CHIRP

Coinbase Hashrate-Indexed Reward Payouts

A non-custodial, weighted-lottery shared-reward scheme for Bitcoin mining

A PyBLOCK White Paper

v1.0 — June 2026

> *"Without power there is no gravitational wave, and without time there is no spacetime."* A gravitational wave needs an energetic source *and* spacetime to travel through. CHIRP needs the same two things from you: **power** and **time**.

Abstract

CHIRP is a Bitcoin mining-pool reward scheme in which a found block's **coinbase transaction itself** pays a set of contributing miners directly — atomically, on-chain, and **without the pool ever holding a single satoshi of anyone's earnings**. Because the coinbase output limit admits only finitely many recipients, CHIRP fills those slots with a **verifiable weighted lottery** whose tickets are earned by two things at once: **tenure** (how long you have mined with PyBLOCK) and **power** (the work you have contributed in a rolling window). Over many blocks, a miner's expected earnings converge to their weight; in any single block, who gets paid is a publicly auditable draw seeded by the previous block hash.

1 The dilemma every small pool faces

A shared mining pool can only ever pay its members **when it finds a block**. The alternative — FPPS, paying per share regardless of luck — forces the operator to **front every payout from reserves** and absorb all variance, which is bankruptcy waiting to happen for anyone without warehouse-scale hashrate.

The honest scheme at small scale is therefore some form of pay-per-last-N-shares: rare, large, fairly-split payouts. But PPLNS as usually deployed has a second problem — **custody**. The block reward lands in the operator's wallet, and the operator then distributes it. CHIRP removes the custody problem entirely.

2 Prior art

- **PPS / FPPS** — predictable pay, operator-fronted, variance on the operator. Needs scale and reserves.
- **PPLNS** — pay over a window of recent shares. Fair, but typically custodial.

- **OCEAN's TIDES** — a PPLNS variant over a rolling window of the last 8 blocks ($8 \times D_{\text{net}}$ of share-work) that pays each miner directly in the coinbase — non-custodial and auditable. TIDES is the closest prior art and the inspiration for CHIRP.

3 CHIRP in one sentence

> When the pool solves a block, its coinbase pays a weighted-lottery sample of eligible miners directly on-chain, where each miner's odds and slice are the average of how long they have mined here (**days**) and how much work they have recently contributed (**power**).

4 The mechanism

4.1 Eligibility — the candidacy gate

A miner is an *aspirant* only if they clear *both* floors:

$$\text{candidate} \iff (\text{days}_i \geq \text{MIN\_DAYS}) \ \wedge \ (\text{power}_i \geq \text{MIN\_POWER}).$$

MIN_POWER eliminates dust; MIN_DAYS sets a loyalty floor. *Whoever fails either floor is not an aspirant*: a CPU idling "connected for years" never clears MIN_POWER, and a whale that parachutes in never clears MIN_DAYS.

4.2 Weight — the average of both

Among candidates, each miner's weight is the **mean** of two normalized factors:

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

The mean — not a product, not a sum — is deliberate: it **balances** the inputs so neither alone dominates. A veteran with a weak machine is dragged down by low p_i; a freshly-joined giant is dragged down by low d_i. To win you need **both**. Here power_i is the miner's accumulated share-work (the sum of share difficulties) inside the rolling window.

4.3 The lottery — filling the coinbase slots

A coinbase can carry only MAX_N outputs before competing with fee-paying transactions for block weight. When candidates exceed slots, CHIRP **draws** winners with probability proportional to weight, using the Efraimidis–Spirakis weighted-reservoir method:

$$\text{seed} = \text{prevBlockHash}_{64}, \qquad \text{key}_i = u_i^{1/w_i}, \qquad u_i = U(\text{seed}, \text{addr}_i) \in (0, 1),$$

$$\text{winners} = \underset{i}{\text{top-MAX\_N}} \ \text{key}_i.$$

The uniforms u_i are derived deterministically from the seed and the miner's address. The seed is the **previous block hash**: unknown when miners began contributing (so it cannot be gamed), yet fully reproducible afterward (so anyone can audit the draw). **The coinbase-size constraint thus becomes the mechanism** — a fair, recurring lottery for the slots.

