easyBTX

El manual de BTX

Qué es BTX, cómo funciona su minería, cómo llegó la cadena hasta aquí y dónde comprobar cada afirmación por tu cuenta.

> Solo con fines educativos y de entretenimiento. No es asesoramiento financiero. easyBTX no es el equipo central de BTX, y BTX no tiene un mercado público establecido.

PRIMERA EDICIÓN · CIFRAS AL 23 DE AGOSTO DE 2026 · EASYBTX.COM/BTX

Contenido

1 Quién escribió esto, y quién no

easyBTX hace software para BTX: un minero, una app de nodo y algunas herramientas gratuitas. **easyBTX no es el equipo central de BTX.** El software de consenso de la cadena lo escribe y lo publica el proyecto BTX, en el que easyBTX no participa y sobre el que no tiene ninguna autoridad. Leemos su código fuente y sus versiones igual que puede hacerlo cualquiera.

Eso importa para la forma en que deberías leer este manual. Nada de lo que hay aquí es un anuncio, una hoja de ruta ni una promesa en nombre de la cadena, porque no nos corresponde hacerlas. Es la lectura que un participante independiente hace de fuentes públicas, escrita para que puedas comprobarla. Donde el registro público no está claro, lo decimos, y donde nos hemos equivocado antes, también lo decimos.

Dos aclaraciones, porque la alternativa es dejar que supongas algo más amable que la verdad. Primero, a easyBTX le conviene que a BTX le vaya bien, y se lleva una comisión de la minería. Segundo, los proyectos que aparecen al final no son todos ajenos a nosotros. BTX en sí es genuinamente independiente, y esa es la separación que más importa. Pero btx.best y btxscan.io los construye easyBTX y así lo dicen en sus propios pies de página, y PQ Wallet, la wallet bonuz y qID comparten gente con easyBTX. Donde este manual describe esos productos, léelo como un participante que describe algo que ayudó a construir. La cadena, los pools y postquantum.wiki no son nuestros. Mencionarlos no es una garantía sobre ellos, y ninguno responde por los demás.

2 Qué es BTX

BTX es un fork de Bitcoin creado para sobrevivir a las computadoras cuánticas.

Bitcoin firma cada transacción con ECDSA, un esquema clásico de curva elíptica. Una computadora cuántica lo bastante grande podría romperlo y gastar monedas que no son suyas. BTX reemplaza ese esquema de firma por firmas poscuánticas, y por eso una dirección de BTX se ve distinta de una de Bitcoin: las direcciones de BTX empiezan con `btx1z`.

Todo lo demás tiene, a propósito, la forma de Bitcoin:

- Un suministro fijo de 21.000.000 de monedas, sin ninguna forma de emitir más.
- Sin preminado. Las monedas nacen únicamente como recompensa de minería, bloque a bloque.
- Minería por prueba de trabajo: no hay permiso que pedir ni filtro que superar.
- Autocustodia. No hay cuentas ni custodio. Tú tienes las claves y las claves tienen las monedas.

La cadena es joven. El bloque 0 lleva fecha del 19 de marzo de 2026, y el primer bloque se minó de verdad el 23 de marzo de 2026.

3 El trabajo es multiplicación de matrices

Los mineros de Bitcoin buscan hashes. Los mineros de BTX multiplican matrices, la misma aritmética densa para la que están construidos los aceleradores de IA modernos. Eso es lo que significa "matmul" allí donde aparezca en la documentación de BTX: multiplicación de matrices, usada como el trabajo que asegura la cadena.

El efecto práctico es que la GPU es la máquina natural para BTX y que el trabajo es un cálculo numérico real, no una lotería de hashes.

Conviene ser preciso sobre lo que eso significa y lo que no, porque es la afirmación que más se exagera. Las entradas de cada cálculo se derivan de la propia cadena, y solo se conserva un resumen criptográfico del resultado. Es decir, el producto calculado no se le entrega a nadie fuera de la cadena. **Hoy BTX no vende cómputo de IA.** Un mercado de cómputo verificable, en el que una parte externa envía un trabajo real y paga por el resultado, aparece en la propia especificación de BTX como una línea de trabajo futura, y no existe.

Lo que sí es cierto hoy es más discreto y más duradero: minar BTX le paga a una multitud distribuida de personas comunes por tener hardware capaz de ejecutar IA y mantenerlo encendido y en línea, en muchas manos independientes en lugar de en unos pocos centros de datos.

El minero easyBTX en easybtx.com, con la altura de la cadena en vivo, la emisión frente al tope de 21.000.000 y la cantidad de nodos públicos alcanzables.

4 Dos funciones de trabajo, y por qué existe la segunda

BTX ha tenido exactamente dos algoritmos de minería en toda su vida. Vale la pena decirlo con claridad, porque los números de versión que aparecen en los documentos de diseño de BTX se prestan a malentendidos: describen una hoja de ruta de investigación, no una sucesión de cadenas en producción.

MatMul v3 funcionó desde el primer bloque. Un intento era una sola multiplicación de matrices de 512 por 512 sobre un cuerpo primo elegido para que la aritmética encajara limpiamente tanto en CUDA como en Metal de Apple. Los intentos tardaban microsegundos, así que una tarjeta hacía millones por segundo, y las tasas de minería se expresaban de esa forma.

Tres cosas jugaban a su favor. El trabajo es álgebra lineal densa estándar, así que la máquina natural es una GPU y no un chip que no sabe hacer ninguna otra cosa. La construcción sobre la que se apoya añade una sobrecarga casi nula frente a una multiplicación de matrices corriente, así que muy poca de la electricidad se desperdicia en la maquinaria de la prueba en sí. Y dejaba abierta una puerta hacia un trabajo que algún día pudiera ser útil fuera de la cadena.

La v3 se endureció varias veces sin que cambiara el trabajo en sí. En el bloque 125.000 las matrices quedaron ligadas a la parte mutable de la cabecera del bloque, de modo que un minero ya no podía reutilizar un par ya preparado a lo largo de muchos intentos. En el bloque 130.500 quedaron ligadas también al bloque padre, de modo que no se podían construir plantillas contra un padre y reproducirlas después contra otro distinto que se hubiera retenido. Ninguno de estos cambios modificó lo que la minería calculaba. Cerraron atajos.

