THE UNIVERSAL USERNAME & PAYMENTS LAYER

·Pagos NFC OnChain ·Omnichain Automático
·DeFi ·Username Universal ·Wallet

@username es la nueva dirección

BINNO

Binno Labs https://binno.network @binnonetwork

Índice

Parte I — Visión y Contexto

Parte II — Arquitectura del Ecosistema

Parte III — Economía y Gobernanza

Parte IV — Ejecución y Transparencia

16. Estrategia Go-to-Market
17. Hoja de Ruta (Roadmap)
18. Equipo
19. Seguridad y Contingencia
20. Riesgos
21. Consideraciones Legales
22. Glosario

Aviso. Este documento describe la arquitectura técnica, el modelo económico y la hoja de ruta del ecosistema Binno. Es un documento informativo y no constituye una oferta de venta de valores, asesoría financiera, legal o de inversión. Las cifras de rendimiento (TPS, finalidad) son objetivos de diseño sujetos a validación mediante benchmarks públicos. Las proyecciones de mercado y de adopción son estimaciones, no garantías. La estructura legal y el cumplimiento regulatorio están sujetos a la asesoría profesional correspondiente en cada jurisdicción.

1. Resumen Ejecutivo

Binno es una infraestructura de pagos, identidad y liquidez on-chain diseñada para que enviar dinero y pagar sea tan simple como escribir un nombre de usuario, sin importar la blockchain, el token o el dispositivo. Su objetivo no es ser "otra blockchain", sino el **estándar abierto sobre el que se construya la próxima generación de pagos digitales** —del mismo modo que las redes de tarjetas son la infraestructura invisible detrás de millones de comercios, pero sin custodia, sin intermediarios bancarios obligatorios y sin las comisiones de las redes tradicionales—.

El ecosistema se organiza en seis componentes interdependientes:

- **BinnoChain** — una Avalanche L1 soberana, construida sobre HyperSDK con consenso Snowman++, optimizada para micropagos masivos. Objetivo de diseño: más de 50.000 TPS y finalidad subsegundo, con transacciones internas gratuitas para el usuario.

- **BinnoWallet** — una wallet de custodia MPC sin frase semilla única, donde el usuario elige cuántos fragmentos necesita para firmar y cuántos para recuperar. Genuinamente no custodial.

- **BinnoHub** — el sistema de identidad universal @username, que permite recibir y enviar valor y ejecutar acciones crosschain sin direcciones ni puentes visibles.

- **BinnoPay** — el estándar abierto de liquidación on-chain para pagos físicos (NFC/QR) y de comercio electrónico, integrable por fabricantes de POS, fintechs y wallets.

- **BinnoDEX** — la capa de liquidez del ecosistema, que convierte y enruta activos de forma determinística para que pagos, envíos y crédito funcionen sin fricción.

- **BinnoCredit** — una capa de crédito no custodial respaldada por colateral productivo, con experiencia de usuario equivalente a una tarjeta de crédito.

El token nativo, **BNN**, captura el valor del ecosistema mediante gobernanza, staking con rendimiento real (no inflacionario) y un flywheel de recompras financiado por ingresos reales del protocolo. BNN no se usa para pagar gas.

2. Misión y Visión

Misión. Permitir que cualquier persona, en cualquier parte del mundo, pueda pagar, enviar valor y operar financieramente usando un único @username, con velocidad superior a las redes tradicionales, comisiones marginales y sin renunciar al control de sus fondos.

Visión. Que el envío de valor y los pagos dejen de depender de direcciones, puentes, tokens de gas o conocimiento técnico —y dejen de depender del dinero fiduciario y de las redes de tarjetas como capa obligatoria—. Binno aspira a que, en los próximos años, millones de personas y comercios usen @username a diario para pagar y cobrar sin notar que usan blockchain.

3. El Problema

El dinero en el mundo se mueve sobre infraestructura cara, lenta y fragmentada, y las soluciones cripto actuales —pese a su promesa— no han resuelto el problema para personas reales.

En el mundo tradicional:

- Las remesas globales movieron alrededor de 905.000 millones de dólares en 2024, con un costo promedio que sigue siendo elevado: enviar 200 dólares cuesta en promedio cerca del 6,5%, y a través de bancos puede superar el 14%. Para millones de familias que dependen de estos envíos, esa diferencia es significativa.

- Los comercios pagan a las redes de tarjetas comisiones de entre 1,4% y 3,9% por transacción, y reciben su dinero en lotes con días de retraso.

En el mundo cripto, persisten barreras que impiden la adopción masiva:

- Direcciones largas e imposibles de recordar, con riesgo de error irreversible.

- Gas impredecible, pagado en tokens distintos en cada red, que el usuario debe adquirir y gestionar.

- Experiencia inconsistente y fragmentada entre cadenas.

- La necesidad de "puentes" (bridges), históricamente la categoría más hackeada del espacio.

- Para gastar cripto en el mundo real, hoy es casi obligatorio pasar por una tarjeta Visa/MasterCard o una wallet custodiada —reintroduciendo al intermediario centralizado y sus comisiones que se supone que cripto venía a eliminar—.

El resultado es un sistema donde la tecnología existe pero la experiencia humana sigue siendo demasiado compleja, y donde "usar cripto para pagar" todavía significa, en la práctica, depender de las mismas redes centralizadas de siempre.

4. La Oportunidad de Mercado

El mercado que Binno aborda es uno de los más grandes del mundo, y atraviesa una transición estructural hacia los rieles on-chain.

Pagos digitales. La industria de pagos generó cerca de 2,5 billones de dólares en ingresos en 2025. El mercado de pagos digitales se estima en torno a los 170.000 millones de dólares en 2025, con proyecciones de crecimiento sostenido de doble dígito hacia 2035. Visa y MasterCard movieron, respectivamente, del orden de 14,5 y 9,2 billones de dólares en volumen anual.

Remesas. Un mercado de aproximadamente 905.000 millones de dólares anuales, con costos que duplican el objetivo del 3% fijado por la ONU, y donde los proveedores digitales ya demuestran ser hasta un 75% más baratos que los bancos. Es un mercado con dolor de precio real y demanda comprobada de alternativas más baratas.

La ola de stablecoins ya está ocurriendo. Las stablecoins procesaron del orden de 28 billones de dólares en volumen económico real en 2025, y más de 4 billones en transacciones solo en la primera mitad del año. Analistas del sector proyectan que el volumen de pagos con stablecoins podría igualar al de Visa y MasterCard entre 2031 y 2039. La infraestructura de pagos se está moviendo hacia los rieles OnChain de forma irreversible.

La brecha que Binno ocupa. Hoy, las tarjetas cripto mueven alrededor de 18.000 millones de dólares anualizados, creciendo a más del 100% anual —pero Visa captura más del 90% de ese volumen OnChain de tarjetas—. Esto revela el problema central: **la forma actual de gastar cripto en el mundo real depende de**

las redes de tarjetas tradicionales y de wallets custodiadas. Binno es la alternativa que elimina esa capa: el primer riel de pago no custodial, omnichain, que no necesita a Visa, MasterCard ni a un custodio centralizado para funcionar.

Dónde empezamos. Los mercados con mayor adopción de pagos sin contacto (NFC) y QR, alta frecuencia de micropagos y menor penetración bancaria tradicional —América Latina y el Sudeste Asiático— son el punto de entrada natural. En esas regiones, los pagos contactless y los sistemas de QR ya alcanzan penetración masiva, y la adopción de stablecoins responde a una necesidad económica real.

(El análisis de mercado detallado, los segmentos y la estrategia de entrada se desarrollan en el capítulo de Estrategia Go to Market.)

5. La Solución Binno

Binno resuelve el problema desde la raíz, integrando seis capas en una sola experiencia donde la complejidad técnica desaparece para el usuario.

El principio de diseño es uno solo: **la infraestructura debe desaparecer ante los ojos de quien la usa.** El usuario no ve direcciones, no gestiona gas, no elige puentes, no entiende de qué cadena a qué cadena viaja su dinero. Solo ve un @username, un monto y una red destino.

- **Identidad universal (@username).** Un nombre único y global que reemplaza todas las direcciones del usuario en todas las cadenas.

- **Custodia sin fricción (MPC).** Sin frase semilla única que perder; el usuario decide su propio equilibrio entre seguridad y comodidad, y nunca cede el control de sus fondos.

- **Pagos reales (NFC/QR).** En tienda física o en línea, con la simplicidad de un pago contactless y la liquidación instantánea de una transacción nativa.

- **Interoperabilidad invisible.** El valor viaja entre cadenas sin que el usuario gestione un solo puente.

- **Liquidez y crédito integrados.** Conversión automática de activos y acceso a crédito sin vender lo que se posee.

- **Economía sostenible.** Un token cuyo valor proviene del uso real del protocolo, no de la inflación ni de la especulación.

Cada uno de estos componentes se detalla en los capítulos siguientes.

6. Por qué una L1 Soberana (y no un rollup)

La decisión de construir BinnoChain como una Avalanche L1 soberana —en lugar de un rollup sobre una capa base existente— es la decisión arquitectónica más consecuente del proyecto, y la abordamos de frente porque es también el mayor compromiso de ejecución que asumimos.

La razón principal: nuestra propuesta de valor central es imposible en un rollup estándar. El corazón de la experiencia Binno es que el usuario no paga gas, no gestiona tokens de gas y opera con un costo medido en una unidad estable en dólares. Un rollup hereda el modelo de gas de su capa base: el usuario paga en el token nativo de esa capa, con comisiones volátiles, y debe poseer ese token para transaccionar. Redefinir cómo funciona el gas —medirlo en USD, hacerlo gratuito para el usuario a nivel interno, y sostenerlo de forma estructural— **requiere control soberano de la máquina virtual y del modelo de tarifas.** Eso solo es posible con una VM propia, no como inquilino del blockspace de otra red.

La segunda razón: rendimiento dedicado. Los micropagos masivos a más de 50.000 TPS con finalidad sub-segundo necesitan una cadena que no compita por blockspace con NFTs, DeFi de terceros o picos de actividad ajenos. Una autopista dedicada, no un carril compartido.

La tercera razón: control de extremo a extremo. La lógica de identidad, pagos, liquidez y crédito se implementa como módulos nativos de la VM, auditables y optimizados, en lugar de depender de contratos genéricos. Esto reduce la superficie de ataque y garantiza costo y latencia predecibles.

Por qué Avalanche L1, específicamente. Tras la actualización ACP-77 (Etna / Avalanche9000), una Avalanche L1 soberana ofrece la soberanía total de una blockchain propia —consenso, validadores, gas, gobernanza— **sin el costo de capital y de seguridad de arrancar una L1 completamente desde cero**, ya que hereda el marco y la infraestructura de seguridad de Avalanche. Es la combinación que buscábamos: soberanía de L1 con costo de arranque reducido.

El compromiso que asumimos con honestidad. Operar una L1 soberana es más difícil y costoso que desplegar un rollup: implica asegurar y descentralizar un conjunto de validadores, mantener el consenso y asumir la responsabilidad de la seguridad de la red. Lo asumimos conscientemente porque nuestra propuesta de valor lo exige, y lo mitigamos apoyándonos en el marco de Avalanche y en un modelo de validadores diseñado para alto rendimiento desde el primer día. No subestimamos la dificultad; la elegimos.

7. Valores del Proyecto

- **La simplicidad primero.** La infraestructura desaparece para el usuario. Sin gas, sin frase semilla única, sin puentes, sin elección de redes.

- **Descentralización progresiva, no dogmática.** Se prioriza la seguridad y el rendimiento, con una transición gradual y honesta hacia el control de la comunidad, declarando en cada fase qué es descentralizado y qué no.

- **Sostenibilidad real.** Todo rendimiento proviene de ingresos reales del protocolo, nunca de inflación ni de emisiones.

- **Transparencia y verificabilidad.** Toda operación crítica —pagos, swaps, intents, gobernanza— es verificable on-chain.

- **Independencia del fiat y de los intermediarios.** El objetivo de largo plazo es que las personas puedan operar su vida financiera sin depender obligatoriamente del dinero fiduciario ni de las redes de tarjetas.

- **Inclusión financiera global.** Pagos y micropagos accesibles desde cualquier país, con foco inicial en los mercados de mayor necesidad y adopción.

Binno — Whitepaper

La capa universal de identidad y pagos para todas las blockchains

Versión 2.0 · 2026

Paga, envía valor y opera en cualquier cadena escribiendo solo un @username.

Capítulo 1: BinnoChain — Arquitectura de Alto Rendimiento para Pagos a Escala Global

BinnoChain no fue diseñada para competir como una blockchain generalista. Es una **infraestructura financiera de propósito específico**, optimizada para una única misión: hacer posible el sistema global de identidad @username, los micropagos instantáneos y la ejecución omnichain sin fricción.

Cada decisión de su arquitectura —consenso, máquina virtual, modelo de gas y diseño de validadores— está subordinada a un solo objetivo medible: que pagar y enviar valor sea más rápido, más barato y simple que en cualquier sistema financiero tradicional, sin renunciar a la verificabilidad on-chain.

Técnicamente, BinnoChain es una **Avalanche L1 soberana** construida sobre la infraestructura de Avalanche, que utiliza el consenso **Snowman++** y una máquina virtual propia, **BinnoVM**, construida sobre **HyperSDK**. Este diseño le permite operar como la capa base del ecosistema Binno: una cadena altamente escalable, segura, interoperable y orientada por completo a la experiencia del usuario final y del comercio.

1. Arquitectura base de BinnoChain

1.1. BinnoChain como Avalanche L1 soberana

Tras la actualización Etna / Avalanche9000 (ACP-77), Avalanche reemplazó el modelo de *Subnets* por el de **Avalanche L1 soberanas**: redes independientes con su propio conjunto de validadores, sus propias reglas de participación y su propio modelo de incentivos. BinnoChain se despliega bajo este modelo, lo que le otorga:

- **Soberanía total** sobre su lógica económica, su entorno de ejecución, su modelo de gas y sus reglas de validación.

- **Costo de operación bajo y predecible.** Bajo ACP-77, los validadores de una L1 ya no necesitan inmovilizar 2.000 AVAX ni validar la Primary Network de Avalanche. En su lugar, pagan una tarifa continua de validación (inicialmente del orden de ~1,33 AVAX por validador al mes), lo que reduce drásticamente la barrera económica de arranque de la red.

- **Gestión de validadores programable.** ACP-77 permite a cada L1 definir su propia lógica de administración del conjunto de validadores mediante un contrato de gestión de validadores (ValidatorManager). BinnoChain

aprovecha esta capacidad para implementar un modelo de validación igualitario y por calificación (Sección 5), en lugar de un esquema convencional de proof-of-stake competitivo.

- **Interoperabilidad nativa.** BinnoChain mantiene interoperabilidad con el ecosistema Avalanche vía Interchain Messaging (ICM/Warp). La interoperabilidad omnichain con redes externas (Ethereum, BSC, Solana y otras) se resuelve en la capa BinnoHub mediante LayerZero V2, descrita en el Capítulo 3.

Esta elección es deliberada: permite a Binno lanzar una red de alto rendimiento, soberana e interoperable, sin el costo de capital de un génesis independiente y sin sacrificar la seguridad heredada del marco de Avalanche.

1.2. Consenso Snowman++

Snowman++ es el mecanismo de consenso de cadenas lineales totalmente ordenadas del ecosistema Avalanche, optimizado para alto throughput mediante un esquema de proponentes que reduce la contención en la producción de bloques. Sus propiedades relevantes para BinnoChain son:

- **Finalidad determinística sub-segundo.** El consenso está diseñado para finalidad rápida y configurable; el objetivo de diseño de BinnoChain es una finalidad inferior a 600 ms bajo condiciones de red de referencia. Los valores definitivos se confirmarán mediante benchmarks públicos sobre el hardware de validador especificado (Sección 5.3).

- **Escalabilidad independiente del número de validadores.** A diferencia del BFT clásico (donde la comunicación crece de forma cuadrática con el número de validadores), Snowman++ opera por muestreo aleatorio sub-seleccionado de tamaño constante: cada nodo consulta a un subconjunto fijo de validadores, sin importar si la red tiene veinte o varios miles. El overhead de comunicación por nodo es, por tanto, independiente del tamaño total del conjunto durante la operación normal. Esta es la propiedad que permite a BinnoChain descentralizar su conjunto de validadores **sin degradar el rendimiento**.

- **Seguridad probabilística robusta**, basada en múltiples rondas de muestreo aleatorio repetido, que hace exponencialmente improbable revertir una decisión ya alcanzada.

- **Tolerancia bizantina configurable.** La seguridad y la vivacidad dependen de umbrales parametrizables del consenso. La verificación de mensajes inter-cadena en la P-Chain de Avalanche, por ejemplo, exige la firma agregada de al menos el 67 % del peso del conjunto de validadores de origen.

