por los nodos secuenciadores y resuelto por el **Mediador**. El flujo implica que el participante prepara la transacción, el secuenciador le asigna un orden temporal, las partes involucradas la validan localmente y envían sus firmas de aprobación de vuelta al Mediador, y este emite finalmente el veredicto definitivo de confirmación (*Commit Verdict*).
- **Latencia Transaccional Típica:** Este flujo distribuido de validación e intercambio de mensajes cifrados introduce una latencia operativa. El tiempo requerido para que un mensaje sea secuenciado, validado localmente de forma P2P y confirmado de forma definitiva por el Mediador oscila típicamente **entre 1 y 2 segundos**. Este modelo sacrifica la inmediatez de sub-segundos a cambio de asegurar que ninguna parte no autorizada tenga visibilidad de la transacción, priorizando la soberanía de datos y la consistencia transaccional estricta (libre de doble gasto) sobre la velocidad transaccional masiva.
- **Escalabilidad Horizontal por Dominios:** No obstante, el rendimiento transaccional de Canton no cuenta con un límite teórico global. Dado que las transacciones se procesan de forma localizada únicamente por sus propios stakeholders (sin congestión global de la red), un único dominio de sincronización puede escalar de forma aislada para procesar miles de transacciones por segundo (TPS) utilizando cómputo paralelo, mientras que la creación de nuevos dominios independientes evita que el tráfico de una dApp (como una emisión de bonos masiva) afecte los recursos o eleve las tarifas del resto de las aplicaciones conectadas al Sincronizador Global.

7.4 Dependencia de Plataforma (Vendor Lock-In)

La elección de una tecnología de registro distribuido a largo plazo para infraestructuras financieras de importancia sistémica exige evaluar con rigor el riesgo de dependencia del proveedor (*vendor lock-in*) y la capacidad de la institución para influir de forma soberana en la evolución técnica del protocolo. En esta dimensión, Cosmos y Canton presentan filosofías opuestas respecto al control de la propiedad intelectual, el mantenimiento del software y el gobierno de la red.

COSMOS	**CANTON NETWORK**
(Gobernanza Abierta)	(Gobernanza Coordinada)

A. Cosmos: Soberanía Tecnológica Completa y Gobernanza Abierta

El ecosistema de Cosmos se fundamenta en un modelo de código 100% abierto y descentralizado, libre de intermediarios o controladores corporativos unilaterales:

- **Ausencia de Control Centralizado:** La pila tecnológica de Cosmos (que incluye Cosmos SDK, CometBFT e IBC) es de código abierto y está mantenida de forma

colectiva por un amplio y diverso ecosistema de colaboradores globales. Ninguna empresa o entidad individual posee la potestad exclusiva sobre el protocolo, las patentes o las decisiones técnicas de evolución del estándar.

- **Propiedad de la Infraestructura:** Las instituciones financieras que construyen sobre Cosmos son dueñas absolutas de su infraestructura. No dependen de la hoja de ruta de producto (*product roadmap*) ni de las decisiones de plataformas de ningún tercero para que sus libros mayores continúen operando con total normalidad. Esto permite realizar adaptaciones regulatorias ágiles o modificar la infraestructura interna sin necesidad de aprobaciones o firmas externas de un consorcio comercial.

B. Canton Network: Gobernanza Coordinada y Dependencia Estructural

Aunque el núcleo de Canton es abierto, su evolución y los componentes de sincronización central de su red global están fuertemente ligados a la empresa que creó la tecnología y a su fundación asociada:

- **Dependencia de Digital Asset Holdings y la Fundación:** El desarrollo técnico del estándar Canton y del lenguaje de programación Daml es gobernado y controlado por la empresa comercial **Digital Asset Holdings** y por la **Canton Network Foundation**. Los adoptantes de Canton asumen un compromiso estratégico a largo plazo con la tecnología y las decisiones de gobernanza de un único proveedor de software comercial, un escenario de dependencia que no existe en el ecosistema Cosmos.
- **Vulnerabilidad de la Hoja de Ruta Compartida:** Para transaccionar a través del Sincronizador Global u otros dominios administrados, los participantes dependen de una infraestructura compartida. Las instituciones participantes tienen una capacidad limitada para modificar o hacer evolucionar estos componentes de sincronización de manera independiente. Si las prioridades estratégicas de Digital Asset cambian, o si las decisiones de gobernanza de la Fundación entran en conflicto con los requisitos internos o el cumplimiento normativo de un banco específico, el coste técnico y financiero de migración hacia otra plataforma es sustancial.

CAPÍTULO 8: Regulación, Cumplimiento y ESG bajo los Marcos MiCA, GDPR y DORA

8.1 Cumplimiento de Prevención de Blanqueo (AML/CFT) con Privacidad Coexistente

La adopción generalizada de la tecnología blockchain por parte de las instituciones financieras de importancia sistémica ha estado históricamente limitada por una tensión fundamental:

---

la necesidad de cumplir con las estrictas normativas contra el blanqueo de capitales y la financiación del terrorismo (AML/CFT) frente a la obligación legal de proteger el secreto bancario y la confidencialidad comercial de sus clientes.