4.4 Payout — the split among winners

The reward, less the pool fee, is divided across winners in proportion to weight:

$$\text{payout}_i \;=\; (R - \text{fee}) \cdot \frac{w_i}{\sum_{j \in \mathcal{W}} w_j}, \qquad R = \text{subsidy} + \text{tx fees}.$$

Every payout is a coinbase `TxOut`. If any miner solves the block, the *network* pays everyone at once — no balances, no withdrawals, no custody.

4.5 The window — a bounded variant of TIDES

POWER is measured over a rolling window of recent share-work. TIDES uses an $8 \times D_{\text{net}}$ window; at a small pool's hashrate that would span millions of years and never slide. CHIRP therefore bounds it:

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

This converges to TIDES at exahash scale while staying meaningful and fair for active miners today. Because share-work is hashrate × time, the window already rewards both contribution and recent presence; the explicit days/power average layers tenure on top.

5 The gravitational-wave principle

CHIRP is named for the **chirp** — the rising signal LIGO detects when two black holes spiral together and merge, radiating ripples through spacetime. The metaphor is exact, and it is also the design's first principle:

- **Without power, there is no wave.** Gravitational waves are radiated by accelerating mass-energy. No source ⇒ no signal. No real hashrate ⇒ no CHIRP weight.
- **Without time, there is no spacetime.** The wave is a ripple of *space-time*; remove the temporal dimension and there is no medium to ripple. No tenure ⇒ no weight.

The dual requirement is not arbitrary — it is **cosmological**. Miners *merge* their hashrate like colliding black holes, and when the block is found the reward **chirps** out as a wave that pays every contributor. (Ocean → TIDES, tides of water. Gravity → CHIRP, ripples of spacetime.)

6 Verifiability & transparency

CHIRP is auditable end to end: **weights** are computed from public inputs (each address's first-seen timestamp and rolling share-work) and published; **the draw** is deterministic given the previous block hash, so anyone can replay it and confirm their odds; **the split** is visible directly in the coinbase of every block found. Don't trust — verify.

7 Anti-gaming

Attack	**Why it fails**
Sybil (split across new addresses)	each new address starts at 0 days → below MIN_DAYS
Idle loyalty (a CPU for years)	never clears MIN_POWER; the average sinks low power
Whale parachute (power, no tenure)	never clears MIN_DAYS; $d_i = 0$ sinks the average
Window-boundary hopping	muted by 24h smoothing and the lottery randomness
Predicting the draw	the seed is the *previous* block hash — unknown until it exists

8 Parameters (v1 defaults, tunable)

Parameter	**Default**	**Role**
MIN_DAYS	7 days	loyalty floor for candidacy
MIN_POWER	≈ 10 shares at min-difficulty	dust floor for candidacy
DAYS_FULL	30 days	tenure at which d_i saturates
POWER_FULL	calibrated to a healthy ASIC / 24h	work at which p_i saturates
MAX_N	100	coinbase slots = lottery winners
Window	$\min(8D_{\text{net}}, 24\text{h})$	rolling power window
Fee	0.9%	PyBLOCK's coinbase cut

9 Deployment

CHIRP runs as a dedicated Stratum V2 pool instance on port **5554**, alongside (and entirely independent of) PyBLOCK's solo/lottery stratum on 5555. Both serve PyBLOCK's own **BIP-110** templates from the same Bitcoin Knots node, so every CHIRP block also signals BIP-110. A per-address stats registry, updated on every accepted share and snapshotted to disk, supplies the tenure and power that become each miner's weight.

10 Limitations & honesty

Variance is real. A small pool finds blocks rarely; CHIRP smooths *who shares* a block, not *how often* blocks arrive. It is a syndicate, not a salary — miners who want steady income should

mine DATUM → OCEAN, which PyBLOCK also offers. POWER_FULL and MIN_POWER require calibration against live hashrate.

11 Conclusion

CHIRP turns three constraints into features. The *custody problem* becomes **non-custody** — the network pays miners directly in the coinbase. The *coinbase-size limit* becomes a **fair, verifiable lottery** for the slots. And the *small-pool variance* becomes the **honest soul of the product** — a syndicate that, by the same logic as the cosmos, pays those who bring both energy and time.

Mine on PyBLOCK. Merge your hashrate. Hear the chirp. ★