- **Bajo overhead de comunicación y alta eficiencia energética**, sin el costo computacional del trabajo de prueba.

La elección de Snowman++ prioriza **latencia ultra baja y finalidad temprana**, condición indispensable para pagos en punto de venta y para el procesamiento masivo de micropagos en tiempo real.

Nota sobre el origen del rendimiento. El throughput de BinnoChain proviene principalmente de la capa de ejecución (BinnoVM sobre HyperSDK) y de su modelo de procesamiento paralelo, no del consenso en sí. Snowman++ aporta finalidad rápida, ordenamiento total y escalabilidad del conjunto de validadores; la capacidad transaccional la determina la VM y el hardware.

2. Motor de ejecución: HyperSDK + BinnoVM

2.1. Por qué HyperSDK

HyperSDK es un framework de alto rendimiento creado por Ava Labs para construir máquinas virtuales personalizadas, diseñado para maximizar el throughput y minimizar la latencia por transacción. A diferencia de un entorno EVM generalista, HyperSDK permite definir desde cero el modelo de cuentas, la lógica de acciones, la estructura de tarifas y las reglas de ejecución. Sus ventajas en el contexto de BinnoChain son:

- **Ejecución de bajísima latencia por transacción**, optimizada para cargas paralelas intensivas.

- **Modelo de tarifas totalmente personalizable**, que habilita el gas denominado en USD descrito en la Sección 4.

- **Eficiencia de CPU, memoria y estado** que permite sostener throughput muy elevado en hardware de servidor de alto rendimiento.

Es importante precisar el alcance de esta elección: **BinnoChain no es una cadena compatible con EVM y no ejecuta contratos en Solidity**. El camino EVM en Avalanche (C-Chain o Subnet-EVM) ofrece compatibilidad con Solidity a costa de

un throughput sustancialmente menor, incompatible con la tesis de micropagos masivos de Binno. BinnoChain elige deliberadamente el camino opuesto: una VM especializada y de alto rendimiento.

2.2. BinnoVM: máquina virtual especializada en pagos

BinnoVM es la máquina virtual propia de BinnoChain, construida sobre HyperSDK. No es una plataforma de contratos inteligentes de propósito general para terceros, sino un **motor de ejecución especializado** cuya lógica está implementada como **módulos nativos de la VM**, auditables y optimizados para el caso de uso de pagos e identidad. Estos módulos incluyen:

- **Módulo de identidad** — registro, unicidad y resolución del @username (capa BinnoHub).
- **Módulo de pagos** — liquidación atómica de pagos y comisiones (capa BinnoPay).
- **Módulo de liquidez** — conversión y enrutamiento determinístico (capa BinnoDEX).
- **Módulo de cuentas y firmas** — soporte para custodia MPC, autorizaciones y operaciones NFC (capa BinnoWallet).

Toda especificación de interfaz incluida en este whitepaper se presenta como **pseudocódigo ilustrativo** con el único fin de describir el comportamiento esperado de estos módulos; no representa contratos desplegables en una EVM. La lógica real se implementa como acciones y transiciones de estado nativas dentro de BinnoVM.

Este enfoque —una VM cerrada, especializada y de alto rendimiento, en lugar de una plataforma de contratos abierta— **es una ventaja deliberada para una red de pagos**: reduce la superficie de ataque, elimina la imprevisibilidad de cómputo de contratos arbitrarios y permite garantizar latencia y costo estables, exactamente lo que un sistema de pagos a escala global requiere.

3. Rendimiento y capacidad

BinnoChain está diseñada para sostener un throughput muy superior al de las redes generalistas actuales. Su **capacidad objetivo de diseño es de más de 50.000**

transacciones por segundo, habilitada por el modelo de ejecución paralela de HyperSDK y por la especialización de BinnoVM.

Es importante interpretar esta cifra correctamente. Se trata de un **objetivo teórico de diseño**, no de un valor sostenido medido y publicado. El rendimiento efectivo de una red depende del tipo de transacción, del hardware de los validadores, de la distribución geográfica del conjunto y de la latencia de red: la capacidad de ejecución escala con el hardware, mientras que el consenso está acotado por la latencia de las rondas de comunicación. Binno publicará benchmarks reproducibles sobre el hardware de validador de referencia (Sección 5.3) a medida que la red avance hacia mainnet, especificando metodología, tipo de transacción, número de nodos y condiciones de medición.

Característica	**BinnoChain**	**Solana**	**zkSync Era**	**Base**	**Avalanche C-Chain**
TPS	>50.000 *(objetivo de diseño)*	~2.500–3.500	~2.000–3.000	~1.500–2.500	~100–200
Finalidad	sub-segundo *(objetivo <600 ms)*	~400–800 ms	~2–5 s	~1–2 s	~1–2 s
Costo para el usuario final	0 (tx internas gratuitas)	$0,0002–0,01	$0,03–0,10	$0,01–0,05	$0,01–0,10
Tarifa estable en USD	Si	No	No	No	No
VM especializada en pagos	Sí	No	No	No	No

4. Modelo económico de gas

4.1. Gas denominado en USD: una unidad de medición estable y predecible

A diferencia de las cadenas tradicionales, donde el costo de transacción fluctúa con el precio de un token nativo, BinnoChain contabiliza el consumo de recursos (gas) en una **unidad anclada al dólar** (USDC/USDT). El modelo de tarifas personalizable de HyperSDK permite medir de forma determinística el peso de cada transacción —del orden de 0,001 USD para una transacción simple y 0,002 USD para una de lógica extendida—.

Es fundamental entender el propósito de esta unidad: **no es una tarifa que se cobre al usuario ni un reembolso que se pague por transacción.** Es una unidad interna de medición de recursos que cumple dos funciones: (1) hacer predecible y estable el costo estructural de la red, y (2) servir de base para el control de recursos y la protección anti-spam. Dentro de BinnoChain, el usuario no paga gas y no existe un reembolso por transacción a los validadores.

4.2. Transacciones internas gratuitas y costo estructural agregado

Todas las transacciones de los usuarios dentro de BinnoChain son **gratuitas para el usuario final**. El usuario interactúa libremente, sin necesidad de gestionar tokens nativos ni stablecoins para comisiones, lo que constituye el habilitador central de una experiencia de usuario equivalente a Web2.

El costo real de operar la red —cómputo, almacenamiento de estado y ancho de banda de los validadores— es un costo físico que existe, pero **no se cobra ni se reembolsa transacción por transacción**. En su lugar, está cubierto de forma **agregada** por el modelo de recompensa de validadores descrito en la Sección 5.4: los validadores son compensados mediante su participación en el pool del 15 % del revenue neto del protocolo (más el retainer mínimo en fase temprana), no mediante micro reembolsos por cada operación. De este modo, el subsidio de gas interno no es un pasivo lineal de la tesorería, sino una propiedad estructural del modelo económico de la red.

La sostenibilidad de las transacciones gratuitas descansa sobre dos pilares explícitos:

1. **El revenue del protocolo financia el costo estructural de la red.** El conjunto de actividades de pago (BinnoPay), liquidez (BinnoDEX) y crédito

(BinnoCredit) genera el revenue del que se nutre el pool de validadores. A mayor uso, mayor revenue, lo que cubre con holgura el costo de procesar las transacciones gratuitas asociadas.

2. **Las transacciones sin comisión están acotadas y protegidas contra abuso.** Operaciones que no generan revenue (registro de @username desde BinnoWallet, operaciones internas de cartera) están sujetas a límites anti-spam y resistencia sybil: el acceso a transacciones gratuitas está vinculado a **cuentas @username verificadas**, con cuotas por cuenta y mecanismos anti-sybil anclados en la capa de identidad. De este modo, el costo de un ataque de saturación se vincula a la fricción de registro de identidad, y el consumo de recursos de la red permanece predecible y gobernable.

Nota sobre operaciones cross-chain. La gratuidad aplica a las transacciones *dentro* de BinnoChain. Las operaciones que salen hacia otra red (cross-chain) conllevan el gas de la red externa y el transporte LayerZero (Capítulo 3), costos que la red no puede subsidiar de forma sostenible a escala masiva y que asume quien inicia la operación.

4.3. Fuentes de financiación de la tesorería

La tesorería se financia exclusivamente con ingresos reales del ecosistema:

- **Comisiones de BinnoPay** (porción de la comisión por pago destinada a tesorería).
- **Comisiones de BinnoDEX** (Capítulo 5).
- **Spread de BinnoCredit** (Capítulo 6).

El modelo es estructuralmente sostenible: el costo de operación escala con el uso, pero los ingresos por comisiones escalan con el mismo uso y a un múltiplo superior.

5. Validadores: modelo igualitario por calificación

El diseño de validadores de BinnoChain rompe deliberadamente con el modelo convencional de proof-of-stake competitivo. La razón es técnica y económica a la vez, y separa con claridad tres conceptos que la mayoría de las redes confunde:

1. **Membresía del conjunto** — quién opera un nodo validador.

2. **Peso de consenso** — cuánto pesa el voto de cada validador en el muestreo de Snowman++.

3. **Staking de usuarios** — el producto económico de rendimiento para los holders de BNN.

5.1. Membresía por calificación, no por subasta de stake

En una red que apunta a más de 50.000 TPS con finalidad sub-segundo, **el validador más lento condiciona el rendimiento de toda la red**. Permitir que la cantidad de stake determine la membresía introduciría el riesgo de validadores con hardware insuficiente degradando la finalidad para todos los usuarios.

Por ello, la membresía del conjunto de validadores de BinnoChain se determina por **calificación técnica**, no por subasta de capital:

- Hardware verificado conforme al estándar de referencia (Sección 5.3).

- Depósito de un **bond** económico sujeto a slashing (Sección 5.2).

- Aprobación inicial gestionada por la Fundación Binno, evolucionando hacia un proceso permissionless y gobernado por la DAO conforme madura la red.

5.2. Peso de consenso igualitario y seguridad económica

El peso de consenso de cada validador es **igual** (o sujeto a un tope uniforme), independientemente del stake que administre. Esto se implementa de forma nativa mediante el ValidatorManager habilitado por ACP-77, y produce dos efectos deseados: ningún actor con gran capital puede dominar el consenso, y el conjunto se mantiene equitativo por diseño, en línea con la filosofía de descentralización del proyecto.

La **seguridad económica del consenso no proviene de stake delegado por terceros, sino de bonds y slashing**. Cada validador deposita un bond compuesto por dos partes:

- **Piso en stablecoin: 50.000 USDC/USDT.** Valor slasheable duro, inmune a la volatilidad del precio de BNN. Garantiza que la seguridad económica de la red se mantenga incluso bajo estrés de mercado.

- **Componente en BNN: equivalente a 50.000–100.000 USD**, bloqueado. Alinea al validador con el ecosistema y le otorga exposición al upside del token.

Este diseño es deliberado: un bond compuesto exclusivamente por el token nativo colapsaría su valor de seguridad justo en los momentos de mayor estrés de mercado. El piso en stablecoin elimina ese riesgo. El bond es un parámetro de gobernanza, escalable conforme crece el valor asegurado por la red.

El bond puede ser parcial o totalmente confiscado (slashing) según un esquema graduado:

Falta	**Penalización**
Equivocación aislada (probable fallo técnico)	Slash 30 % del bond + jail + revisión
Equivocación correlacionada (≥ f+1 validadores en la misma ventana)	Slash hasta 100 % + expulsión permanente
Downtime < 99 % uptime/época	Pérdida de recompensas de la época (sin slash)
Downtime < 95 % uptime/época	Slash 0,1 % + jail temporal
Downtime severo (> 24 h offline o 3 jails/trimestre)	Slash 5 % + expulsión
Censura demostrable de transacciones válidas	Slash 10–30 % + expulsión (vía gobernanza)

El esquema es **graduado y proporcional**: tolera el error técnico honesto con penalizaciones moderadas, pero aniquila económicamente el ataque coordinado. La censura se trata como una escalada mediada por gobernanza, dado que su

detección automática produciría falsos positivos. Tras la salida voluntaria de un validador, su bond permanece bloqueado y slasheable durante un período de **unbonding de 21 días**, que cubre faltas descubiertas con posterioridad.

5.3. Hardware de referencia para validadores

BinnoChain exige hardware de servidor de alto rendimiento para sostener su throughput objetivo. El estándar de referencia es:

- **CPU:** servidor de última generación (AMD EPYC / Intel Xeon), ≥ 32 núcleos de alto rendimiento.
- **Memoria:** 256 GB RAM ECC DDR5.
- **Almacenamiento:** NVMe Gen5, ≥ 4 TB, de alto IOPS y baja latencia.
- **Red:** conectividad simétrica de 10 Gbps, de baja latencia y alta disponibilidad (≥ 99,9 %), con redundancia.

Cada componente contribuye directamente al rendimiento de la red: el alto número de núcleos habilita la ejecución paralela de HyperSDK, el NVMe Gen5 y la memoria abundante minimizan la latencia de acceso al estado, y la conectividad de 10 Gbps garantiza la propagación de bloques sin cuellos de botella a alto volumen.

5.4. Economía del validador: ingreso por uso real, no por staking de terceros

El modelo de remuneración de validadores de BinnoChain es **distintivo y se sostiene en el uso real de la red, no en la inflación ni en el rendimiento del staking de terceros**:

- **Los validadores no obtienen rendimiento del staking de otros usuarios.** Su ingreso proviene de su participación en los ingresos reales del protocolo, ponderada por uptime y desempeño operativo, más el rendimiento de su propio bond en igualdad de condiciones que cualquier holder.
- **Garantía mínima en fase temprana (retainer).** Durante los primeros meses de bajo volumen, la tesorería garantiza un retainer mínimo mensual de **2.250 USD por validador**, calibrado para cubrir con margen el costo operativo de la infraestructura de referencia adquirida (amortización, electricidad,

conectividad de 10 Gbps y la tarifa continua de validación L1). Este retainer decrece progresivamente a medida que el ingreso orgánico por comisiones lo sustituye.

La fórmula de reparto del pool de recompensas de validadores es:

recompensa_i = pool_época × (score_i / Σ score_j)

score_i = uptime_i × responsiveness_i (uptime exigido ≥ 99 %)

pago_i = max(retainer_mínimo, recompensa_i)

La base es **igual para todos** los validadores, modulada por el uptime y por un factor secundario y acotado de capacidad de respuesta —que premia el buen hardware y red sin inducir centralización geográfica. El pool de recompensas de validadores se fija en el **15 % del revenue neto del protocolo**, un parámetro ajustable por votación de gobernanza. El mecanismo max(retainer, recompensa) garantiza que en fase temprana el validador cobre el piso, y que cuando el revenue crece, el ingreso real lo supere y el subsidio se extinga de forma natural.

Ejercicio ilustrativo de rentabilidad (supuestos explícitos). Con un costo operativo de hardware propio del orden de ~1.000 USD/mes, un retainer de 2.250 USD garantiza rentabilidad desde el primer día, aún a volumen cero. Asumiendo un ingreso neto de tesorería de ~$0,0115 por pago y un pool de validadores del 15 % del revenue neto, la rentabilidad evoluciona así:

Volumen diario	**Pool validadores/mes**	**Ingreso por validador (21)**	**Ingreso por validador (100)**
Bootstrap (~0)	—	2.250 (retainer)	2.250 (retainer)
1 M pagos/día	~52 k	2.250 (retainer)	2.250 (retainer)
10 M pagos/día	~517 k	~24.600	~5.175

Volumen diario	Pool validadores/mes	Ingreso por validador (21)	Ingreso por validador (100)
100 M pagos/día	~5,18 M	~246.400	~51.750

El retainer deja de ser determinante alrededor de ~900.000 pagos diarios, punto en que el ingreso real por comisiones lo supera. La carga máxima de tesorería en fase bootstrap es (21 × 2.250 USD ≈ 567.000 USD/año, decreciente).

Este diseño demuestra un punto clave: el porcentaje que un validador obtendría del rendimiento del staking de terceros en un modelo PoS convencional es **económicamente trivial** comparado con su participación en el ingreso transaccional real a escala. Renunciar a ese corte no compromete la rentabilidad del validador y, a cambio, permite que el usuario reciba el 100 % de su rendimiento de staking, simplifica la experiencia (el usuario no elige validador) y refuerza la filosofía igualitaria de la red.

5.5. Descentralización progresiva y honestidad del modelo de confianza

Binno prioriza **descentralización progresiva sobre descentralización prematura**. Es importante ser preciso sobre el modelo de confianza en cada fase:

- **Fase inicial (mainnet temprano).** Con un conjunto génesis de **21 validadores** de peso igual, calificados y respaldados por bonds, el modelo de confianza de BinnoChain se asemeja a un **BFT con bonds y membresía gestionada**, más que a un proof-of-stake permissionless pleno. Esta es una decisión consciente que garantiza latencia sub-segundo y estabilidad comercial desde el día uno.

