dvb-WarpPool

Tu propio pool de minería en solitario de Bitcoin

Pool público al 0 % en solitario — Manual del operador

Ejecutar dvb-WarpPool como un pool abierto, non-custodial y sin comisiones

Versión 1.52.0 · Edición noviembre 2026

Contenido

1 Qué es un pool público al 0 %

2 Activar el modo per-worker

3 Qué introducen los mineros

4 Páginas públicas de wallet y el panel del propietario

5 Privacidad del operador

6 Aceptar donaciones (opcional)

7 Perfil de endurecimiento público

8 TLS

9 Detrás de un proxy inverso

10 Lista de verificación de despliegue

11 Soporte y enlaces

1 · Qué es un pool público al 0 %

Un pool público al 0 % convierte dvb-WarpPool en un **pool en solitario abierto, non-custodial y sin comisiones**: cualquier minero que se conecte mina hacia *su propia* dirección de Bitcoin —tomada del login de Stratum— y la recompensa de bloque completa va directamente a quien encuentra el bloque, on-chain. El pool nunca retiene fondos. No hay nada que retirar, ni nada en lo que confiar.

Técnicamente esto es el **modo de pago per-worker**. En el modo `single` por defecto, la recompensa completa paga a una sola dirección del operador —la configuración habitual de «solitario + amigos», donde cada minero trabaja para *tu* wallet—. En el modo **per-worker** cada minero aporta su propia dirección como nombre de usuario de Stratum, y el coinbase se construye por conexión para pagar exactamente esa dirección: **una salida, el subsidio completo, sin comisión.**

Las cuatro propiedades que lo definen

- **Non-custodial.** El pool nunca toca las monedas de nadie. La red de Bitcoin paga directamente a quien encuentra el bloque.
- **Per-worker.** Distintos mineros pueden usar distintas direcciones; cada uno conserva la recompensa completa de los bloques que encuentra.
- **Recompensa completa para quien lo encuentra.** Una única salida de coinbase paga todo el subsidio más las comisiones a la dirección del login del minero ganador: 0 % de recorte.
- **A prueba de fallos (fail-closed).** El daemon se niega a arrancar si se configura una comisión o una donación al operador junto con el modo per-worker, de modo que no puedes ejecutar por accidente un pool «público» que recorte silenciosamente la recompensa.

Salvaguarda de honestidad — por favor, léela. dvb-WarpPool **aún no ha encontrado un bloque en mainnet.** La ruta de consenso (coinbase per-worker → un nodo real de Bitcoin Core acepta el bloque → la recompensa paga a quien lo encuentra) está verificada de extremo a extremo en regtest y signet, pero el primer bloque en mainnet sigue siendo un **«aún no»**. Anuncia el pool exactamente por lo que es —un pool en solitario nuevo, abierto y non-custodial— y **nunca** como «probado en batalla». Si publicas una página de aterrizaje, mantén esa salvaguarda visible.

Contraste con el modo `single`. Si solo quieres minar tus propios equipos, o un grupo fijo de amigos, todos pagando a una sola wallet, quédate en el modo `single` —consulta el *Manual de usuario* principal—. Este manual del operador trata específicamente de abrir el pool para que desconocidos puedan apuntar sus mineros a él y cada uno conserve lo que encuentra.

2 · Activar el modo per-worker

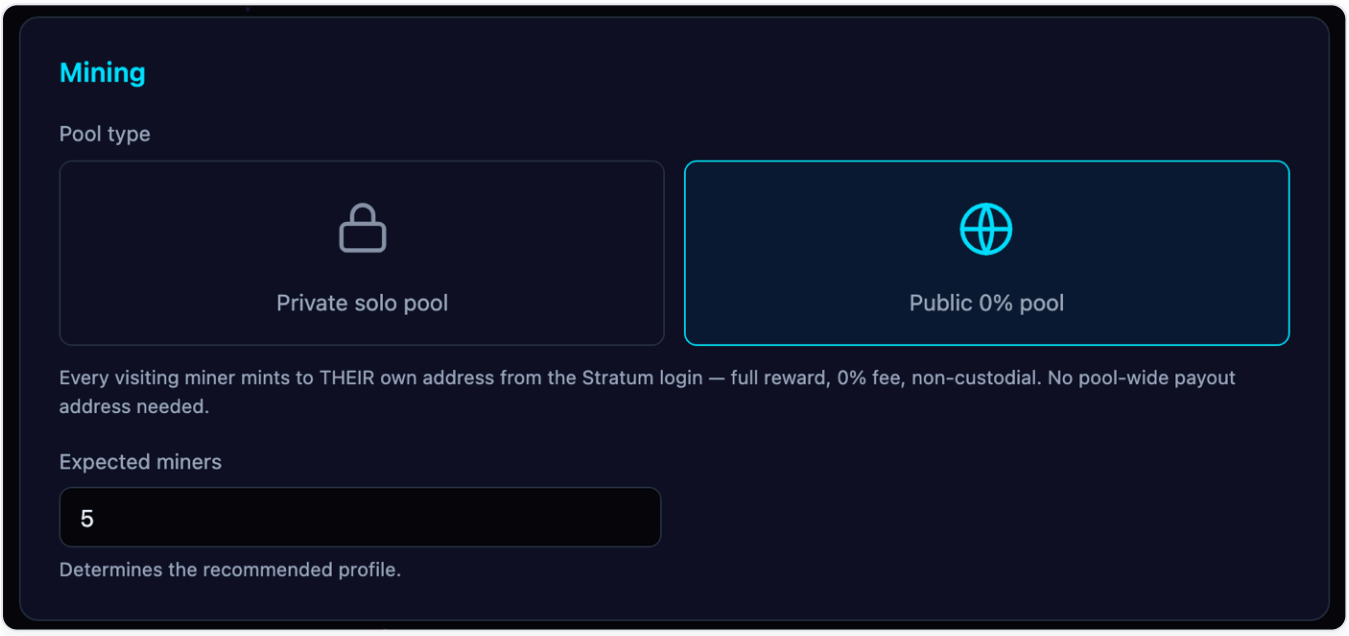
Hay dos caminos hacia el mismo resultado: el setup wizard (el asistente de configuración, recomendado para una instalación nueva) o una edición de una sola línea en `config.toml`. Ambos escriben el mismo flag `payout_mode = "per_worker"`.