MatMul v4.7 reemplazó la función de trabajo en el bloque 185.000, el 10 de agosto de 2026. Un intento dejó de ser una multiplicación pequeña y pasó a ser un único episodio indivisible: cuatro rondas secuenciales sobre dieciséis capas, matrices de 4.096 de ancho, unos 141 billones de operaciones enteras de multiplicación y acumulación, unos 4,8 GB de memoria de GPU y del orden de treinta segundos de trabajo continuo. No se puede pausar un episodio, ni reanudarlo, ni hacer el sesenta por ciento de uno y recibir el sesenta por ciento del crédito.

Vale la pena entender el razonamiento, porque es lo contrario de lo que la gente supone. Una lotería con boletos extremadamente baratos invita a que alguien construya una máquina que no hace más que comprar boletos muy rápido. Encarecer cada boleto y volverlo secuencial y exigente con la memoria elimina casi todo ese margen: el trabajo ya es la operación para la que existen los núcleos tensoriales, así que queda poco que un chip especializado pueda hacer con más astucia, y no se puede saltar ningún paso porque comprobar un bloque reproduce el episodio exactamente. Los documentos de diseño mencionan directamente un segundo motivo: encarecer el alquiler de GPU de consumo hasta dejarlo fuera del alcance de un ataque contra una cadena joven.

El costo fue real y el proyecto nunca ha fingido lo contrario. Las Mac no pudieron minar en absoluto durante nueve días, porque el código que resuelve el nuevo trabajo no existía para Metal el día en que se activó. Los nodos que ejecutaban software antiguo se detuvieron en el bloque 184.999 y ahí se quedaron. La dificultad tuvo que recalibrarse en un factor de aproximadamente 120.000 de una sola vez. Los shares aceptados se volvieron lo bastante raros como para que una máquina en buen estado pueda pasar ahora una hora en silencio. Las tarjetas que minaban BTX con ganancia en julio hoy no lo minan en absoluto.

5 Cómo se comprueba un bloque, y cómo eso también cambió

La historia de la verificación es la parte que más vale la pena entender, y se movió en la dirección contraria a la que uno esperaría.

Con la v3, comprobar era ingenioso y barato. En lugar de rehacer una multiplicación de 512 por 512, quien verificaba multiplicaba la respuesta declarada por un par de vectores aleatorios y comparaba. Eso es el algoritmo de Freivalds, y con dos rondas un resultado falso tiene menos de una posibilidad entre 2 elevado a 62 de colarse. Caro de producir, barato de comprobar, que es justo la propiedad que uno quiere.

Con la v4.7 tal como funciona hoy, la red verifica reproduciendo el episodio entero de forma exacta y comparando resúmenes criptográficos. No hay comprobación barata. Esta es una decisión deliberada de despliegue por etapas, no un descuido: las pruebas sucintas, que volverían barata la comprobación otra vez, figuran como épocas posteriores y **ninguna de ellas tiene altura de activación**. El plan publicado menciona cuatro, de las cuales solo la primera está activa.

El proyecto lo dice sin rodeos, y vale más citarlo que parafrasearlo:

> El panorama de la verificación cambió de forma. En la etapa de la v4.7 que está activa ahora, la red verifica reproduciendo el episodio de forma exacta y comparando resúmenes criptográficos. Las pruebas sucintas que volverían barata la comprobación aparecen como una etapa posterior sin altura de activación. Así que la elegante propiedad de ser cara de producir y barata de comprobar es, por el momento, un objetivo de diseño y no el comportamiento desplegado.

Hay una consecuencia que importa a cualquiera que ejecute un nodo. Reproducir un episodio requiere una GPU que cumpla los requisitos, así que la mayoría de las máquinas no pueden comprobar por sí mismas el trabajo más reciente. En su lugar siguen un pequeño registro firmado, de 208 bytes por bloque. Por eso a la red le importa tanto que haya nodos dispuestos a servir esos registros, y por eso una interrupción en la firma congeló partes de la red dos veces en agosto de 2026, mientras la cadena en sí estaba bien.

6 Lo que aquí es genuinamente inusual

Dejando de lado el marketing, unas cuantas cosas de este diseño le resultan notables a cualquiera que lea código de consenso para ganarse la vida.

