PBC

PRIVACY BANK CHAIN

P B C

«Private money that works for you.»

La primera cadena de bloques que une la privacidad de Monero con auténticas herramientas bancarias nativas — y resistentes a lo cuántico.

Sin contratos inteligentes. Sin oráculos. Sin custodia. Sin tail emission.
Solo C++ verificable, determinista y con una oferta estrictamente finita.

Depósitos a plazo 2 **Mercado de bonos on-chain** 2 **Herencia sin confianza** 2 **Poscuántico híbrido**

Documento de presentación — 2026

El dilema que nadie había resuelto

PRIVACIDAD O RENTABILIDAD — HABÍA QUE ELEGIR

Monero resolvió la privacidad. Tus monedas son invisibles, imposibles de rastrear, fungibles. Pero una vez en tu monedero… duermen. Sin rendimiento, sin ahorro, sin transmisión. Dinero digital, nada más.

Las finanzas descentralizadas (Ethereum y sus clones) ofrecen depósitos, rendimiento y seguros — pero cada transacción, cada saldo y cada posición son públicos. Todo se apoya en contratos inteligentes: código que se puede hackear, modificar y controlar mediante claves de administración. Más de 2.000 millones de dólares fueron robados por fallos de contratos en 2023-2024.

> **La elección impuesta hasta ahora**
>
> - **A — La privacidad (Monero)** — tus monedas están protegidas, pero inertes.
> - **B — La rentabilidad (DeFi)** — tus monedas trabajan, pero todo el mundo te observa.

Privacy Bank Chain elimina ese dilema. Todas las herramientas financieras están codificadas directamente en el protocolo, en C++, validadas por consenso en cada bloque. Sin máquina virtual, sin capa 2, sin interfaz alojada, sin custodia de terceros.

Cómo funciona, en una frase

> **Depositas monedas, generan rendimiento, y nadie sabe que eres tú.**
>
> Se sabe CUÁNTO. Nunca se sabe QUIÉN.

La transparencia híbrida — un enfoque inédito

Los importes de las operaciones financieras son públicos: el consenso los necesita para calcular los pesos y repartir las recompensas hasta la última moneda. Pero las identidades permanecen ocultas tras las firmas en anillo y las direcciones sigilosas de CryptoNote.

Un observador ve que «alguien depositó 10.000 PBC durante 1 año». No puede identificar el monedero ni vincular ese depósito con un futuro retiro o una reclamación. Esto es estrictamente superior a todas las DeFi, donde los importes Y las identidades son totalmente públicos.

	Transferencias	Importes de las operaciones	Identidad
Monero	Privadas (RingCT)	—	—
DeFi Ethereum	Ninguna	Públicos	Pública
PBC	Privadas (RingCT)	Públicos (por diseño)	Privada (firma en anillo)

Las funciones que cambian las reglas del juego

Cada una es nativa, escrita en C++ y verificada por consenso — y ya está cubierta por baterías de pruebas automatizadas (depósitos, reclamaciones, herencia, mercado, poscuántico: cientos de verificaciones superadas).

01 Depósitos a plazo con rendimiento real

Bloquea tus PBC de 30 días a 1 año y percibe un rendimiento financiado por la emisión monetaria, no por deuda. Cinco tramos de duración, con un multiplicador creciente que premia la paciencia.

- **Recompensas por reclamación**: reclamas tus ganancias cuando quieras. Sin pagos masivos en la coinbase, sin inflar los bloques, sin excluir a los pequeños depositantes.
- **Antifraccionamiento por construcción**: el peso es lineal (importe × multiplicador de duración). Trocear un depósito grande en varios pequeños nunca rinde más.
- **Sin comisión de apertura**: al abrir un depósito solo se aplica la comisión de red estándar.
- **Principal bloqueado hasta el vencimiento**: el capital queda inmovilizado a nivel de consenso (salida UTXO bloqueada hasta la madurez), mientras que las recompensas siguen siendo reclamables en todo momento.
- Salida antes del plazo: cede tu depósito en el mercado secundario al precio que tú fijes (función 06) — cero ventanillas, cero intermediarios, sin penalización.