Camino A — el setup wizard

Cuando instalas mediante el setup wizard, su tarjeta **Minería** ofrece una elección de **Tipo de pool**: **Pool solo privado** frente a **Pool público 0%**. Elegir **Pool público 0%** hace tres cosas por ti:

- escribe `payout_mode = "per_worker"`;
- oculta el campo de **dirección de pago** de todo el pool (no se usa en este modo: cada minero trae la suya);
- fuerza la **comisión del pool** a 0 y oculta los campos de comisión.

No se requiere ninguna edición manual.



La tarjeta «Minería» del asistente: elegir «Pool público 0%» cambia el pool a pagos per-worker y oculta los campos de dirección de pago y comisión.

Camino B — `config.toml`

Si gestionas la configuración a mano, un solo flag es todo el interruptor de la función:

```
[mining]
payout_mode = "per_worker"
# payout_address is IGNORED in per_worker mode (each miner brings its own).
# pool_fee_percent / operator_donation_percent MUST be 0 — the daemon
# refuses to start otherwise (full reward goes to the finder).
```

Fail-closed ante comisión o donación

El daemon **falla en cerrado (fail-closed)** al arrancar si se configura un `pool_fee_percent` u `operator_donation_percent` distinto de cero junto con `per_worker`. No arrancará hasta que la

comisión y la donación vuelvan a cero. Se trata de un invariante de seguridad deliberado: un pool per-worker paga a quien encuentra el bloque la recompensa *completa*, así que no hay configuración alguna en la que pueda quedarse con una parte de forma silenciosa.

> **Los errores tipográficos nunca pagan a la persona equivocada.** Una dirección de login inválida o de la red equivocada es **rechazada** en `mining.authorize` (Stratum V1) o en la apertura de canal (Stratum V2). **No hay respaldo** hacia una dirección del operador: una dirección mal escrita se rechaza, nunca se redirige silenciosamente.

3 · Qué introducen los mineros

Un minero que se une a tu pool público configura su login de Stratum exactamente como en cualquier pool en solitario, con una regla: **el nombre de usuario es la propia dirección de Bitcoin del minero**, seguida opcionalmente de una etiqueta de equipo tras un punto.

```
Username:  bc1qyour-own-address.rig1
Password:  x   (cualquiera, no se usa)
```

- Todo lo que va **antes del primer punto** es la dirección de pago; cualquier cosa después es una etiqueta de equipo libre, usada solo para estadísticas.
- La contraseña puede ser cualquier cosa (habitualmente `x`).

Tipos de dirección admitidos

Funciona cualquier dirección válida de mainnet. El pool acepta:

Tipo	Prefijo de ejemplo
P2PKH (legacy)	`1…`
P2SH (incl. SegWit envuelto)	`3…`
P2WPKH (SegWit nativo)	`bc1q…`
P2WSH (script SegWit nativo)	`bc1q…`
P2TR (Taproot)	`bc1p…`

> **Dirección equivocada = rechazada, no redirigida.** Si el login no es una dirección válida para esta red, el minero se rechaza en el momento de autorizar. No hay dirección de respaldo, así que un error tipográfico simplemente no consigue conectar, en lugar de pagar la recompensa de bloque al destinatario equivocado.

4 · Páginas públicas de wallet y el panel del propietario

Cada dirección que mina en tu pool obtiene su propia página de estado sin login —el flujo de «consultar mi dirección» que se espera de un pool público en solitario—. Los mineros guardan como favorito el suyo; nadie necesita una cuenta.

La página pública en `/users/<address>`

Abre `/users/<address>` y verás, para esa dirección:

- el **hashrate total** en letra grande, sumado entre todos los equipos conectados con esa dirección, con un conmutador de ventana de 1 m / 5 m / 1 h / 1 d / 7 d;
- un **gráfico de hashrate de 24 horas** con las mejores shares dibujadas como puntos;
- la **mejor dificultad de share histórica**, los **equipos en línea** y las **shares aceptadas en total**;
- una **tabla por equipo**: una fila por login `address.rig`, con un indicador de conexión, hashrate, mejor share, última share y firmware, más una columna WarpTune si el propietario comparte esa insignia;
- un **panel de probabilidades de bloque** honesto (ver más abajo).

Sin login, sin intervención del operador: cualquiera que tenga la dirección puede abrirla.

El **panel de probabilidades de bloque** sustituye al antiguo «tiempo estimado hasta un bloque» —una media que para un equipo doméstico se lee como «nunca» y oculta el sentido de la minería en solitario: el proceso **no tiene memoria**, cada segundo es un sorteo nuevo sin nada que se acerque—. En su lugar muestra la distribución real: la **probabilidad en las próximas 24 horas** y **en un año** (las probabilidades muy bajas como «1 entre N», los porcentajes redondeados hacia abajo para que nunca exageren), el **punto 50/50** (la mediana, no la media) y la **suerte hasta ahora** —bloques esperados frente a encontrados, con un honesto «el N % de los mineros con tu historial tampoco tendría ninguno todavía»—. Una nota al pie sobre la falta de memoria deja claro el punto central: ninguna cantidad de espera hace más probable un bloque.



Una página pública por wallet en /users/<address>: hashrate agregado, desglose por equipo y mejor share, sin login requerido.