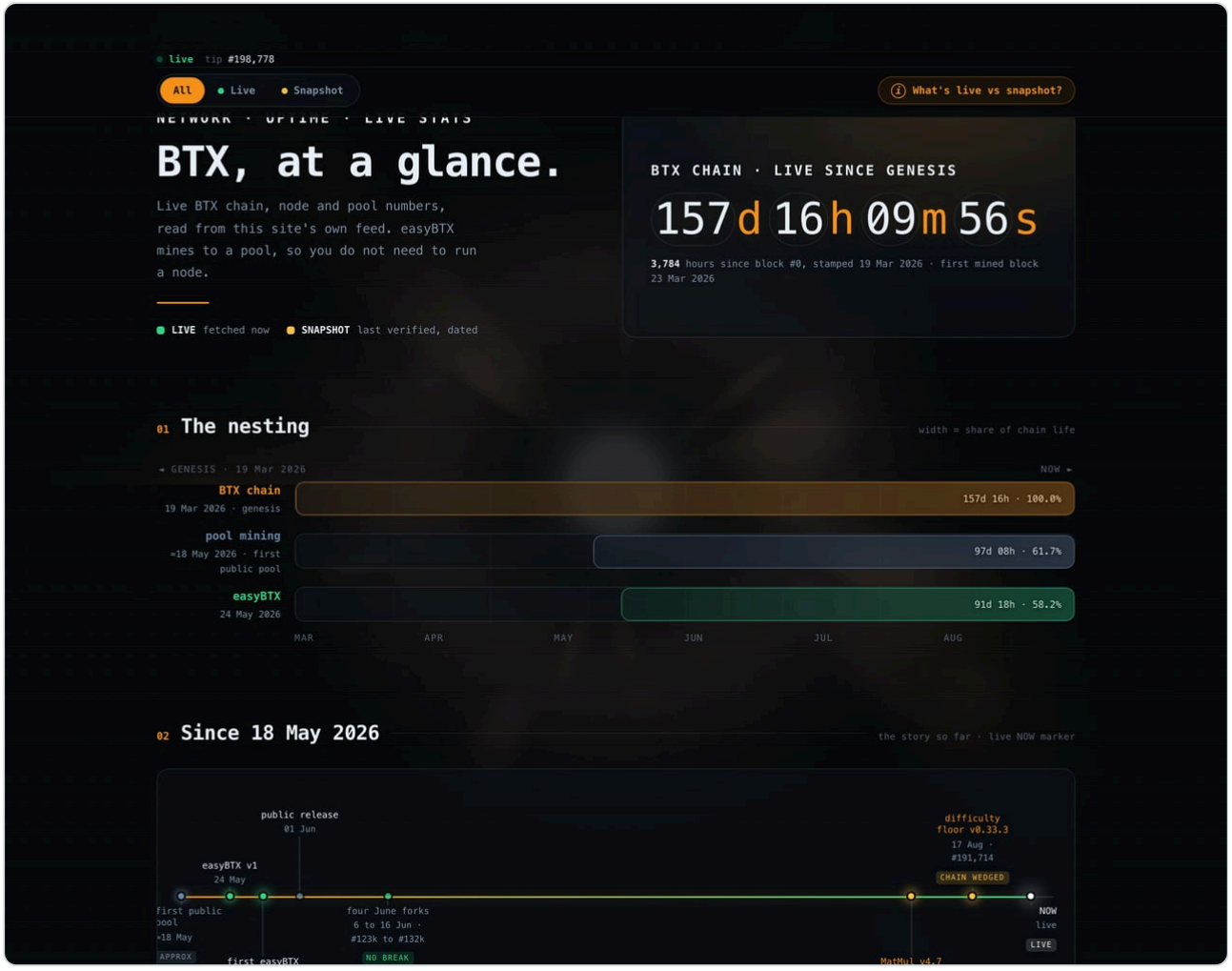
- **El trabajo es de verdad álgebra lineal densa de enteros**, determinista y exacto byte a byte en dos backends de GPU independientes. El hardware de dos fabricantes distintos tiene que producir un resumen criptográfico idéntico.
- **El cambio en el costo por intento es un cambio de categoría**, de microsegundos a unos treinta segundos. Muy pocas cadenas lo intentan, y hace que un intento sea genuinamente indivisible.
- **La elegibilidad para minar es una medición, no una lista.** El software le pide a un dispositivo que reproduzca un resultado conocido y da por buena la respuesta, en lugar de comparar el nombre del chip con una lista de permitidos. Tanto easyBTX como el fabricante del motor publicaron requisitos de hardware que resultaron ser incorrectos, y en ambos casos la corrección vino de medir.
- **La cabecera nunca cambió.** Un reemplazo total de la prueba de trabajo se lanzó sin añadir un solo byte a la cabecera de bloque de 182 bytes, y por eso los pools, los mineros y los protocolos de

red sobrevivieron intactos al cambio. Eso no tiene glamour y es genuinamente difícil.

Nada de esto significa que el trabajo le sirva todavía a alguien fuera de la cadena. No le sirve, y la sección 2 lo dice. Pero la maquinaria es real, las cifras de arriba están en el código fuente del consenso y no en un folleto, y el proyecto documenta sus propias elecciones de parámetros descartadas y deshabilita en código sus propios componentes sin terminar. Eso es mejor señal que cualquier afirmación.

7 Breve historia de la cadena

CUÁNDO	ALTURA	QUÉ PASÓ
19 mar 2026	`0`	Se sella el bloque génesis, con MatMul v3 como función de trabajo desde el principio. El primer bloque se minó el 23 de marzo.
principios de jun 2026	`~123.000`	El fork de la v0.31.0.
8 jun 2026	`125.000`	Las semillas quedan ligadas a la cabecera, así que un par de matrices ya preparado no puede servir para muchos intentos.
mediados de jun 2026	`~130.500`	Las semillas quedan ligadas también al bloque padre, lo que cierra un atajo de reutilización de plantillas. La función de trabajo no cambia.
mediados de jun 2026	`~132.000`	Una actualización del nodo.
10 ago 2026	`185.000`	Se activa MatMul v4.7. Un intento pasa a ser un episodio de treinta segundos.
17 ago 2026	`191.690`	La red se traba. BTX Core v0.33.3 sale el mismo día con un piso de dificultad en el bloque 191.714, y la cadena se recupera.
22 ago 2026	`197.000+`	Unos 3,96 millones de BTX emitidos, alrededor del 19 por ciento del tope.



La página de estadísticas en vivo en easybtx.com/stats, que lee la cadena, el censo de nodos y todos los pools en funcionamiento.

8 Suministro y emisión

Cada bloque paga 20 BTX. El intervalo objetivo es de 90 segundos, aunque el promedio observado a lo largo de la vida de la cadena ha sido más rápido que eso. La recompensa se reduce a la mitad cada 525.000 bloques, y el calendario es exacto: 525.000 bloques a 20, luego a 10, luego a 5 y así sucesivamente suman exactamente 21.000.000.

Todavía no ha ocurrido ningún halving. El primero está por venir.

Al momento de escribir esto la cadena había pasado el bloque 197.000, así que se habían emitido unos 3.960.000 BTX, algo menos del 19 por ciento del tope. Para cifras actuales en lugar de estas, consulta la página de estadísticas en vivo que aparece al final de este manual.

9 ¿Se puede falsificar BTX?

No, y las razones son estructurales, no promesas.

El suministro está fijado en 21.000.000, no hubo preminado y las monedas solo se crean minando. BTX es una cadena derivada de Bitcoin y sin capa de tokens, así que no existe ningún mecanismo para emitir una moneda falsa sin romper las reglas que cada nodo hace cumplir de forma independiente. Cada moneda es rastreable, bloque a bloque, hasta una recompensa de minería.

Esa es una pregunta distinta de si la cadena puede ser atacada. Una fracción suficientemente grande de la potencia de minería de la red podría reordenar los bloques recientes, lo cual es cierto en toda cadena de prueba de trabajo, incluida Bitcoin. El archivo de investigación incluye un estudio completo de lo que es posible y lo que no, junto con los pasos para verificar la autenticidad por tu cuenta.

