CHIRP

Coinbase Hashrate-Indexed Reward Payouts

Pagos de recompensa indexados por hashrate, en la coinbase

Un esquema de recompensa compartida, no-custodial y por lotería ponderada, para minería Bitcoin

Libro Blanco de PyBLOCK

v1.0 — Junio 2026

> *"Sin power no generás la onda gravitacional, y sin tiempo no hay espacio-tiempo."*
> Una onda gravitacional necesita una fuente energética *y* espacio-tiempo por donde viajar. CHIRP te pide exactamente las mismas dos cosas: **potencia** y **tiempo**.

Resumen

CHIRP es un esquema de recompensa para pools de minería Bitcoin en el que la **propia transacción coinbase** de un bloque encontrado paga directamente a un conjunto de mineros contribuyentes — de forma atómica, en cadena, y **sin que el pool retenga jamás un solo satoshi de las ganancias de nadie**. Como la coinbase admite sólo un número finito de salidas, CHIRP llena esos cupos con una **lotería ponderada verificable** cuyos boletos se ganan con dos cosas a la vez: **antigüedad** (cuánto hace que minás con PyBLOCK) y **potencia** (el trabajo que aportaste en una ventana rodante). A lo largo de muchos bloques, la ganancia esperada de un minero converge a su peso; en cada bloque, quién cobra es un sorteo públicamente auditable sembrado por el hash del bloque anterior.

1 El dilema de toda pool chica

Una pool compartida sólo puede pagar a sus miembros **cuando encuentra un bloque**. La alternativa — FPPS, pagar por share sin importar la suerte — obliga al operador a **adelantar cada pago de sus reservas** y absorber toda la varianza, lo que es quiebra asegurada para cualquiera sin hashrate a escala industrial.

El esquema honesto a escala chica es entonces alguna forma de pago-por-últimos-N-shares: pagos raros, grandes y repartidos con justicia. Pero el PPLNS habitual tiene un segundo problema: **la custodia**. La recompensa cae en la billetera del operador, y él la reparte. CHIRP elimina por completo el problema de la custodia.

2 Estado del arte

- **PPS / FPPS** — pago predecible, adelantado por el operador, varianza sobre el operador. Requiere escala y reservas.

- **PPLNS** — pago sobre una ventana de shares recientes. Justo, pero normalmente custodial.
- **TIDES de OCEAN** — una variante de PPLNS sobre una ventana rodante de los últimos 8 bloques ($8 \times D_{\text{red}}$ de share-work) que paga a cada minero directo en la coinbase — no-custodial y auditable. TIDES es el antecedente más cercano y la inspiración de CHIRP.

3 CHIRP en una frase

> Cuando el pool resuelve un bloque, su coinbase paga a una muestra por lotería ponderada de mineros elegibles, directo en cadena, donde las probabilidades y la tajada de cada uno son el promedio de cuánto hace que mina acá (**días**) y cuánto trabajo aportó últimamente (**power**).

4 La mecánica

4.1 Elegibilidad — el filtro de candidatura

Un minero es *aspirante* sólo si cumple *ambos* mínimos:

$$\text{candidato} \iff (\text{días}_i \geq \text{MIN\_DÍAS}) \ \wedge \ (\text{power}_i \geq \text{MIN\_POWER}).$$

MIN_POWER elimina el polvo (dust); MIN_DÍAS fija un piso de lealtad. *Quien no cumple, no es aspirante*: una CPU "conectada por años" nunca alcanza MIN_POWER, y un ballenón que aterriza de golpe nunca alcanza MIN_DÍAS.

4.2 Peso — la media de ambas

Entre los candidatos, el peso de cada minero es el **promedio** de dos factores normalizados:

$$w_i \ = \ \frac{d_i + p_i}{2}, \qquad d_i = \min\Big(\frac{\text{días}_i}{\text{DAYS\_FULL}}, 1\Big), \qquad p_i = \min\Big(\frac{\text{power}_i}{\text{POWER\_FULL}}, 1\Big).$$

La media — ni producto, ni suma — es deliberada: **balancea** las entradas para que ninguna domine sola. Un veterano con una máquina débil se hunde por p_i bajo; un gigante recién llegado se hunde por d_i bajo. Para ganar necesitás **las dos**. Aquí power_i es el share-work acumulado del minero (la suma de las **dificultades** de sus shares — por altura, no por cantidad) dentro de la ventana rodante.

4.3 La lotería — llenar los cupos de la coinbase

La coinbase admite a lo sumo MAX_N salidas antes de competir por peso de bloque con las transacciones que pagan comisión. Cuando hay más candidatos que cupos, CHIRP **sortea** ganadores con probabilidad proporcional al peso, con el método de reservorio ponderado de Efraimidis–Spirakis:

$$\text{semilla} = \text{hashBloquePrevio}_{64}, \qquad \text{clave}_i = u_i^{1/w_i}, \qquad u_i = U(\text{semilla}, \text{addr}_i) \in (0, 1),$$

$$\text{ganadores} = \text{las } \textsc{max\_\_n} \text{ direcciones con mayor clave}_i.$$

Los uniformes u_i se derivan de forma determinista de la semilla y la dirección del minero. La semilla es el **hash del bloque anterior**: desconocido cuando los mineros empezaron a aportar (no se puede amañar), pero totalmente reproducible después (cualquiera audita el sorteo). **Así, el límite de tamaño de la coinbase deja de ser una restricción y se vuelve la mecánica** — una lotería justa y recurrente por los cupos.