JSON compatible con ckpool. Los mismos números se sirven en `GET /api/users/<address>` en el formato de campos de ckpool (`hashrate1m`, `hashrate1hr`, `bestshare`, `worker[]`, …), de modo que el firmware de los mineros y herramientas de estadísticas como `ckstats` pueden leerlo directamente. Ambas rutas son HTTP plano bajo el puerto de estado, tras el mismo proxy inverso que el dashboard.

El panel del propietario opcional (opt-in)

Por defecto una página de wallet es pública. Un minero que quiera más control puede **demostrar la propiedad** de la dirección y desbloquear un panel del propietario —enteramente por minero, nada que el operador configure—:

1. La página entrega un breve **mensaje de desafío** de un solo uso.
2. El minero lo firma en el cuadro *Sign Message* (Firmar mensaje) de su propia wallet —la función estándar BIP-137 de «verificar dirección» en Electrum, Sparrow, Bitcoin Core y wallets de hardware—. **Ninguna clave privada sale de la wallet, no se mueven fondos, no se crea ninguna cuenta**: el pool solo comprueba la firma.
3. Una firma válida establece una cookie de propietario de corta duración para esa dirección y revela tres controles:
   - **Privacidad** — oculta la dirección de la lista pública de wallets y deja en blanco sus datos en `/users/<address>` para todos salvo para el propietario verificado (el enlace directo sigue funcionando, para él).
   - **Notificaciones** — apunta un topic de ntfy personal o un webhook a los hitos de esta dirección: *bloque encontrado*, un nuevo *mejor share personal* (sumando todos sus equipos), la primera entrada en el *top 100 histórico* del pool y *equipo fuera de línea*. Cada uno tiene su propio tiempo de espera contra el spam, y un bloque encontrado envía un único titular en lugar de tres alertas.
   - **Insignia WarpTune** (desde v1.31.0) — crea un **token de envío** para esta dirección, guárdalo en la variable de entorno cuyo nombre se indica en `warptune.toml` (`pool_push_token_env`) en la máquina donde se ejecuta tu programa auxiliar dvb-WarpTune y pon `pool_push = true`. El programa auxiliar envía entonces su snapshot a este pool y la tabla «Equipos» muestra una insignia por equipo: modo, frecuencia, simulación / en vivo / control desactivado / obsoleto; pasa el ratón por encima para ver la última decisión. Los visitantes solo ven la insignia reducida después de hacer clic en **Mostrar la insignia a los visitantes**. El token se muestra una sola vez, se puede renovar o revocar aquí, y el pool nunca envía nada de vuelta a un minero.

Texto en la coinbase (v1.45, pools per-worker): una vez demostrada la propiedad de tu dirección puedes fijar hasta 16 caracteres (letras, dígitos, puntuación, espacios; sin `/`) que entran en la coinbase de cada bloque que este pool construye para tu dirección, justo después de la etiqueta del pool — tu huella en la cadena, visible en cualquier explorador. Se aplica a partir del siguiente trabajo; el operador puede desactivar la función.

Taproot ahora también funciona. La firma de propiedad cubre direcciones de clave única **P2PKH / P2WPKH / P2SH-P2WPKH** (BIP-137) y **Taproot (P2TR)** mediante **BIP-322**: firma con un monedero que lo admita, como Sparrow. El panel del propietario **no necesita ninguna configuración del operador**: lo controla enteramente el minero.

5 · Privacidad del operador

Un pool público en mainnet no debería repartir una lista enumerable de la dirección y la configuración de equipos de todo el mundo. dvb-WarpPool te da **dos capas independientes** de control. Ambas tienen por defecto el comportamiento abierto, así que el endurecimiento aquí es opt-in.

Capa A — configuración: exposición del directorio y del ranking

Dos claves en `[privacy]` fijan la exposición por defecto de toda la interfaz. En ambos casos el **operador con la sesión iniciada sigue viendo los datos completos**: estas solo afectan a los visitantes anónimos, así que mantén la autenticación de administrador habilitada.

```
[privacy]
# Hide the browsable Workers/wallet directory from anonymous visitors. Each
# /users/<address> page still works by direct link; the logged-in operator
# still sees the full directory (so keep admin auth enabled).
wallet_directory_public = false
# Mask the Bitcoin address in the public best-shares leaderboard, server-side.
# The logged-in operator still sees full addresses.
leaderboard_addresses_public = false
```