Las redes públicas tradicionales obligan a difundir la totalidad de los datos e historiales de transacciones por todos los nodos de la red para su validación, violando las leyes de protección de datos; mientras que las redes completamente opacas impiden que los oficiales de cumplimiento identifiquen flujos de fondos ilícitos.

Para resolver este desafío, la arquitectura de Canton Network se integra con las soluciones de inteligencia de blockchain de **TRM Labs**. Este marco conjunto aborda la privacidad y el cumplimiento no como principios opuestos, sino como un **problema de diseño integral**, estableciendo que ambos pueden coexistir mediante la combinación de un modelo de privacidad configurable y controles de gobernanza criptográfica.

A. El rol de control del Guardián (Guardian)

En el modelo de Canton y TRM Labs, el control sobre los datos encriptados no recae sobre una base de datos centralizada ni se expone públicamente. En su lugar, el sistema introduce el rol del **Guardián (*Guardian*)**:

- **Definición y responsabilidad:** El Guardián es la entidad técnica o jurídica responsable de gobernar las políticas de acceso y visibilidad de los datos encriptados de las transacciones para un activo tokenizado específico.
- **Gobernanza programática:** El Guardián define a nivel de código quién tiene autorización para ver los datos, bajo qué condiciones regulatorias exactas y con qué finalidad específica, garantizando un acceso estrictamente controlado, auditable y alineado con los requisitos legales de cada jurisdicción.

B. Divulgación Basada en Riesgos (Risk-based Disclosure)

Para evitar la monitorización intrusiva y masiva de todas las cuentas honestas, el sistema aplica el principio de la **Divulgación Basada en Riesgos (*Risk-based Disclosure*)**:

- **Análisis sin visibilidad completa:** Los oficiales de cumplimiento y los sistemas automatizados de TRM Labs pueden evaluar riesgos de manera continua sin necesidad de disponer de acceso visual directo a los datos privados de cada transacción de la red.
- **Evaluación de señales y metadatos:** El sistema analiza metadatos, flujos y conexiones criptográficas para identificar señales de riesgo específicas, tales como la interacción directa o indirecta con direcciones de billeteras pertenecientes a entidades de alto riesgo, organizaciones sancionadas o mercados negros on-chain.
- **Revelación condicionada:** La identidad de las contrapartes o los detalles comerciales de una transferencia permanecen completamente encriptados y protegidos. Únicamente en el escenario de que una transacción supere de forma fehaciente un umbral crítico de alerta AML o muestre una exposición severa a actores de riesgo, se activa el protocolo para descifrar y revelar de forma selectiva los datos necesarios a las autoridades competentes o al oficial de cumplimiento a cargo de la investigación.

C. Divulgación Selectiva (Selective Disclosure) y Roles de Observador

El proceso de descifrado y entrega de información se ejecuta de manera nativa e irrevocable mediante la **Divulgación Selectiva (*Selective Disclosure*)** integrada en la capa contractual:

- **Definición:** Es el mecanismo técnico de Canton que permite compartir metadatos o fragmentos de transacciones encriptadas con terceros autorizados bajo condiciones lógicas preprogramadas en el contrato inteligente.
- **Roles de Observadores Designados (*Designated Observer Roles*):** Las plantillas de contratos inteligentes de Daml incorporan campos específicos para definir observadores. Esto permite otorgar de forma programática acceso de solo lectura (*read-only*) y en tiempo real a las transacciones que cumplan con criterios normativos específicos (por ejemplo, transacciones que excedan el límite de la

Travel Rule), permitiendo auditorías regulatorias continuas y sin fricciones sin comprometer la privacidad del resto del mercado.

A través de esta sofisticada combinación de cifrado de extremo a extremo, análisis inteligente de riesgos y revelación selectiva condicionada, Canton y TRM Labs demuestran que es técnicamente viable construir una infraestructura financiera que respete las rigurosas garantías de confidencialidad comercial exigidas por la banca institucional, al tiempo que proporciona a los supervisores del mercado herramientas de monitorización y cumplimiento radicalmente más eficientes que las del sistema financiero tradicional

8.2 Conexión con Supervisores: El nodo observador

En los mercados financieros tradicionales, la supervisión de operaciones se realiza de manera diferida mediante complejos procesos de reporte regulatorio (como los informes diarios T+1 o semanales).

Esto genera altos costes de conciliación para las entidades y una visibilidad fragmentada para las autoridades supervisoras.

La arquitectura de Canton Network y el lenguaje Daml transforman este paradigma al introducir la primitiva técnica del **Observer (Observador)**, permitiendo que organismos reguladores —como la **CNMV** o el **Banco de España**— se conecten directamente a la infraestructura y auditen flujos financieros en tiempo real de manera pasiva y no intrusiva.