10 Tres formas de participar

Mínalo. easyBTX es una sola app para Mac, Windows y Linux. Se une a un pool de minería, paga a una wallet que tú controlas y se mantiene actualizada sola. Una Mac necesita Apple silicon y macOS 26.4 o posterior, y si una Mac concreta puede minar lo decide una comprobación de medio segundo que la app ejecuta sobre la GPU, no el nombre del chip. En Windows se ejecuta la compilación de Linux bajo WSL2. En Linux hace falta una GPU NVIDIA. Todas las comisiones se indican por adelantado: easyBTX cobra el 4,99%, el pool cobra la suya y, en Windows y Linux, el motor MATADOR cobra un 1% adicional. Hoy no hay minería en solitario en ninguna plataforma.

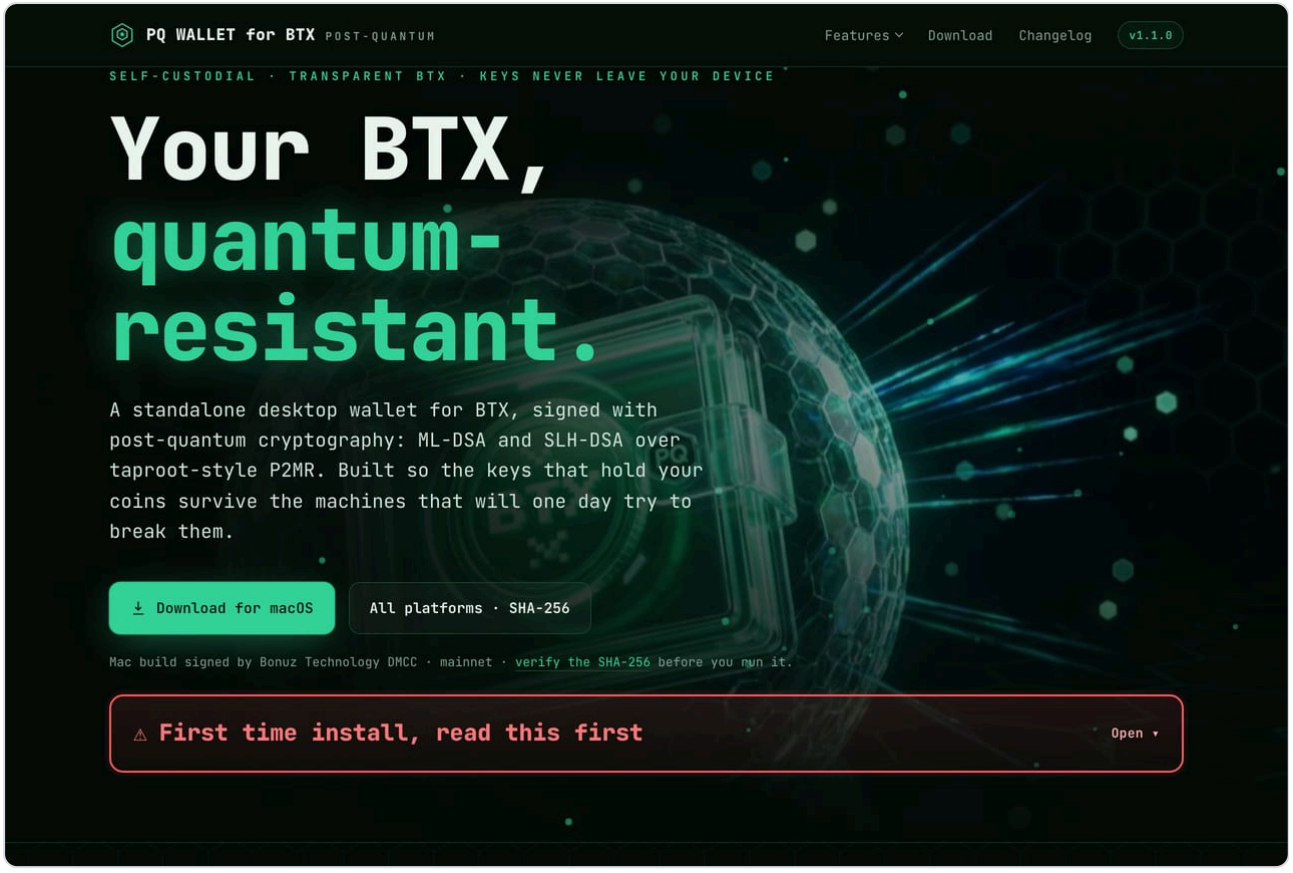
Verifícalo. Ejecutar un nodo completo es la única manera de responder preguntas sobre la cadena sin confiar en el servidor de otra persona. easyNode lo reduce a un clic en las tres plataformas. Node Guardian diagnostica un nodo que dejó de avanzar, y Keeper convierte una máquina que tengas de sobra en una que sirve confirmaciones de bloque firmadas, el recurso más escaso de la red.

Guárdalo. Las direcciones de BTX son poscuánticas y las claves se quedan en tu máquina. El minero trae una wallet integrada; dos wallets dedicadas van más lejos, una de escritorio y otra móvil.