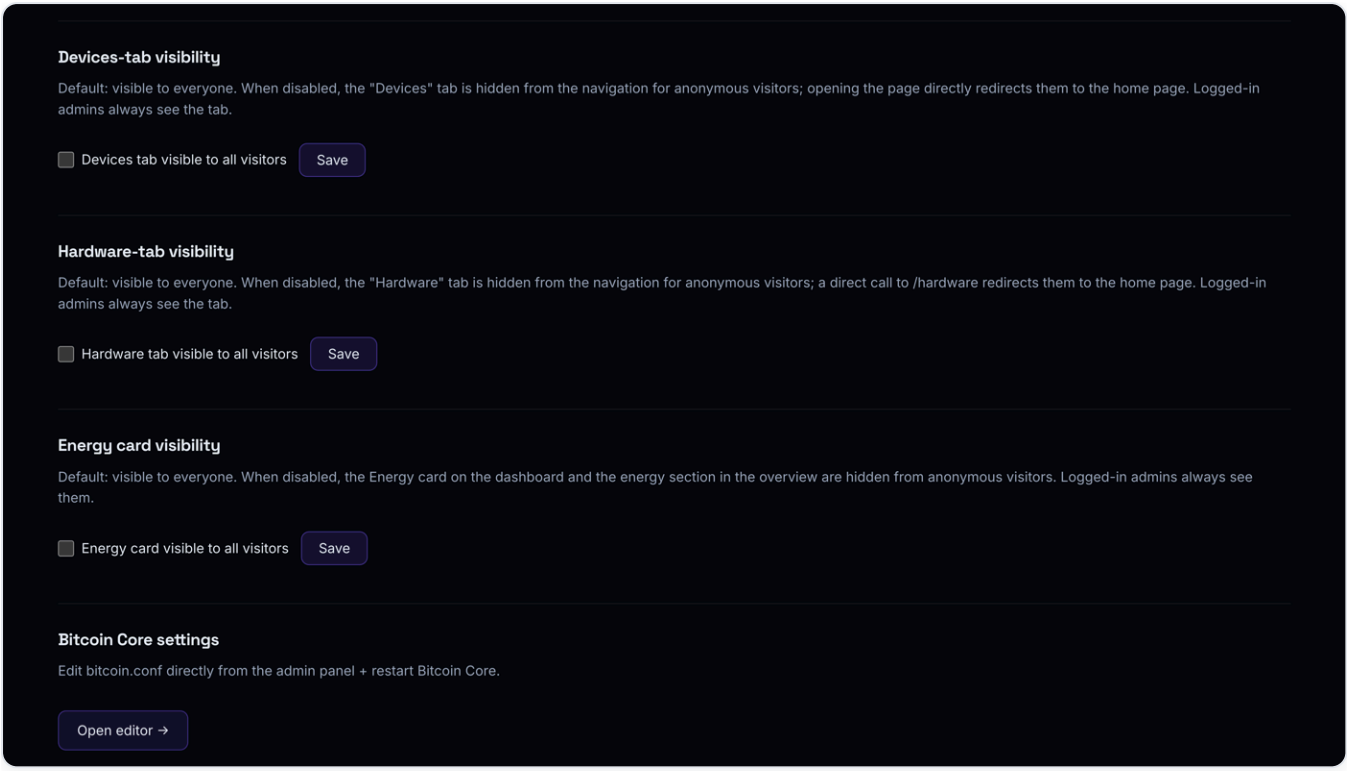
Con esta postura, los mineros llegan a su propia página mediante el enlace, pero el pool no publica una lista navegable de todos, y las direcciones del ranking se enmascaran en el lado del servidor. No toca ni los pagos ni la construcción de bloques.

Capa B — interruptores de visibilidad en la interfaz de administración

En **Admin** → **Perfil**, un conjunto de interruptores de visibilidad oculta vistas completas a los visitantes anónimos:

- la pestaña **Dispositivos** (la ruta `/miners`: el gestor interactivo de dispositivos con telemetría por dispositivo);
- la pestaña **Hardware** (recursos del host e imagen del perfil de tamaño);
- la tarjeta **Energía** del dashboard.

> **¿Qué pestaña oculta el interruptor?** El interruptor de visibilidad controla la pestaña **Dispositivos** —la ruta `/miners` con telemetría de dispositivos en vivo—, **no** el listado de Mineros/workers. Los nombres se confunden con facilidad (Workers = wallets, Mineros = logins de Stratum, Dispositivos = el hardware); el interruptor se refiere a la vista del gestor de dispositivos.



Admin → Perfil: los interruptores de visibilidad ocultan las vistas Dispositivos/Hardware/Energía a los visitantes anónimos; las direcciones del ranking público se enmascaran en el lado del servidor.

> **Postura recomendada para mainnet público.** Fija `wallet_directory_public = false` y `leaderboard_addresses_public = false`, y oculta las vistas Dispositivos, Hardware y Energía a los visitantes anónimos. Los mineros siguen llegando a su propia página `/users/<address>` mediante el enlace; el operador conserva la imagen completa con la sesión iniciada.

Eliminar un worker

Si un minero te pide salir del ranking, o hay nombres de prueba antiguos que lo ensucian, abre **Admin → Workers**. **Eliminar** olvida un worker que no esté conectado: su entrada, sus mejores shares (con lo que desaparece del ranking) y su memoria VarDiff. El historial de shares y los bloques encontrados se conservan. Un worker conectado no se puede eliminar: el minero tiene que desconectarse primero, y si vuelve a conectarse más tarde, simplemente empieza de cero. Un minero que acaba de parar aparece como **activo hace poco** y ya se puede eliminar. Los nombres cuya entrada de worker ya eliminó la retención, pero que siguen en el ranking, aparecen en una segunda tabla, **Restos sin entrada de worker**, y se eliminan igual. Cada intento queda en el registro de auditoría.

6 · Aceptar donaciones (opcional)