02 Redistribución de comisiones — rendimiento real

Las comisiones de cada transacción de la red se reparten en dos mitades iguales: **50 % para los mineros, 50 % para los depositantes**, estos últimos mediante un segundo índice global independiente. Cuanto más activa es la red, más sube tu rendimiento. Es rendimiento procedente de una actividad económica real, no de inflación disfrazada.

- **Un reparto impuesto por el consenso**: la parte del minero se calcula al construir la coinbase y se vuelve a verificar al validar cada bloque. Ningún minero puede atribuirse más de su mitad.
- **Doble fuente de ingresos**: Deposit Pool (emisión) + Fee Pool (comisiones de red), reclamados en el mismo momento.
- **Círculo virtuoso para los mineros**: el rendimiento atrae al ahorrador, que bloquea oferta, lo que sostiene estructuralmente la cotización de la moneda que minan.
- **Comisiones autoajustadas**: el suelo de comisiones de la red sube automáticamente con la proporción de ahorro bloqueado (hasta ×2). Cuanto más se adopta PBC, más remunera el Fee Pool, por construcción.

03 Vesting antidumping de las recompensas de minería

Cada recompensa de bloque de un minero se fracciona en 4 salidas con desbloqueo escalonado: ~24 h, ~30 d, ~60 d y ~90 d. Es imposible venderlo todo de golpe el día del minado: la presión vendedora se suaviza y la cotización se estabiliza. El vesting lo impone el consenso, directamente sobre la coinbase: ningún software de pool puede eludirlo.

04 Fondo de seguro, deflación automática — y oferta finita

El 1 % de cada bloque alimenta un Insurance Pool. Una red de seguridad nativa que sostiene los rendimientos en periodos de baja actividad: automática, con tope, sin gobernanza ni votaciones.

El tope del fondo es de 184.467 PBC, exactamente el 1 % de la oferta máxima. Todo excedente se quema definitivamente, en cada bloque, por consenso: una deflación determinista, sin quema manual, sin decisión de equipo, sin claves de administración.

- **El contraste con Monero**: Monero y los forks de CryptoNote emiten hasta el infinito (tail emission perpetua). PBC tiene una oferta estrictamente finita —18.446.744 PBC, ni uno más— Y quema sus excedentes. El contraste es total.
- **Estabilidad por diseño**: por encima del 60 % de la oferta circulante bloqueada en depósitos, un estabilizador (Locked Supply Multiplier) amortigua automáticamente la distribución para preservar la liquidez de la red: los rendimientos siguen siendo sanos, nunca reflexivos.

05 Herencia sin confianza — el «Dead Man's Switch»

Una primicia en una cadena de bloques con privacidad. Designa a un heredero; si te ocurre algo, presenta una solicitud on-chain — y si no das ninguna señal de vida durante 18 meses, tus fondos, incluidos tus depósitos en curso y tu saldo líquido, le son transferidos automáticamente por el consenso.

- **Cero terceros de confianza**: sin notario, sin abogado, sin tribunal. Solo consenso.
- **Un plazo grabado en el protocolo**: el plazo de 18 meses es una regla de consenso, idéntica para todos; el heredero nunca puede acelerarlo ni modificar la configuración.
- **Mantienes el control total**: cualquier operación firmada con tu clave de gasto (nuevo depósito, retiro, reconfiguración de la herencia) anula la solicitud en curso. Y puedes revocar la designación en cualquier instante, con una sola transacción.
- **Testamento automático**: tu monedero mantiene automáticamente un «testamento» prefirmado que cubre tu saldo líquido, refirmado en cuanto tu saldo evoluciona — y respaldado on-chain para sobrevivir a todo.
- **Bloqueado por el consenso**: un cerrojo de consenso hace imposible toda ejecución prematura del testamento; antes del vencimiento, la red entera la rechaza.
- **Confidencial**: tanto la identidad del propietario (firma en anillo) como la del heredero (dirección sigilosa) permanecen ocultas. Se ve que existe una herencia, jamás a quién concierne.
- **Robusto**: estado reconstruido de forma determinista tras cualquier reorganización de la cadena.