4.4 Pago — el reparto entre ganadores

La recompensa, menos la comisión del pool, se divide entre los ganadores en proporción al peso:

$$\text{pago}_i \;=\; (R - \text{fee}) \cdot \frac{w_i}{\sum_{j \in \mathcal{W}} w_j}, \qquad R = \text{subsidio} + \text{comisiones}.$$

Cada pago es una salida `TxOut` de la coinbase. Si cualquier minero resuelve el bloque, es la *red* la que paga a todos a la vez — sin saldos, sin retiros, sin custodia.

4.5 La ventana — una variante acotada de TIDES

POWER se mide sobre una ventana rodante de share-work reciente. TIDES usa una ventana de $8 \times D_{\text{red}}$; al hashrate de una pool chica eso abarcaría millones de años y nunca deslizaría. CHIRP por eso la acota:

$$\text{ventana} \;=\; \min\big(\, 8 \times D_{\text{red}},\; 24\text{h} \,\big).$$

Converge a TIDES a escala exahash y se mantiene significativa y justa para los mineros activos hoy. Como el share-work es hashrate × tiempo, la ventana ya premia el aporte y la presencia reciente; el promedio explícito de días/power le agrega la antigüedad encima.

5 El principio de la onda gravitacional

CHIRP se llama así por el **chirp** — la señal ascendente que LIGO detecta cuando dos agujeros negros giran uno sobre el otro y colisionan, radiando ondulaciones por el espacio-tiempo. La metáfora es exacta, y es también el primer principio del diseño:

- **Sin potencia no hay onda.** Las ondas gravitacionales las radia masa-energía acelerando. Sin fuente ⇒ sin señal. Sin hashrate real ⇒ sin peso CHIRP.
- **Sin tiempo no hay espacio-tiempo.** La onda es una ondulación del *espacio-tiempo*; quitá la dimensión temporal y no hay medio que ondular. Sin antigüedad ⇒ sin peso.

El requisito doble no es arbitrario — es **cosmológico**. Los mineros *fusionan* su hashrate como agujeros negros colisionando, y cuando cae el bloque la recompensa **"chirpea"** hacia afuera como una onda que paga a cada contribuyente. (Ocean → TIDES, mareas de agua. Gravedad → CHIRP, ondas del espacio-tiempo.)

6 Verificabilidad y transparencia

CHIRP es auditable de punta a punta: los **pesos** se computan de entradas públicas (el timestamp de primera aparición y el share-work rodante de cada dirección) y se publican; **el sorteo** es determinista dado el hash del bloque anterior, así que cualquiera lo replica y confirma sus probabilidades; **el reparto** es visible directo en la coinbase de cada bloque encontrado. No confíes — verificá.

7 Anti-trampa

Ataque	**Por qué falla**
Sybil (dividir en direcciones nuevas)	cada dirección nueva arranca en 0 días → bajo MIN_DÍAS
Lealtad ociosa (una CPU por años)	nunca alcanza MIN_POWER; la media hunde el power bajo
Ballena paracaídas (power, sin antig.)	nunca alcanza MIN_DÍAS; $d_i = 0$ hunde la media
Salto en el borde de la ventana	atenuado por el suavizado de 24h y la aleatoriedad del sorteo
Predecir el sorteo	la semilla es el hash del bloque *anterior* — desconocido hasta que existe

8 Parámetros (defaults v1, ajustables)

Parámetro	**Default**	**Rol**
MIN_DÍAS	7 días	piso de lealtad para candidatura
MIN_POWER	$\approx$ 10 shares a min-dificultad	piso anti-dust para candidatura
DAYS_FULL	30 días	antigüedad a la que d_i satura
POWER_FULL	calibrado a un ASIC sano / 24h	work al que p_i satura
MAX_N	100	cupos de coinbase = ganadores del sorteo
Ventana	$\min(8D_{\text{red}}, 24\text{h})$	ventana rodante de power
Fee	0.9%	comisión de PyBLOCK en la coinbase

9 Despliegue

CHIRP corre como una instancia dedicada de pool Stratum V2 en el puerto **5554**, junto a (y totalmente independiente de) el stratum solo/lotería de PyBLOCK en el 5555. Ambos sirven las plantillas **BIP-110** propias de PyBLOCK desde el mismo nodo Bitcoin Knots, así que cada bloque CHIRP también señaliza BIP-110. Un registro de estadísticas por dirección, actualizado con cada share aceptado y persistido a disco, provee la antigüedad y el power que se vuelven el peso de cada minero.

10 Límites y honestidad

La varianza es real. Una pool chica encuentra bloques rara vez; CHIRP suaviza *quién comparte* un bloque, no *cada cuánto* llegan los bloques. Es un sindicato, no un sueldo — los mineros que quieren ingreso estable deben minar DATUM → OCEAN, que PyBLOCK también ofrece. POWER_FULL y MIN_POWER requieren calibración contra el hashrate real.

11 Conclusión

CHIRP convierte tres restricciones en virtudes. El *problema de custodia* se vuelve **no-custodia** — la red paga a los mineros directo en la coinbase. El *límite de tamaño de la coinbase* se vuelve una **lotería justa y verificable** por los cupos. Y la *varianza de pool chica* se vuelve el **alma honesta del producto** — un sindicato que, por la misma lógica que el cosmos, paga a quienes traen tanto energía como tiempo.

Miná en PyBLOCK. Fusioná tu hashrate. Escuchá el chirp. ★