11 Wallets, y cómo iniciar sesión sin cuenta

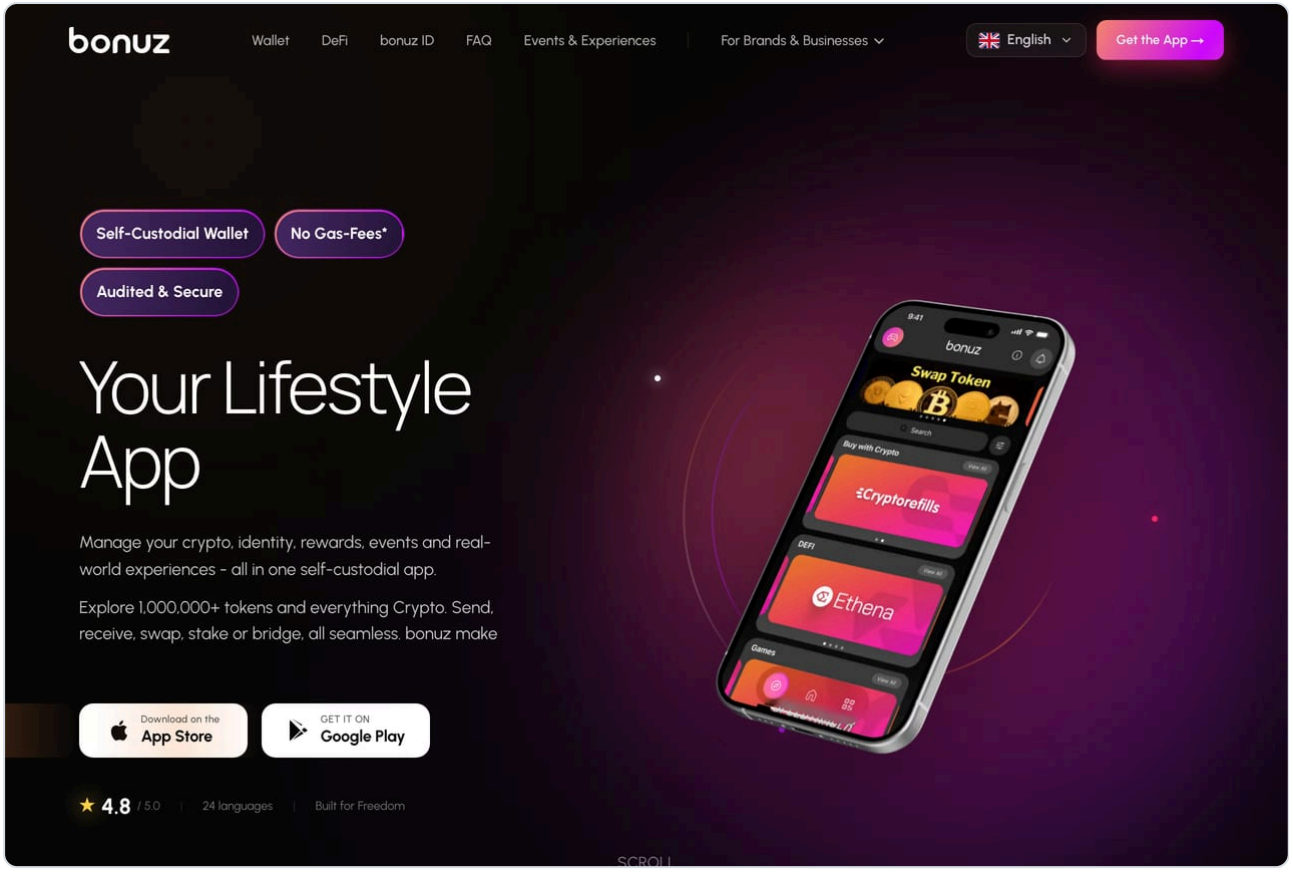
Una wallet de BTX es una clave que tú controlas, así que elegir una es elegir dónde vive esa clave.

PQ Wallet es la wallet de escritorio, para macOS, Windows y Linux. Firma con esquemas poscuánticos y guarda la clave en la máquina.



PQ Wallet, la wallet de escritorio poscuántica para BTX.

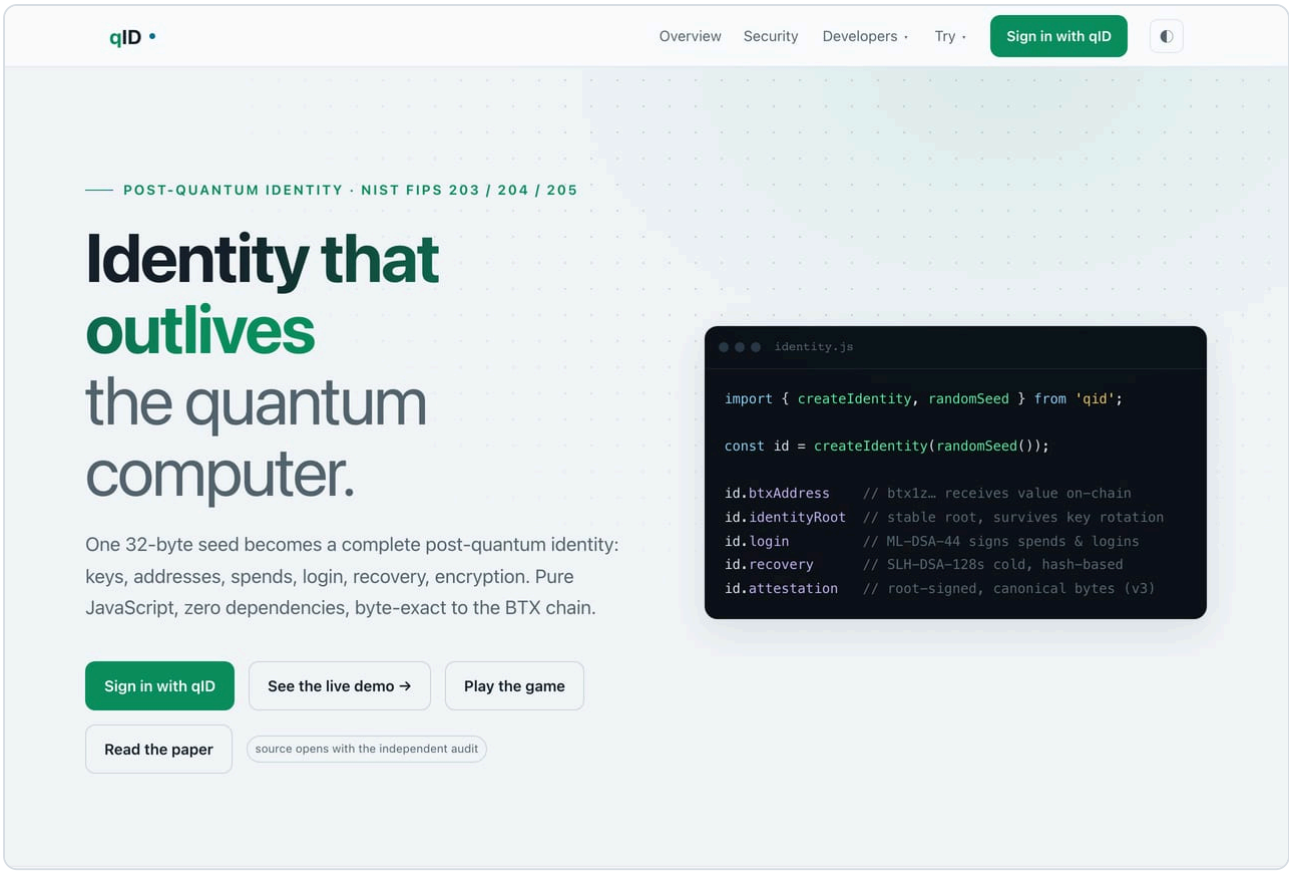
bonuz es la wallet móvil, para iPhone y Android, y lleva tu identidad en la cadena junto con las monedas.



bonuz, la wallet móvil para BTX.