06 Mercado de bonos on-chain — tus depósitos son bonos

Un depósito a plazo PBC es, económicamente, un bono privado al portador: un principal, un vencimiento, un rendimiento. PBC lo convierte en un título libremente negociable: el primer mercado de bonos nativo en una cadena con privacidad de tipo Monero. ¿Necesitas liquidez antes del plazo? Cede tu depósito a un comprador, íntegramente on-chain, sin terceros de confianza y sin penalización.

El comprador inmoviliza el importe de compra en un cerrojo de garantía (collateral lock), exactamente como un depósito inmoviliza su principal. La transferencia es después atómica, en un solo bloque: el depósito pasa al comprador, el pago va al vendedor. Todo o nada.

Y sobre todo: ninguna suma confiscada, ninguna comisión cobrada. Allí donde un banco impone su penalización de salida, PBC te deja soberano: tú fijas tu precio, vendes cuando lo decides, a quien quiera comprar. Decide el mercado, libremente, no un intermediario.

- **Seguro de extremo a extremo**: cancelación voluntaria del comprador, expiración automática de los cerrojos con devolución de la garantía, transferencia validada contra el cerrojo y restauración íntegra en caso de reorganización de la cadena.
- **Precio libre**: cede tu depósito por encima o por debajo del principal según la urgencia de tu necesidad de liquidez: el arbitraje es tuyo.

07 Resistencia poscuántica híbrida — nativa desde el lanzamiento

La ventaja decisiva. Monero, Zcash y todos los forks de CryptoNote actuales no tienen ninguna resistencia cuántica, ni siquiera un plan a corto plazo. Un ordenador cuántico suficientemente potente podría algún día romper sus firmas y desanonimizar todo su historial.

PBC integra una protección híbrida: a los mecanismos clásicos (Ed25519) se suman, en paralelo, primitivas poscuánticas normalizadas por el NIST.

- **Firmas**: ML-DSA-65 (Dilithium, NIST FIPS 204). Desde el hard fork de activación, toda autorización de retiro de depósito o de pago de mercado exige esta cofirma además de la firma clásica.
- **Intercambio de claves sigilosas**: ML-KEM-768 (Kyber, NIST FIPS 203) combinado con el ECDH clásico mediante derivación HKDF, con direcciones v2 que comprometen las claves poscuánticas.
- **Dos capas, una garantía**: si Ed25519 cae mañana, lo poscuántico aguanta; si un fallo afecta a Dilithium, aguanta lo clásico. La seguridad está garantizada mientras resista una de las dos capas. PBC sería la primera cadena con privacidad de tipo Monero con resistencia cuántica híbrida tanto en las firmas COMO en el intercambio de claves.

08 Un banco completo, en tu casa — la WebUI

Todas estas funciones se pilotan desde una interfaz web local incluida, conectada exclusivamente a tu propio nodo: panel de control, depósitos y reclamaciones en un clic, alertas de herencia en tiempo real, mercado de bonos integrado. Cero nube, cero cuenta, cero custodia: tus claves nunca salen de tu máquina.

Seguridad: cero concesiones

SIN MÁQUINA VIRTUAL · SIN CUSTODIA · SIN CLAVES DE ADMINISTRACIÓN

Sin contratos inteligentes = sin hackeos

Cada función se compila en C++ y la valida el consenso. Sin máquina virtual, sin bytecode interpretado, sin superficie de ataque ampliable. El código es fijo, auditable e idéntico en cada nodo.

Sin custodia de terceros = sin phishing

PBC se usa mediante un monedero CLI o RPC en local. Sin custodia de terceros, sin interfaz alojada que hackear, sin claves en la memoria del navegador. Tus claves nunca salen de tu máquina. (Una interfaz de gestión local opcional se conecta únicamente a tu propio nodo.)

Solvencia demostrada matemáticamente

El mecanismo de índice global garantiza por construcción que la suma de todas las recompensas reclamables nunca puede superar el saldo del pool correspondiente: suma de las recompensas por periodo = variación exacta del pool. Aunque todos los depositantes reclamaran a la vez, el sistema seguiría siendo solvente. Nunca se promete ningún tipo fijo: todo tipo fijo crearía una deuda implícita que la cadena no puede garantizar.