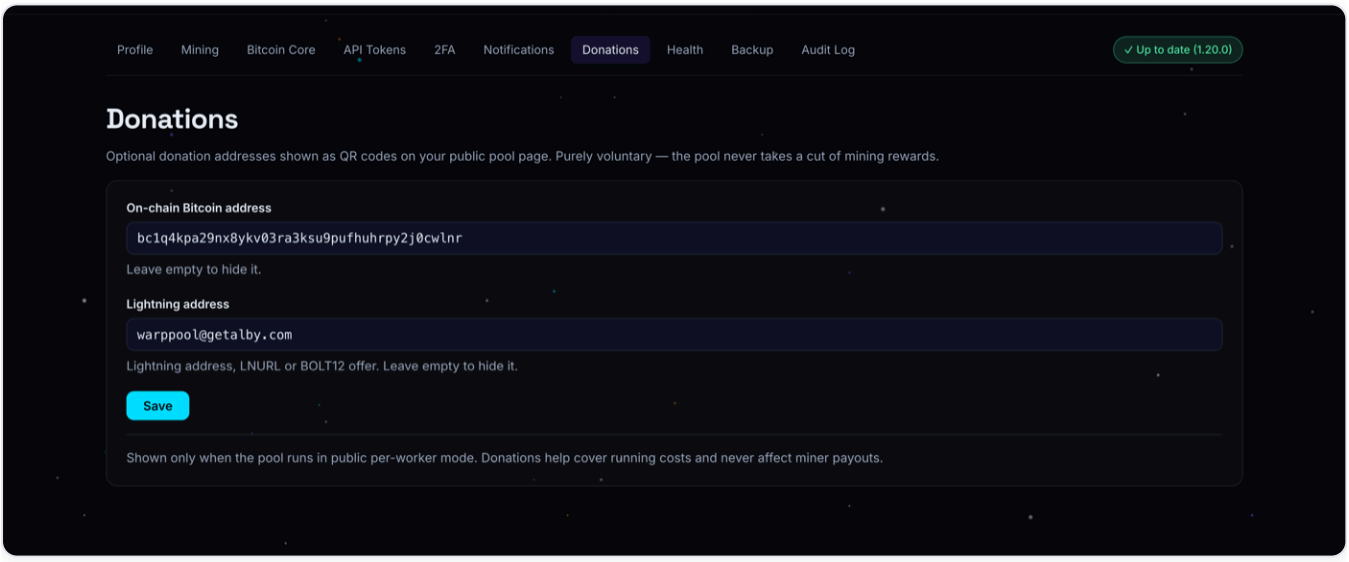
Como un pool per-worker se queda con el **0 %** de cada recompensa, la única forma de financiar el alojamiento es una donación voluntaria. El dashboard tiene soporte integrado para esto, y toda la función aparece **solo en el modo per-worker**: un pool privado en solitario nunca la muestra.

Fijar las direcciones

Fíjalas en **Admin** → **Donaciones**. La entrada de navegación está **oculta salvo que el pool se ejecute en modo per-worker**.

Campo	Qué introducir
Dirección Bitcoin on-chain	Cualquier dirección de Bitcoin válida. Se valida al guardar y se muestra como un código QR `bitcoin:` que la wallet del visitante puede abrir directamente.
Dirección Lightning	Una dirección Lightning, LNURL o cadena BOLT12, almacenada tal como la introduces. Se muestra con su propio campo de copia y código QR.

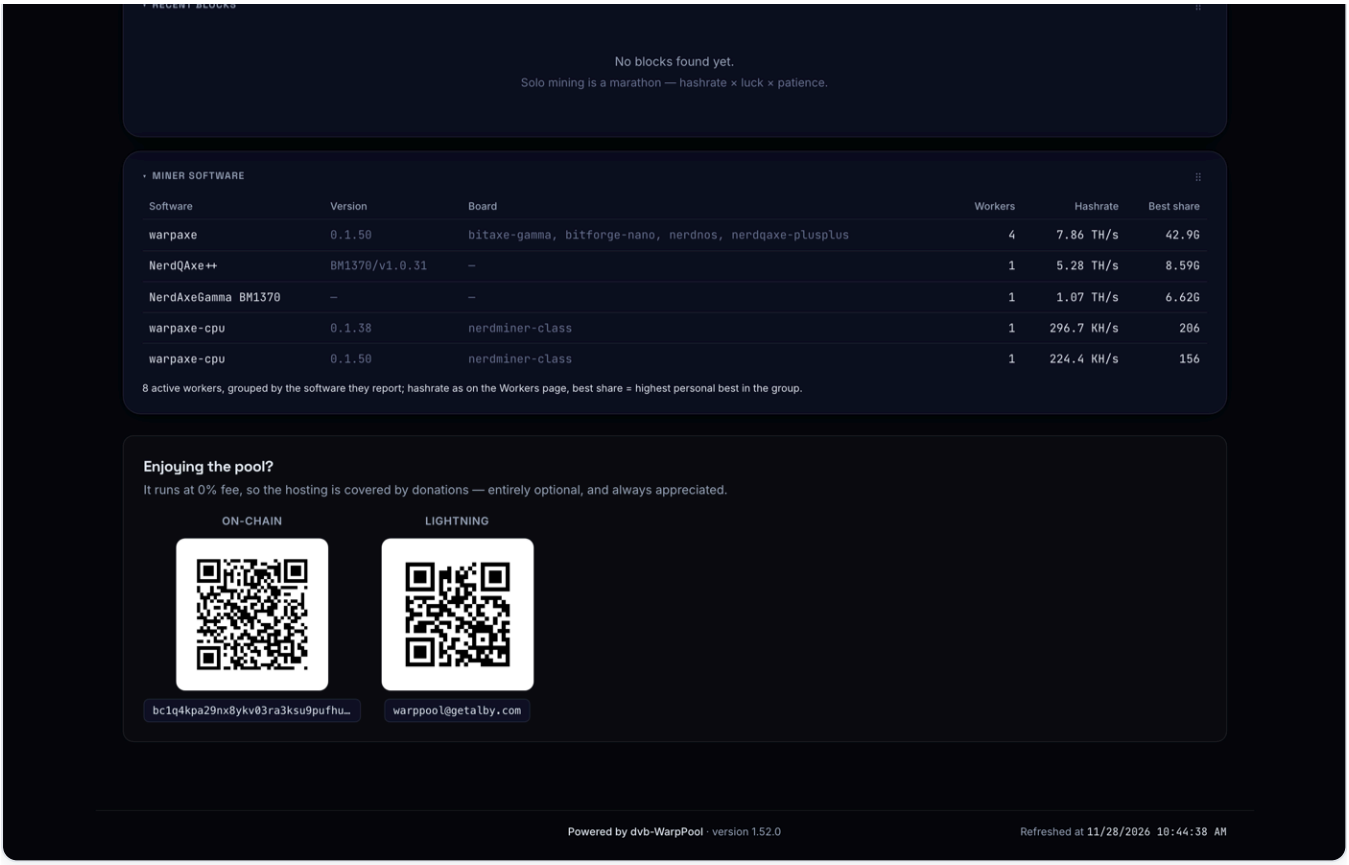
Deja cualquiera de los campos en blanco para ocultar esa opción. Cuando al menos uno está fijado, aparece una tarjeta **«¿Te gusta el pool?»** con códigos QR y direcciones que se copian con un clic en la **parte inferior del dashboard público**.