- **Trayectoria de descentralización.** El conjunto se expande de forma gobernada por la DAO siguiendo una ruta de **21 → ~50 → 100+ validadores**, y el proceso de admisión evoluciona hacia un modelo permissionless. Gracias a la propiedad de muestreo de tamaño constante de Snowman++, esta expansión **no degrada el rendimiento de la red**: el overhead de comunicación por nodo permanece independiente del tamaño del conjunto. No existe, por tanto, un tope ideológico permanente; el crecimiento del conjunto es competencia de la gobernanza.

Esta transparencia sobre las garantías de seguridad en cada etapa es deliberada: el valor de la red se construye sobre afirmaciones verificables, no sobre sobrepromesas.

6. Rol del token BNN

El token nativo **BNN cumple tres funciones económicas claramente delimitadas**:

- **Gobernanza** — votación sobre parámetros de la VM, parámetros económicos, conjunto de validadores y expansiones de la red.

- **Staking con rendimiento real** — participación en los ingresos del protocolo mediante un producto de staking *desacoplado del consenso* (los usuarios obtienen rendimiento sin necesidad de elegir ni asignar validadores).

- **Bond de validador** — garantía económica sujeta a slashing que respalda la seguridad del consenso.

La característica distintiva y deliberada del diseño es que **BNN no se utiliza para pagar gas**. El consumo de recursos se contabiliza en una unidad anclada al dólar como medida interna, y las transacciones internas son gratuitas para el usuario final. Esto desacopla el medio de pago de la especulación sobre el token y garantiza un costo operativo estable para comercios y usuarios.

7. Seguridad de BinnoChain

La seguridad de BinnoChain no está orientada a proteger balances especulativos, sino **flujos de pago reales, comercios físicos y millones de transacciones diarias**. Sus pilares son:

- **Seguridad de consenso.** Finalidad rápida que mitiga el riesgo de reorganizaciones profundas; muestreo probabilístico resistente a colusión; conjunto de validadores calificados y respaldados por bonds slasheables.

- **Seguridad de red.** Atestación criptográfica por bloque, canales P2P con rate-limiting contra ataques de saturación y verificación determinística del estado.

- **Seguridad de ejecución (BinnoVM).** Al ser una VM especializada con módulos nativos auditados —y no una plataforma de contratos arbitrarios— BinnoChain elimina clases enteras de vulnerabilidad propias de entornos de contratos abiertos. Los módulos se someten a auditoría externa y a límites estrictos de consumo de recursos.

- **Seguridad de interoperabilidad.** La interoperabilidad omnichain se canaliza por la capa BinnoHub (Capítulo 3), que emplea mensajería verificada y prevención de replay; los detalles de su modelo de seguridad cross-chain se desarrollan en ese capítulo.

8. Caso de uso principal: omnichain y micropagos on-chain reales

Toda la arquitectura converge en un caso de uso central: **micropagos on-chain a escala global**. BinnoChain está diseñada para habilitar:

- Identidad y pagos omnichain automáticos.

- Pagos on-chain NFC/QR instantáneos en tiendas físicas.

- Integraciones invisibles para el usuario final.

- Eliminación de las barreras históricas de la blockchain: gestión de tokens para gas, puentes y comprensión técnica.

9. Conclusión del capítulo

BinnoChain es la base tecnológica sobre la que se construye todo el ecosistema Binno. Su arquitectura —Avalanche L1 soberana, consenso Snowman++, BinnoVM sobre HyperSDK, transacciones internas gratuitas con costo estructural agregado, validadores igualitarios por calificación respaldados por bonds, e interoperabilidad canalizada por BinnoHub— resuelve uno de los mayores desafíos de la industria: ofrecer una blockchain **usable a escala masiva**, con la simplicidad y la velocidad de las soluciones financieras tradicionales, pero conservando la verificabilidad y la seguridad propias de Web3.

No es una L1 más. Es una infraestructura de pagos e identidad diseñada, desde el consenso hasta la experiencia de usuario, para desaparecer ante los ojos de quien la usa.

Capítulo 2: BinnoWallet — Custodia MPC Flexible y Experiencia de Usuario sin Fricción

BinnoWallet no es un producto independiente: es la **interfaz humana** del sistema @username y de BinnoPay. Su función no es almacenar claves, sino permitir que millones de personas paguen, envíen valor y operen en Web3 **sin comprender cómo funciona Web3**.

Es la cartera nativa del ecosistema Binno, diseñada para eliminar la complejidad de la tecnología blockchain y permitir que cualquier usuario —independientemente de su nivel técnico— interactúe con BinnoChain y sus aplicaciones de forma segura, rápida y transparente. Proporciona una interfaz sencilla sobre un sistema criptográfico robusto, ofreciendo una experiencia equivalente a Web2 sin sacrificar las garantías criptográficas de Web3.

Su diseño se apoya en tres pilares:

- **Custodia descentralizada mediante MPC** (Multi-Party Computation).
- **Flujos simplificados** para pagos diarios y experiencias Web3.
- **Recuperación avanzada, modular y a elección del usuario.**

BinnoWallet es 100 % compatible con el ecosistema Web3: integra **WalletConnect v2** completo para conexión instantánea con cualquier dApp, y un *deep link* prioritario para pagos BinnoPay.

1. Arquitectura criptográfica de BinnoWallet

1.1. Custodia MPC como modelo base

BinnoWallet emplea Multi-Party Computation como mecanismo principal de generación, firma y recuperación de llaves. Esto significa que:

- La clave privada **nunca existe como un valor completo** en ningún dispositivo, en ningún momento.
- Se genera de forma distribuida y se divide en **fragmentos criptográficos independientes** (key shares).

- Las firmas se realizan mediante protocolos MPC, **sin recomponer la llave** en ninguna etapa.

BinnoWallet implementa el protocolo **Threshold ECDSA sobre secp256k1, basado en la especificación GG20** (Canetti et al., 2020), incorporando las mejoras de rendimiento y seguridad introducidas por la investigación del sector en 2023–2024. GG20 es un protocolo ampliamente analizado y auditado por firmas como Trail of Bits, Kudelski Security y NCC Group en implementaciones de referencia de la industria (Zengo, Fireblocks) que operan a escala de más de 10 millones de wallets activas. La **implementación específica de BinnoWallet será sometida a auditoría externa independiente antes de mainnet.**

Este modelo proporciona protección contra la extracción física de claves, resistencia ante compromisos parciales de infraestructura, y una seguridad estructuralmente superior al modelo tradicional basado en una única frase semilla.

1.2. Configuraciones MPC elegidas por el usuario

BinnoWallet elimina la seed phrase única tradicional y la sustituye por un esquema flexible **m-de-n elegido por el usuario**, que separa de forma explícita dos umbrales independientes:

- **Umbral de firma** — cuántos fragmentos se requieren para autorizar transacciones.

- **Umbral de recuperación** — cuántos fragmentos se requieren para restaurar la wallet completa.

Esta separación —poco común en el mercado— permite que la operación diaria sea ágil mientras la recuperación permanece altamente protegida. Los esquemas disponibles son:

Umbral	Esquemas estándar	Esquemas avanzados (alta exigencia)
Firma	2-de-2, 2-de-3, 3-de-5	4-de-5, 5-de-5
Recuperación	2-de-3, 3-de-5	4-de-5, 5-de-5

El umbral de firma es **siempre de al menos dos fragmentos**: nunca existe un único fragmento capaz de controlar la wallet por sí solo. Un ejemplo típico de operación diaria es *enclave del teléfono + 2FA (2-de-2)*.

Invariante de no custodia. El usuario puede alcanzar tanto el umbral de firma como el de recuperación **sin depender de ningún fragmento custodiado por Binno**. De hecho, el usuario puede optar por **no almacenar ningún fragmento en la infraestructura de Binno**. En consecuencia, Binno nunca puede firmar de forma unilateral, ni censurar, ni bloquear el acceso del usuario a sus fondos. El fragmento opcional alojado en servidores de Binno actúa exclusivamente como un factor de conveniencia y 2FA —nunca como una dependencia custodial—. BinnoWallet es, por diseño, genuinamente no custodial.

2. Métodos de distribución y almacenamiento de fragmentos

Una de las innovaciones de BinnoWallet es que **el usuario elige dónde se almacenan sus key shares**, adaptando la cartera a su nivel deseado de seguridad y conveniencia. Los métodos disponibles son:

- **Secure Enclave del dispositivo** — fragmento protegido por FaceID, huella o contraseña, que asiste en la firma de transacciones diarias y nunca permite su extracción.

- **Frase de 24 palabras** — que representa **un fragmento**, no la llave completa.

- **Dispositivo USB offline** — fragmento en almacenamiento físico desconectado.

- **Nube personal** — fragmento cifrado en Drive, iCloud, Samsung Pass u otros.

- **Fragmento 2FA en servidores de Binno** *(opcional)* — cifrado y protegido por doble factor; sujeto al invariante de no custodia descrito en la Sección 1.2.

- **Guardianes humanos** — recuperación social, descrita a continuación.

Recuperación social mediante guardianes. Los guardianes representan, en su conjunto, **un único fragmento** dentro del esquema m-de-n del usuario. Para reconstituir ese fragmento se aplica un quórum pequeño y elegido por el usuario (por ejemplo, 2-de-3 guardianes, o 2-de-2 para quien disponga de solo dos personas de confianza). Este diseño aporta dos garantías simultáneas:

- Ningún guardián individual posee el fragmento por sí solo, y la pérdida de un guardián no implica la pérdida del fragmento.

- Dado que los guardianes representan **como máximo un fragmento del total**, incluso una colusión completa entre todos los guardianes les otorgaría un solo share —nunca la wallet—, pues el umbral del usuario seguiría exigiendo otros fragmentos.

Compatibilidad con hardware wallets. BinnoWallet es compatible con carteras de hardware externas (Ledger Nano X/S Plus, Trezor Safe 3/5, Keystone 3 Pro) como **lugar de custodia y firma externa** —por ejemplo, alojando un fragmento de forma offline o actuando como firmante externo en el flujo de alto valor—. El dispositivo de hardware funciona como uno de los métodos de custodia del usuario, no como participante de la ceremonia MPC.

3. Modelo de firma y operación diaria

3.1. Transacciones normales y pago NFC instantáneo

Para las operaciones cotidianas —pagos físicos, interacciones con dApps, transferencias regulares— solo se requieren los fragmentos definidos en el umbral de firma del usuario. El objetivo es que el usuario pague sin procesos complejos y sin perder seguridad.

El **pago NFC instantáneo** se logra mediante pre-cómputo de la firma: cuando el usuario abre la pantalla de pago NFC, BinnoWallet solicita de inmediato los factores de seguridad elegidos (biometría del Secure Enclave y/o 2FA) e **inicia en segundo plano las rondas de cómputo del protocolo MPC**. De este modo, mientras el usuario confirma el monto y acerca el teléfono al terminal, el trabajo criptográfico pesado ya se ha realizado, y la confirmación final del pago se reduce a un paso casi instantáneo. La latencia definitiva del flujo de firma se confirmará mediante mediciones sobre dispositivos de referencia.

3.2. Operaciones de alto valor (opción avanzada)

Los usuarios avanzados o institucionales pueden activar la función **"Protección de Alto Valor"**. Una vez activada, el usuario define un umbral personalizado (por ejemplo, transacciones superiores a 5.000 USDT) que exige fragmentos de firma adicionales. Esta capa es completamente opcional y está **desactivada por defecto**.

3.3. Recuperación completa de la wallet

Para restaurar la cartera en un nuevo dispositivo o ante la pérdida del teléfono, se requieren los fragmentos definidos en el **umbral de recuperación** del usuario —independiente del umbral de firma—. Esto permite mantener una firma diaria ágil sin comprometer la robustez de la recuperación.

4. Experiencia de usuario y flujo de interacción

4.1. Eliminación de la complejidad

BinnoWallet abstrae por completo los procesos criptográficos. El usuario **nunca ve** claves privadas, frases semilla completas, procesos de firma ni operaciones de gas o tarifas. Sus acciones se reducen a aceptar un pago, confirmar una transacción y elegir dónde conservar sus fragmentos.

4.2. Integración nativa con BinnoChain

BinnoWallet está diseñada específicamente para BinnoChain: no requiere que el usuario posea USDT/USDC para gas ni tokens nativos, todas las transacciones dentro de BinnoChain son gratuitas para el usuario, y la experiencia transcurre sin esperas, sin puentes y sin fricción.

5. Seguridad operativa

5.1. Protección contra extracción y malware

Gracias al modelo MPC, ningún fragmento reconstruye la clave completa y la clave íntegra jamás se expone en el dispositivo. Un atacante necesitaría comprometer **múltiples fragmentos almacenados en ubicaciones físicas y lógicas distintas** —y alcanzar el umbral de firma del usuario— para operar la cartera.

5.2. Tolerancia a pérdida parcial

La wallet continúa operativa aunque el usuario pierda uno de sus elementos —el smartphone, un USB, un servicio en la nube o un guardián— siempre que conserve fragmentos suficientes para alcanzar su umbral. Esta resiliencia es una consecuencia directa del esquema m-de-n.

5.3. Protección ante ataques coordinados

Dado que ningún guardián posee un fragmento completo, que los guardianes representan como máximo un share del total, que la nube y los servidores almacenan únicamente fragmentos cifrados, y que el Secure Enclave no permite extracción, el sistema es resistente a ataques físicos, phishing avanzado, compromisos parciales de infraestructura y fallos de proveedores externos (Google, Apple, etc.).

6. Conclusión del capítulo

BinnoWallet redefine la experiencia de usuario en Web3 al combinar custodia descentralizada MPC de nivel institucional, separación de umbrales de firma y recuperación, recuperación social robusta basada en quórum, transacciones sin gas y una interfaz intuitiva orientada a micropagos reales. Su arquitectura elimina las barreras históricas que frenan la adopción masiva —sin sacrificar los fundamentos técnicos de seguridad y descentralización— y materializa el principio rector del ecosistema: que la tecnología desaparezca ante los ojos de quien la usa.

Capítulo 3: BinnoHub — Usuario Universal (@username), Interoperabilidad Automática y Web3 Omnichain

BinnoHub es la primera insignia del ecosistema Binno y su núcleo operativo. Persigue un objetivo único y radical: **la simplificación absoluta de la blockchain**. Que enviar valor o ejecutar una acción en cualquier cadena se reduzca a escribir un @username y una red destino —sin direcciones, sin puentes, sin gestión de gas, sin fragmentación—.

Así como el DNS convirtió las direcciones IP en nombres legibles por humanos, BinnoHub convierte el conjunto de todas las blockchains en un único espacio continuo donde la complejidad técnica desaparece ante los ojos del usuario.

BinnoHub combina tres componentes en un único protocolo verificable:

- **Usuario universal** basado en @username.
- **Receiving addresses determinísticas**, el mecanismo de transición que convive con el modo @username.
- **Ejecución Web3 Omnichain** de transferencias, swaps e interacción con dApps externas mediante intents seguros.

1. Visión del usuario — evolución realista hacia el usuario universal

BinnoHub está diseñado para convivir con dos mundos: el de las wallets que ya integran @username y el de las que aún no lo hacen. Durante la transición, el sistema elige automáticamente el camino más eficiente sin que el usuario note diferencia.

Acción	Fase inicial	Fase de madurez
Recibir desde otra cadena	El remitente envía a tu receiving address	El remitente escribe @username + tu red y pulsa "enviar"

Acción	Fase inicial	Fase de madurez
Enviar a otra cadena	Pegas la wallet destino y seleccionas la red	El remitente escribe @username + red, ahora universal
Intents con dApps externas	1 clic desde BinnoWallet	1 clic desde cualquier wallet compatible con @username

2. Arquitectura global — tres capas acopladas

Capa 1 — BinnoHub (sobre BinnoChain): la fuente única de verdad. Reside en BinnoChain y concentra: el registro, unicidad global y control del @username; la generación determinística de receiving addresses; la resolución omnichain de usuarios; la construcción y autorización del payload cross-chain; el enrutamiento vía LayerZero V2 (OFT/OApp); la gestión de intents; la sincronización del estado de identidad con todos los SatelliteHubs; y la asignación de nonces globales con prevención de replay.

BinnoChain posee dos identificadores que no deben confundirse: su **blockchainID de Avalanche** (formato base58, que la identifica como L1) y su **Endpoint ID de LayerZero** (entero, que la identifica como endpoint en la red de mensajería).