Las dos son de autocustodia y ninguna te pide registrarte. El minero también trae una wallet integrada, que basta para recibir lo que mines, y si lo prefieres puedes dirigir los pagos a cualquiera de las dos wallets anteriores.

qID es la pieza que conecta una wallet con un sitio web. Los sitios de BTX la usan para iniciar tu sesión: en lugar de un correo y una contraseña, demuestras que controlas tu clave. Vale la pena ser preciso sobre lo que el sitio llega a saber. No sabe tu nombre, ni tu correo, ni tu clave. Sí sabe tu dirección de BTX, y una dirección de BTX es una entrada pública en el libro contable de la cadena, así que un sitio en el que inicies sesión puede consultar qué tiene esa dirección y qué ha hecho. Eso es una contrapartida real, y no es lo mismo que el anonimato. Hay algo que qID hace bien y que merece decirse con todas las letras: una prueba de inicio de sesión nunca puede mover tus monedas. Los inicios de sesión y las transacciones se firman sobre resúmenes criptográficos distintos y etiquetados por separado, así que una firma hecha para iniciar sesión no puede reutilizarse como la firma de una transacción. Una sola semilla de 32 bytes se convierte en toda una identidad poscuántica: claves, direcciones, gastos, inicio de sesión y recuperación, y esa misma semilla puede guardar valor en la cadena. Si has usado wallet-connect en otra cadena, qID es esa misma idea reconstruida para que sobreviva a una computadora cuántica.

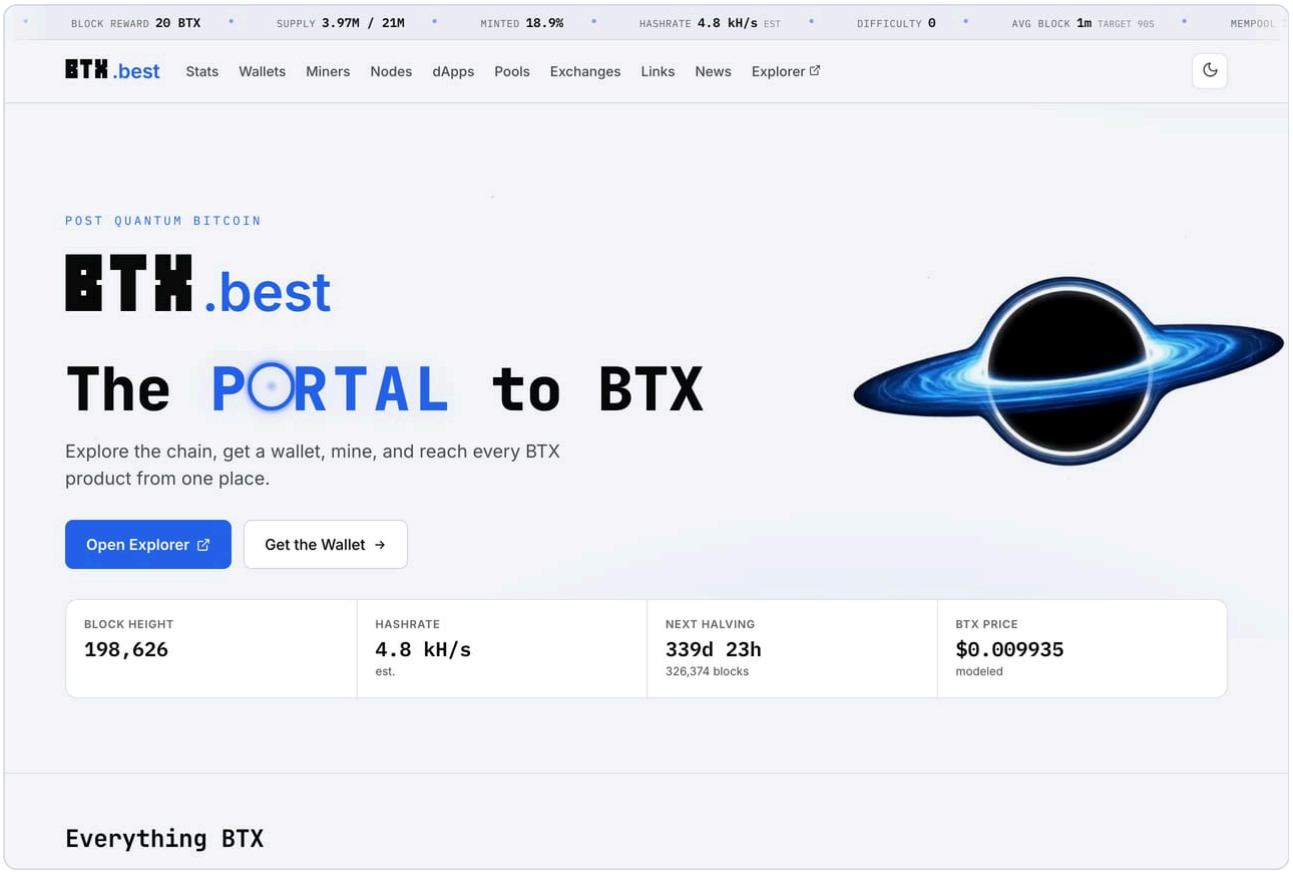


qid.dev, la identidad poscuántica que los sitios de BTX usan para iniciar sesión.

