



La red Bitcoin activó exitosamente la bifurcación suave Taproot

La red Bitcoin activó exitosamente la bifurcación suave Taproot, después de un consenso de bloqueo del 90% de los mineros y los grupos de minería entre los bloques 709,488 y 709,632. Este hito significa la primera actualización importante para Bitcoin desde agosto de 2017, que vio el lanzamiento de la solución líder de capa dos de Bitcoin, Lightning Network y Segregated Witness (SegWit).

La actualización de Taproot tiene como objetivo mejorar las capacidades de scripting y la privacidad de la red Bitcoin. Para hacer esto, la bifurcación suave introduce el concepto de árbol de sintaxis abstracta merkelizada (MAST). Según un [sitio web](#) dedicado a Taproot dirigido por el destacado desarrollador de Bitcoin, Hampus Sjöberg.

«MAST puede ayudar a que los contratos inteligentes sean más eficientes y privados al revelar solo las partes relevantes del contrato cuando se gasta».

Sjöberg señaló que la activación de Taproot muestra que Bitcoin puede realizar actualizaciones de red nuevamente, lo cual es extremadamente importante para la longevidad de la red Bitcoin. «Creo que es la mejor victoria», agregó.

Sjöberg, quien también es un desarrollador de una billetera Blixt Wallet de bitcoin Lightning, cree que la actualización de Taproot permite explorar las capacidades fuera de la cadena, para no poner demasiada carga en los nodos de Bitcoin de la red.

Además, Sjöberg cree que MAST también puede ayudar a mejorar la privacidad de la antigua Lightning Network «si las implementaciones Lightning optan por adoptar Taproot». Los desarrolladores de las diversas implementaciones en nodos de Lightning Network se reunieron en Zurich, Suiza, hace solo unas semanas en la [LN Summit 2021](#) para discutir posibles rutas de actualización:

«Una de las cosas que se discutieron en la reunión fue si es mejor actualizar Lightning en pequeñas iteraciones o hacerlo como un paquete grande».



Además, Sjöberg explicó cómo los canales de pago en circunstancias normales pueden hacerse indistinguibles de las transacciones normales utilizando Taproot para Lightning Network:

«No es posible saber si una transacción de Taproot es solo un pago normal o si pertenece a un canal Lightning. Esto es importante para la fungibilidad, y por lo tanto, la resistencia a la censura de Bitcoin».

La activación exitosa de Taproot se atribuye a Speedy Trial, un método de implementación de bifurcación suave que requiere que el 90% de los mineros señalen la implementación de la actualización. Como explicó Sjöberg, *«el método de señalización funciona en períodos de bloques de 2016, lo que significa que dentro de un período de bloque de 2016, el 90% o 1815 de los bloques de 2016 deben indicar que están listos».*

En junio de 2021, los mineros de Bitcoin lograron un consenso del 90% por primera vez y Sjöberg tuiteó el anuncio.

Sin embargo, la actualización de Taproot también marca el final de las implementaciones de Speedy Trial y las actualizaciones futuras de la red de Bitcoin requerirán la provisión de nuevos métodos de implementación de bifurcaciones suaves.

Taproot abre un mundo de posibilidades, pero lo primero que personalmente me gustaría ver es una transacción MuSig2, dijo Sjöberg.

«Si bien no debemos dar nada por sentado en Bitcoin, personalmente me gustaría ver eventualmente la agregación de firmas de entrada cruzada como una futura bifurcación para Bitcoin», agregó.

En los casi 13 años de existencia de Bitcoin, la red ha pasado por numerosas bifurcaciones



La red Bitcoin activó exitosamente la bifurcación suave Taproot

duras y blandas impulsadas por la comunidad. Aunque la actualización Taproot aún debe demostrar su valor en el futuro, Lightning Network sigue alcanzando nuevas alturas.

El 28 de septiembre, Lightning Network fue testigo de un aumento del 160% en la cantidad de nodos en el lapso de 12 meses, además de ver un salto del 170% en la cantidad de canales desde enero de 2021.

A partir del 11 de noviembre, la capacidad de la red de Bitcoin antes de la bifurcación suave Taproot estaba en un máximo histórico de 3220 BTC, con un valor de casi 210 millones de dólares.