*El código de BinnoHub que se presenta en este capítulo es **pseudocódigo ilustrativo** que describe el comportamiento de las acciones nativas de BinnoVM. No representa contratos Solidity desplegables sobre BinnoChain. Los SatelliteHubs (Capa 2), en cambio, sí son contratos reales en las cadenas externas: en cadenas EVM (Ethereum, BSC, Base) son contratos Solidity reales; en Solana, programas nativos.*

Capa 2 — SatelliteHubs (contratos ultraligeros en cada cadena externa). Traductores de menos de 300 líneas, sin estado soberano, que exponen un conjunto mínimo de funciones (resolveUsername, executeIntent, notifyDeposit). Cada SatelliteHub **solo acepta mensajes que (a) provienen del peer BinnoHub autorizado y (b) han sido verificados por la Security Stack de DVNs**.

Capa 3 — Mensajería Omnichain (LayerZero V2: Security Stack de DVNs + Executors). Es el sistema nervioso que garantiza que todas las cadenas converjan

al mismo estado final. En LayerZero V2, la verificación de mensajes la realiza una Security Stack de **DVNs (Decentralized Verifier Networks)** y la ejecución la realizan **Executors**, en fases separadas. BinnoHub configura su Security Stack para exigir la verificación de **2 de 3 DVNs independientes** por cada mensaje cross-chain: un mensaje solo es válido en destino si dos verificadores independientes confirman su integridad, eliminando cualquier punto único de fallo en el transporte.

Las garantías de esta capa son:

- **Integridad de transporte verificada por múltiples DVNs.** El payload que llega al destino es, demostrablemente, el que BinnoHub autorizó. Falsificarlo exigiría corromper simultáneamente a 2 verificadores independientes.

- **Soberanía y resiliencia.** LayerZero es permissionless a nivel de verificación: si los DVNs externos fallaran, BinnoHub conserva la capacidad de desplegar y operar su propio DVN para mantener la continuidad del protocolo (una opción de contingencia que implica operar infraestructura de verificación propia, activable según necesidad).

- **Autenticación de peer**, ordenamiento por nonces globales y prevención de replay.

- **Abstracción del gas de destino.** El Executor de LayerZero cubre el gas de ejecución en la red destino; el usuario paga una sola vez en origen y no necesita poseer el token de gas de la red destino.

3. Cómo se confirma una transacción — el modelo de dos fases

Una transacción omnichain de BinnoHub se confirma en dos fases claramente separadas, que constituyen el corazón de su seguridad:

a) **Autorización y orden (en BinnoChain).** BinnoHub es la fuente de verdad: resuelve el @username a la dirección destino, verifica la **firma del usuario**, comprueba límites y nonce, y construye el payload autoritativo (wallet destino, monto, red, emisor). Aquí se origina y autoriza el dato.

b) **Transporte, verificación y ejecución (LayerZero + red destino).** LayerZero no origina ni posee los datos: transporta el payload que BinnoHub construyó, y su Security Stack de DVNs garantiza que llegue al destino exactamente

como fue autorizado. El SatelliteHub destino ejecuta la entrega final, aceptando el mensaje solo si proviene del peer autorizado, fue verificado por los DVNs y coincide con el nonce y el hash autorizados.

Dos elementos criptográficos operan en planos distintos: la **firma MPC del usuario** autoriza la intención (se valida en BinnoChain), mientras que la **autenticación de peer y la verificación de los DVNs** garantizan la integridad del mensaje en tránsito. La autorización ocurre en BinnoChain; la ejecución final, en la red destino; LayerZero garantiza que lo ejecutado es exactamente lo autorizado.

4. Modelo de datos — usuario universal

El perfil de usuario es la estructura central *(pseudocódigo ilustrativo de una acción de BinnoVM)*:

```
struct UserProfile {
  owner          // Control MPC del usuario en BinnoChain
  username       // Inmutable y único global (@alice)
  addresses      // mapping(red → dirección nativa verificada criptográficamente)
  receivingAddrs  // mapping(red → receiving address determinística)
  lastUpdate     // Último bloque de actualización
  frozen         // Bloqueo manual o por gobernanza
}
```

El @username es la identidad y el control. En BinnoWallet no existe un "número de wallet" visible: el @username *es* la cuenta. Recuperar el control MPC del perfil (mediante el umbral de recuperación descrito en el capítulo de BinnoWallet) equivale a recuperar el @username y todo lo asociado a él. No hay forma de perder uno conservando el otro: son lo mismo. Esto unifica identidad y recuperación en un solo mecanismo.

La asociación de direcciones externas requiere firma on-chain verificable (ECDSA secp256k1 + ecrecover en EVM; Ed25519 o equivalentes en Solana/SVM/Move), lo que hace imposible la suplantación.

5. Vinculación de direcciones y onboarding

Un usuario puede tener un @username y querer asociarle wallets en distintas redes, o llegar al ecosistema por distintas puertas. BinnoHub resuelve ambos casos con un mecanismo de **doble prueba de propiedad** que hace imposible la vinculación fraudulenta:

a) **Autorización desde el @username.** El dueño del perfil, con su firma, autoriza on-chain la vinculación de una dirección nueva.

b) **Prueba de control de la dirección nueva (challenge-response).** La dirección a vincular debe firmar un nonce único emitido por BinnoHub con su propia clave, demostrando que el usuario realmente la controla.

El vínculo solo se registra cuando ambas firmas coinciden. Necesitar el control de **ambos** lados elimina el secuestro de identidad.

Caminos de onboarding y costos:

- **Crear el @username al abrir BinnoWallet:** gratuito (es una operación interna en BinnoChain y un usuario nativo del ecosistema).

- **Crear el @username desde una wallet de terceros (primera vez, en cualquier red):** 0,5 USD + gas, repartido 0,3 USD integrador / 0,2 USD tesorería. Cobrar el registro completo independientemente de dónde se cree evita el abuso de crear identidades "baratas" que nunca se usan.

- **Vincular cada red adicional** a un @username ya existente: 0,1 USD, repartido 0,05 USD integrador / 0,05 USD tesorería.

- **Traer a BinnoWallet un @username ya creado y pagado** en otra red: gratuito (ya se pagó).

En todos los casos, el gas de red y, cuando aplica, la mensajería LayerZero de sincronización cross-chain son costos adicionales y separados de la tarifa de

protocolo, asumidos por quien realiza la operación (o, desde BinnoWallet, por el ecosistema como inversión en retención).

6. Receiving addresses — el mecanismo de transición

Las receiving addresses permiten recibir valor desde wallets que **aún no integran** @username. No son el futuro del sistema, sino el puente hasta que el @username sea universal.

Creación determinística y lazy (bajo demanda): al crear un @username se despliegan 0 receiving addresses (0 gas inicial). La primera vez que el usuario pulsa "Recibir en [red]", BinnoWallet despliega la dirección vía **CREATE2 (cadenas EVM)** o **PDA (Solana)**, y queda activa de forma permanente.

La derivación es pública y verificable a partir de un salt versionado y público:

receivingAddress = derive(username, chainId, saltVersion)

Esta derivación es **pública y determinística por diseño** —cualquiera puede recalcular y verificar la dirección, lo que permite su uso sin coordinación previa—. La seguridad no depende de ocultar ningún valor, sino del control del contrato/cuenta efectivamente desplegado. El versionado del salt permite evolucionar el esquema bajo gobernanza sin romper las direcciones existentes.

Cobertura por familias de cadenas. El despliegue determinístico está soportado de forma nativa en cadenas EVM (CREATE2) y Solana (PDA). El soporte para otras familias (Move, Cosmos) se incorpora progresivamente por fases; no se asume soporte universal inmediato.

Limitación honesta de la fase de transición. Cuando un pagador usa una wallet **sin integración de Binno** y envía a una receiving address, su wallet no conoce el protocolo: muestra una transferencia común y cobra solo el gas de su red, sin desglosar las comisiones de Binno. En ese caso, las comisiones de protocolo se deducen del monto al procesarse en destino (el receptor recibe el neto, y BinnoWallet se lo muestra con transparencia). Esta es precisamente la razón por la que la integración nativa del @username es superior: una wallet integrada muestra el desglose completo antes de firmar. Funciona en ambos casos; el camino integrado ofrece mejor experiencia, lo que constituye el incentivo natural para que las wallets integren el estándar.

7. Envíos Omnichain

(Pseudocódigo ilustrativo de una acción de BinnoVM):

action sendToUsername(username, token, amount, targetChainId)

Flujo interno: conversión automática vía BinnoDEX si falta el token en destino; envío OFT al SatelliteHub destino vía LayerZero V2 (verificado por la Security Stack); entrega final en la dirección nativa o receiving address del destinatario. Las operaciones **dentro de BinnoChain** son gratuitas; las **cross-chain** conllevan el gas y el transporte LayerZero, que asume quien inicia la operación (incluidos los usuarios de BinnoWallet, ya que la red no puede subsidiar costos de redes externas a escala masiva).

8. Web3 Omnichain — ejecución de intents segura

La ejecución automática de intents permite que un usuario, desde una única wallet, interactúe con cualquier dApp de cualquier cadena. Como esto implica ejecutar acciones en nombre del usuario en redes externas, BinnoHub implementa una arquitectura de seguridad por capas con **aislamiento por usuario**:

a) **Cuenta de ejecución por-usuario en destino.** Cada usuario tiene una cuenta inteligente determinística por red, desplegada de forma lazy. Los intents se ejecutan **desde la cuenta del propio usuario**, no desde un proxy compartido. El radio de impacto de cualquier fallo queda confinado a la cuenta individual y nunca se propaga entre usuarios.

b) **Autorización vinculante, sin firma a ciegas.** BinnoWallet decodifica y muestra cada intent en lenguaje humano antes de firmar (p. ej. "Swap 100 USDC por ETH en Uniswap (Base), mínimo 0,03 ETH"). El usuario autoriza con su firma MPC sobre datos estructurados que vinculan identidad, red, contrato destino, acción, monto, límites, nonce y deadline.

c) **Validación en BinnoChain antes del envío:** firma MPC, nonce (anti-replay), límites por-usuario, estado frozen y **allowlist de contratos destino** (en fases iniciales, solo dApps verificadas; se amplía por gobernanza).

d) **Integridad en tránsito:** el intent viaja con su hash autorizado; los 2-de-3 DVNs garantizan que llega intacto; la cuenta destino solo procede si el peer

es autorizado, los DVNs verificaron, el hash coincide, el nonce no se usó y el deadline no venció.

e) **Controles a nivel de protocolo:** límites por-intent y diarios, expiración obligatoria, congelamiento por usuario (frozen) y un **circuit breaker / pausa global** gobernado por timelock para emergencias.

f) **Simulación previa opcional** del resultado esperado antes de autorizar.

Resumen del modelo de confianza: el usuario solo firma lo que ve; su autorización viaja a prueba de manipulación; la ejecución ocurre en su propia cuenta aislada; las acciones se dirigen solo a contratos vetados; cada intent tiene límites y expiración; y existe un freno de emergencia gobernado. Web3 crosschain automática, potente y a la vez segura y auditable.

9. Manejo de fallos en pagos y operaciones cross-chain

Un sistema de pagos debe contemplar el camino infeliz, no solo el feliz. Si una operación cross-chain falla en la ejecución de destino (falta de gas, congestión, error transitorio de la infraestructura de mensajería), **los fondos no se pierden**. BinnoHub implementa una arquitectura de mensajería **non-blocking**: el mensaje fallido se almacena de forma verificable on-chain y puede reintentarse (retry) sin bloquear el resto de operaciones de esa ruta. Si tras los reintentos la operación no puede completarse en destino, el protocolo ejecuta un **reembolso verificable al origen** (el valor regresa al pagador). En ningún caso un fallo individual deja fondos en un estado donde desaparezcan ni congela la cola de pagos. Un fallo de este tipo es atribuible a la infraestructura (mensajería, gas mal estimado), no al usuario, y el diseño lo convierte en una contingencia recuperable.

10. Economía e integraciones de terceros

El modelo económico de BinnoHub está diseñado para **incentivar la adopción del estándar @username por wallets de terceros** (MetaMask, Trust Wallet, etc.) sin imponer costos perceptibles a los usuarios nativos de BinnoWallet.

Concepto	Desde BinnoWallet	Desde wallet de terceros	Reparto
Registro de @username (primera vez)	Gratuito	0,5 USD + gas	0,3 integrador · 0,2 tesorería
Vincular red adicional	Gratuito	0,1 USD + gas	0,05 integrador · 0,05 tesorería
Transacción dentro de BinnoChain	Gratuita	—	—
Transacción cross-chain (envío/intent)	Gas + transporte (sin tarifa de protocolo)	Gas + transporte + 0,002 USD	0,001 protocolo · 0,001 integrador

Cuando una operación se realiza desde BinnoWallet (sin integrador de terceros), la porción de integrador la captura BinnoWallet (Binno Labs), que actúa como integrador de su propio producto. El reparto exacto entre flujos a la empresa y flujos al protocolo se detalla en el capítulo de Tokenomics.

La tarifa de 0,002 USD por transacción cross-chain es deliberadamente marginal: sobre un micropago de 5 USD representa el 0,04%, frente al 2–3% de las procesadoras tradicionales. Imperceptible para el usuario y, a escala de millones de transacciones, sostenible para protocolo e integradores —alineando el interés de las wallets de terceros con el crecimiento de la red—. Los parámetros son ajustables por gobernanza.

11. Tabla de transparencia de costos

Es fundamental separar lo que cobra Binno de lo que cuesta la infraestructura subyacente. Una operación cross-chain incurre en: gas de la red de origen, transporte LayerZero (tarifas de DVNs y Executor, que ya incluyen el gas de ejecución en destino), y —solo para stablecoins y tokens que no son OFT nativos— la tarifa de Stargate (~0,06% en condiciones normales, variable al alza bajo

desbalance de liquidez de la ruta). Los activos OFT nativos (como BNN) no usan Stargate ni incurren en esa tarifa, pues se queman y acuñan sin necesidad de liquidez. El siguiente desglose es ilustrativo; el gas y el transporte fluctúan según las redes y la congestión:

Escenario	**Gas red origen**	**Transporte LayerZero**	**Tarifa Stargate (solo no-OFT)**	**Comisión Binno**	**Quién lo asume**
Envío interno en BinnoChain	0	—	—	0	Gratis total
Envío de BNN (OFT) crosschain desde BinnoWallet	0	~0,05–0,20 USD	0 (OFT)	0,002 (0,001+0,001)	Pagador
Envío de USDC crosschain (Stargate) desde BinnoWallet	0	~0,05–0,20 USD	~0,06 %	0,002 (0,001+0,001)	Pagador
Envío de USDC crosschain desde wallet de terceros	gas origen	~0,05–0,20 USD	~0,06 %	0,002 (0,001+0,001)	Pagador
Operación con destino Ethereum L1	según origen	~1–8 USD (domina gas L1)	~0,06 % si no-OFT	0,002	Pagador

Escenario	Gas red origen	Transporte LayerZero	Tarifa Stargate (solo no-OFT)	Comisión Binno	Quién lo asume
Recibir vía receiving address (USDC desde otra red)	lo paga el remitente	~0,05–0,20 USD	~0,06 USD si cruza	deducido del neto (~centavos)	El receptor

Tres conclusiones se desprenden: la comisión de Binno es siempre **marginal** frente al costo real; el costo dominante es el gas de la red subyacente (en especial Ethereum L1) y el transporte, que el protocolo no controla; y los activos OFT nativos son la ruta más barata, lo que incentiva su uso de forma natural y honesta.

12. Mecanismos de seguridad

- **Nonces globales incrementales** → ordenamiento fuerte cross-chain.
- **Firmas MPC del owner** → la clave privada nunca se recompone.
- **Security Stack de 2-de-3 DVNs** → integridad de transporte sin punto único de fallo, con opción de DVN propio como contingencia.
- **Commit-Reveal + ventana de desafío de 3 bloques** → protección contra front-running, sniping y typosquatting en el registro de nombres.
- **Verificación criptográfica estricta** de todas las direcciones externas (doble prueba de propiedad en vinculación).
- **Aislamiento por usuario** en intents (cuentas de ejecución individuales) + allowlist + límites + expiración.
- **Manejo non-blocking de fallos** con retry y refund al origen.
- **Congelamiento de perfil** (frozen) y **circuit breaker global** gobernado por timelock.

El sistema está diseñado para que ningún mensaje pueda ejecutarse fuera de orden, duplicarse o falsificarse bajo el modelo de confianza de su Security Stack, incluso ante congestión extrema o intentos coordinados de ataque.

13. Evolución del contrato y gobernanza

BinnoHub es el núcleo de identidad del ecosistema y debe combinar **estabilidad de reglas** con **capacidad de corrección a largo plazo**. En lugar de un contrato absolutamente inmutable —que dejaría cualquier error sin posibilidad de corrección durante años— adopta un modelo de **lógica núcleo inmutable con rutas de evolución estrictamente acotadas y gobernadas**:

- La lógica crítica (unicidad del @username, propiedad del usuario, reglas de resolución) es estable y no se altera de forma discrecional.