A. La primitiva técnica del Observer en Daml

En la capa de contratos inteligentes de Daml, la gobernanza de datos no se delega a sistemas externos, sino que se define en la propia plantilla (*template*) del contrato de manera declarativa. El lenguaje implementa de forma nativa la directiva **observer** junto a la directiva obligatoria **signatory**:

- **Garantías de Solo Lectura (*Read-Only*):** El participante definido bajo el rol de observer tiene garantizados criptográficamente los derechos de visibilidad y acceso de lectura (*fetch*) sobre todos los campos y estados del contrato activo. Sin embargo, carece por completo de la facultad de firmar la creación del contrato o de ejercer de manera unilateral acciones de tipo controlador (*choices*) que alteren o archiven el estado del activo, salvaguardando la validez legal del acuerdo original firmado por las contrapartes comerciales.
- **Exclusión estricta por defecto:** Cualquier nodo participante o competidor del mercado que no esté registrado explícitamente como firmante (*signatory*) o como observador (*observer*) en un contrato inteligente de Daml **no tiene posibilidad alguna de visualizar los datos, balances ni metadatos del activo**.

B. Supervisión pasiva e inmediata sin latencia de reporte

La inclusión del supervisor como observador técnico del contrato inteligente elimina la necesidad de sistemas de reporting reactivos o procesos de auditoría forense posteriores a la negociación:

- **Monitoreo en Tiempo Real:** El nodo participante operado por el supervisor financiero recibe las actualizaciones del estado de los contratos inteligentes en el instante exacto en que el Mediador emite su veredicto de confirmación (*Commit Verdict*). El supervisor puede consultar de manera automatizada su conjunto de contratos activos (ACS) locales para visualizar exposiciones a riesgos, posiciones de colateral soberano o movimientos de efectivo intradía.
- **Acceso No Intrusivo:** El regulador obtiene acceso visual a los datos de negocio de manera totalmente pasiva, interactuando con el ledger a través de interfaces de consulta estándar (*Ledger API*) sin necesidad de interferir en la validación activa de las transacciones ni añadir latencia a la infraestructura de liquidación de las entidades privadas.

C. Divulgación selectiva condicionada y programable

Gracias a la programabilidad de Daml, la visibilidad del supervisor no tiene por qué ser de todo o nada. Se pueden codificar flujos de trabajo de **divulgación dinámica basados en umbrales de riesgo**:

- **Alertas y divulgación dinámica:** Una dApp de pagos o transferencia de colaterales puede estructurarse de modo que, si una transacción se mantiene por debajo de los 10.000 € u opera dentro de parámetros normales, el regulador no figure en el contrato inteligente. No obstante, si se inicia una propuesta de transferencia (*TransferProposal*) que excede un importe umbral o muestra parámetros de riesgo inusuales, las reglas del contrato inteligente añaden de manera dinámica y obligatoria la identidad criptográfica del regulador como **Observer** en el nuevo contrato generado, forzando la revelación selectiva de los datos para su investigación.

D. Preservación del Sharding de Privacidad del mercado general

Una de las mayores preocupaciones bancarias al conectar a un regulador a un libro mayor compartido es la potencial centralización de datos y el riesgo de filtraciones masivas de información financiera ajena a su jurisdicción. Canton anula esta vulnerabilidad estructural a través de su modelo de estado fragmentado (*sharded*):

- **Aislamiento de bases de datos por nodo:** Debido a que el estado global de Canton es virtual y está shardeado físicamente, el nodo participante del supervisor financiero **solo recibirá y almacenará de forma física aquellos fragmentos del libro mayor contable (ACS) en los que haya sido explícitamente declarado como Observer**.
- **Invisibilidad del resto del mercado:** El supervisor no tiene acceso físico ni capacidad criptográfica para descifrar o analizar transacciones de otras dApps, pools de liquidez u operaciones bilaterales de otras entidades financieras de la red en las que no esté explícitamente involucrado, preservando la confidencialidad de

mercado y garantizando que la visibilidad reguladora se limite de forma matemática al principio de "necesidad de saber" (*need-to-know*).

8.3 Estatus de Canton Coin (CC) según la Regulación MiCA de la UE

El marco regulatorio impuesto por el Reglamento (UE) 2023/1114 sobre los Mercados de Criptoactivos (MiCA) establece una tipología estricta de activos digitales con el fin de mitigar los riesgos sobre la estabilidad financiera y proteger a los consumidores en el espacio de la Unión Europea.

Para la banca regulada, el correcto encuadre del token de utilidad nativo de la red, **Canton Coin (CC)**, bajo estas directrices es un requisito fundamental para garantizar su viabilidad regulatoria y de cumplimiento.

