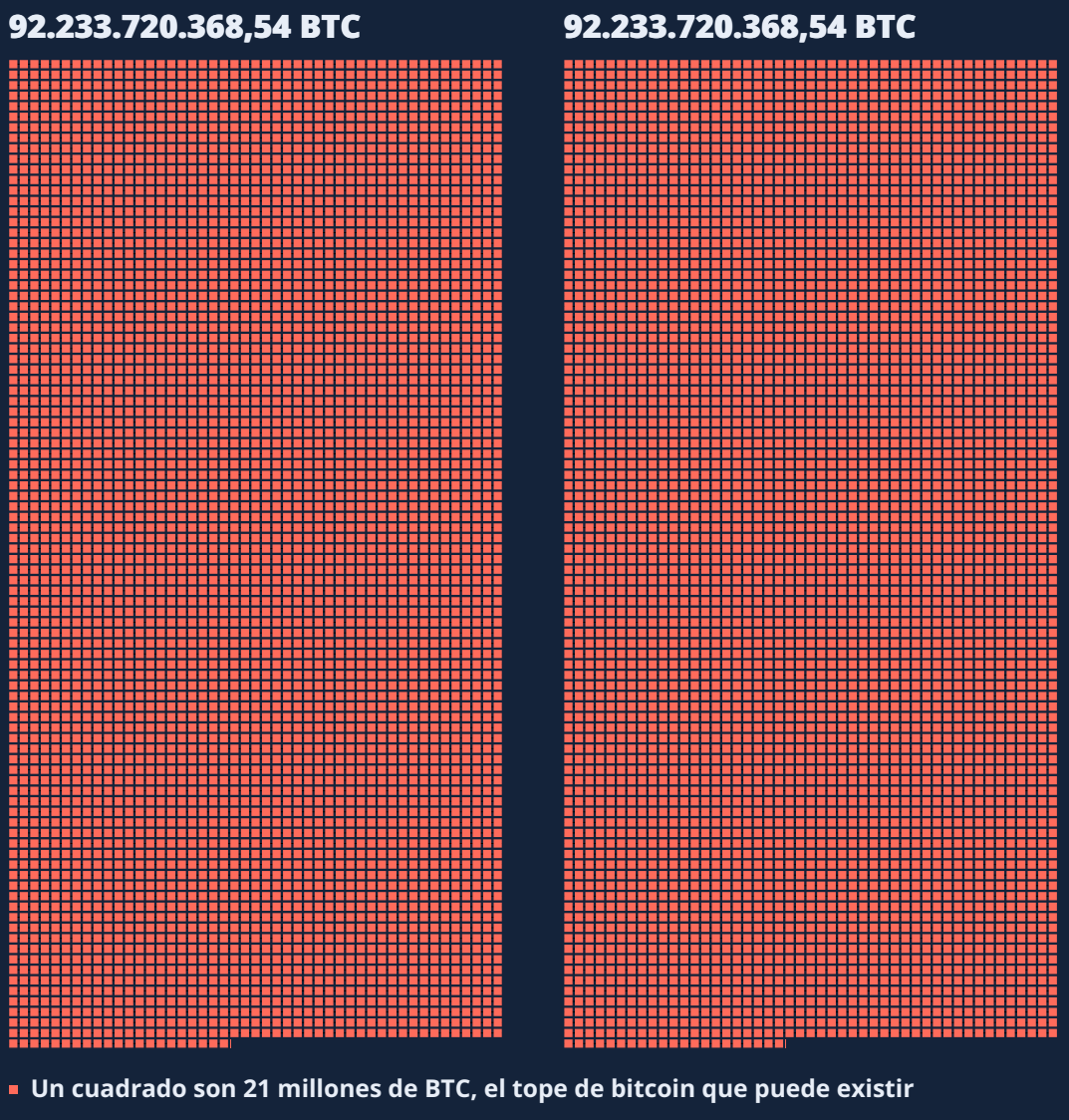
Satsumap análisis de cadena

El bug que creó 184 mil millones de bitcoin

Bloque 74.638 · 15 de agosto de 2010

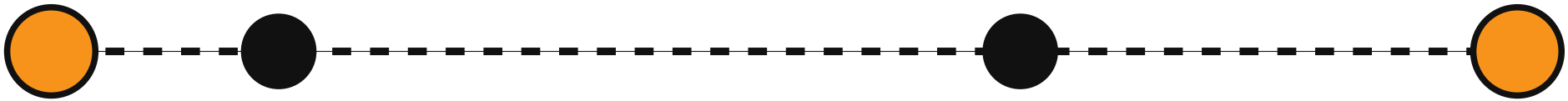


LA HISTORIA

01

Siete horas de agosto de 2010

15/08/2010, hora UTC



17:05
el bloque

18:08
el aviso

21:35
el arreglo

23:53
la cadena nueva

El bloque 1

El bloque 74.638 trae una transacción que crea **184 mil millones** de bitcoin. Solo pueden existir 21 millones.

El aviso 2

Un usuario del foro Bitcoin Talk lee el bloque y publica que el número es «bastante raro».

El arreglo 3

Satoshi le agrega al programa un tope. Desde la versión nueva, una transacción no puede crear más de 21 millones de bitcoin.

La cadena nueva 4