- Las actualizaciones —corrección de errores, ajuste de parámetros, ampliación de allowlists y contingencias críticas como la **migración criptográfica post-cuántica** (esquemas tipo Dilithium/Falcon)— se realizan exclusivamente mediante gobernanza de la DAO con **timelock**, garantizando transparencia y un período de revisión pública antes de cualquier cambio.

Este modelo preserva el espíritu del "contrato eterno" —nadie cambia las reglas a capricho— sin la fragilidad de la inmutabilidad absoluta, y resuelve la necesidad de evolucionar la criptografía a lo largo de las décadas.

14. Dependencia de la capa de interoperabilidad — declaración honesta

BinnoHub se construye sobre LayerZero V2 y su estándar OFT porque es la infraestructura de interoperabilidad más madura y probada del mercado, con la mayor cobertura de cadenas y, vía Stargate, la mayor liquidez para activos no-OFT. Es una **dependencia consciente y declarada**. El estándar OFT es propio de LayerZero; reemplazar la capa de interoperabilidad por otra (Wormhole, Axelar, CCIP) sería un esfuerzo de ingeniería significativo, no una simple reconfiguración. Binno asume esta dependencia como parte de elegir la mejor tecnología disponible hoy, y la mitiga a nivel de seguridad mediante la Security Stack de 2-de-3 DVNs, la capacidad de operar un DVN propio, el manejo non-blocking de fallos y el circuit breaker de emergencia. Esta dependencia se detalla, junto con su mitigación, en el capítulo de Riesgos.

15. Conclusión

BinnoHub convierte la promesa de la interoperabilidad en una experiencia real: enviar valor o ejecutar acciones en cualquier cadena con la simplicidad de escribir un nombre. Lo logra con una arquitectura de tres capas (BinnoHub como fuente de verdad, SatelliteHubs como traductores ligeros, LayerZero V2 con Security Stack multi-DVN como transporte verificado), un modelo de intents seguro y aislado por usuario, un manejo honesto de fallos, y un modelo económico que incentiva la adopción del estándar sin costos perceptibles. Es la primera insignia del ecosistema porque encarna su tesis central: que la blockchain, en manos del usuario, simplemente desaparezca.

Capítulo 4. BinnoPay — El Estándar Abierto de Liquidación On-Chain para Pagos

BinnoPay es la capa de pagos del ecosistema Binno. Su propósito no es ser un banco ni un procesador de pagos cerrado, sino el **estándar abierto de liquidación on-chain** que cualquier tercero —fabricantes y distribuidores de POS, fintechs, plataformas de e-commerce y wallets— puede integrar en sus productos.

La analogía es precisa: así como Visa y Mastercard no son bancos, sino la red y la tecnología que terceros integran para mover dinero, **BinnoPay es el riel de liquidación; los integradores construyen los productos de cara al comercio y al usuario, y comparten los ingresos generados.** Binno no compite con sus integradores: les provee la infraestructura.

BinnoPay introduce un sistema de pagos con un conjunto de propiedades difícil de igualar:

- **Finalidad instantánea** para pagos nativos: liquidación real en menos de un segundo (<600 ms) en BinnoChain.

- **Comisión ultra-baja:** 0,02 USD + 0,1 % por transacción, una fracción del 1,4–3,9 % de las redes tradicionales.

- **Universalidad omnichain:** el pagador puede pagar desde cualquier cadena y con cualquier token, gracias a BinnoHub; el comercio recibe siempre liquidación en stablecoin (USDC/USDT).

- **Micropagos físicos reales:** pagos en tienda mediante NFC o QR, con una experiencia equivalente a la de las tarjetas contactless.

1. Filosofía y objetivos de diseño

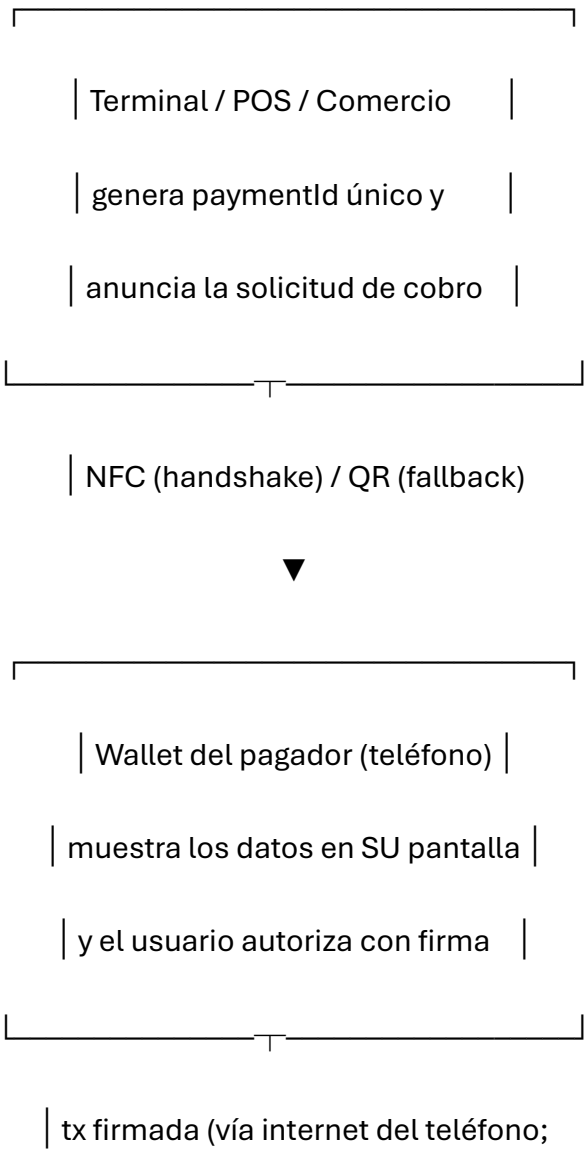
BinnoPay se diseña como infraestructura neutral: un estándar que cualquiera puede integrar sin permisos a nivel de protocolo, y sobre el cual se construye un mercado competitivo de productos de pago.

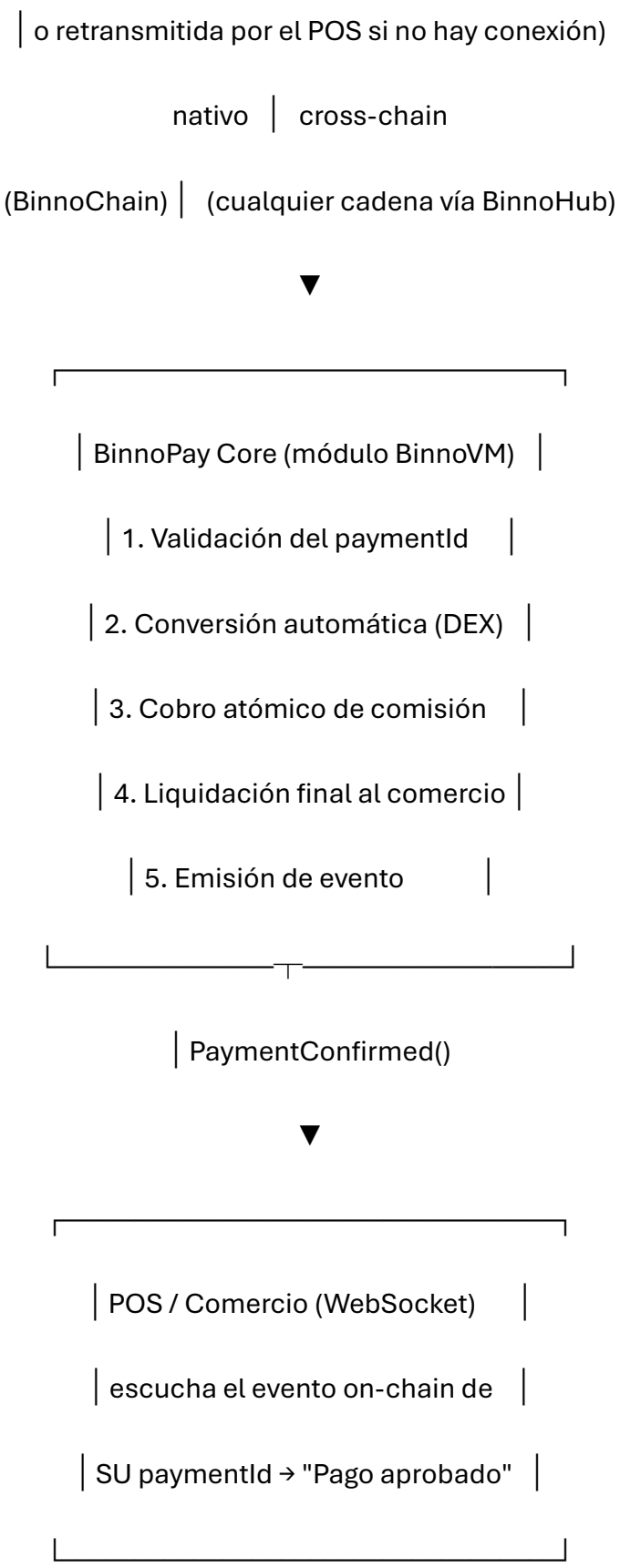
Característica	Sistemas actuales (2025)	BinnoPay
Confirmación comercial	2–30 s	<600 ms (pago nativo)
Costo para el usuario	0,01–0,30 USD + gas	0 dentro de BinnoChain
Costo para el comercio	1,4–3,9 %	0,02 USD + 0,1 %
Multichain real	No	Sí (cualquier token → USDC/USDT)
Integración POS	Cerrada	Abierta (SDK, sin permisos de protocolo)
Liquidación al comercio	Lote al día siguiente	Stablecoin on-chain, inmediata (pago nativo)
Modelo de confianza	PCI / intermediarios	Verificable on-chain + firma

El modelo de distribución: integrar al fabricante, no al comercio. BinnoPay no busca convencer a comercios uno por uno, sino integrarse mediante acuerdos con **fabricantes y distribuidores de terminales POS** (Ingenico, Verifone, PAX y similares), que integran el SDK de BinnoPay como un método de pago adicional en sus dispositivos —separado e independiente del riel EMV de las tarjetas, del mismo modo que Alipay y WeChat Pay operan junto a las tarjetas en un mismo terminal—. Un solo acuerdo con un distribuidor pone a BinnoPay en manos de toda su red de comercios. La integración se realiza por familia de dispositivos programables (POS con sistema operativo abierto, típicamente Android), y no depende de los rieles de las redes de tarjetas.

Closed-loop sobre NFC y QR. BinnoPay opera en modo *closed-loop*: su propio circuito de pago sobre NFC o mediante QR. Esto significa que **nunca emula una tarjeta ni utiliza el protocolo EMV de Visa/Mastercard** —lo que evitaría el riel y las comisiones de las tarjetas—; en su lugar intercambia su propio payload de pago que va directo a la blockchain. El método NFC funciona en terminales que permiten el acceso al lector NFC en modo de datos (POS Android programables); el **método QR ofrece cobertura universal**, pues solo requiere una pantalla y no toca el lector NFC ni el firmware de pago certificado, funcionando incluso en terminales cuyo NFC está restringido a EMV. El QR es, por tanto, la vía garantizada que no depende de ningún fabricante; el NFC es la experiencia premium donde el dispositivo lo permite.

2. Arquitectura general del flujo de pago




o retransmitida por el POS si no hay conexión)
nativo
cross-chain
(BinnoChain)
(cualquier cadena vía BinnoHub)
BinnoPay Core (módulo BinnoVM)
1. Validación del paymentId
2. Conversión automática (DEX)
3. Cobro atómico de comisión
4. Liquidación final al comercio
5. Emisión de evento
PaymentConfirmed()
POS / Comercio (WebSocket)
escucha el evento on-chain de
SU paymentId → "Pago aprobado"

El principio rector de seguridad es que **el árbitro de verdad es la cadena, no el teléfono ni el POS**: el comercio confía en el evento on-chain irreversible, no en un mensaje del dispositivo del cliente.

3. El flujo de pago NFC en detalle

El flujo está diseñado para combinar la comodidad del contactless con la seguridad de la autorización on-chain. Ningún acercamiento físico ejecuta un pago por sí solo: el acto de acercar el teléfono es la confirmación deliberada del usuario, nunca un disparador automático.

a) **El POS anuncia el cobro.** El comercio introduce el monto; el POS genera el paymentId y expone el payload del cobro vía NFC (y/o QR como alternativa): dirección del comercio, monto, paymentId, red de liquidación y deadline. En esta fase el POS solo *propone*; no recibe nada del teléfono.

b) **El teléfono lee la solicitud y la muestra en su propia pantalla.** Al acercar el teléfono, este recibe los datos del cobro y los muestra en la pantalla del usuario —no en la del comercio—. Esto es clave: el usuario verifica el monto y el destinatario en una interfaz que el comercio no controla, lo que neutraliza un POS manipulado que muestre un monto y cobre otro.

c) **El usuario autoriza con su firma MPC.** Confirma el monto y autoriza con el factor de seguridad que haya configurado (biometría del Secure Enclave / 2FA). Gracias a las pre-firmas descritas en el Capítulo 2, el cómputo MPC pesado se inicia al abrir la pantalla de pago, de modo que la autorización final es casi instantánea.

d) **La transacción firmada llega a BinnoPay Core.** Por defecto, el teléfono transmite la transacción firmada a BinnoChain mediante su propia conexión a internet, sin depender de un canal NFC bidireccional.

e) **El POS recibe la confirmación on-chain.** El POS está suscrito vía WebSocket al evento PaymentConfirmed correspondiente a su paymentId. Cuando BinnoPay Core ejecuta el pago y emite el evento, el POS lo recibe (<600 ms en el caso nativo) y muestra "Pago aprobado". El comercio se entera por la cadena, no por el teléfono del cliente.

El QR como alternativa equivalente. Si el NFC no está disponible, el POS muestra un QR con el mismo paymentId; el usuario lo escanea y el resto del flujo es idéntico.

Un mismo backend, dos formas de handshake (NFC o QR), lo que facilita la integración para cualquier fabricante de POS.

4. paymentId — Identificador único e idempotente

Cada pago genera un paymentId de 256 bits que garantiza una probabilidad de colisión astronómicamente baja (idempotencia: un paymentId se ejecuta una sola vez) y verificabilidad total on-chain. Se genera en el POS/comercio y viaja en el payload del pago (NFC o QR).

(Pseudocódigo ilustrativo de una acción de BinnoVM):

```
paymentId = hash(
  merchantAddress,
  amount,
  randomNonce256,   // generado con un CSPRNG en el POS
  deadline
)
```

Dos consideraciones de seguridad son esenciales y se especifican como requisito de implementación:

- **El nonce debe provenir de un generador criptográficamente seguro (CSPRNG).** La unicidad e imprevisibilidad del paymentId descansan enteramente en la calidad de este nonce; un generador débil en un dispositivo POS de bajo costo abriría la puerta a la predicción o pre-cómputo de identificadores.

- **El cobro se vincula a la autorización del comercio.** El paymentId se asocia a una autorización verificable del comercio, de modo que un tercero que observe el QR/NFC no pueda redirigir ni falsificar el cobro.

5. BinnoPay Core — proceso atómico (caso nativo)

Para los pagos que se liquidan en BinnoChain, todo el flujo —conversión de token, cobro de comisión y liquidación al comercio— ocurre en una **única transacción atómica**. No existen estados intermedios, custodia temporal ni posibilidad de ejecución parcial: o el pago se completa entero, o no ocurre.

(Pseudocódigo ilustrativo de una acción de BinnoVM):

```
action executePayment(paymentId, payer, merchant, integrator, grossAmount, tokenIn):

  require not payments[paymentId].executed     // idempotencia

  require now <= payments[paymentId].deadline    // no expirado



  # 1. Conversión a stablecoin si es necesario (vía BinnoDEX interno)

  stableAmount = (tokenIn in [USDC, USDT])

        ? grossAmount

        : binnoDex.swapToStable(tokenIn, grossAmount)



  # 2. Cálculo de comisión: 0,02 USD fijo + 0,1 % variable

  flatFee = 0.02

  varFee  = stableAmount * 0.001

  totalFee = flatFee + varFee

  # 3. Liquidación atómica

  transfer(merchant,    stableAmount - totalFee)
```

```
    transfer(treasury,    flatFee/2 + varFee/2)    # porción de protocolo
    transfer(integrator,  flatFee/2 + varFee/2)    # porción del integrador
    payments[paymentId].executed = true
    emit PaymentConfirmed(paymentId, merchant, stableAmount - totalFee)
```

Nota de modelo de ejecución: el flujo NFC/QR de BinnoPay es de tipo "push" —el pagador autoriza y origina la transferencia con su firma MPC—, no un modelo "pull" basado en autorizaciones previas. El pseudocódigo anterior describe la lógica de liquidación, no el mecanismo de transferencia de fondos, que parte siempre de la autorización explícita del pagador.