A. Notificación formal del Libro Blanco

La base de cumplimiento de Canton Coin de cara al mercado de la Unión Europea se ha consolidado mediante la elaboración de su documentación regulatoria formal:

- **Notificación formal:** El **9 de septiembre de 2025**, de conformidad con las exigencias de divulgación estructurada impuestas por las autoridades de la UE (como la Autoridad Europea de Valores y Mercados - ESMA), se notificó formalmente a las autoridades competentes el libro blanco oficial de Canton Coin preparado conforme a las normas de MiCA.
- **Responsabilidad de la Emisión:** Al igual que ocurre con los criptoactivos estándar, la presentación de Canton señala que el libro blanco ha sido notificado a las autoridades competentes sin haber sido aprobado explícitamente por ninguna de ellas. La responsabilidad de la veracidad y el contenido del documento reside de forma exclusiva en el emisor del activo.

B. Clasificación bajo el Título II: Criptoactivo estándar de utilidad de red (Utility Token)

El libro blanco oficial de Canton Coin encuadra de forma unívoca la naturaleza del token bajo el **Título II del Reglamento (UE) 2023/1114**. Esta clasificación determina formalmente que Canton Coin es un **criptoactivo que no es un token referenciado a activos (ART) ni un token de dinero electrónico (EMT)**:

- **Token de utilidad (*Utility Token*):** Su función principal dentro de la red es servir exclusivamente para pagar las comisiones de infraestructura en el *Global Synchronizer* y para recompensar la actividad útil de los supervalidadores, validadores y creadores de aplicaciones que aportan valor medible a la red.
- **Exclusión de los marcos restrictivos (ART y EMT):** Al clasificarse bajo el Título II, Canton Coin queda **completamente fuera de las directrices restrictivas aplicadas a los tokens referenciados a activos o de dinero electrónico**. Esto evita que el token de red sufra las severas exigencias aplicadas a las stablecoins corporativas, facilitando su integración en las tesorerías bancarias únicamente como combustible de red sin incurrir en las limitaciones de emisiones de divisas.

C. Advertencias y salvaguardas de protección al consumidor

De acuerdo con las obligaciones de transparencia recogidas en MiCA, el libro blanco oficial de Canton Coin incorpora advertencias explícitas sobre las limitaciones de las garantías tradicionales en esta clase de activos:

- **Exclusión de esquemas de compensación:** Canton Coin **no está cubierto por los regímenes de compensación de inversores de la Unión Europea**.
- **Exclusión de garantía de depósitos:** El token **no cuenta con el respaldo ni la protección de los sistemas de garantía de depósitos de la UE**.

A través de esta estructuración jurídica rigurosa alineada con MiCA, Canton Network proporciona a las instituciones de la Unión Europea la seguridad regulatoria indispensable para participar en los flujos de su Global Synchronizer, eliminando la incertidumbre jurídica que pesa sobre muchas blockchains públicas

---

8.4 El Euro Tokenizado EURØP como liquidación DvP regulada

La culminación de la programabilidad financiera y la mitigación de los riesgos de liquidación intradía en los mercados de activos digitales regulados de la Unión Europea se materializa mediante el uso de representaciones de dinero digital autorizadas bajo marcos normativos oficiales.

Para asegurar procesos de **Entrega contra Pago (DvP)** atómicos y exentos de volatilidad cambiaria dentro del ecosistema, Canton incorpora de forma nativa soporte para la stablecoin **EURØP**.

A. Emisión y Cumplimiento Normativo de EURØP bajo MiCA

El token **EURØP** es un criptoactivo referenciado al euro con paridad estable 1:1, diseñado para operar de manera transparente dentro del marco legal e institucional europeo:

- **Emisor Autorizado:** EURØP es emitido por **Schuman Financial**, una institución financiera establecida en la Unión Europea y autorizada como **Electronic Money Institution (EMI - Entidad de Dinero Electrónico)** en Francia por la **Autorité de Contrôle Prudentiel et de Résolution (ACPR)**.
- **Cumplimiento con el Título IV de MiCA:** El libro blanco de EURØP se encuentra formalmente notificado a la ACPR (habiendo sido presentado inicialmente el 7 de agosto de 2024 y enmendado el 23 de marzo de 2026), cumpliendo de manera estricta con los requisitos normativos del **Título IV del Reglamento (UE) 2023/1114 (MiCA)** para tokens de dinero electrónico (EMTs).
- **Estructura de Respaldo y Protección de Fondos:** Cada unidad de EURØP emitida en la red está respaldada al 100% por euros físicos y activos denominados en euros de alta calidad y liquidez. Estos fondos de reserva son custodiados bajo un estricto

régimen de segregación en cuentas protegidas abiertas en instituciones de crédito reguladas, quedando blindados contra reclamaciones de acreedores y salvaguardando en todo momento el derecho permanente de reembolso de los titulares a la paridad original.

