

Zcash, la nueva criptomoneda que podría sustituir al Bitcoin

La nueva moneda digital se basa en los métodos clásicos de financiación del sistema económico actual, ofreciendo una alternativa libre, anónima y con la protección de la privacidad

Los usuarios, los inversores y hasta el mismísimo Edward Snowden, todos parecen entusiasmados por una nueva criptomoneda que ha nacido hoy, pero que lleva meses causando revuelo en la red. Se llama Zcash, y promete ser una alternativa al Bitcoin que cuida de la privacidad de los usuarios mientras se ofrece como un negocio real para los inversores.

Zcash ha nacido a partir del proyecto Zerocoin, que tras empezar siendo una capa de anonimato criptográfico para el Bitcoin acabó convirtiéndose en una criptomoneda independiente. Como las expectativas son muchas y puede que a partir de ahora escuchéis hablar bastante de ella, os vamos a contar qué es exactamente Zcash y cuales son sus diferencias fundamentales con el Bitcoin.

¿Qué es lo que hace el Zcash tan atractivo?

Mucho se ha hablado sobre la privacidad y el pseudoanonimato que hay detrás de la tecnología del Bitcoin. A diferencia de la mítica criptomoneda, el Zcash oculta automáticamente las identidades de emisores y receptores, así como el monto de todas las transacciones que realizamos en su blockchain. Solo quienes tengan una clave de visualización podrán ver el contenido de las operaciones.

Esto es posible gracias un algoritmo llamado zero-knowledge proofs (conocimiento cero pruebas). Este algoritmo permite que el creador de la transacción pueda incluir en ella una prueba validez sin necesidad de transmitir ninguna información aparte del hecho de que la transacción es cierta. Por lo tanto, no se transmite información que cualquiera pueda leer.

Estas características han hecho que voces tan destacadas en el mundo de la privacidad como Edward Snowden hablen bien del proyecto, refiriéndose a él como una solución a los riesgos de vigilancia de los registros de las transacciones públicas en Bitcoin.

Otra de sus diferencias fundamentales entre la mayoría de las criptomonedas y esta es la manera en al que se organiza. Como el Bitcoin y todas las basadas en él, su código es abierto, aunque no es administrado como una comunidad como la mayoría, sino que Zcash es una empresa. Eso hace el producto atractivo para los inversores.

La manera de desarrollar el proyecto también ha sido el inverso, ya que en vez de lanzar la moneda y buscar luego financiación, los creadores de Zcash han buscado inversores para crear la moneda antes de lanzarla. También prometen recompensar a estos inversores y trabajadores con un impuesto al que llaman "Founders reward", descrita así en su web:

"La base monetaria de Zcash será el mismo que el de Bitcoin - 21 millones de unidades de moneda Zcash (ZEC o ?) serán minadas. El 10% de los beneficios serán distribuidos entre los accionistas - fundadores, inversores, empleados y consejeros".

Esto ha hecho que la moneda haya crecido exponencialmente antes de ser lanzada. El 15 de septiembre su valor era de 18 dólares o 0,027 BTC, pero hace dos días ya había subido hasta los 260 dólares o 0,379 BTC, marcándose un crecimiento de cerca del 1.300%. Es más, algunos analistas del mercado creen que el precio de un ZEC sobrepasará al de un bitcoin para finales de año, ya que los inversores no quieren dejar pasar esta oportunidad.

Por lo tanto, tenemos una criptomoneda que no intenta ir contra el sistema, sino que se basa en sus métodos clásicos de financiación para ofrecer una alternativa libre, anónima y que promete poner la privacidad de sus usuarios por encima de todo. Y lo que es más importante, que los inversores no quieren dejar escapar al próximo Bitcoin, lo que está impulsando muy fuertemente su crecimiento inicial.

La aventura no está exenta de riesgos

Pero como todas las nuevas tecnologías, no hay nada que pueda garantizar un éxito asegurado, y siempre hay un factor de riesgo a tener en cuenta. Expertos en Bitcoins han descrito el Zcash como una propuesta interesante y novedosa, pero que su alta privacidad no deja de tener sus retos tecnológicos.

El desarrollador y operador de Bitcoins BTCDrak se ha referido a la moneda como lo último en criptografía, aunque dice que hay muchas pruebas de que van a necesitar una gran cantidad de CPU para firmar las transacciones. De hecho, casi todos los detractores están preocupados por las exigencias y la escalabilidad de la cadena de bloques.

Además, quienes llevan tiempo queriendo regular el mercado de las criptomonedas posiblemente tampoco estén muy contentos, así como quienes ven en ella un vehículo para cometer más crímenes en la red. Los creadores se defienden de esto último asegurando que eso es como culpar a todo Internet de los crímenes de unos pocos, y que la mayoría de las operaciones que se van a realizar con su moneda van a ser legítimas.

La noticia Qué es el Zcash y por qué muchos ven en esta criptomoneda el sustituto perfecto al Bitcoin fue publicada originalmente en Xataka por Yúbal FM .

Datos de contacto:

Nota de prensa publicada en:

Categorías: [Finanzas E-Commerce](#)

NotasdePrensa

<https://www.notasdeprensa.es>