6. Procesamiento omnichain — tres rutas, una misma confirmación

BinnoPay aprovecha BinnoHub (Capítulo 3) para aceptar pagos desde cualquier cadena. Existen tres rutas, y en todas, el comercio recibe el mismo evento PaymentConfirmed verificable:

Ruta	Origen	Liquidación	Latencia
Nativa	BinnoWallet / activos en BinnoChain	Atómica en BinnoChain	<600 ms
Cross-chain a receiving address	Wallet externa sin @username	Vía SatelliteHub → BinnoHub → BinnoPay Core	Segundos (ver más abajo)
Cross-chain directa	Wallet con BinnoHub integrado (sendToUsername)	Vía BinnoHub → BinnoPay Core	Segundos (ver más abajo)

Precisión sobre la atomicidad y la latencia cross-chain. La liquidación atómica en <600 ms aplica a los pagos **nativos** en BinnoChain. Un pago que se origina en

otra cadena no puede ser atómico ni instantáneo de extremo a extremo: depende de la finalidad de la red de origen y de la verificación de la Security Stack de DVNs (Capítulo 3), lo que toma del orden de segundos —y notablemente más si la red de origen es Ethereum L1—. En este caso, BinnoPay ofrece **liquidación garantizada en segundos**, no instantánea: el comercio recibe la confirmación on-chain en BinnoChain una vez que el transporte verificado completa la entrega. Esta distinción es deliberada y honesta: el caso nativo —que constituye el grueso de los pagos dentro del propio ecosistema— es instantáneo; el caso cross-chain es rápido y garantizado.

7. Estructura de comisiones

BinnoPay cobra una comisión al comercio de **0,02 USD fijo + 0,1 % variable**, repartida en partes iguales entre la tesorería del protocolo y el integrador que aporta el punto de venta. Esta porción de tesorería (0,01 USD + 0,05 %) corresponde al modelo económico descrito en el Capítulo 1.

Componente	Valor	Tesorería	Integrador
Comisión fija	0,02 USD	0,01 USD	0,01 USD
Comisión variable	0,1 %	0,05 %	0,05 %

Ejemplo: un pago de 100 USD genera una comisión de 0,12 USD (0,02 + 0,10). El comercio recibe **99,88 USD** netos en USDC/USDT; la tesorería y el integrador reciben 0,06 USD cada uno.

El reparto al integrador es deliberado y estratégico: alinea el interés de los fabricantes y distribuidores de POS, las fintechs y las plataformas de e-commerce con la adopción del estándar. El integrador gana en cada transacción que procesa con su hardware o software, lo que convierte a BinnoPay en un negocio atractivo de distribuir —exactamente el mecanismo por el cual una red de pagos alcanza escala global—. Los parámetros son ajustables por gobernanza.

8. Liquidación: el comercio recibe stablecoin, y es libre

El comercio recibe siempre, a nivel de protocolo, **liquidación en stablecoin (USDC/USDT)**. Aquí termina —deliberadamente— la responsabilidad y la superficie regulatoria de BinnoPay. Este es un principio de diseño fundamental: el protocolo no convierte a moneda fiduciaria, no custodia fondos fiat y no realiza KYC. Esto es lo que mantiene a BinnoPay descentralizado y libre de la carga regulatoria de un banco o un procesador de pagos.

A partir de ahí, el comercio es **libre**: puede conservar sus stablecoins, usarlas para pagar a sus proveedores o empleados dentro del propio ecosistema (vía @username), o convertirlas a su moneda local cuando quiera mediante el servicio de off-ramp de su elección, completamente externo al protocolo. Binno no impone, no intermedia ni recomienda ningún convertidor: la decisión es enteramente del comercio.

Esta neutralidad es coherente con la visión del proyecto: el objetivo de largo plazo no es facilitar la conversión a fiat, sino **reducir la dependencia del fiat**. Un comercio que recibe en stablecoin y paga a sus trabajadores en stablecoin no necesita convertir nada. Cuanto más se use el dinero digital de extremo a extremo, menos relevante se vuelve el momento de conversión —y ese momento, cuando ocurra, queda fuera del protocolo, en manos de servicios regulados que el comercio elige libremente—.

9. Denominación de precio en moneda local

Para facilitar la adopción de comercios que piensan en su moneda local, BinnoPay permite **mostrar el precio en moneda local y cobrar el equivalente en stablecoin**, sin que ello implique conversión real de fiat ni centralización. Es importante la distinción: el protocolo solo *muestra* un precio convertido como referencia; el comercio sigue recibiendo stablecoin (USDC/USDT), nunca moneda fiduciaria.

El cálculo del equivalente se realiza según el tipo de moneda:

- **USD:** 1:1 con la stablecoin (USDC/USDT), sin oráculo. Si el comercio cobra 100 USD, el usuario paga 100 USDT.

- **EUR / GBP con stablecoin del mismo tipo** (por ejemplo, una stablecoin EUR): 1:1, sin oráculo.

- **EUR / GBP pagando con USDC/USDT:** se usa la tasa de cambio FX vía oráculo Chainlink, por su estabilidad y fiabilidad, solo para calcular el monto equivalente.

- **Otras monedas (por ejemplo, de América Latina):** se usa una **tasa de mercado real agregada de múltiples plataformas P2P** (no la tasa forex oficial, que en muchos de estos mercados difiere notablemente de la tasa real), tomando el punto medio entre compra y venta y cruzando varias fuentes para descartar manipulación. Es el mismo enfoque que utilizan las fintech y los servicios de conversión de la región.

En todos los casos, la tasa mostrada es un **precio de referencia de mercado, no una garantía de conversión**: el comercio recibe stablecoin y decide libremente qué hacer con ella. Este mecanismo es plenamente descentralizado, ya que el protocolo no custodia ni convierte moneda fiduciaria en ningún momento.

10. Botón "Pay with Crypto" para Web2

BinnoPay extiende su estándar al comercio electrónico Web2 (tiendas online, marketplaces, SaaS, suscripciones) mediante un botón de pago integrable con una sola línea de código:

- **En escritorio:** un popup muestra un QR con la red destino; el usuario escanea, firma en su wallet y el pago se aprueba.

- **En móvil:** un deep link abre directamente la wallet instalada (BinnoWallet de forma prioritaria); el usuario firma sin necesidad de escanear.

- **Fallback automático:** QR si no se detecta ninguna wallet.

- **Confirmación:** webhook instantáneo payment.success al comercio, disparado por el evento on-chain.

El comercio decide si conserva sus USDC/USDT o las convierte a moneda local con el servicio externo que prefiera, igual que en el punto de venta físico.

11. Devoluciones y reembolsos

Dado que los pagos on-chain son irreversibles por diseño (no existe el chargeback unilateral de las tarjetas), BinnoPay implementa los reembolsos como una

operación explícita iniciada por el comercio: un reembolso es una nueva transacción de pago del comercio hacia el pagador, referenciada al paymentId original. Esto preserva la verificabilidad y la trazabilidad on-chain, evita el fraude de contracargos que afecta a las redes tradicionales, y deja un registro auditable de cada devolución. Los integradores pueden exponer esta función en sus POS y paneles de comercio.

12. Seguridad de BinnoPay

- **Idempotencia estricta** (executed = true): un paymentId no puede ejecutarse dos veces.

- **Nonces de 256 bits desde un CSPRNG** en el POS, con vinculación a la autorización del comercio.

- **Atomicidad completa** del flujo nativo (conversión + comisión + liquidación) sin estados intermedios.

- **Autorización mediante firma MPC** del pagador (Capítulo 2): la clave nunca se recompone, y el usuario confirma el monto en su propia pantalla.

- **Integridad cross-chain** garantizada por la Security Stack de 2-de-3 DVNs y la autenticación de peer de los SatelliteHubs oficiales (Capítulo 3), con resistencia robusta a replay.

- **El comercio confía en la cadena, no en el dispositivo del cliente**: la confirmación proviene del evento on-chain irreversible.

13. Integración abierta y economía del protocolo

BinnoPay se distribuye como un estándar abierto, diseñado para que integrarse sea trivial (el modelo que convierte a una plataforma en estándar):

- **Componente de pago pre-construido para Android:** un botón "BinnoPay" listo para usar que el integrador incorpora en su aplicación con mínimo esfuerzo. Maneja internamente la generación del paymentId, el QR y el NFC (donde el dispositivo lo permita), la suscripción al evento de confirmación y los estados del pago. El integrador solo introduce el monto y recibe el resultado (aprobado/rechazado).

- **Componentes de interfaz personalizables** sobre ese botón, para que el integrador aplique su marca y su flujo sin tocar la lógica de pago.

- **API abierta y documentada** por debajo, para el integrador avanzado que desee control total y construir su propia interfaz.

- **SDKs** para Android, iOS, React Native y hardware POS, diseñados sin dependencia obligatoria de los servicios de Google (GMS), de modo que funcionen en cualquier terminal Android, con o sin GMS.

- **Suscripción directa por WebSocket** al evento PaymentConfirmed.

- **Revenue-share automático** con el integrador, liquidado on-chain en cada transacción.

- **Sin permisos a nivel de protocolo** para integrar.

Los ingresos del protocolo generados por BinnoPay se destinan al sostenimiento y crecimiento del ecosistema —incluyendo el pool de recompensa de validadores, los buybacks de BNN, el fondo de seguro y la expansión— según el modelo económico detallado en el capítulo de Tokenomics.

14. Conclusión del capítulo

BinnoPay no busca reemplazar frontalmente a Visa, Apple Pay o Solana Pay, sino convertirse en el **riel de liquidación abierto** sobre el que la próxima generación de productos de pago se construya —del mismo modo que las redes de tarjetas son la infraestructura invisible tras millones de comercios—. Con finalidad instantánea para pagos nativos, liquidación garantizada para pagos omnichain, comisiones marginales, liquidación descentralizada en stablecoin y plena libertad del comercio sobre qué hacer con sus fondos, BinnoPay ofrece a los distribuidores de POS, fintechs y comercios una infraestructura más rápida, más barata y más simple de integrar que cualquier alternativa actual. El objetivo de largo plazo es que aceptar un pago deje de significar "aceptar cripto" y pase a significar, simplemente, recibir un @username mediante BinnoPay.

Capítulo 5. BinnoDEX — La Capa de Liquidez del Ecosistema

BinnoDEX no es un exchange descentralizado más, diseñado para traders. Es la **capa de liquidez que hace funcionar a todo el ecosistema Binno**: el motor silencioso de conversión y enrutamiento de activos que permite que un pago se liquide en la stablecoin correcta, que un envío llegue en el token que el destinatario quiere, que BinnoCredit liquide colateral sin colapsar precios, y que la tesorería ejecute sus recompras. Su éxito no se mide en volumen especulativo, sino en que **el usuario nunca tenga que pensar en él**.

1. Función en el ecosistema

BinnoDEX existe para resolver un problema concreto: en un sistema donde el usuario paga, envía y recibe en cualquier token y cualquier cadena, **alguien tiene que convertir y enrutar el valor de forma instantánea, barata y sin fricción**. Esa es su única misión. Sus consumidores son los otros módulos del protocolo:

- **BinnoPay** lo usa para convertir el token que paga el usuario a la stablecoin que recibe el comercio.
- **BinnoHub** lo usa para que un envío llegue en el activo correcto en la red destino.
- **BinnoCredit** lo usa para liquidar colateral de forma controlada, sin sobreventa.
- **La tesorería** lo usa para ejecutar recompras de BNN con los ingresos del protocolo.

2. Arquitectura: estado contable unificado e inventario distribuido

El reto técnico de una capa de liquidez omnichain es que **los tokens existen físicamente en cadenas distintas** y no se pueden teletransportar. BinnoDEX lo resuelve con un diseño híbrido honesto:

- **Estado contable unificado en BinnoChain.** La contabilidad de la liquidez —cuánta hay, de qué, y dónde— es una fuente de verdad única en

BinnoChain. Esto elimina la fragmentación *contable* y permite enrutamiento determinístico.

- **Inventario físico distribuido.** Los activos viven en las cadenas donde se necesitan. Para los tokens principales, BinnoDEX no reinventa la liquidez: se apoya en la infraestructura OFT/Stargate de LayerZero (Sección 3).

- **Motor CLMM para los pares del ecosistema.** Para los pares propios —especialmente BNN y las conversiones de pago— BinnoDEX implementa un Concentrated Liquidity Market Maker (modelo tipo Algebra v3) con comisiones dinámicas, que concentra la liquidez donde más se usa y maximiza la eficiencia de capital.

Es importante ser preciso: lo que está unificado es la **contabilidad y el enrutamiento**, no la ubicación física de los tokens. Afirmar que "no existe liquidez fragmentada" sería inexacto; lo correcto es que **la fragmentación contable desaparece, y la física se gestiona mediante inventario distribuido y la capa OFT/Stargate**. Este diseño reduce —no elimina— la superficie de ataque de los puentes tradicionales, ya que minimiza la liquidez bloqueada en contratos puente custodios.

3. Liquidez de tokens: OFT nativo vs. Stargate

BinnoDEX y BinnoHub distinguen dos clases de activos, con economías de liquidez distintas:

- **Tokens OFT nativos (como BNN).** No necesitan liquidez: se queman en la cadena de origen y se acuñan en la de destino. El único costo es el mensaje LayerZero. Es la ruta más eficiente y barata, y constituye un incentivo natural para el uso de BNN y de stablecoins que adopten el estándar OFT.

- **Tokens no-OFT (USDC, USDT y otros).** Existen físicamente y no se pueden quemar/acuñar libremente. Para moverlos entre cadenas, BinnoHub se apoya en **Stargate** (la capa de liquidez de LayerZero), que mantiene pools de liquidez nativa en las cadenas principales: bloquea en origen y libera del pool en destino. Esto añade la tarifa de Stargate (~0,06% en condiciones normales, variable al alza bajo desbalance de liquidez de la ruta), que se refleja con transparencia en la tabla de costos del capítulo de BinnoHub.

BinnoDEX no se liga a Stargate para su operación interna; Stargate es un recurso que el ecosistema utiliza específicamente para el transporte cross-chain de stablecoins no-OFT. Esta es una dependencia de terceros declarada, tratada en el capítulo de Riesgos.

4. Funcionamiento técnico

- **CLMM con comisiones dinámicas.** Liquidez concentrada que se adapta a la volatilidad del par, maximizando el rendimiento de los proveedores de liquidez (LPs) y minimizando el slippage para el ecosistema.

- **Pathfinding determinístico.** Ante cualquier conversión, el motor encuentra la ruta óptima (directa o multi-salto) de forma determinística y verificable.

- **Abstracción de gas.** El usuario puede pagar el resultado de un swap con cualquier token, sin gestionar el gas del proceso.

- **Latencia.** Las conversiones dentro de BinnoChain se confirman con la finalidad de la red (objetivo sub-segundo). Las conversiones que implican transporte cross-chain heredan la latencia de ese transporte (segundos), como se describe en el capítulo de BinnoHub.

5. Comisiones

La comisión de swap de BinnoDEX es del **0,05%**, claramente separada de la comisión de BinnoPay (que es una comisión de *pago*, no de *swap*). Esta comisión se reparte entre los proveedores de liquidez y la tesorería del protocolo, y es ajustable por gobernanza. Las comisiones dinámicas del CLMM pueden ajustar este valor según la volatilidad del par, dentro de los parámetros que defina la gobernanza.

6. Liquidación controlada para BinnoCredit

Una de las funciones críticas de BinnoDEX es servir de **camino de liquidación controlado** para BinnoCredit. Cuando una posición de crédito debe liquidarse, BinnoDEX ejecuta la venta del colateral de forma escalonada y con límites estrictos de slippage, evitando la sobreventa que provoca cascadas de liquidación. Este diseño es deliberado: protege tanto al usuario liquidado (que no sufre una venta a precio de remate) como al ecosistema (que no sufre un colapso de precio en espiral). El detalle se desarrolla en el capítulo de BinnoCredit.

7. Rendimiento para proveedores de liquidez

Los proveedores de liquidez del DEX obtienen un rendimiento proveniente de las comisiones de swap reales del ecosistema. Este rendimiento es **variable según el uso real del protocolo**, no una tasa fija garantizada. En la fase inicial, parte de la asignación de Comunidad/Ecosistema (descrita en el capítulo de Tokenomics) incentiva a los primeros LPs, y la tesorería siembra la liquidez inicial de los pares críticos hasta que el ecosistema atraiga liquidez orgánica suficiente. Esto resuelve el arranque de liquidez sin comprometer la sostenibilidad: el rendimiento de largo plazo proviene del volumen real, no de emisiones perpetuas.