Fondo de desarrollo transparente por construcción

La clave de visualización del fondo de desarrollo está publicada en el código fuente: cualquiera puede auditar cada entrada del fondo, de forma permanente. Un 2 % por bloque, ni más ni menos, verificado por todos los nodos y visible para todos.

Minería CPU descentralizada, compatible con pools

Minería RandomX v2 (variante rx/pbc), solo CPU y resistente a ASIC. Compatible con cualquier pool Stratum existente, sin ninguna modificación: los mineros solo ven la estructura coinbase estándar. Todas las funciones financieras son operaciones de monedero.

Tokenómica

SIN PREMINADO · SIN ICO · SIN TOKENS RESERVADOS

Sin preminado. Sin ICO. Sin tokens reservados. Una oferta estrictamente finita de 18.446.744 PBC. Cada bloque se reparte así:

Asignación por bloque	Parte	Destino
Mineros	91 % de R + 50 % de las comisiones	4 salidas con vesting (antidumping)
Fondo de desarrollo	2 % de R	Apoyo al proyecto (auditable por todos)
Fee Pool	3,5 % de R + 50 % de las comisiones	Rendimiento de las comisiones de red
Deposit Pool	2,5 % de R	Rendimiento de los depósitos a plazo
Insurance Pool	1 % de R	Red de seguridad + deflación (quema)

Parámetro	Valor
Algoritmo	RandomX v2 — variante rx/pbc (solo CPU, anti-ASIC)
Tiempo de bloque	1 minuto (1.440 bloques/día)
Periodo de distribución	~1 día (1.440 bloques)
Oferta máxima	18.446.744 PBC — cero tail emission
Recompensa en el génesis (R)	~4,40 PBC/bloque (decrecimiento suave)
Tramos de depósito	30 / 90 / 180 / 270 / 365 días
Multiplicadores de duración	1,0× — 1,3× — 1,6× — 1,8× — 2,0×
Depósito mínimo	10 PBC
Depósitos activos por dirección	10 como máximo
Salida antes del vencimiento	Mercado secundario (precio libre)
Plazo de herencia	18 meses (consenso)
Prefijo de dirección	«Pbc...»
Privacidad	CryptoNote (RingCT, firma en anillo, sigilosas) + PQC híbrida

> **Estrategia «Mine & Deposit»**
>
> PBC está diseñada para que minería y depósitos se compongan. Minas PBC y luego los depositas para generar un rendimiento adicional: una doble fuente de ingresos con el mismo capital de hardware. Los primeros depositantes captan mecánicamente los rendimientos más altos: el pastel (6 % de cada bloque + 50 % de las comisiones) se reparte entre muy pocos al arranque.

Proyecciones de rentabilidad

CIFRAS ILUSTRATIVAS — NO SON UNA PROMESA DE RENDIMIENTO

Cifras ilustrativas, calculadas sobre los parámetros del protocolo (bloque de 1 minuto) y el modelo de peso lineal.

Hipótesis de cálculo

Parámetro	Valor
Hashrate de la red	15 MH/s
Potencia de un AMD Ryzen 9 9950X	~23 KH/s (RandomX v2)
Equivalente de red	~652 máquinas 9950X
Ritmo de bloque	1 minuto (1.440 bloques/día)
Recompensa en el génesis (R)	~4,40 PBC/bloque
Emisión diaria	~6.333 PBC/día
Oferta máxima	18.446.744 PBC
Minería mediante pools	~80 % del hashrate

Ingresos de minería

El 91 % de cada recompensa de bloque va a los mineros (con vesting en 4 tramos), es decir ~5.763 PBC/día a repartir a prorrata de la potencia — a lo que se añade la mitad de las comisiones de red:

Configuración	Al día	Al mes	Al año
1 × 9950X (23 KH/s)	~8,8 PBC	~265 PBC	~3.225 PBC
3 × 9950X (69 KH/s)	~26,5 PBC	~795 PBC	~9.675 PBC
5 × 9950X (115 KH/s)	~44,2 PBC	~1.325 PBC	~16.125 PBC
10 × 9950X (230 KH/s)	~88,4 PBC	~2.650 PBC	~32.250 PBC

Nota: ingresos en PBC, sin contar el valor fiat ni la parte de las comisiones de red. Si la dificultad se duplica, el ingreso por máquina se divide por dos.