Admin → Donaciones (solo pools per-worker): fija una dirección de propina on-chain o Lightning; entonces aparece una tarjeta de donación en el dashboard público.

> **Las donaciones nunca tocan la recompensa de bloque.** Estas direcciones se almacenan como ajustes del pool (no en `config.toml`), así que guardar surte efecto de inmediato **sin reinicio**. Son simples metadatos del operador: **nunca se mezclan en la construcción del coinbase**, de modo que fijar una no puede afectar a la regla fail-closed de que un pool per-worker paga a quien encuentra el bloque la recompensa completa. Una «donación» aquí es un visitante que envía sats a una dirección mostrada, no una parte de la recompensa de bloque de nadie.


dvb-WarpPool
Dashboard
Hashrate
Overview
Blocks
Workers
Miners
RPC READY
IPC
LARGE (≤100 MINERS)
LIVE
EN
Login
Dashboard
Live status of your Bitcoin solo pool.
How to connect your miner
POOL
POOL HASHRATE LIVE
15.63 TH/s
24h avg 14.88 TH/s · 32.0 /min (2.13 /worker)
BLOCKS
0
WORKERS
16
39 miner
BEST SHARE
42.92G
bc1qtg…eqz0.bitaxe602
upd. 7/23/2026
UPTIME
1d 4h
ACTIVE MINERS
4 / 15
4 worker · 15 miner
3 TLS · 6 SV2
POOL FEE
0.00 %
POOL HASHRATE (24H)
Full view →
BEST SHARE
588M
441M
294M
147M
0
35.0 TH/s
30.0 TH/s
25.0 TH/s
20.0 TH/s
15.0 TH/s
10.0 TH/s
5.00 TH/s
0 TH/s
10:43
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
NETWORK
NETWORK HASHRATE
948.77 EH/s
DIFFICULTY
145.09 T
LAST DIFF CHANGE
+7.61 %
at Block #977.760
DIFF FORECAST
-4.95 %
at Block #979.776
NEXT DIFF
13d 13h
1.855 blocks remaining
BLOCK HEIGHT
977.922
BTC PRICE
$59,539
54.533 €
upd. 1m ago
CHAIN
main
Bitcoin Core 31.3.0
BLOCK
Block assembly checked by Core: OK (9m ago, height 977922)
ACTIVE WORKERS
USER
HASHRATE
DIFF
SHARES
LAST SEEN
bc1qtg…eqz0.WarpMiner
224.4 KH/s
0.009
0.36 /min
0s ago
bc1qtg…eqz0.bitaxe602
1.11 TH/s
2.84k
5.44 /min
6s ago
bc1qtg…eqz0.NerdQaxe++
4.90 TH/s
11.63k
5.89 /min
6s ago
bc1qtg…eqz0.BitForgeNano
1.83 TH/s
6.21k
4.11 /min
18s ago
15Hifh…TMUY
5.51 TH/s
14.44k
5.33 /min
40s ago
bc1qtg…eqz0.NerdNOS
189.5 GH/s
1.04k
2.56 /min
57s ago
bc1qk0…syhp.TimsNerdAxeGamma
1.07 TH/s
5.51k
3.00 /min
1m ago
bc1q4y…zspt.LilyGO
296.7 KH/s
0.005
0.50 /min
2m ago
1Bitco…9kuE
–
–
–
46m ago
All workers →
BEST SHARES
All Time
Per Worker
Rank
Worker
Difficulty
When
Hash
bc1qtg…eqz0.bitaxe602
42.92G
7/23/2026
199dee6cefbe…3c9ca18fcc56
bc1qtg…eqz0.NerdQaxe++
19.53G
11/17/2026
384af3541a97…c1afd81f916c
bc1qtg…eqz0.NerdQaxe++
11.51G
11/27/2026
5f8e5adef237…f55da7a8b992
#4
bc1qtg…eqz0.NerdOctaxe
10.71G
8/13/2026
66a824b0acd9…35508ca9498c
#5
bc1qtg…eqz0.NerdOctaxe
9.72G
8/14/2026
711d7240efea…3ae7aeb509eb
#6
15Hifh…TMUY
8.59G
9/27/2026
8002a41fdc00…ad0d47121dbb
#7
bc1qtg…eqz0.AvalonQ
8.52G
7/17/2026
8113f47a8de1…757e58a6141d
#8
bc1qtg…eqz0.NerdQaxe++
7.05G
9/12/2026
9bf171c07dc0…5befad08c821
#9
bc1qtg…eqz0.NerdAxeGamma
6.89G
8/25/2026
9f942b44525b…25197368acfd
#10
bc1qk0…syhp.TimsNerdAxeGamma
6.62G
10/28/2026
a607b0f96e9f…ddfa06a6485f
Show all (50)



El dashboard público tal como lo ve un visitante anónimo: estadísticas en vivo del pool y de la red, un ranking de mejores shares con direcciones enmascaradas (cada minero conserva su etiqueta de equipo) y la tarjeta de donación opcional con códigos QR en la parte inferior.