B. Integración Nativa en Canton Network y Liquidaciones DvP Atómicas

A diferencia de las integraciones tradicionales que requieren puentes descentralizados propensos a fallas o tokens sintéticos de alto riesgo, **EURØP opera de manera nativa en Canton Network mediante utilidades de tokenización basadas en Daml**:

- **Liquidaciones DvP Libres de Fricción:** Al ejecutarse de forma directa sobre la capa de Layer 1 de Canton, EURØP actúa como la pata de efectivo líquida en flujos de transacciones síncronas complejas. Los participantes pueden liquidar transacciones de Entrega contra Pago (DvP) o Pago contra Pago (PvP) en tiempo real (T+0), intercambiando activos tokenizados (como bonos de deuda soberana o fondos de inversión) de forma atómica e irreversible por depósitos de EURØP, eliminando de raíz el riesgo de principal y los tiempos de conciliación tradicionales de varios días hábiles (T+2).
- **Gobernanza Criptográfica Contractual:** La emisión, transferencia y destrucción de EURØP en Canton se controlan mediante contratos inteligentes multifirma en Daml, lo que garantiza que solo Schuman Financial o las partes legítimamente autorizadas puedan validar e instruir cambios de estado contables. Además, las plantillas contractuales permiten implementar controles de seguridad on-chain, tales como la congelación temporal o la incorporación automática de listas de bloqueo regulatorias en casos de fraude o investigaciones de blanqueo de capitales, garantizando el cumplimiento en tiempo real de los requerimientos de la directiva de transferencia de fondos y de prevención AML/CFT.

De este modo, la coexistencia de un marco legal de Dinero Electrónico plenamente supervisado en la Unión Europea (ACPR/MiCA) y una infraestructura DLT que implementa por diseño el principio de necesidad de saber (Canton) proporciona a la banca mayorista una plataforma de liquidación óptima, donde la liquidez intradía fluye las 24 horas del día, los 7 días de la semana, bajo la máxima certeza técnica, financiera y regulatoria

---

8.5 Análisis del Impacto ESG y de Sostenibilidad

De conformidad con las directrices ambientales de la Unión Europea y los objetivos corporativos de transición climática de las entidades financieras, la sostenibilidad de las infraestructuras de registro distribuido (DLT) se ha consolidado como un criterio de evaluación crítico para los despliegues de grado institucional.

Bajo este contexto, **Canton Network presenta métricas de sostenibilidad altamente eficientes que la posicionan como una solución óptima y de bajo impacto ecológico en comparación con los ecosistemas blockchain tradicionales.**

A. Alineación con las Métricas de Sostenibilidad de la UE (MiCA)

Para promover la transparencia en el impacto climático, Schuman Financial ha alineado la divulgación de las métricas de EURØP con los indicadores de sostenibilidad negativos establecidos en el Reglamento Delegado de la Comisión (UE) 2025/422, adoptado al amparo del Artículo 51de la regulación MiCA:

- **Consumo Energético Anual Reducido:** Canton Network registra un consumo aproximado de apenas **131.115 kWh anuales**. Esta demanda de energía es sumamente baja, colocándose por debajo del consumo mínimo anual de las redes Proof-of-Work (PoW) y de una gran parte de las redes Layer 1 tradicionales (tales como Solana con más de 14 millones de kWh o Ethereum con más de 4,8 millones de kWh).
- **Emisión de Carbono Mínima:** La huella climática de la red se estima en apenas **60,2 toneladas de CO2 equivalente al año**. Esto representa una reducción de emisiones drástica en comparación con las redes PoW tradicionales y se posiciona por debajo de otras redes de consenso eficiente, limitando de manera rigurosa la contribución al calentamiento global en las operaciones financieras de la banca.
- **Producción de Residuos Eléctricos y Electrónicos (WEEE):** Debido a la arquitectura permisionada de la red y la limitada disponibilidad de datos de sostenibilidad pública en este segmento, Schuman Financial señala en su white paper que no dispone actualmente de información suficiente para calcular de forma precisa la generación anualizada de residuos de aparatos eléctricos y electrónicos (WEEE) de Canton. No obstante, debido a la ausencia de hardware de minería o validación altamente especializado de tipo ASIC, se prevé que el impacto por WEEE de la red sea de carácter minimalista o desdeñable, alineándose con las tendencias de redes de bajo coste computacional.

B. La Eficiencia Energética mediante la Validación Selectiva (Stakeholder-Driven Validation)

Los sobresalientes niveles de eficiencia y el bajo consumo de recursos de Canton Network no son accidentales, sino el resultado directo del diseño de su arquitectura descentralizada y su protocolo de consenso:

- **El Modelo de Validación Selectiva:** A diferencia de las blockchains convencionales que imponen un modelo de replicación total del estado y obligan a que todos los validadores de la red ejecuten y verifiquen recursivamente cada una de las transacciones globales, Canton implementa un modelo de **validación selectiva impulsada por las partes interesadas (*Stakeholder-Driven Validation*)**.
- **Eliminación de Redundancia Computacional:** Bajo este esquema, únicamente los nodos participantes de las entidades que son stakeholders directos de una transacción específica son responsables de ejecutar, validar y actualizar de forma

física el estado del contrato inteligente Daml en sus registros locales. Los secuenciadores y mediadores del dominio de sincronización simplemente ordenan y coordinan las transacciones de manera ciega sobre metadatos encriptados, sin reejecutar la lógica de los contratos ni consumir recursos de procesamiento masivo.