Los nodos con la regla rechazan el bloque y vuelven a minar desde el anterior.

La transacción ya no está en la cadena.

Seis palabras para este caso

Salida
Una moneda nueva que crea una transacción. Lo que sale **no puede ser más** que lo que entra.

Comisión
Lo que entra menos lo que sale. Se la lleva el minero que mete la transacción en su bloque.

Satoshi
La cien millonésima parte de un bitcoin. El programa guarda los montos en satoshis, como números enteros.

Desborde
Un número guardado en un lugar fijo tiene un máximo. Si una suma lo pasa, **da la vuelta** y aparece negativo.

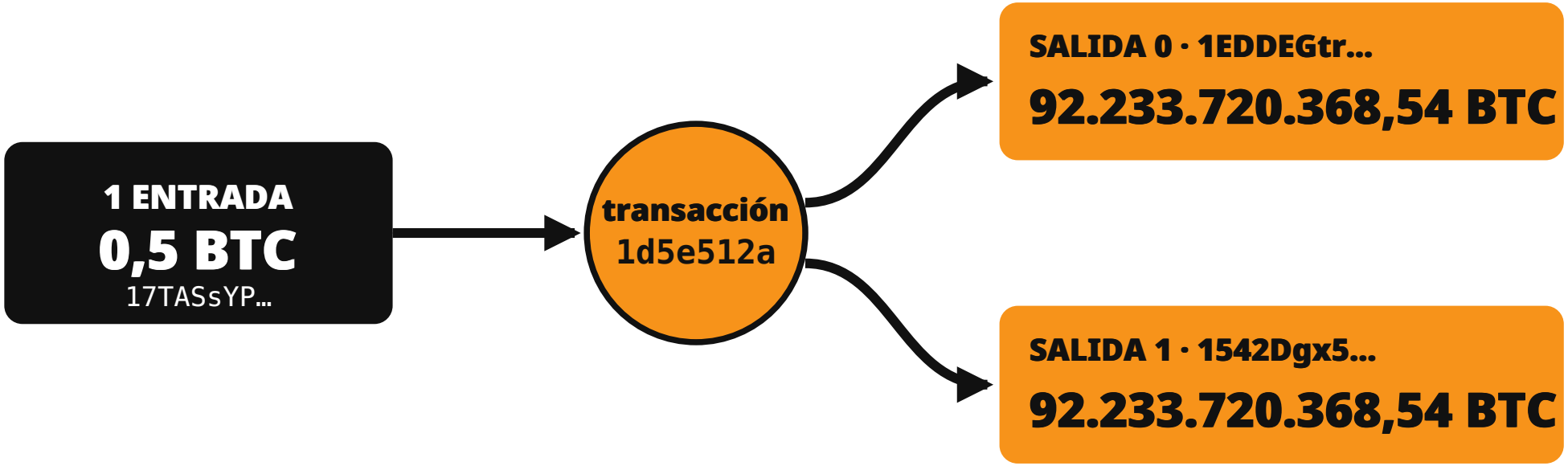
Rama
Si dos bloques apuntan al mismo bloque anterior, la cadena se parte en dos. La red se queda con una y la otra se descarta.

