¿Cómo pagar menos tarifas en una transferencia de Bitcoin ?

Guillermo Vidal
tip@oowiki.com

Para las personas que desean entrar en el mundo de las llamadas monedas digitales y en particular Bitcoin que es la líder en el mercado de criptomonedas o tokens, inicialmente se encontrarán sin duda con el pago de comisiones en la red de bitcoin llamada (Blockchain). Estas comisiones son la tarifa que cobra la red de Bitcoin para que sea ejecutada tu transferencia (operación de gasto de efectivo de una cuenta Bitcoin a otra).

La comisión o tarifa anterior en la red de Bitcoin se calcula basándose principalmente por tres parámetros:

Solo uno de los tres parámetros que a continuación enunciamos no podemos modificar, ya que esto se establece mediante cálculos internos dentro de la red de Bitcoin conocida comúnmente como Blockchain, como breviario la blockchain es el software o programa que controla todas las operaciones de la moneda digital Bitcoin, es el que transfiere pagos y depósitos almacenados en una base de datos que tiene un nivel de seguridad muy alta para no ser modificada por un externo, todo se hace por medio de un consenso entre computadoras distribuidas en todos el mundo.

Continuando con nuestra meta de cómo pagar menos comisión en una operación en la red de Bitcoin el único parámetro que no podemos modificar es:

1. Qué tan saturada esta la red de Bitcoin, es decir cuál es la demanda de operaciones dentro de la red en un momento determinado que determinara el gasto de poder de cómputo para procesar la transacción enviada. Dependiendo de la carga que tengan la red de Bitcoin, el siguiente punto (2) subirá o bajara.

El segundo parámetro a considerar la “Fee” o “Tarifa promedio” establecida por los sistemas que se encargan de ejecutar las transacciones a nivel mundial, a estos sistemas distribuidos (computadoras) en todo el mundo se les llama “Mineros” y dichos sistemas establecen esta tarifa después de realizar un consenso entre todos los sistemas de forma automática y en tiempos tan reducidos como segundos (actualmente son alrededor de 9,700 computadoras distribuidas en todo el mundo, que contienen la misma información y se actualizan en cualquier instante que se ejecuta una transacción).

2. “Tarifa promedio” establecida por los mineros en Bitcoin este valor es dinámico y cambia según este saturada o no la red de Bitcoin. Los mineros son personas con ayuda de computadoras que son las encargadas de ejecutar las transacciones (pagos y depósitos) dentro de la red de Bitcoin.

Este segundo parámetro normalmente no se modifica, ya que es la tarifa promedio propuesta para que la transacción que se envié sea procesada en un tiempo razonable (entre 10 y 30 minutos), en caso de bajar la tarifa esto implicaría que la transacción se ejecute en un tiempo más largo que puede ser días o semanas o simplemente no ejecutarse.

Hay un tercer punto en donde si podemos modificar de manera positiva para reducir las comisiones o tarifas a pagar cuando solicitamos una transferencia en Bitcoin.

3. El tipo de cuenta o dirección que usamos para realizar la transferencia como remitentes.

Este último punto es donde centraremos nuestra atención. Pero antes veremos los tipos de cuentas o direcciones (address) que podemos tener en la red de Bitcoin.

La dirección en Bitcoin es haciendo una similitud con bancos tradicionales el siguiente comparativo, entendiendo que solo es similar en sus componentes para identificar como se integra o compone una cuenta o dirección en Bitcoin y poder rastrear de que cuenta sale la transferencia y a donde es depositada, entendiéndose que en los bancos tradicionales internamente funcionan totalmente diferentes a la red de Bitcoin, este ejemplo es únicamente para entender los componentes de una cuenta corriente o conocida comúnmente como dirección (address) en Bitcoin.

Similitud de una cuenta bancaria con una cuenta en la red de Bitcoin.

Otro punto muy importante es saber que en una dirección (address) de Bitcoin está compuesta de una serie de números y letras combinados, esta cadena de caracteres para nosotros no será de mucho sentido pero para la red de Bitcoin es una dirección que entiende perfectamente, es bueno saber que cada vez que se genera una dirección en Bitcoin se aplican una serie de procesos matemáticos en donde la red de Bitcoin puede identificar de forma única, segura y de forma precisa estas direcciones para hacer sus operaciones.

Con lo anterior y partiendo que sabemos que es una dirección en Bitcoin, entraremos de lleno a ver el tipo de direcciones (addresses) puede haber en la red de Bitcoin.

Hay 3 tipos de direcciones que hay en la red de Bitcoin:

- P2PKH o Legacy-address (formato de dirección común) es la primera versión y la más común usada de una dirección de Bitcoin que comienza con el número "1" y tiene de 26 a 36 caracteres. La tarifa promedio cuando se envía desde una dirección P2PKH suele ser más alta que cuando se envía desde una dirección Segwit, porque las transacciones con direcciones obsoletas son de mayor tamaño en Bytes de información enviados.
  Ejemplo: **1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa**