- **Reducción del Gasto Eléctrico Interbancario:** Este desacoplamiento entre el ordenamiento y la validación lógica disminuye drásticamente la sobrecarga de cálculo redundante del ecosistema. Las transacciones se procesan de forma paralela y localizada exclusivamente entre los participantes directos, optimizando la utilización de los servidores, limitando la necesidad de adquirir hardware costoso y garantizando un crecimiento sostenible que respeta los límites ecológicos del planeta y las directrices de inversión prudencial ESG más exigentes de la banca internacional.

CONCLUSIÓN, RETORNO DE INVERSIÓN (ROI) Y HOJA DE RUTA C-LEVEL

Redefinición del rol de la custodia bancaria en la era digital

Este documento ofrece un análisis riguroso y formal sobre la **Redefinición del rol de la custodia bancaria en la era digital**, detallando técnicamente los siguientes aspectos:

1. **Abolición del *Custody Drag* sin desintermediación:** Explica cómo Canton Network no elimina a los custodios de confianza (como **BNY Mellon**, **Euroclear** o **Iberclear**), sino que rediseña su infraestructura para eliminar las ineficiencias de su operativa tradicional.

2. **El custodio como Nodo Atestiguador:** Detalla la transformación del custodio, que pasa de depender de reportes asíncronos legados y conciliaciones diferidas en T+2, a operar un **Nodo Participante** que actúa como un **atestiguador criptográfico en tiempo real**, firmando transiciones de estado de forma atómica e inmediata.

3. **Composibilidad e Integridad Multidominio:** Explica cómo la atestiguación y las **pruebas de inclusión** de los custodios respaldan la reasignación de activos (*Topological Change*) sin necesidad de usar puentes vulnerables de terceros.

4. **Beneficios en Capital y Liquidez:** Describe el impacto cuantitativo de la liquidación síncrona 24/7 de colaterales, liberando miles de millones de dólares ociosos y optimizando la gestión de riesgos en mercados regulados

Métricas financieras de Retorno de Inversión (ROI) proyectadas

- Liberación estimada de más de **$1.000 millones de dólares anuales** en capital global atrapado preventivamente gracias a la movilidad del colateral síncrono 24/7
- Reducción neta de entre el **25% y el 50% en los costes de compensación** y post-trading mediante repos y DvP intradía.

- Mitigación de costes por riesgo de contraparte de entre **$3M y $5M de dólares** debido a la indivisibilidad y atomicidad de la liquidación T+0 instantánea.

Hoja de ruta estratégica de implementación en 3 fases para la alta dirección

Para que una institución financiera de importancia sistémica asuma el control soberano de su infraestructura sin alterar la continuidad de sus operaciones tradicionales, se propone un plan de despliegue pragmático y estructurado en tres fases secuenciales:

1. Fase de Planificación y Piloto (Meses 1-3): Validación Lógica y Entorno Local

La fase inicial se enfoca en el diseño de las reglas de negocio y la validación de la de por sí segura lógica contractual dentro de la zona de seguridad interna del banco:

- **Modelado Declarativo de Contratos inteligentes:** El equipo de desarrollo utiliza el lenguaje **Daml (versiones 3.4/3.5)** para codificar las plantillas de los activos, especificando explícitamente los roles de *Signatories* y *Observers* para incrustar la privacidad y los permisos a nivel de la capa base (Layer 1) del protocolo.
- **Despliegue del Entorno DevNet:** Para facilitar la iteración ágil y el testeo técnico, se despliega una red de desarrollo local (**DevNet**) utilizando contenedores **Docker** o clústeres de **Kubernetes** bajo una arquitectura de microservicios corporativa.
- **Integración con APIs Legadas:** Los sistemas centrales tradicionales del banco (core bancario, bases de datos y plataformas de negociación legacy) se conectan al nodo participante de prueba a través de bindings generados automáticamente en **Python (mediante el SDK dazl)** o **Java**. Las llamadas legadas se traducen de forma transparente en comandos dirigidos a la *Ledger API (LAPI)* expuesta por el nodo participante.