Regla de consenso
Lo que cada nodo revisa en cada bloque. Si un bloque no la cumple, ese nodo lo rechaza.

Un nodo es una computadora que corre el programa de Bitcoin y guarda su propia copia de la cadena.

15/08/2010, 17:05 UTC · BLOQUE 74.638

De 0,5 BTC a 184 mil millones



4.392
veces los 21 millones que pueden existir, en cada salida

2
transacciones en el bloque, la del minero y esta

50,51
BTC para el minero: los 50 del bloque y 0,51 de comisión

0,01
BTC de más en esa comisión. La entrada era de 0,5

TXID `1d5e512a9723cbef373b970eb52f1e9598ad67e7408077a82fdac194b65333c9`. Los montos, como los publicaron en el foro esa tarde.

EL ERROR DEL PROGRAMA

04

La suma da la vuelta

Una salida sola pasa

El programa revisaba que ninguna salida fuera negativa. Las dos eran positivas.

La suma no entra

Las dos juntas suman 18.446.744.073.708.551.616 satoshis. El programa sumaba en un lugar que llega hasta 9.223.372.036.854.775.807.

Queda en −0,01 BTC

Pasado el máximo, el número da la vuelta y aparece negativo, como un cuentakilómetros que pasa de 99999 a 00000.

La regla la deja pasar

Lo que sale (−0,01) no es más que lo que entra (0,5). La comisión da 0,5 − (−0,01) = 0,51.

CADA SALIDA

2^{63} − 500.000 sats

LAS DOS JUNTAS

2^{64} − 1.000.000 sats

LO QUE VIO EL PROGRAMA

−1.000.000 sats

Que alguien eligió esos montos a propósito no queda registrado en la cadena. Se deduce de la forma, porque la suma da apenas negativa.

15/08/2010 · FORO BITCOIN TALK

Una hora después, en el foro

18:08 UTC · JGARZIK, «STRANGE BLOCK 74638»

«El "valor de salida" de este bloque #74638 es bastante raro [...] ¿92233720368.54277039 BTC?»

«The "value out" in this block #74638 is quite strange [...] 92233720368.54277039 BTC?»

Publica el bloque entero, en texto, **una hora después** de la hora que le puso el minero.

18:55 UTC · LFM, EN EL MISMO HILO

«La suma de las dos salidas desborda a un negativo. Es un error en los chequeos de las transacciones, que no la rechazaron.»

«The sum of the two outputs overflows to a negative. Its a bug in the transaction checks which did not reject it [...]»

Y pide apagar lo que se pueda y no mandar ni aceptar pagos.

jgarzik copió el bloque de su nodo. theymos lo mostró desde el suyo, 20 minutos después.

LO QUE YA NO ESTÁ

06

Cómo se comprueba una transacción borrada

Hoy no se puede consultar

En la cadena actual, la transacción y su bloque no existen. Si se la busca en mempool.space, responde que no la encuentra.

En el foro quedó entera

jgarzik publicó la firma, la clave, la moneda que gasta y las dos salidas.

Se arma de nuevo, byte por byte

Con esos datos, su huella (el TXID) da **exactamente** 1d5e512a…65333c9. Un byte distinto cambiaría la huella entera.

La clave es la dueña de la moneda

La clave que firma es la de la moneda de 0,5 BTC que gasta, que sí está en la cadena.

Lo que prueba

Que el volcado del foro es fiel. De ahí salen el monto exacto de cada salida y las dos direcciones.

NO SE COMPROBÓ

La firma en sí. La aceptaron los nodos de 2010, y la cadena de hoy ya no la guarda.

El programa de 2010 escribía los datos del script con los bytes al revés. Dados vuelta, la huella cierra.

15/08/2010, 21:35 UTC · EL CÓDIGO

07

Una regla nueva en 4 horas y media

```
MAX_MONEY = 21000000 * COIN;

foreach (txout in vout) {
  if (txout.nValue < 0) error("negative");
  if (txout.nValue > MAX_MONEY)
      error("txout.nValue too high");
  nValueOut += txout.nValue;
  if (nValueOut > MAX_MONEY)
      error("txout total too high");
}
```

En verde, lo nuevo, resumido. Ninguna salida, y ninguna suma de salidas, puede pasar los 21 millones de bitcoin.