12 Dónde aprender más

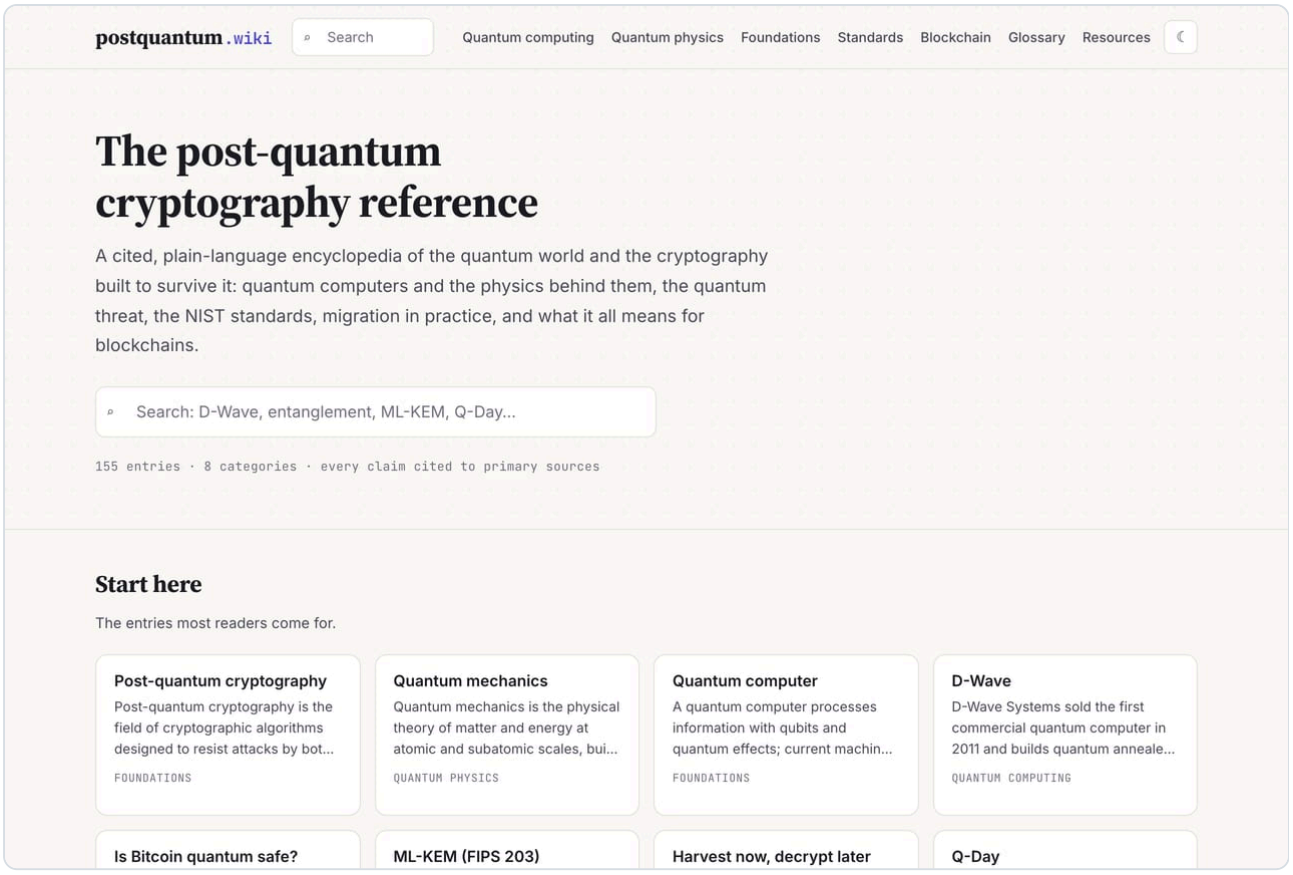
Dos lugares valen más que el resto.

btx.best es el portal. Reúne en una sola página todos los productos, herramientas, exploradores, wallets, pools y dApps de BTX, organizados según lo que quieras hacer. Si de este manual solo vas a guardar una dirección y no sabes cuál, que sea esa.



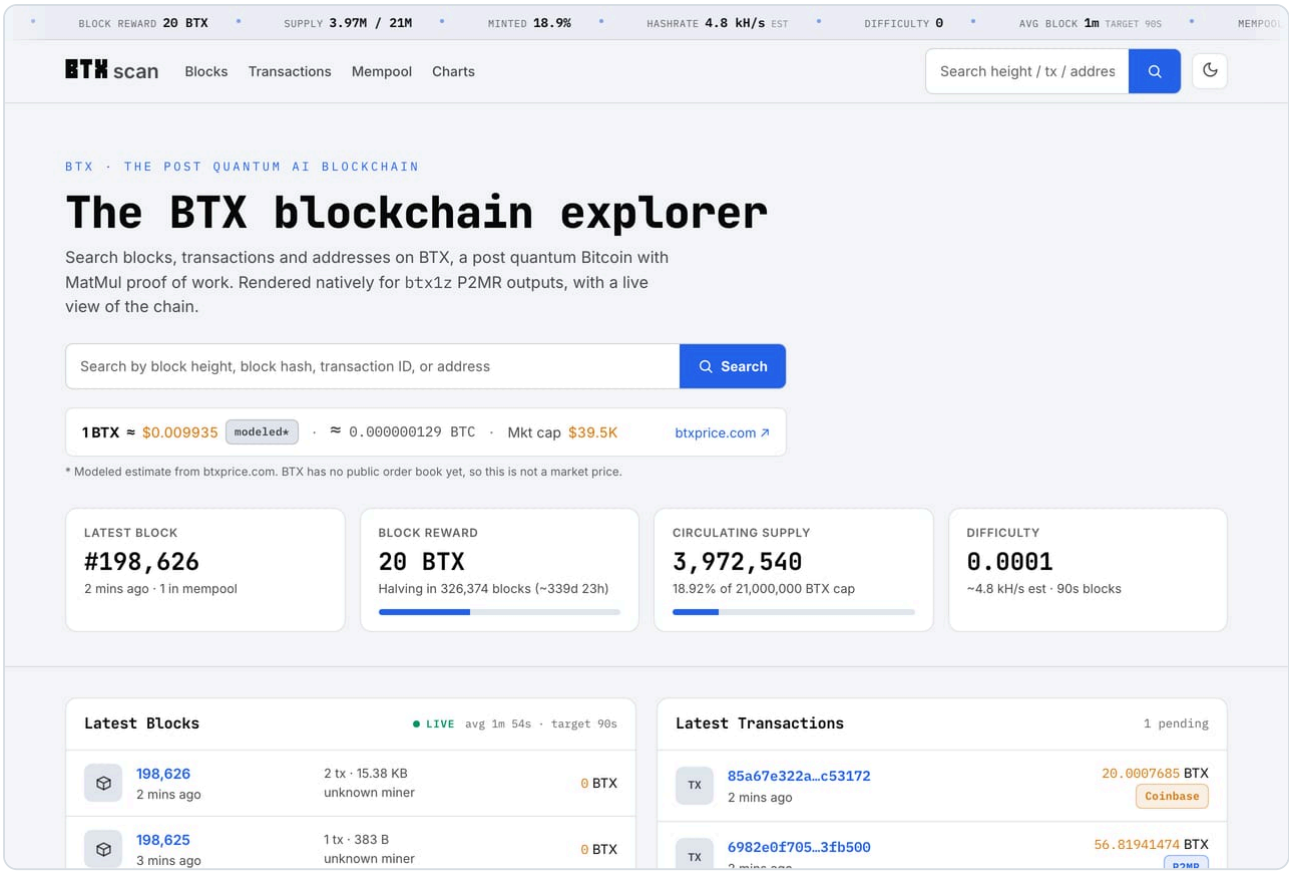
btx.best, el portal que reúne todos los productos y enlaces de BTX en un solo lugar.