8. Seguridad

- **Oráculos de precio redundantes** (Chainlink como fuente principal) para evitar manipulación de precios, con especial cuidado en el par BNN —cuyo mercado, al ser un token nuevo, requiere protección reforzada contra manipulación de precio—.

- **Liquidación con límites de slippage** para prevenir cascadas.

- **Verificación on-chain** de cada conversión y enrutamiento.

- La integridad cross-chain se hereda de la Security Stack de 2-de-3 DVNs descrita en el capítulo de BinnoHub.

9. Conclusión

BinnoDEX es la capa de liquidez invisible que hace posible la experiencia sin fricción del ecosistema. No compite por ser el DEX más grande para traders; compite por ser tan eficiente y confiable que el usuario nunca note que existe. Es infraestructura, no producto de cara al especulador, y esa especialización es precisamente su fortaleza.

Capítulo 6. BinnoCredit — Crédito No Custodial con Colateral Productivo

BinnoCredit es la capa de crédito del ecosistema: permite a los usuarios acceder a liquidez sin vender sus activos, con una experiencia equivalente a la de una tarjeta de crédito, pero construida sobre infraestructura DeFi no custodial y verificable. Su principio rector es que **nadie decide quién paga y quién no; el código ejecuta reglas matemáticas transparentes que el usuario acepta al abrir su línea de crédito.**

1. Concepto: colateral productivo

La innovación central de BinnoCredit es el **colateral productivo**: el activo que el usuario deposita como garantía (BNN, BTC, ETH, o posiciones de liquidez) no permanece inerte, sino que **genera rendimiento mediante staking**, y ese rendimiento se destina a pagar los intereses del crédito. De este modo, el usuario puede acceder a liquidez mientras su colateral sigue trabajando para él.

- **Préstamo contra colateral**, sin vender el activo.
- **El rendimiento del colateral paga los intereses** de forma automática.
- **Experiencia de usuario tipo tarjeta de crédito**, sobre una base DeFi robusta.

2. Parámetros del crédito

- **LTV (Loan-to-Value) máximo: 50%** sobre el principal del colateral. Conservador por diseño, para resistir la volatilidad de los activos cripto.
- **Contratos de duración definida** (de 1 a 60 meses), que dan claridad al usuario y reducen el riesgo sistémico frente al crédito perpetuo.
- **Tasas variables según utilización.** Las tasas de interés —tanto la que pagan los prestatarios como el rendimiento que reciben los depositantes— son **variables según el uso real del protocolo**, no cifras fijas garantizadas. El modelo está diseñado para sostener un spread saludable entre ambas (del orden de unos pocos puntos porcentuales) que financia la sostenibilidad del sistema. En la fase inicial, la tesorería puede subsidiar parcialmente el

rendimiento como un mecanismo de arranque decreciente, claramente identificado como subsidio de bootstrap y no como rendimiento orgánico.

3. El rendimiento futuro paga el interés (sin prestar contra el futuro)

El rendimiento que genera el colateral en staking se destina, de forma automática, a servir los intereses del crédito mientras exista deuda. Es importante una distinción de diseño deliberada: **BinnoCredit NO presta contra rendimientos futuros no materializados** (no los capitaliza como colateral adicional). El rendimiento futuro solo se usa para **pagar el interés**, que es su flujo de caja natural, no para ampliar el monto prestable. Esta decisión elimina el riesgo de prestar contra un activo que podría no materializarse, un patrón que ha provocado crisis en otros protocolos.

El cobro del rendimiento para pagar el interés está **autorizado por el usuario al abrir la línea de crédito**, como una condición del contrato que acepta. A partir de ahí, lo ejecuta el código automáticamente mientras haya deuda. No es una decisión discrecional del protocolo "cobrar a la fuerza"; es la ejecución de las reglas que el usuario aceptó.

4. Liquidaciones: automáticas, escalonadas, regidas por código

Este es el punto donde BinnoCredit demuestra ser genuinamente descentralizado. **El protocolo no "sustrae" colateral por decisión de nadie.** Existe un **Health Score** (salud crediticia) calculado on-chain a partir de la relación entre la deuda (más intereses acumulados) y el valor del colateral. Si el Health Score cae por debajo de un umbral —porque la deuda creció o el colateral perdió valor—, el contrato ejecuta una **liquidación automática y escalonada**, regida exclusivamente por código:

- La liquidación es **escalonada** (por ejemplo, 10% → 20% → 30% del colateral), nunca una venta total súbita.

- Se ejecuta a través del **camino de liquidación controlado de BinnoDEX**, con límites de slippage, evitando la sobreventa y las cascadas.

- **Nadie decide ni dirige la liquidación.** Es un umbral matemático y una ejecución automática que cualquiera puede verificar on-chain.

Las **notificaciones de advertencia** ("tu salud crediticia está bajando, paga o añade colateral") son una **capa de conveniencia de UX**, no un mecanismo de seguridad ni un requisito para la operación justa del protocolo. El estado crediticio reside on-chain como fuente de verdad pública: cualquiera puede leerlo mediante un explorador o un servicio de terceros, no solo BinnoWallet. Que BinnoWallet ofrezca estas notificaciones no centraliza el protocolo, porque la liquidación la dispara el código según el estado on-chain, y el dato es público y no exclusivo de Binno.

5. El staking como colateral: bloqueo y prioridad de deuda

Cuando un usuario usa su staking como colateral:

- **El colateral queda bloqueado** mientras exista deuda. El usuario no puede retirar staking si ello dejara su posición por debajo del umbral de salud (no puede sacar y dejar menos de lo que debe).

- **El rendimiento del staking sirve la deuda** de forma prioritaria y automática, según lo autorizado al abrir la línea.

- Si la deuda no puede cubrirse y el Health Score toca el umbral, opera la liquidación escalonada de la Sección 13.4.

6. Riesgo reflexivo de BNN como colateral

BinnoCredit reconoce abiertamente un riesgo específico: como BNN es el token nativo del ecosistema y un colateral aceptado, una caída fuerte de su precio podría disparar liquidaciones de BNN que, vendidas en el mercado, presionen aún más el precio —un riesgo de espiral reflexiva—. BinnoCredit lo mitiga con varias defensas:

- **Límites de exposición:** un tope sobre cuánto BNN puede usarse como colateral en el sistema en su conjunto.

- **Liquidación escalonada y controlada** vía BinnoDEX, sin venta súbita.

- **Backstop de tesorería sin venta de mercado:** la tesorería puede absorber colateral BNN en liquidaciones **sin venderlo al mercado**, usando su reserva de stablecoins (proveniente de las comisiones del ecosistema) para romper la espiral. Esto funciona mientras la tesorería mantenga una reserva de stablecoins suficiente relativa a la exposición a BNN, dimensionamiento que se aborda en el capítulo de Tokenomics.

Reconocer este riesgo de forma explícita y mostrar sus mitigaciones es parte del compromiso de transparencia del proyecto.

7. Reducción de riesgo frente al crédito tradicional

El diseño de BinnoCredit —LTV conservador del 50%, liquidaciones escalonadas en lugar de súbitas, contratos de duración definida y colateral productivo— reduce sustancialmente el riesgo frente tanto al crédito tradicional como a los modelos de lending DeFi más agresivos. No prometemos cifras de reducción de riesgo no verificables; afirmamos que la combinación de estos mecanismos está diseñada para minimizar el riesgo de liquidación desordenada y de pérdida para el usuario.

8. Naturaleza descentralizada y consideraciones regulatorias

BinnoCredit está diseñado como un protocolo no custodial: los fondos y el colateral viven en contratos auditados, las reglas se ejecutan por código, y no existe una entidad que tome decisiones discrecionales sobre los créditos de los usuarios. Estas propiedades —no custodia, ejecución automática por código inmutable y auditado, ausencia de intervención discrecional— son las que diversos marcos regulatorios consideran al distinguir un protocolo descentralizado de un servicio financiero regulado.

Esta descripción no constituye asesoría legal, y el tratamiento regulatorio de los protocolos de crédito descentralizado varía por jurisdicción y evoluciona constantemente. Binno aborda el cumplimiento con la asesoría legal correspondiente, como se detalla en el capítulo de Consideraciones Legales y Riesgos.

9. Conclusión

BinnoCredit ofrece acceso a liquidez sin vender activos, con la simplicidad de una tarjeta de crédito y la transparencia de un protocolo on-chain. Su colateral productivo, su LTV conservador, sus liquidaciones automáticas y escalonadas, y su honesto reconocimiento de los riesgos reflexivos lo posicionan como una capa de crédito diseñada para durar, no para maximizar el apalancamiento a costa de la estabilidad. Es la pieza que completa el ecosistema financiero de Binno: pagar, enviar, convertir y —ahora— acceder a crédito, todo sin custodia y sin fricción.

Capítulo 7. Tokenomics — El Token BNN

BNN es el token nativo del ecosistema Binno. Su diseño se rige por un principio innegociable: **todo su valor proviene del uso real del protocolo, nunca de la inflación ni de la especulación.** BNN no es un token de gas ni un instrumento de pago; es el activo que captura el valor económico que el ecosistema genera y lo redistribuye entre quienes lo construyen, lo aseguran y lo usan.

1. Funciones del token

BNN cumple tres funciones económicas claramente delimitadas:

- **Gobernanza** — voto sobre parámetros del protocolo, parámetros económicos, el conjunto de validadores y las expansiones de la red.

- **Staking con rendimiento real** — participación en los ingresos del protocolo mediante un producto de staking desacoplado del consenso; los usuarios obtienen rendimiento sin necesidad de elegir ni asignar validadores.

- **Bond de validador** — garantía económica sujeta a slashing que respalda la seguridad del consenso de BinnoChain.

La característica distintiva y deliberada del diseño es que **BNN no se usa para pagar gas.** El consumo de recursos de la red se mide en una unidad anclada al dólar, y las transacciones internas son gratuitas para el usuario. Esto desacopla el medio de uso de la red de la especulación sobre el token.

2. Suministro y distribución

El suministro total de BNN es **fijo: 1.000.000.000 (mil millones) de tokens**, sin inflación ni emisión futura. La distribución está diseñada para priorizar la comunidad y la descentralización, manteniendo a los participantes internos (equipo, inversores, empresa) en una minoría del suministro:

Categoría	%	Tokens	Propósito
Comunidad / Ecosistema	33%	330.000.000	Recompensas por uso, incentivos a liquidez, adquisición de comercios y POS, airdrop de testnet
Tesorería / DAO	21%	210.000.000	Liquidez del DEX, subsidio de staking de arranque, recompras, reservas
Inversores privados	17%	170.000.000	Early backers (3%) + rondas privadas (14%), todos con vesting
Equipo (Core Team)	15%	150.000.000	Core team, vesting largo.
Venta pública (Public Sale)	7%	70.000.000	Distribución pública con tracción
Company & Advisors	7%	70.000.000	Operación de Binno Labs (4%) y advisors (hasta 3%)
Total	**100%**	**1.000.000.000**	

Esta distribución sitúa a la comunidad, el ecosistema, la tesorería y la venta pública en conjunto en el 61% del suministro, frente al 39% de los participantes internos (equipo, inversores privados, empresa y advisors). Los inversores privados agrupan a los *early backers* (personas cercanas que aportaron el capital inicial más temprano, en la fase de mayor riesgo) y a las rondas privadas de financiación; todos están sujetos a vesting en igualdad de condiciones, sin términos preferentes para los participantes tempranos.

3. Calendario de adquisición (vesting)

El vesting está diseñado a estándar institucional, con la señal deliberada de que **los participantes internos no tienen acceso temprano y soportan los bloqueos más largos**, mientras la comunidad y el mercado acceden antes.

Categoría	TGE	Cliff	Vesting	Nota
Equipo	0%	12 meses	4 años lineal	—
Inversores privados (early + rondas)	0%	6–12 meses	24–36 meses lineal	Sin términos preferentes para early backers
Company & Advisors	0%	6–12 meses	24–36 meses	Advisors con cliff potencialmente menor
Venta pública	10–25%	—	6–12 meses lineal	Liquidez de mercado
Comunidad / Ecosistema	variable	—	Liberación contra métricas de uso, 4–5 años	Por actividad real
Tesorería / DAO	0%	—	Liberación lineal gobernada, 4–5 años	Liquidez y recompras

4. Estrategia de distribución comunitaria (el 34%)

La asignación del 33% a Comunidad/Ecosistema no es un "regalo": es **capital de crecimiento desplegado contra uso real, con vesting, durante 4–5 años.** Su objetivo es construir adopción genuina y descentralización amplia, evitando el

patrón de los airdrops indiscriminados que solo atraen especuladores que venden de inmediato. Los mecanismos son:

- **Recompensas por uso real.** El grueso de la asignación premia actividad económica medible on-chain: volumen de pagos procesado, transacciones cross-chain reales, liquidez aportada y tiempo como usuario activo. Atrae usuarios que *usan* el producto, no cazadores de airdrop.

- **Incentivos a proveedores de liquidez del DEX.** Para sembrar y profundizar la liquidez de los pares críticos, especialmente BNN y stablecoins.

- **Programa de adquisición de comercios y distribuidores de POS.** El diferenciador único de Binno: subsidios en BNN a comercios que procesan volumen real y a distribuidores que activan terminales. Convierte la asignación comunitaria en una fuerza de adopción física —algo que ningún protocolo puramente digital puede replicar—.

- **Recompensas a wallets integradoras.** Incentivos a las wallets de terceros que adopten el estándar @username, acelerando la red.

- **Airdrop retroactivo a usuarios de testnet.** Una porción menor que premia la lealtad temprana y genera prueba social, sin ser el mecanismo principal.

Todos estos mecanismos liberan tokens **contra métricas verificables on-chain y con vesting**, de modo que quien recibe BNN está incentivado a permanecer, no a vender. Es capital de adquisición y retención, medido y plurianual.

5. El flywheel económico

El modelo de captura de valor de BNN es un flywheel financiado por ingresos reales, no por emisiones:

1. El uso del ecosistema (pagos, swaps, crédito) genera **ingresos reales** en comisiones.

2. Los ingresos fluyen a la tesorería, que cubre los costos del protocolo y destina una porción a **recompras de BNN** en el mercado.

3. El **staking** distribuye rendimiento real (proveniente de esos ingresos) a quienes bloquean BNN.

4. Las recompras y el staking reducen el suministro circulante efectivo, mientras el uso crece.

5. Mayor uso → mayores ingresos → mayor capacidad de recompra y rendimiento → mayor incentivo a participar.

Las recompras reducen el suministro circulante; el efecto sobre el valor del token depende de las condiciones de mercado. Este documento no proyecta ni garantiza apreciación de precio.

6. Flujo de ingresos del protocolo

Los ingresos del protocolo no van "100% a la tesorería" de forma indiferenciada; siguen un flujo definido:

Ingresos del ecosistema (Pay, DEX, Credit, Hub)

├─ Porción del integrador → pagada al tercero integrador (o a Binno Labs cuando opera como integrador vía BinnoWallet)

└─ Porción del protocolo → Tesorería

  ├─ Pool de recompensa de validadores (15% del revenue neto)

  ├─ Rendimiento de staking (BNN stakers)

  ├─ Recompras de BNN

  ├─ Fondo de seguro / reservas

  └─ Operación y expansión

El **"exceso de tesorería"** que financia las recompras se define como el revenue neto del protocolo **después** de cubrir todos sus gastos: el pool de validadores, el rendimiento de staking, el fondo de seguro y la operación. Solo el excedente sobre esos compromisos se destina a recompras, garantizando que el flywheel no comprometa la sostenibilidad operativa.

7. Sostenibilidad del staking

El rendimiento del staking de BNN es **variable según el revenue real del protocolo**. En la fase inicial, mientras el revenue orgánico crece, la tesorería puede subsidiar un rendimiento de arranque con la asignación correspondiente (parte del 22%), claramente identificado como un **subsidio de bootstrap decreciente**, no como rendimiento orgánico permanente. A medida que el uso del ecosistema crece, el revenue real sustituye al subsidio. El proyecto no promete una cifra de APR fija y perpetua; describe un objetivo de arranque conocido en la fase inicial que transiciona a un rendimiento variable sostenido por ingresos reales.

8. Estructura legal del token

Siguiendo el estándar de proyectos serios del sector, el token BNN se emite y administra a través de una **fundación independiente (estructura tipo Cayman Foundation)**, separada de la empresa operativa **Binno Labs (constituida en Delaware, EE.UU.)**. Esta separación es deliberada: la empresa desarrolla el software y opera los productos; la fundación custodia el token y la tesorería del protocolo y evoluciona hacia el control de la DAO. La estructura está sujeta a la asesoría legal correspondiente y se detalla en el capítulo de Consideraciones Legales.

