BIP 174 o Propuesta de Mejora de Bitcoin 174, fue agregada al repositorio de Bitcoin, por lo que ahora las Transacciones Parcialmente Firmadas (PSBT) facilitan las transacciones multifirma.

Con esto es posible que se firmen transacciones offline y que exista un formato común para la información necesaria para realizar el proceso. Algunos desarrolladores de Bitcoin han trabajado desde hace un mes realizando pruebas para incluir esta modificación definitivamente al protocolo.

El objetivo principal de BIP es crear un formato común para realizar PSBT, lo cual permitiría que las transacciones de bitcoin puedan ser firmadas aún cuando no exista una conexión a Internet.

22 días atrás, la propuesta fue añadida al repositorio de bitcoin por Andrew Chow, quien la creó en un principio, en conjunto con el desarrollador Peter Wuille para las pruebas de funcionamiento.

Por otro lado, al especificar un formato binario único para el suministro de la información, la BIP 174 garantiza que cualquier implementación del protocolo pueda aprovechar dicha característica, lo que significa que las carteras no deberán coincidir en la implementación para que la firma fuera de línea de las transacciones sea exitosa. Con esto, se amplía la complejidad de las transacciones, permitiendo a la red el trabajo con pasos progresivos de firma y no solo las claves privadas.

Actualmente, al crear transacciones sin firmar o parcialmente firmadas, el usuario depende de la implementación de cada cliente o aplicación. Al aplicar esta BIP, se elimina dicho problema, beneficiando así los desarrollos sobre la red.

> *«Estamos entrando en una era de uso masivo de monedas con contratos que no se acomodan en un par de plantillas. Para expandir la complejidad de los contratos necesitamos protocolos que puedan manejar comandos de cumplimiento y pasos de*

> *firmas progresivos, no sólo llaves privadas»,* dijo Alex Bosworth.

Por otro lado, Peter Gray, fundador de Coinkite, explicó que ya se creó un hardware que aprovecha la potencialidad de las PSBT, mediante una cartera llamada Coldcard.

> *«La cartera permite agregar firmas a los archivos PSBT entregados en la tarjeta MicroSD o por medio de USB, y es capaz de finalizar archivos PSBT para muchos casos simples. Ya funciona bien contra la solicitud de extracción BIP174 existente»,* dijo Gray.