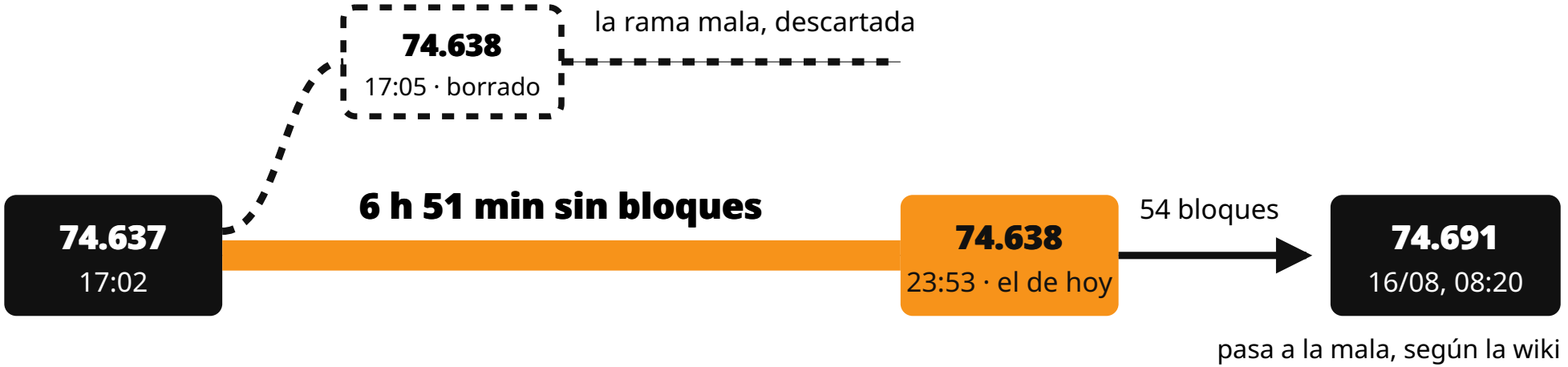
UTC	QUÉ PASÓ
17:05	El bloque con el desborde
18:08	El aviso en el foro
20:39	Gavin Andresen publica un primer parche
21:06	Satoshi pide dejar de minar: «probablemente haya que rehacer una rama»
21:35	El arreglo entra al código (SVN 132)
23:48	Satoshi anuncia la versión 0.3.10

Commit d4c6b90 del repositorio de Bitcoin: «fix for block 74638 overflow output transaction». Las horas, del foro y del repositorio.

EN LA CADENA DE HOY

08

6 h 51 min sin bloques



23:53
la hora del 74.638 de hoy. La del 74.637 es 17:02

35,6 min
el hueco que le sigue, entre los 90 bloques de alrededor

5 min 37 s
entre el anuncio de la 0.3.10 y el primer bloque de la rama buena

8 h 26 min
para minar los 54 bloques hasta el 74.691

La rama mala no está en la cadena. Cuántos bloques tuvo, o en qué bloque la alcanzó la buena, sale de la Bitcoin Wiki. Las horas son las que escribió cada minero.

CÓMO SE VE

Satsumap dice que no existe

ID de transacción o dirección `970eb52f1e9598ad67e7408077a82fdac194b65333c9` Buscar

No existe una transacción con ese ID en ningún proveedor.