Rendimiento de los depósitos

El rendimiento depende del peso total de los depositantes: cuantos más son, más se reparte el pastel. El Deposit Pool y el Fee Pool reciben juntos el 6 % de cada bloque (~380 PBC/día) más el 50 % de las comisiones de red. Tres escenarios para un depósito único de 10.000 PBC a 365 días (multiplicador 2,0×):

Escenario	Deposit Pool	Fee Pool	Total/año	APY
Early Bird (~50 depositantes)	~11.860 PBC	~16.750 PBC	~28.610 PBC	~286 %
Crecimiento (~500)	~1.460 PBC	~2.060 PBC	~3.520 PBC	~35 %
Maduro (~2.000)	~460 PBC	~650 PBC	~1.110 PBC	~11 %

> **¿Por qué el Early Bird es tan elevado?**
>
> Con pocos depositantes, el flujo diario se reparte entre muy poca gente. Esos rendimientos elevados atraen rápidamente a nuevos depositantes, lo que hace converger de forma natural el APY hacia los escenarios siguientes. El sistema respira: las salidas al vencimiento hacen subir de nuevo el APY de los fieles.

Simulaciones — tres perfiles de ahorrador

Tres ejemplos concretos, con condiciones de red constantes durante la duración del depósito. En todos los casos el principal se restituye al 100 % al vencimiento: las ganancias se suman, y puedes reclamarlas en cualquier momento, sin tocar el depósito, incluso después del vencimiento.

Perfil	Early Bird (~50)	Crecimiento (~500)	Maduro (~2.000)
Prudente — 1.000 PBC / 90 d (×1,3)	~460 PBC (+46 %)	~56 PBC (+5,6 %)	~18 PBC (+1,8 %)
Equilibrado — 5.000 PBC / 180 d (×1,6)	~5.640 PBC (+113 %)	~695 PBC (+13,9 %)	~220 PBC (+4,4 %)
Convicción — 10.000 PBC / 365 d (×2,0)	~28.610 PBC (+286 %)	~3.520 PBC (+35 %)	~1.110 PBC (+11 %)

- **El reflejo early bird**: 1.000 PBC bloqueados 3 meses en fase de lanzamiento pueden generar ~460 PBC de ganancias: casi la mitad del capital, en 90 días.
- **Cero capital sacrificado**: las ganancias se reclaman cuando quieras, el principal vuelve íntegro al vencimiento — y mientras tanto tu depósito sigue siendo cedible en el mercado de bonos.
- **Lectura honesta**: ganancias en PBC, sin contar la evolución de la cotización; porcentajes calculados sobre la duración real del depósito, no anualizados.

Estrategia combinada: Mine + Deposit

Ingreso total = minería + rendimiento de los depósitos (sobre 10.000 PBC depositados). Comparado con la minería sola:

Con 1 × 9950X (minería ~3.225 PBC/año)

Escenario	Minería	Depósitos	Total	vs minería sola
Early Bird	3.225 PBC	28.610 PBC	31.835 PBC	× 9,9
Crecimiento	3.225 PBC	3.520 PBC	6.745 PBC	× 2,1
Maduro	3.225 PBC	1.110 PBC	4.335 PBC	× 1,3

Con 10 × 9950X (minería ~32.250 PBC/año)

Escenario	Minería	Depósitos	Total	vs minería sola
Early Bird	32.250 PBC	28.610 PBC	60.860 PBC	× 1,9
Crecimiento	32.250 PBC	3.520 PBC	35.770 PBC	× 1,1
Maduro	32.250 PBC	1.110 PBC	33.360 PBC	× 1,03

Sin tipo fijo — un índice, no una promesa

Tu recompensa = peso × (índice actual − índice de entrada). El índice solo sube; tus ganancias adquiridas nunca disminuyen. El APY mostrado es un cálculo retroactivo que fluctúa periodo tras periodo, como un cuentakilómetros que nunca retrocede.