Capítulo 8. Gobernanza

La gobernanza de Binno se rige por el principio de **descentralización progresiva y honesta**: el control del protocolo migra gradualmente hacia la comunidad, pero el proyecto es transparente sobre qué está descentralizado y qué no en cada fase.

1. Distinción entre protocolo y empresa

Es fundamental distinguir dos planos:

- **El protocolo Binno** (BinnoChain, BinnoHub, BinnoPay, BinnoDEX, BinnoCredit, el token y la tesorería) avanza hacia el control progresivo de la **DAO**, gobernado por los holders de BNN.

- **Binno Labs** (la empresa) opera productos comerciales sobre el protocolo —como la aplicación BinnoWallet— del mismo modo que cualquier empresa puede construir sobre una infraestructura abierta. Binno Labs no es una DAO ni pretende serlo.

2. Evolución de la gobernanza

- **Fase inicial.** El protocolo arranca con la Fundación Binno gestionando los parámetros críticos y el conjunto de validadores génesis, con mecanismos de seguridad (timelocks, circuit breakers) ya en código. En esta fase, el control de la comunidad sobre el núcleo es limitado, y el proyecto lo declara abiertamente.

- **Fase de transición.** La DAO asume progresivamente el control de los parámetros económicos, las allowlists, la expansión del conjunto de validadores y la asignación de la tesorería, mediante votación de los holders de BNN con timelock.

- **Fase de madurez.** El protocolo opera bajo control sustancial de la DAO, con la Fundación en un rol de facilitación.

3. Alcance de la gobernanza

La DAO gobierna el protocolo y sus parámetros. Los productos comerciales operados por Binno Labs (como BinnoWallet y sus servicios) no son gobernados por

la DAO, igual que la DAO no gobierna a ningún tercero que construya sobre el protocolo. Los pagos a Binno Labs por su trabajo de desarrollo y operación se realizan mediante grants de la tesorería basados en hitos, de forma transparente y verificable.

4. Transparencia del modelo de confianza

En coherencia con todo el proyecto, la gobernanza se describe con honestidad sobre sus límites en cada fase. El valor de Binno se construye sobre afirmaciones verificables y sobre una ruta creíble de descentralización, no sobre la pretensión de una descentralización total e inmediata que sería falsa.

Capítulo 9. Estrategia Go-to-Market

La tecnología de Binno resuelve un problema real, pero el éxito depende de la adopción. Binno reconoce con honestidad que su mayor desafío no es técnico, sino la conquista del clásico problema del "huevo y la gallina" de toda red de pagos: los comercios aceptan un medio de pago si los usuarios lo usan, y los usuarios lo usan si los comercios lo aceptan. La estrategia está diseñada para romper ese ciclo de forma deliberada y por fases, no por difusión espontánea.

1. El beachhead: corredores de remesas y economías dolarizadas de facto

En lugar de atacar "el mundo", Binno comienza por nichos donde el dolor es máximo y la adopción de stablecoins ya es una realidad por necesidad económica:

- **Corredores de remesas de alto costo** (por ejemplo, Estados Unidos hacia América Latina), donde el costo actual de enviar dinero ronda o supera el 6,5% y donde el receptor a menudo ya prefiere preservar valor en dólares digitales.

- **Economías con alta dolarización de facto y adopción de stablecoins** (varios países de América Latina), donde trabajadores y freelancers ya cobran en USDT pero carecen de una forma simple de gastarlo en su vida diaria.

- **Mercados con penetración masiva de pagos por QR y NFC** (América Latina y Sudeste Asiático), donde la infraestructura de aceptación y el hábito del usuario ya existen.

El usuario inicial natural es **quien ya tiene stablecoins y no puede gastarlas fácilmente**: ese usuario tiene una necesidad inmediata que Binno resuelve, sin necesidad de evangelizar sobre cripto.

2. La palanca de distribución: integradores, no comercios uno a uno

Binno no busca convencer a comercios individuales uno por uno. Su modelo de distribución se apoya en **integradores** —distribuidores y fabricantes de terminales POS, fintechs y wallets— que ya tienen relación con miles de comercios. Un solo

acuerdo con un distribuidor de POS pone a BinnoPay en manos de su red completa. El revenue-share y los incentivos en BNN (del 33% de Comunidad/Ecosistema) alinean el interés del integrador con la adopción real, no con la mera distribución de hardware.

3. Fases de adopción

- **Fase 1 — Validación.** Demostración funcional (pago NFC real desde wallet no custodial), pilotos de usabilidad con comercios y usuarios reales, y obtención de cartas de intención con integradores. El objetivo es probar que el producto funciona y es usable en condiciones reales.

- **Fase 2 — Beachhead.** Despliegue en un corredor de remesas y un mercado local específicos, con programas de arranque para comercios (incentivos de adopción) y campañas dirigidas a usuarios que ya poseen stablecoins.

- **Fase 3 — Expansión.** Replicación del modelo a nuevos corredores y mercados, integración con más distribuidores de POS y wallets, y consolidación del estándar @username.

4. Honestidad sobre el estado actual

Binno aún no cuenta con cartas de intención firmadas ni acuerdos de distribución cerrados; ha priorizado construir tecnología funcional antes de comprometer adopción. La validación de demanda con integradores y comercios reales es el foco inmediato del uso de fondos de la primera ronda. Esta transparencia es deliberada: el proyecto no presenta hipótesis de adopción como si fueran tracción comprobada.

Capítulo 10. Hoja de Ruta (Roadmap)

El roadmap refleja el estado real del proyecto y una secuencia técnica con dependencias explícitas, no una lista de promesas.

1. Estado actual (2026)

- **BinnoChain:** operativa en testnet (Avalanche L1 sobre HyperSDK con consenso Snowman++).
- **BinnoHub:** funcional en testnet, ejecutando transacciones cross-chain reales vía LayerZero entre Ethereum y BNB Chain mediante receiving addresses.
- **BinnoWallet (MPC):** construida en testnet, bajo pruebas.
- **BinnoPay:** pago con NFC y QR construido, bajo pruebas.

2. Fases siguientes

- **Tras la ronda de financiación:** ampliación del equipo de desarrollo; auditorías de seguridad con firmas reconocidas (consenso, BinnoVM, contratos de SatelliteHubs, MPC); finalización de BinnoWallet y BinnoPay; expansión de la cobertura de cadenas.
- **Camino a mainnet:** endurecimiento de seguridad, programa de bug bounty, conjunto de validadores génesis, y pruebas de carga públicas con metodología documentada sobre el hardware de validador de referencia.
- **Lanzamiento de mainnet y TGE:** activación de la red principal, generación del token (TGE) y venta pública en torno al lanzamiento de mainnet.
- **Post-mainnet:** despliegue del estándar @username con integradores, expansión de BinnoCredit y BinnoDEX, y transición progresiva de la gobernanza hacia la DAO.

(Las fechas específicas se ajustan al progreso real y se comunican de forma responsable; el proyecto evita comprometer fechas que dependan de auditorías y validaciones de seguridad aún no completadas.)

3. Proyecciones — escenarios, no promesas

Binno opera en mercados de gran tamaño (pagos digitales, remesas, stablecoins), y su potencial de largo plazo es significativo si la adopción se materializa. No obstante, este documento **no presenta proyecciones de usuarios, volumen o ingresos como cifras garantizadas ni como "escenarios conservadores".** Cualquier proyección debe entenderse como un escenario ilustrativo, dependiente de la ejecución, la adopción y las condiciones de mercado, y anclado al porcentaje del mercado direccionable que el proyecto logre capturar. El valor de Binno se sustenta en su tecnología verificable y en la magnitud del problema que resuelve, no en proyecciones optimistas.

Capítulo 11. Equipo

Binno es construido por un equipo que combina obsesión por el problema con experiencia directa en infraestructura de pagos.

- **José Daniel Ramírez — CEO y Fundador.** Ingeniero civil de formación, inmerso en el ecosistema cripto desde 2015. La visión de Binno nació de ocho años estudiando y viviendo el problema de la fricción de los pagos y la dependencia de intermediarios. No es un fundador técnico de código, sino un fundador de producto y visión, obsesionado con resolver un problema concreto y con la capacidad de orquestar el equipo que lo ejecuta.

- **Leonardo Melendez— Ingeniero Senior / Co-fundador técnico.** Más de 12 años de experiencia en desarrollo de software, con trayectoria internacional en sistemas de pago bancarios y terminales POS.

- **Leonardo Alvarado— Ingeniero Senior.** Más de 12 años de experiencia, con experiencia directa en infraestructura de pagos y POS a nivel bancario.

- **Luis Lugo — Diseño de Producto y Experiencia.** Responsable del diseño de las interfaces y la comunidad.

Fortaleza del equipo. La experiencia directa de los ingenieros en pagos bancarios y POS es especialmente relevante: el reto de Binno es, en gran medida, de infraestructura de pagos, y el equipo conoce ese dominio de primera mano.

Capítulo 12. Seguridad y Contingencia

La seguridad de Binno se aborda en capas, y el proyecto es explícito tanto sobre sus defensas como sobre los riesgos que asume.

1. Seguridad por capa

- **Consenso:** finalidad rápida, muestreo probabilístico resistente a colusión, validadores calificados con bonds slasheables.
- **Ejecución (BinnoVM):** VM especializada con módulos nativos auditados, sin la superficie de ataque de una plataforma de contratos arbitrarios.
- **Custodia (BinnoWallet):** MPC sin clave única reconstruible, con umbrales de firma y recuperación separados.
- **Interoperabilidad (BinnoHub):** Security Stack de 2-de-3 DVNs, autenticación de peer, nonces globales y prevención de replay.
- **Auditoría:** todos los componentes críticos se someten a auditoría externa independiente antes de mainnet, con programa de bug bounty continuo.

2. Manejo de fallos cross-chain

Las operaciones cross-chain emplean mensajería **non-blocking**: un fallo de ejecución en destino no bloquea la cola ni hace desaparecer fondos; el mensaje fallido se almacena y puede reintentarse, y si no se completa, se ejecuta un reembolso verificable al origen.

3. Dependencia de terceros (declaración honesta)

Binno depende de **LayerZero V2 (y Stargate)** como capa de interoperabilidad y liquidez cross-chain para activos no-OFT. Es una dependencia consciente, elegida por ser la infraestructura más madura del mercado. Se mitiga mediante: la Security Stack multi-DVN (que requiere corromper varios verificadores independientes para falsificar un mensaje), la capacidad de operar un DVN propio como contingencia, y un circuit breaker que pausa la mensajería ante anomalías protegiendo los fondos. Reemplazar la capa de interoperabilidad por otra (Wormhole, Axelar, CCIP) sería un

esfuerzo de ingeniería significativo, dado que el estándar OFT es propio de LayerZero; el proyecto asume esta dependencia con transparencia.

4. Otros vectores

- **MEV / reordenamiento:** al controlar su propio secuenciamiento y operar con validadores de peso igualitario sin subasta de blockspace, BinnoChain mitiga estructuralmente la extracción de valor por reordenamiento, especialmente irrelevante para flujos de pago.

- **Disponibilidad del estado:** todo el estado crítico reside on-chain en BinnoChain, accesible mediante exploradores y servicios de terceros, sin depender de la infraestructura de Binno Labs.

Riesgos

Binno presenta sus riesgos con honestidad. Un proyecto que oculta sus riesgos es menos confiable que uno que los reconoce y los mitiga.

- **Riesgo de adopción.** El mayor riesgo del proyecto. Romper el ciclo "huevo y gallina" de una red de pagos es difícil y no está garantizado. *Mitigación:* estrategia de beachhead enfocada, distribución vía integradores, e incentivos del 33% de Comunidad/Ecosistema.

- **Riesgo de ejecución de una L1 soberana.** Operar y asegurar una L1 es costoso y complejo. *Mitigación:* apoyo en el marco de Avalanche, modelo de validadores diseñado para rendimiento, y uso de fondos enfocado en desarrollo y auditoría.

- **Riesgo de dependencia de terceros.** Dependencia de LayerZero/Stargate y de oráculos (Chainlink). *Mitigación:* multi-DVN, DVN propio, circuit breaker, oráculos redundantes.

- **Riesgo regulatorio.** Un sistema de pagos no custodial a escala atraerá escrutinio (AML, transmisión de dinero) en algunas jurisdicciones. *Mitigación:* protocolo neutral que no toca fiat, conversión a fiat empujada fuera del protocolo, estructura legal Delaware + Cayman, y asesoría legal continua.

- **Riesgo reflexivo del token.** BNN como colateral en BinnoCredit conlleva riesgo de espiral en caídas fuertes. *Mitigación:* límites de exposición, liquidación escalonada, y backstop de tesorería sin venta de mercado.

- **Riesgo de mercado y financiación.** La capacidad de completar el desarrollo depende de la financiación; las condiciones de mercado cripto son volátiles. *Mitigación:* dimensionamiento prudente del capital, hitos claros, y secuencia de financiación por etapas.

- **Riesgo de equipo.** Equipo sin experiencia previa en cripto en producción. *Mitigación:* auditorías Tier-1, incorporación de advisors con experiencia cripto, y experiencia directa del equipo en infraestructura de pagos.

Consideraciones Legales

- **Estructura.** El ecosistema se organiza en dos entidades: **Binno Labs, Inc. (Delaware, EE.UU.)** como empresa operativa que desarrolla el software y opera los productos, y una **fundación independiente (estructura tipo Cayman)** que emite y administra el token BNN y la tesorería del protocolo, evolucionando hacia la gobernanza de la DAO. Esta estructura está sujeta a la asesoría legal correspondiente.

- **Naturaleza del token.** BNN es un token de utilidad y gobernanza del protocolo, no un instrumento de inversión ni una promesa de rendimiento. Su valor depende del uso del protocolo y de las condiciones de mercado.

- **No es asesoría.** Este documento es informativo y no constituye asesoría financiera, legal, fiscal o de inversión, ni una oferta de venta de valores. La participación en cualquier ronda de financiación o venta de tokens está sujeta a los términos legales correspondientes y a las restricciones de cada jurisdicción.

- **Cumplimiento.** El protocolo está diseñado como infraestructura neutral y no custodial. Los servicios regulados (como la conversión a moneda fiduciaria) quedan fuera del protocolo, en manos de terceros licenciados que el usuario o comercio elige libremente. El cumplimiento regulatorio varía por jurisdicción y evoluciona; Binno lo aborda con asesoría profesional.

Glosario

- **@username** — identidad universal única y global que reemplaza las direcciones del usuario en todas las cadenas.

- **Avalanche L1 soberana** — red independiente con su propio consenso, validadores y reglas, bajo el marco de Avalanche (post-ACP-77).

- **BinnoVM** — la máquina virtual propia de BinnoChain, construida sobre HyperSDK, especializada en pagos e identidad.

- **Bond (de validador)** — colateral económico slasheable que un validador deposita como garantía de buen comportamiento.

- **CLMM** — Concentrated Liquidity Market Maker; modelo de DEX que concentra la liquidez para mayor eficiencia de capital.

- **DVN** — Decentralized Verifier Network; red de verificadores de LayerZero que confirma la integridad de los mensajes cross-chain.

- **FDV** — Fully Diluted Valuation; valoración teórica del proyecto si todo el supply de tokens estuviera en circulación.

- **Finalidad** — momento en que una transacción se vuelve irreversible.

- **Gas sponsoring / transacciones internas gratuitas** — modelo por el cual el usuario no paga por transaccionar dentro de BinnoChain; el costo estructural lo cubre el modelo de recompensa de validadores.

- **MPC (Multi-Party Computation)** — técnica criptográfica que distribuye una clave en fragmentos, de modo que nunca se reconstruye por completo.

- **OFT (Omnichain Fungible Token)** — estándar de LayerZero para tokens que se mueven entre cadenas quemándose en origen y acuñándose en destino, sin necesidad de liquidez.

- **Receiving address** — dirección determinística que permite recibir valor desde wallets que aún no integran @username; mecanismo de transición.

- **SAFE / SAFT** — instrumentos de inversión para recibir equity futuro (SAFE) o tokens futuros (SAFT/warrant).

- **SatelliteHub** — contrato ultraligero en cada cadena externa que conecta con BinnoHub.

- **Slashing** — confiscación parcial o total del bond de un validador por mal comportamiento.

- **Snowman++** — mecanismo de consenso de Avalanche, de muestreo sub-seleccionado, con overhead independiente del número de validadores.

- **Stablecoin** — token anclado al valor de una moneda fiduciaria (USDC, USDT, etc.).

- **Stargate** — capa de liquidez de LayerZero para mover activos no-OFT (como USDC/USDT) entre cadenas.

- **TGE (Token Generation Event)** — momento en que el token se genera y comienza a cotizar.