Anunciar el mantenimiento a tus mineros

Un pool público tiene visitantes a los que no puedes localizar por Discord. En **Admin** → **Banner** puedes poner un aviso breve —una ventana de mantenimiento, una resincronización planificada del nodo— como una franja deslizante en la parte superior de la página del pool, donde lo verá todo el que mine contigo. Tú fijas cuánto tiempo debe estar activo (minutos, horas o días) y desaparece solo cuando se cumple ese plazo, de modo que un aviso olvidado no puede quedarse ahí; un botón Detener lo termina antes. El texto se muestra como texto plano y está limitado a 200 caracteres. Anunciar así las paradas planificadas es sencillamente buena educación en un pool del que dependen otras personas.

7 · Perfil de endurecimiento público

Un pool expuesto a internet necesita los controles antiabuso que un pool solo para amigos puede saltarse. Todas las claves de abajo ya existen; ninguna es específica de per-worker: se aplican a cualquier despliegue público.

```
[stratum]
# Bound how many simultaneous V1 connections one source IP may hold. On a
# public pool this stops a single host from hogging slots. Leave 0 only if you
# expect many miners behind one NAT.
max_connections_per_ip = 50

[ratelimit]
enabled = true
connects_per_sec = 5
connect_burst = 20
auths_per_sec = 1.0
auth_burst = 10

# Auto-ban IPs that keep tripping the connect limit (escalating). Loopback and
# private LAN are never banned.
autoban_enabled = true
autoban_strikes = 3
autoban_base_secs = 60
autoban_max_secs = 86400
autoban_window_secs = 600

# Ban a worker that floods invalid shares (share-flood defence). Off by
# default; turn on for a public pool.
reject_ban_enabled = true
reject_ban_min_samples = 100
reject_ban_ratio = 0.9

# Optional subnet access control. `ban_cidrs` denies ranges outright;
# `allow_only = true` flips to a strict whitelist (only allow_cidrs connect).
# ban_cidrs = ["203.0.113.0/24"]
# allow_only = false
# allow_cidrs = ["192.168.0.0/16"]
```

Los clientes IPv6 se cuentan por su /64 (desde la v1.50). Una conexión a internet con IPv6 suele recibir todo un bloque de direcciones — un «/64», la primera mitad de la dirección — y el dispositivo que hay detrás puede elegir cualquier dirección de ese bloque. Para que ese único cliente no pueda saltarse los límites cambiando de dirección, cada límite por cliente de arriba (tasas de conexión y de inicio de sesión, el auto-ban, el ban por inundación de shares, `max_connections_per_ip`) cuenta a un cliente IPv6 público por su /64. Un ban que pongas a mano en **Admin → Perfil → Lista de IPs bloqueadas** sobre una dirección IPv6 bloquea todo su /64; la lista sigue mostrando y desbloqueando la dirección tal como la introdujiste. Las direcciones **unique-local** (`fc00::/7`) y **link-local** (`fe80::/10`) cuentan como tu propia LAN, igual que las direcciones IPv4 privadas: por dirección, y nunca se banean automáticamente. Para IPv4 no cambia nada.

Caídas del nodo y tus mineros. Si Bitcoin Core no entrega ninguna plantilla de bloque durante 10 minutos, el pool desconecta a todos los mineros y rechaza conexiones nuevas hasta que vuelvan las plantillas, para

que los mineros minen en su pool de respaldo en lugar de sobre un trabajo obsoleto (activado por defecto desde la v1.45; `[server] node_unhealthy_disconnect` y `node_unhealthy_grace_secs`). Pide a quienes minan en tu pool que configuren un pool de respaldo en su firmware.

Variante solo por invitación

Combina los pagos per-worker con una **lista de direcciones permitidas (allowlist)** para que solo direcciones conocidas puedan minar. Un minero cuya dirección de pago no figure en la lista es rechazado en ambos transportes (autorización de V1 y apertura de canal de Sv2):

```
[mining]
payout_mode = "per_worker"
address_allowlist = ["bc1qalice...", "bc1qbob..."]
```

Un `address_allowlist` vacío (el valor por defecto) deja el pool abierto a cualquiera. Ten en cuenta que `allow_only` / `allow_cidrs` controlan *qué redes* pueden conectarse, mientras que `address_allowlist` controla *qué direcciones de pago* pueden minar: las dos son independientes.

8 · TLS

El firmware que solo confía en autoridades de certificación públicas necesita un certificado real. Las claves relevantes viven en `[stratum]`:

```
[stratum]
stratum_tls_listen = ":3334"
tls_cert_path = "/etc/dvb-warppool/tls/cert.pem"
tls_key_path  = "/etc/dvb-warppool/tls/key.pem"
tls_reload_secs = 300
```

Deja las dos rutas **sin fijar** para usar el certificado autofirmado generado automáticamente por el daemon —adecuado para firmware de clase NerdMiner/Bitaxe que te permite fijarlo (pin)—.

Con el certificado autofirmado, el panel «Cómo conectar tu minero» del pool muestra además una línea **«Huella de la clave TLS (SHA-256)»**, una cadena como `AB:CD:…` que identifica la clave del pool. El firmware que fija un certificado autofirmado por su huella muestra el mismo valor antes de confiar en el pool — **WarpAxe 0.1.41 y posteriores** lo hace y pide al dueño del minero que lo confirme —, así que quienes minan en tu pool pueden comparar ambos. Con un certificado firmado por una CA la línea no aparece, porque no hace falta esa comprobación.

Las renovaciones se resuelven solas. Un certificado real de Let's Encrypt se sustituye cada pocos meses, y lo que lo haya emitido —Caddy, certbot, tu propia PKI— se limita a reescribir esos dos archivos. El pool lo detecta y empieza a servir el certificado nuevo por su cuenta. No hace falta que lo reinicies, y los mineros que estén conectados en ese momento siguen conectados: conservan el certificado que ya habían acordado y solo las conexiones nuevas reciben el recién emitido. `tls_reload_secs` define cada cuánto lo comprueba el pool (300 segundos por defecto; ponlo a `0` para desactivar la comprobación). Si una renovación se pilla a medio escribir, el pool sigue sirviendo el certificado antiguo y lo vuelve a intentar en la siguiente comprobación en lugar de tirar el listener.