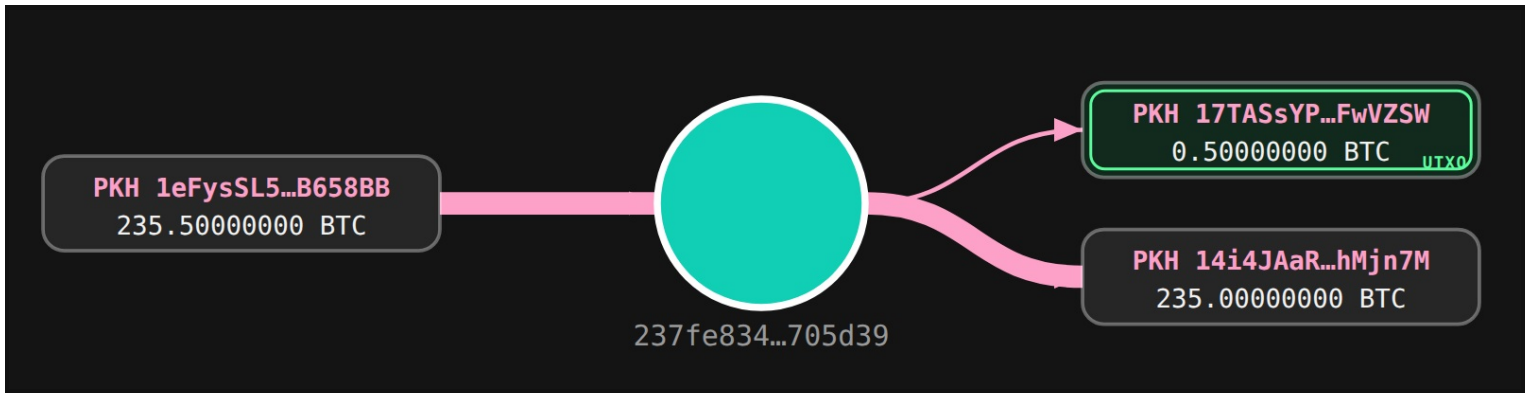
Lo que se busca
El TXID de la transacción del desborde, escrito en el buscador.

Lo que responde
Que no existe. Lo contesta mempool.space, que guarda la cadena de hoy.

La transacción existió durante unas horas en la rama mala. La cadena que guardan los nodos hoy no la tiene.

14/08/2010, 23:05 UTC · BLOQUE 74.421

La moneda del ataque sigue sin gastar



Arriba a la derecha, los 0,5 BTC

La moneda que gastó la transacción del desborde, en 17TASsYP… FwVZSW. Satsumap la marca UTXO: **sin gastar**.

Por qué sigue sin gastar

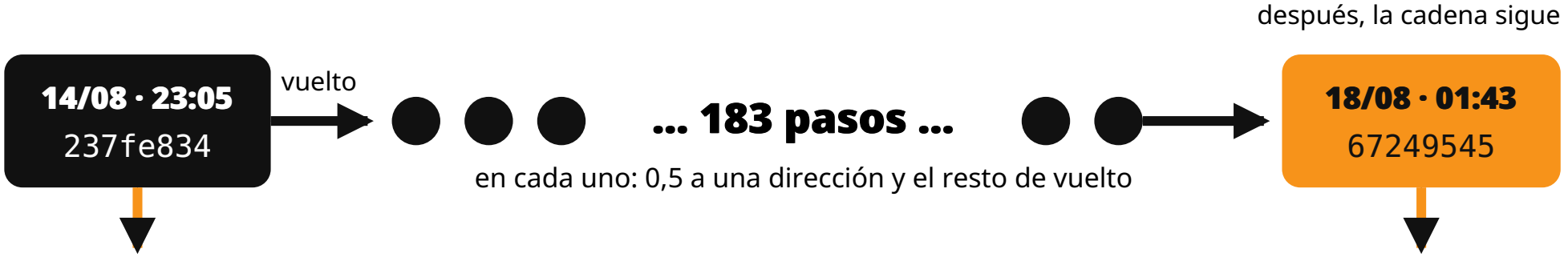
Su gasto estaba en el bloque borrado. Desde 2010 nadie la volvió a mover.

1

transacción en la historia de esa dirección, la que le dio la moneda.

TXID 237fe8348fc77ace11049931058abb034c99698c7fe99b1cc022b1365a705d39, salida 0. La otra salida, 235 BTC, se gastó 17 minutos después.