2. Fase de Interoperabilidad en TestNet (Meses 3-6): Ensayos DvP y Cumplimiento AML

Una vez validada la lógica local, el banco expande su alcance hacia redes distribuidas multi-nodo externas para emular workflows interbancarios reales:

- **Integración con Stablecoins y Dinero Digital:** El nodo se conecta a la red de prueba **TestNet** de Canton para interactuar con sistemas de pagos mayoristas regulados. Se simulan liquidaciones de Entrega contra Pago (DvP) atómicas e instantáneas utilizando el Euro Tokenizado **EURØP** (emitido por Schuman Financial como EMI autorizada bajo el Título IV de MiCA) y el dinero digital de depósito **Kinexys (JPM Coin)** de J.P. Morgan.
- **Cumplimiento Normativo bajo Privacidad Coexistente:** Se acoplan las herramientas de análisis continuo de **TRM Labs** para monitorizar las transacciones sin comprometer el secreto bancario. Las alertas y señales de cumplimiento se procesan dentro de un Entorno de Ejecución Seguro (TEE) de TRM utilizando el modelo de **Divulgación Basada en Riesgos (Risk-based Disclosure)**, permitiendo auditar operaciones sospechosas o que superen los umbrales de control de forma pseudonimizada de extremo a extremo.

3. Fase de Producción y Sincronización Global (Meses 6-12): Alta Disponibilidad y Movilidad Continuada

La fase de implementación definitiva consolida la migración de los activos financieros reales hacia los rieles de la DLT institucional:

- **Aprovisionamiento de Infraestructura de Producción:** El banco despliega su **Nodo Participante** oficial utilizando soluciones administradas de grado empresarial con alta disponibilidad y copias de seguridad automatizadas (tales como Catalyst Blockchain Manager de IntellectEU o soluciones on-premises).
- **Conexión definitiva al Global Synchronizer:** Tras someterse al proceso de gobernanza y validación de la *Global Synchronizer Foundation (GSF)* para la aprobación e incorporación del nodo participante, la institución conecta su infraestructura al tejido común de sincronización de Canton Network utilizando canales cifrados.
- **Colateralización síncrona 24/7:** Con la conexión al Sincronizador Global, la porción del libro mayor asignada al banco (*Active Contract Set* o ACS) se sincroniza temporalmente bajo el ordenamiento de los **Super Validadores** mediante consenso BFT. El banco pasa a movilizar colaterales de alta calidad de forma instantánea 24/7 de forma líquida y exenta de riesgo cambiario o limitaciones de horario

El Coste de la Inacción y el Nuevo Paradigma de la Liquidez Global

La reconstrucción silenciosa de la infraestructura financiera global ha dejado de ser una proyección de futuro para convertirse en un hecho consumado. Mientras los debates públicos se pierden en la volatilidad de los criptoactivos minoristas, las mayores instituciones financieras del mundo han construido un ecosistema que procesa volúmenes transaccionales que eclipsan la totalidad de las finanzas descentralizadas (DeFi) públicas.

A través de **Canton Network**, el engranaje profundo de Wall Street se está mudando, de forma definitiva, a rieles de tecnología de registro distribuido (DLT) privados, seguros y estrictamente regulados.

Para la alta dirección de cualquier entidad financiera, ignorar esta transición ya no representa una postura prudente de "esperar y ver"; constituye un riesgo estratégico de exclusión operativa de proporciones sistémicas.

A. La Realidad Inapelable de los Números

La escala de actividad y negociación actual de Canton Network desmantela cualquier intento de calificar a esta tecnología como un mero "proyecto piloto":

- **Volumen Transaccional Acumulado:** Canton Network ya gestiona un volumen superior a los **6 billones de dólares** en activos reales tokenizados (RWA) de más de 600 instituciones participantes.
- **Financiación Interbancaria en Producción:** La plataforma **Distributed Ledger Repo (DLR) de Broadridge** procesa de forma nativa más de **8 billones de dólares mensuales** en acuerdos de recompra (repos), operando flujos que superan los **100.000 millones de dólares diarios** en transacciones de repos de bonos del Tesoro de EE. UU..
- **Emisiones Nativas de Valores:** La red registra más de **15.000 millones de dólares** en activos y valores financieros emitidos de forma nativa on-chain.
- **Métricas Operativas Diarias:** La red registra un volumen diario de más de **500.000 transacciones y operaciones operativas**, respaldado por más de **15 millones de transacciones mensuales** que utilizan el token nativo Canton Coin (CC) en sus flujos de coordinación.
- **Liquidez y Dinero Digital Regulado:** Con la integración nativa de **JPM Coin (Kinexys)** de J.P. Morgan y el Euro Tokenizado **EURØP** de Schuman Financial (entidad de dinero electrónico autorizada por la ACPR en Francia bajo el Título IV de MiCA), Canton unifica de forma síncrona el colateral de alta calidad y el dinero de liquidación comercial más líquido del mercado mayorista.
- **Tokenomics y Estructura del Ecosistema de Canton Coin (CC):**
    - **Lanzamiento Justo:** El token nativo CC se lanzó sin minado previo, preventas ni asignaciones para iniciados, distribuyéndose el suministro dinámico en base al valor aportado a la red.