Stratum V2. Si además ejecutas Stratum V2, escucha en su propia dirección `sv2_listen` (por ejemplo `:34254`). El transporte Sv2 siempre está cifrado con NOISE, así que no necesita un certificado TLS aparte. Los mineros necesitan además la clave pública de autoridad NOISE del pool para poder conectarse. Los mineros eligen entre un canal *estándar* y uno *extendido* en su propio firmware; recomiéndales *extendido*, porque así pueden verificar la coinbase que están hasheando. Aquí se aceptan los dos y ninguno necesita configuración por tu parte.

Un solo puerto para todo. Con `single_port = true` en `[stratum]`, el puerto sin cifrar (`[server] pool_listen`, 3333) acepta también Stratum V1 sobre TLS y Stratum V2. Cada conexión se distingue por sus primeros bytes y se entrega al servidor correspondiente, con los mismos límites, bloqueos y contadores que en el puerto propio de ese protocolo. TLS y Sv2 siguen necesitando sus propios listeners configurados como arriba, y esos puertos siguen funcionando. Detrás de un balanceador TCP, la cabecera PROXY va primero y se comprueba antes de reconocer el protocolo (capítulo 9). Desactivado por defecto.

9 · Detrás de un proxy inverso

Cuando la interfaz de estado se sirve por HTTPS a través de nginx o Caddy, fija tres claves en `[server]`:

```
[server]
status_public_url = "https://pool.example.com"
trust_proxy_headers = true    # so per-IP limits see the real client IP
cookie_secure = true          # UI is HTTPS
```

`status_public_url` indica la dirección pública del propio pool: un minero cuya configuración de pool apunta a ese host cuenta como minando aquí (pestaña «Mineros», aviso «El minero cambió a otro pool»). Fija `cookie_secure = true` siempre que se acceda a la interfaz por HTTPS.

> **Confía solo en las cabeceras de proxy que controlas.** Con `trust_proxy_headers = true` el daemon confía en la cabecera `X-Forwarded-For` para identificar la IP real del cliente. Actívalo **solo** cuando un proxy que controlas fije realmente esa cabecera; de lo contrario, un cliente podría **falsear su IP** saltándose directamente tus límites y baneos por IP.

Stratum detrás de un balanceador TCP: el protocolo PROXY

Los puertos Stratum son TCP puro y pasan por un balanceador L4 (HAProxy en modo TCP, nginx `stream`), nunca por el proxy HTTP. Detrás de un balanceador así el pool solo vería la dirección del balanceador — un solo minero problemático podría hacer que lo bloqueen. Desde v1.45 el balanceador puede enviar primero la dirección real del cliente (protocolo PROXY v1/v2, HAProxy `send-proxy-v2`, nginx `proxy_protocol on`); el pool la lee **solo** de las direcciones que indiques, que entonces **deben** enviarla:

```
[server]
pool_listen = "127.0.0.1:13333"       # daemon en puertos internos, el balanceador posee 333
[stratum]
stratum_tls_listen = "127.0.0.1:13334"
sv2_listen = "127.0.0.1:13336"
proxy_protocol = true
proxy_protocol_trusted = ["127.0.0.1"]   # direccion(es) del balanceador
```

Los límites de tasa, los bloqueos, el tope por IP y la página de workers muestran entonces al minero, no al balanceador. Ten en cuenta que toda conexión desde una dirección de confianza debe llevar la cabecera — un minero o sidecar local que se conecte directamente a los puertos del daemon se desconecta; apúntalo al balanceador.

10 · Lista de verificación de despliegue

Repasa esto antes de abrir el pool al público:

- ☐ `payout_mode = "per_worker"`, **sin** comisión del pool ni donación al operador (el daemon arranca; de lo contrario, falla en cerrado).
- ☐ Bitcoin Core accesible; considera `[node] template_source = "ipc"` para menor latencia (requiere Core ≥ 31 compilado con IPC; GBT sigue siendo el valor por defecto).
- ☐ `[ratelimit] enabled = true` con `autoban_enabled` y `reject_ban_enabled` activados.
- ☐ `max_connections_per_ip` fijado (salvo que tus mineros estén detrás de un solo NAT).
- ☐ TLS delante de Stratum (tu propio certificado para el firmware que solo admite CA públicas).
- ☐ Proxy inverso: `trust_proxy_headers` y `cookie_secure` fijados correctamente.
- ☐ Prueba un minero con `your-address.rig1`; confirma que aparece en `/users/<address>` y que sus shares se aceptan.
- ☐ Si publicas una página de aterrizaje, mantén las salvaguardas de honestidad: nada de «probado en batalla»; el bloque en mainnet es un «aún no».
- ☐ Pie de página `[legal]` opcional (enlaces de términos/privacidad) para un despliegue público o comercial.

11 · Soporte y enlaces

Guía en línea	docs.warppool.org/public-pool-setup.html
Código e incidencias	git.warppool.org/dvb-projekt/dvb-WarpPool
Comparativa de funciones	docs.warppool.org/comparison.html
Contacto	dvbprojekt@gmx.de

dvb-WarpPool es software libre y de código abierto (AGPL-3.0-or-later, con una licencia comercial disponible). Este manual describe la versión 1.52.0. Las pantallas pueden diferir ligeramente entre versiones. La minería en solitario es inherentemente probabilística; nada de lo aquí escrito es una promesa de recompensa. Un pool público al 0 % es non-custodial: el pool nunca retiene las monedas de nadie, y a quien encuentra el bloque le paga la recompensa completa directamente la red de Bitcoin.



Abierto, non-custodial, sin comisiones — y que quien lo encuentre se lo quede todo.