postquantum.wiki es la referencia para la criptografía que hay debajo. Es una enciclopedia con fuentes y en lenguaje claro sobre computación cuántica y los esquemas creados para sobrevivir a ella, incluidos los estándares del NIST en los que se basan las firmas de BTX. Sirve tanto si quieres la versión de un párrafo como si quieres los estándares mismos.



postquantum.wiki, una enciclopedia de criptografía poscuántica con fuentes y en lenguaje claro.

Para BTX en concreto, el explorador de bloques es donde compruebas cualquier cosa que te hayan dicho.



btxscan.io, el explorador de bloques de BTX.

13 La parte honesta

Un manual que solo enumera buenas noticias es un anuncio. Esto es lo que vale la pena saber antes de gastar electricidad o atención.

- **BTX no tiene un mercado público establecido.** Cualquier precio que encuentres son dos personas poniéndose de acuerdo en privado. Trata lo que mines como algo incierto, nunca como ingreso.
- **Minar cuesta electricidad de verdad** y exige mucho a tu GPU, lo que significa calor y consumo.
- **Las apps todavía no tienen firma de código.** Por eso algunos antivirus las marcan, y por eso también cada compilación publica un SHA-256 que puedes comprobar tú mismo antes de ejecutarla.
- **Los shares son raros después del fork.** Una hora en silencio suele ser suerte, no una falla.
- **Haz una copia de seguridad de tu wallet.** Ninguna parte de este proyecto puede recuperar tus claves, que es el sentido de la autocustodia y también su costo.

Dónde está todo

Vale la pena guardar todas las direcciones de esta lista. Ninguna te pide una cuenta, y las marcadas como datos devuelven JSON sin necesidad de clave. No todos son ajenos a nosotros: btx.best y btxscan.io los construye easyBTX, y PQ Wallet, la wallet bonuz y qID comparten gente con easyBTX. La cadena, los pools y postquantum.wiki no son nuestros. Si alguna vez un enlace contradice esta página, hazle caso al enlace.

EMPIEZA POR AQUÍ

`easybtx.com/btx`	Este manual como página web viva, siempre actualizada.
`btx.dev`	El sitio del proyecto BTX.
`btx.best`	El portal de BTX. Todos los productos, herramientas y enlaces del ecosistema, en un solo lugar.
`btxscan.io`	El explorador de bloques. Consulta cualquier bloque, dirección o transacción.

SOFTWARE

`easybtx.com/install`	easyBTX, el minero de un clic para Mac, Windows y Linux.
`easybtx.com/node`	easyNode, un nodo BTX completo como app de escritorio.
`easybtx.com/guardian`	Node Guardian, un script gratuito que diagnostica un nodo que dejó de avanzar.
`easybtx.com/keeper`	Keeper, un pequeño nodo podado que sirve confirmaciones de bloque firmadas.

GUARDAR BTX

`easybtx.com/wallet`	Qué wallet usar y por qué hay dos.
`pq-wallet.com`	PQ Wallet, poscuántica, para macOS, Windows y Linux.
`bonuz.xyz`	bonuz, la wallet móvil.
`qid.dev`	qID, la identidad poscuántica que los sitios de BTX usan para iniciar sesión.

LECTURAS Y EVIDENCIA

easybtx.com/research/	El archivo de investigación. Con fuentes, fechado y nunca reescrito en silencio.
easybtx.com/stats	Cifras en vivo de la cadena, los nodos y los pools.
easybtx.com/nodes	Un mapa en vivo de cada nodo público alcanzable.
postquantum.wiki	Una enciclopedia de criptografía poscuántica con fuentes y en lenguaje claro.

PARA MÁQUINAS

easybtx.com/ai	Escrito para agentes autónomos: endpoints abiertos y límites honestos.
easybtx.com/api/network	Altura de la cadena, emisión, censo de nodos y pools, en JSON, sin clave.
easybtx.com/llms.txt	Un resumen de este sitio para modelos de lenguaje.

PERSONAS

t.me/easyBTX	El Telegram de easyBTX, donde se responden las preguntas.
x.com/easyBTX	Notas de versión y actualizaciones breves.
github.com/MendeMatthias/EasyBTX-releases/releases	Todas las compilaciones publicadas, con sus sumas de verificación.

LÉELO, POR FAVOR

Solo con fines educativos y de entretenimiento. Nada en este manual es asesoramiento financiero, una oferta ni una recomendación para comprar, vender o minar nada. Publicado por easyBTX, que crea software para BTX y no es el equipo central de BTX. Este no es un documento oficial. BTX no tiene un mercado público establecido, minar puede no darte nada, y eres responsable de tus propias decisiones.