Advertencia — Estimaciones ilustrativas, en ningún caso una promesa de rendimiento. El rendimiento real depende del número de participantes, del volumen de transacciones, del hashrate de la red y de la cotización del PBC. Los parámetros finales se fijarán antes del bloque génesis y pueden diferir de estos valores.

PBC frente a lo existente

COMPARATIVA FUNCIÓN POR FUNCIÓN

	PBC	Monero	DeFi Ethereum
Privacidad de las transferencias	**Total (RingCT)**	Total	Ninguna
Privacidad de la identidad	**Firmas en anillo**	Firmas en anillo	Pública
Oferta monetaria	**Finita (18,45 M) + quema**	Infinita (tail emission)	Variable
Depósitos a plazo nativos	**Sí (5 tramos)**	No	Sí (contrato)
Rendimiento real	**Emisión + comisiones**	No	Variable (riesgo)
Herencia on-chain	**Sí (1.ª en cadena privada)**	No	No
Mercado de bonos (depósitos cedibles)	**Sí (atómico)**	No	Parcial
Resistencia poscuántica	**Híbrida nativa**	No	No
Deflación automática	**Sí (quema del seguro)**	No	Variable
Prueba de solvencia	**Formal**	—	No
Dependencia de oráculos	**Ninguna**	Ninguna	Crítica
Riesgo de contrato inteligente	**Cero**	Cero	Alto
Minería CPU (RandomX v2)	**Sí**	Sí	No (PoS)

¿Para quién es PBC?

CUATRO PERFILES, UNA CADENA

Los holders a largo plazo

¿Tus monedas no hacen nada? Depositálas. El rendimiento es real, no especulativo, y tu privacidad queda intacta.

Los mineros

Minería CPU RandomX v2, compatible con todas las pools Stratum. El 91 % del bloque para el minero, más la mitad de las comisiones de cada transacción de la red, con vesting antidumping que sostiene la cotización. Mina y luego deposita: doble ingreso.

Quienes cuidan su privacidad

Transferencias CryptoNote completas (RingCT, direcciones sigilosas). Sin KYC, sin rastro, sin monedero de terceros — y con una protección que anticipa la era cuántica.

Quienes planifican el futuro

La herencia sin confianza transmite tus fondos sin notario, sin tribunal y sin revelar tu identidad. El mercado secundario te ofrece una puerta de salida líquida en todo momento.

En resumen

La privacidad de Monero + el rendimiento de las DeFi + una oferta finita + la herencia sin confianza + la resistencia cuántica.

Sin oráculos. Sin custodia. Sin claves de administración. Solo criptografía y matemáticas.

Lo que ninguna otra cadena de bloques reúne

LA DIFERENCIA PBC

- **Depósitos a plazo integrados** — un producto de ahorro con rendimiento real, en el corazón del consenso, sobre una cadena tan privada como Monero. Inédito.
- **Redistribución de comisiones integrada** — las comisiones de la red se reparten 50/50 entre mineros y depositantes: rendimiento procedente de la actividad real, no de la inflación.
- **Mercado de bonos integrado** — cada depósito es un bono privado al portador, revendible antes del vencimiento mediante transferencia atómica on-chain, sin terceros ni comisión; o sal de inmediato con un 2 % destinado al seguro. Sigues siendo soberano.
- **Herencia sin confianza integrada** — una primicia en una cadena con privacidad: transmisión automática de tus fondos, sin notario, sin tribunal, sin revelar tu identidad — bajo el cerrojo del consenso.
- **Resistencia poscuántica híbrida** — ML-DSA-65 + ML-KEM-768, allí donde Monero, Zcash y todos los forks de CryptoNote no tienen estrictamente nada.
- **Escasez programada sin gobernanza** — oferta estrictamente finita y excedente del fondo de seguro quemado por el consenso, allí donde Monero y los forks de CryptoNote emiten hasta el infinito.
- **Cero superficie de ataque** — sin contratos inteligentes, sin oráculos, sin custodia: exactamente la superficie que ha costado miles de millones a las DeFi, suprimida por construcción.
- **Solvencia probada, privacidad total** — garantizada matemáticamente, jamás prometida; importes públicos, identidades ocultas en cada etapa.

PRIVACY BANK CHAIN

«Private money that works for you.»