183 pagos de 0,5 BTC



183
pagos hasta el de 1542Dgx5..., cada uno con el vuelto del anterior

173
direcciones distintas que reciben los 0,5

19
pagos juntos en el bloque 74.642, el primero con pagos de esta cadena después del hueco

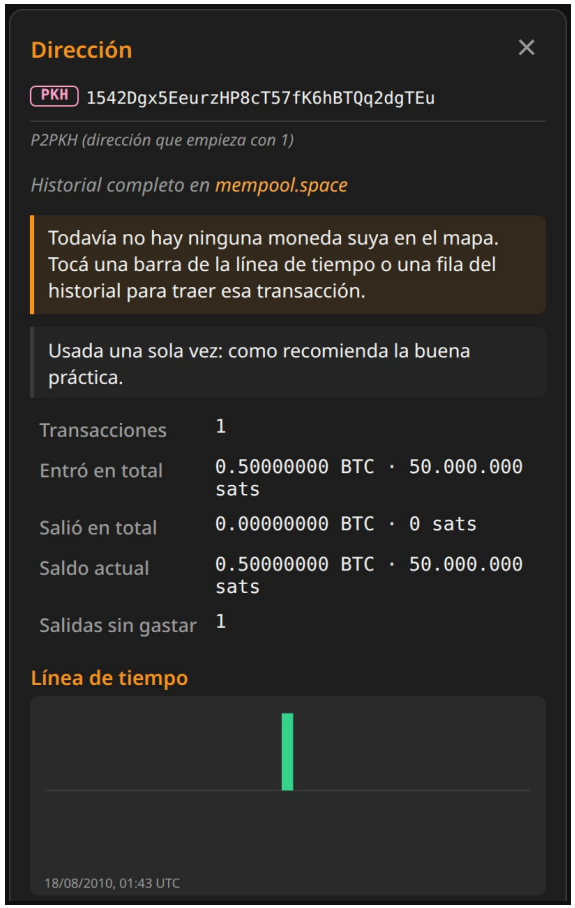
235 → 143,5
BTC de vuelto en esos 183 pasos, de a 0,5 menos por paso

En el mismo bloque 74.642, la transacción `fb9c3667…` junta seis monedas de 0,5 en una sola salida de 3 BTC. Cinco son pagos de esta cadena. Para gastar cada moneda hace falta su clave, así que lo más probable es que esas cinco direcciones tuvieran un mismo dueño.

173 DIRECCIONES NO SERÍAN 173 PERSONAS

Los vueltos se siguieron salida por salida. La forma es la de una canilla, un sitio que regalaba bitcoin para probar. De quién era no se confirmó.

Un pago a una salida del desborde



Lo que se lee en la cadena

El pago 183 de la cadena va a 1542Dgx5…, la salida 1 del desborde, 56 horas después del bloque malo. Es su única transacción, y esos 0,5 BTC siguen sin gastar. La cadena sigue después de ese pago.

La otra dirección

1EDDEGtr…, la salida 0, no tiene transacciones en la cadena de hoy.

INFERENCIA

Es compatible con que la misma persona armó el desborde y pidió los dos pagos. **No lo prueba.** Una canilla le manda a la dirección que le escriben, y cualquiera que supiera sacar esa dirección del volcado del foro podía pedirlo.

En el foro la dirección no aparece escrita, porque el volcado traía sus bytes al revés. Se buscó en los tres hilos del incidente.

Lo que deja el desborde

La regla la aplica cada nodo

El 15/08 los nodos aceptaron el bloque porque esa regla no existía. Con la 0.3.10, cada nodo actualizado lo rechazó por su cuenta.

El aviso salió de un nodo

jgarzik publicó el bloque que había recibido su nodo. lfm lo explicó 47 minutos después.

Se minó otra rama

Nadie editó bloques. La red minó otra rama desde el 74.637 y se quedó con esa.

Cómo decide un nodo

Revisa cada bloque por su cuenta, con las reglas del programa que tiene instalado. Solo suma el trabajo de una rama si sus bloques cumplen esas reglas. Por eso, después de actualizar, la rama del bloque malo dejó de contar para ese nodo, aunque fuera más larga.

Los nodos sin actualizar

Para el programa viejo, las dos ramas eran válidas, y el nodo seguía la más larga. Cuando la rama buena pasó a la mala, el nodo se pasó a la buena sin que nadie lo tocara.

