Masterhacks – Las carteras bitcoin móviles envían transacciones a la blockchain convencional, pero de una forma diferente a las opciones predeterminadas del monedero. Esto podría causar problemas a partir de noviembre, ya que el protocolo de bitcoin experimentará otro cambio importante.

Luego de la activación del código de actualización de SegWit, un grupo de empresas tratan de activar un hard fork para aumentar el tamaño de los bloques de bitcoin y ampliar más su capacidad de transacción. El código forma parte de una actualización más grande denominada como SegWit2x, que podría hacer que el bitcoin sufra otra división, esto si no todos apoyan dicha actualización.

Los desarrolladores de SegWit2x tratan de que todos los usuarios de bitcoin permanezcan en la misma cadena de bloques.

Jeff Garzik, desarrollador principal de SegWit2x, afirmó a CoinDesk lo siguiente:

> *«El objetivo del diseño de SegWit2x, al igual que el último fork ethereum, es actualizar bitcoin, no crear una nueva criptomoneda».*

Para esto, los desarrolladores que respaldan el proyecto tomaron algunas decisiones, controvertidas para algunos, que tienen que ver con mantener la compatibilidad con las billeteras de *«verificación simplificada de pagos»,* un término técnico para aplicaciones de monedero bitcoin basadas en teléfonos inteligentes.

Sin embargo, los desarrolladores alegan que existen pros y contras sobre cómo se trata de lograr esto, ya que por un lado, no es muy seguro para los usuarios de monederos móviles realizar transacciones inmediatamente después de que se promulgue el hard fork.

Entre las decisiones de diseño de este hard fork está la de omitir la *«protección de reproducción».* Esto describe lo que ocurre cuando un blockchain se divide en dos, ya que los usuarios de pronto tendrán el mismo valor en ambas cadenas de bloques. Esto quiere decir

que cuando los usuarios mueven tokens en una cadena de bloques, los tokens también se «reproducen» en la otra.

Pero esto no es visible para los usuarios que podrán no saber que tienen dinero en dos redes durante una división de red. Lo peor, es que los usuarios podrían perder parte de su dinero y ni siquiera darse cuenta.

«Se vuelve impredecible qué dinero se está moviendo y cuando», dice el CMO Bread Wallet Aaron Lasher a CoinDesk.

Debido a que no todos están de acuerdo con SegWit2x, algunos llegaron a escribir manifiestos en la oposición, por lo que es probable que se divida en dos redes competidoras, lo que podría ser confuso para los usuarios generales.

Los desarrolladores de SegWit2x por su parte, tienen una razón para dejar la protección de reproducción, esta es mantener SegWit2x compatible con las billeteras móviles SPV.

> *«La protección de reproducción, como ustedes lo llaman, divide la cadena. Simplemente no tiene sentido. Se estarían rompiendo más de 10 millones de clientes SPV que de otra forma funcionarían bien. Es un objetivo de SegWit2x ayudar a evitar esto»,* dijo el CEO de BitGo, Mike Belshe, a CoinDesk por correo electrónico.

Esto significa que la protección de reproducción causaría inconvenientes para los usuarios de carteras móviles que quieran pasar a la cadena de bloques SegWit2x, por lo que los desarrolladores de esta no planean agregarlo.

Las decisiones respecto a carteras móviles

Muchos proveedores de este tipo de carteras, como Electrum y Bread Wallet, confían en SPV.

Con esto se elimina la necesidad de contar con una copia completa de la cadena de bloques, por lo que los datos son más fáciles de almacenar en los teléfonos celulares con poca capacidad de almacenamiento.

Pero esto tiene algunos inconvenientes. Los monederos SPV seguirán automáticamente a cualquier versión de bitcoin que tenga la mayor cantidad de mineros que la respalden. Por lo que si bitcoin se divide y SegWit2x atrae más potencia de cómputo que la blockchain heredada, todas las carteras SPV le seguirán.

Por lo tanto, algunos proveedores de carteras móviles no están felices con esto, ya que no encuentran forma de explicar a los usuarios lo que ocurre.

«Es realmente difícil para nosotros porque estamos muy afectados», afirma Lasher.

Esto definitivamente también causaría problemas técnicos. Si existen dos bitcoins, el software de monedero móvil podría confundirse sobre qué cadena seguir, especialmente si los mineros cambian entre blockchains con el tiempo.

> *«Podría confundir a los clientes de SPV y provocar que los clientes cambien de cadena en cadena, haciendo que pierdan dinero dependiendo de qué cadena tenga más trabajo y en qué punto»,* afirma Matt Corallo, ingeniero de Chaincode.
>
> Por su parte, Novak afirmó a CoinDesk que *«con SPV no se sabe si el nodo al que está conectando le está mintiendo. Por ejmplo, un nodo SegWit2x puede suplantar como un nodo bitcoin en la otra cadena, lo que significa que sin la protección de reproducción su billetera puede gastar los fondos en la cadena incorrecta y perderlos en la cadena correcta».*

De forma general, los desarrolladores crean una varierad de escenarios «si entonces». Lasher admite esto y afirma que no está claro cuales se desarrollarán realmente.

«Muchas cosas pueden suceder y todas están en la escala de algo molesto a francamente peligroso», dice Lasher. Agrega también que Bread Wallet planea alentar a los usuarios a dejar de hacer transacciones durante el hard fork.

Debido al desorden en la capa de aplicaciones, los desarrolladores de protocolos han estado discutiendo acerca de la mejor forma de manejar lo que podría suceder.

James Hilliard, colaborador de Bitcoin, sugirió un cambio en la base de código SegWit2x que argumenta que daría a las carteras móviles mayor control sobre el bitcoin en el que finalmente aterrizarían.

Sin embargo, los desarrolladores de SegWit2x afirman que este cambio dificultaría a los usuarios la transición a una cadena de bloques con un aumento de tamaño de bloque, lo muchos usuarios planean hacer, para poder realizar transacciones más baratas.

Pero nuevamente, otros aseguran que esto confundirá a los usuarios y podría hacer que quieren no conozcan la situación pierdan dinero.

Algunos desarrolladores están de acuerdo en que es necesario que exista un aumento en el parámetro de tamaño de bloque, pero no están de acuerdo con algunas decisiones de diseño de SegWit2x.

> *«Puede haber algunos méritos en un aumento del tamaño de un bloque. Pero no estamos de acuerdo con la forma actual en que se está llevando a cabo»,* concluye Lasher.