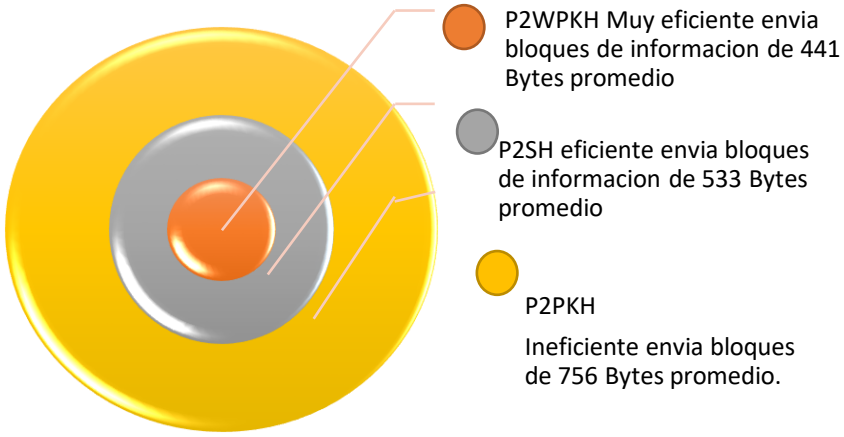
- P2SH El segundo más usado un nuevo tipo de dirección está estructurado de manera similar a P2PKH, pero comienza con "3" en lugar de "1". P2SH proporciona una funcionalidad más compleja que el tipo de dirección anterior. Para gastar bitcoins enviados a través de P2SH, el destinatario debe proporcionar un script correspondiente al hash y los datos del script, lo que hace que el script sea verdadero. Sin embargo, todo lo que un usuario común necesita saber es que al usar este tipo de dirección en lugar de P2PKH, la tarifa promedio de transacción será menor.
  Ejemplo: **3GRdnTq18LyNveWa1gQJcgp8qEnzijv5vR**

- P2WPKH o Bech32 es un tipo avanzado de dirección que se usa para reducir los tamaños de bloque de blockchain para acelerar el tiempo de respuesta de la transacción. Las direcciones comienzan con "bc1" y son más largas que P2PKH y P2SH. Bech32 es el formato de direccionamiento de Segwit nativo (aunque P2SH también puede ser una dirección de Segwit), por lo que generalmente se refiere al uso de direcciones de Segwit.
  La ventaja es la tarifa de envío de transacción más baja y la alta velocidad de procesamiento.
  La desventaja de tales direcciones es que aún no todas las billeteras y sistemas lo admiten.
  Ejemplo: **bc1qnkyhslv83yyp0q0suxw0uj3lg9drgqq9c0auzc**

La comisión o tarifa que se cobra está basado en los tres puntos anteriores (Tarifa puesta por los mineros, saturación de la Red Bitcoin y el tipo de dirección que se tenga), en el caso de las direcciones (addresses) veremos por qué y cómo podemos bajar dicha tarifa o comisión.

En la red de Bitcoin cada tipo de dirección puede manejar diferentes tipos de información digital, cada vez que se envía una transacción (Pago o Deposito) se envían bloques o paquetes de información en la red de Bitcoin, estos bloques se ponderan o se miden en la unidad común de una computadora (Bytes) mientras más información se envie por relación normal la red de Bitcoin necesitara más poder de cómputo para procesarla, si los bloques de información son pequeños el poder de computo será menor, lo anterior es la clave del ahorro en la tarifa global que cobra la red de Bitcoin y esto es debido a que la dirección que envía bloques más grandes es la dirección P2PKH, direcciones que empiezan con “1” es la más ineficiente, sin embargo es la más común debido a que con estas dirección inicio la tecnología del Bitcoin, posteriormente con el tiempo se mejoraron los procesos para enviar información y de optimizar esta información para reducir la cantidad de información enviada, así nacieron las otras dos diferentes direcciones que a diferencia de la primera (P2PKH) tiene o proveen otras funcionalidades de seguridad.

Para darnos una idea visual de la cantidad de bloques (Bytes) cuando usamos cada tipo de dirección tenemos el siguiente ejemplo:



De manera sencilla y simple cada tipo de dirección maneja cantidades diferentes de información (Bytes) mayor o menor información enviada a la red de Bitcoin, esto se debe a que cada vez que hay adelantos tecnológicos se encuentran formas de reducir u optimizar los datos enviados.

Por lo anterior tenemos el siguiente comparativo de desempeño de cada tipo de dirección de Bitcoin usada.

OOwiki.com
OpencryptO wiki

Tabla comparativa de rendimiento de direcciones de Bitcoin

Para simplificar, utilizamos las siguientes abreviaturas:
I – P2PKH, la dirección comienza con "1"
II – P2SH, la dirección comienza con "3"
III – Bech32, la dirección comienza con "bc1"

Tipo de dirección del remitente	Tipo de dirección del destinatario	Peso promedio de la transacción	
I	I	764	La transacción más **ineficiente**, el tipo de dirección del remitente juega un papel clave, la dirección del destinatario afecta la eficiencia no es significativa en todos los ejemplos
I	II	756	
I	III	752	
II	I	541	Las transacciones con una dirección de remitente P2SH son más de un 29% más baratas que con una dirección P2PKH desactualizada
II	II	533	
II	III	529	
III	I	449	Las transacciones con una dirección de remitente Bech32 son más de un 40% más baratas que con una dirección P2PKH desactualizada; y más del 15% más barato que con una dirección P2SH
III	II	441	
III	III	437	

En resumen, si se desea tener un menor pago de comisiones o tarifas en la red de Bitcoin, debemos usar las direcciones de tipo P2WPKH que comiencen con “bc1”.