- **Flotante y Capitalización:** Cuenta actualmente con aproximadamente **38.300 millones de CC en circulación** (de un suministro máximo de referencia proyectado de 100.000 millones) y una capitalización de mercado que ronda los **5.800 millones de dólares**.
- **Naturaleza Estrictamente Institucional:** A pesar de su alta capitalización, el volumen spot diario en mercados abiertos se mantiene por debajo de los **10 millones de dólares**. Esto se debe a que el token actúa principalmente como combustible de utilidad para pagar comisiones en el Global Synchronizer y recompensar la provisión de infraestructura y creación de dApps, quedando aislado de la volatilidad puramente especulativa de los criptoactivos minoristas.

B. El FOMO Estructural: El Coste de Oportunidad de Operar en T+2

Las entidades que decidan posponer su entrada en Canton Network se enfrentarán a una desventaja competitiva insalvable en tres frentes críticos:

1. El Drag de Custodia e Inmovilización de Capital (Custody Drag)

A nivel global, existen aproximadamente **255 billones de dólares** en títulos de deuda y valores de alta calidad potencialmente utilizables como colateral para respaldar operaciones de repo, derivados y márgenes de compensación.

Sin embargo, debido a las limitaciones tecnológicas de los custodios tradicionales y las cámaras de compensación asíncronas, **solo 28 billones (el 11%) se encuentran realmente activos y movilizados** en el mercado.

El 89% restante permanece inactivo en balances bancarios como capital inmovilizado debido a retrasos operativos e ineficiencias de liquidación. Canton Network desbloquea este "drag de custodia" permitiendo pignoraciones, swaps atómicos y llamadas de margen intradía inmediatas (T+0), proyectando ahorros de más de **1.000 millones de dólares anuales** en costes de capital de repo para valores de EE. UU. y reducciones de un **25-50% en costes de compensación**.

2. La Frontera del Fin de Semana (24/7 frente a Horario Bancario)

El hito alcanzado donde se completaron las primeras financiaciones de bonos del Tesoro de EE. UU. contra dinero digital en un sábado demostró que **el fin de semana ya no es un tiempo muerto para el capital**.

Las entidades fuera de Canton continuarán sufriendo el coste de mantener colchones de liquidez de reserva improductivos e inmovilizados para cubrir el riesgo de liquidación del fin de semana; mientras tanto, las entidades integradas en Canton movilizarán su colateral las 24 horas del día, los 7 días de la semana, maximizando el rendimiento de sus carteras sin interrupciones horarias.

3. Silos Tecnológicos frente a Composibilidad Síncrona

El modelo tradicional de mensajería (tipo SWIFT) fuerza a las entidades a realizar integraciones puntuales (*pairwise*) complejas, seguidas de pesadas tareas de reconciliación post-transacción que duran días (T+2). Canton unifica la red bajo un **Libro Mayor Virtual Global**.

No pertenecer a esta "red de redes" significa quedar marginado de los flujos de activos que interactúan de forma atómica y síncrona bajo contratos inteligentes unificados en Daml, forzando a la institución excluida a depender de puentes o interfaces manuales lentas y costosas de mantener.

C. Reflexión Final: El Rol de la Dirección en la Nueva Arquitectura Financiera

---

"La tecnología no neutraliza los riesgos financieros; redefine quién es capaz de gestionarlos con éxito."

El verdadero valor de la tecnología de registro distribuido en las finanzas mayoristas no reside en la desintermediación salvaje, sino en la **capacitación de los intermediarios de confianza con herramientas criptográficas impenetrables**. Como hemos analizado a lo largo de este White Paper, Canton Network preserva la soberanía, la gobernanza, el control de acceso y el cumplimiento normativo que exigen las autoridades financieras.

No participar en este cambio estructural ya no es una opción de reducción de riesgos; es la asunción de un riesgo operacional pasivo.

Mientras su entidad sopesa si la DLT es una tecnología madura, sus principales competidores, custodios y reguladores ya están validando bloques, movilizando colaterales de madrugada y liquidando transacciones de forma atómica a nivel global.

La nueva autopista de la liquidez global está abierta. Permanecer en el arcén analógico, operando bajo procesos de reconciliación manuales y asíncronos del siglo pasado, es la vía más rápida hacia la obsolescencia técnica y la ineficiencia de capital.

La pregunta para el Comité de Dirección ya no es si deben adoptar estas herramientas, sino cuánto capital está dispuesto a seguir perdiendo cada día de retraso en su implementación estratégica.

Este paper se ha realizado utilizando Canton Network por que es la red institucional más desarollada y utilizada a día de hoy pero sus conclusiones son de válida aplicación en proyectos similares que puedan existir, que apliquen las tecnologías DLT al entorno bancario institucional aportando eficiencia y cumpliendo con todos los requerimientos regulatorios.