La regla sigue en el programa de hoy, Bitcoin Core. Un nodo rechaza una transacción si una salida, o la suma de las salidas, pasa los 21 millones de BTC.

PARA QUIEN EMPIEZA

Una regla nueva y los bloques viejos

La regla de 2010 no tenía bloque de inicio

El arreglo valía para la cadena entera. Por eso dejó inválido al 74.638, que ya estaba minado.

Para limpiar había que volver a bajar los bloques

A las 21:40, Satoshi pidió apagar el programa, reemplazar los bloques guardados por una copia anterior al 74.000, actualizar y dejar que baje el resto. Los bloques que faltaban se bajaban con el programa ya actualizado.

La 0.3.10 traía otro chequeo

Se agregó a las 22:21 (SVN 133). Rechazaba un bloque nuevo si su rama pasaba por el 74.638 malo, reconocido por su hash.

Al otro día alcanzaba con actualizar

El 16/08 la rama buena ya tenía más trabajo. Un nodo actualizado se pasaba a ella solo, sin borrar nada.

Hoy una regla nueva arranca en un bloque fijo

Taproot se activó en el bloque 709.632, el 14/11/2021. Los bloques anteriores se siguen validando con las reglas de su época.

Bitcoin Core permite volver a verificar la cadena guardada (-reindex) o marcar a mano un bloque como inválido (invalidateblock).

PARA LEER CON CUIDADO

Qué se puede leer en la cadena y qué no

AFIRMACIÓN	DE DÓNDE SALE
La transacción y su bloque no están en la cadena de hoy	**Cadena**
Los montos, la firma y las direcciones de la transacción	El foro, comprobado con la huella reconstruida, que da el TXID
La suma da −0,01 y la comisión 0,51	La cuenta, sobre esos montos
El minero cobró 50,51 BTC	El foro (esa transacción tampoco está)
El hueco de 6 h 51 min después del bloque 74.637	**Cadena**
Las horas del aviso, del parche y de la 0.3.10	El foro y el repositorio de código
La rama buena pasó a la mala en el bloque 74.691	Bitcoin Wiki. No se puede comprobar en la cadena
La moneda de 0,5 BTC sigue sin gastar	**Cadena**
Los 183 pagos hasta el que llega a 1542Dgx5…, y que la cadena sigue	**Cadena**
Los pagos que se gastan juntos tenían un mismo dueño	**Inferencia** por la forma
Los pagos eran de una canilla	**Inferencia** por la forma, y la wiki dice «parece»
Quién armó el desborde	**No se sabe**

Lo que está en la cadena lo puede comprobar cualquiera, con los datos de la hoja siguiente.

COMPROBALO VOS

Los datos, a la vista

Bloque 74.421 · la moneda de 0,5 BTC que gastó el desborde (salida 0)
`237fe8348fc77ace11049931058abb034c99698c7fe99b1cc022b1365a705d39` mempool.space

Bloque 74.638 de hoy (23:53 UTC) · su primera transacción
`2ae30f63b1507761b5541f7a723f566abb0701e5f8a97927980381341b5d8cbd` mempool.space

Bloque 74.923 · el pago de 0,5 BTC a una dirección del desborde
`672495458201c55cdf4fa47cd40ff0bc8cbbd898b5dd564f84b81b0a87423417` mempool.space

Dirección de la moneda del ataque
`17TASsYPbdLrJo3UDxFfCMu5GXmxFwVZSW` mempool.space

Salida 1 del desborde · recibió 0,5 BTC el 18/08/2010
`1542Dgx5EeurzHP8cT57fK6hBTQq2dgTEu` mempool.space

Salida 0 del desborde · sin transacciones hoy
`1EDDEGtrZ5877WPsLU5o9TwjJDqaUqhvte` mempool.space

La transacción del desborde, para buscarla y ver que no está: `1d5e512a9723cbef373b970eb52f1e9598ad67e7408077a82fdac194b65333c9`

Fuentes de fuera de la cadena: Bitcoin Talk, hilos 822, 823 y 827 (2010) · commit d4c6b90 del repositorio de Bitcoin · Bitcoin Wiki, «Value overflow incident».