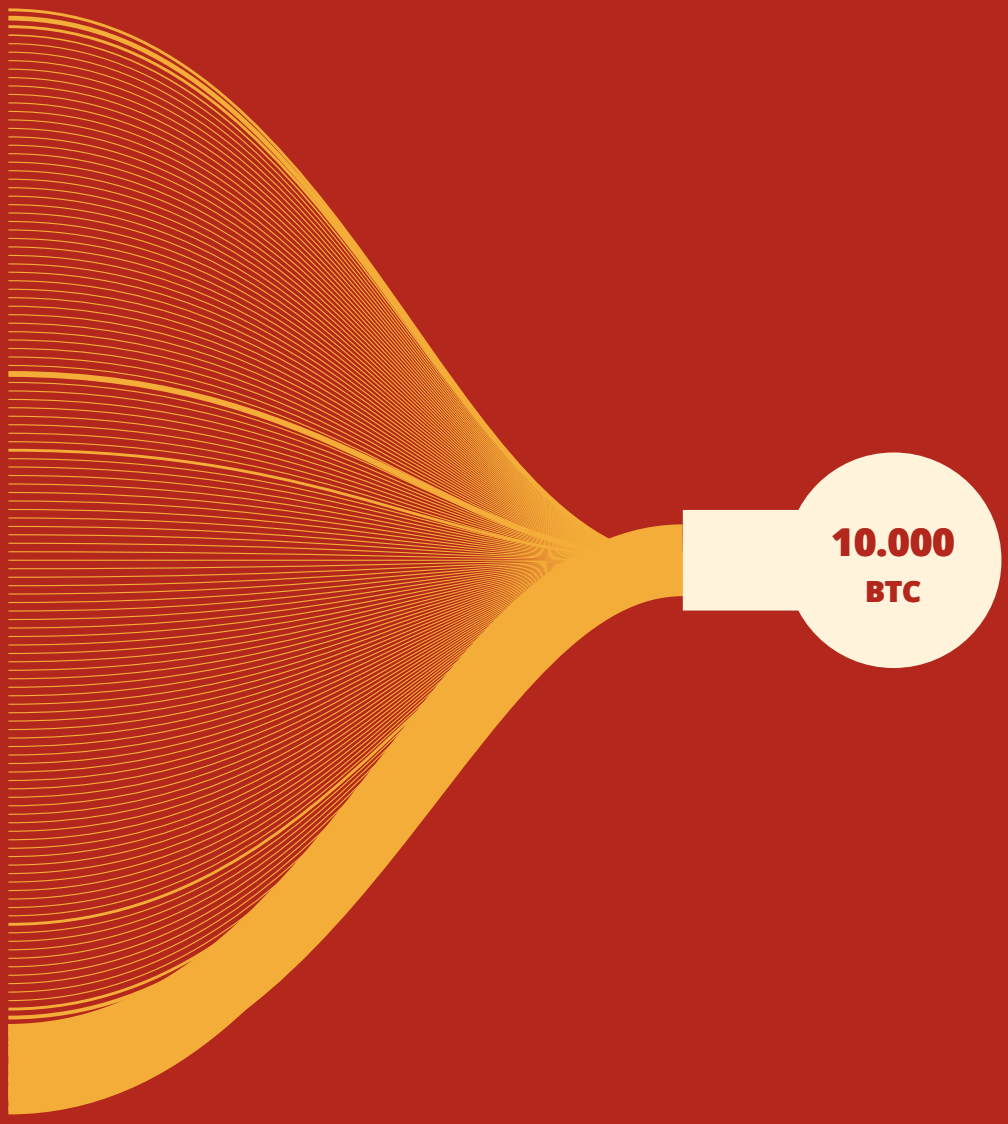
Satsumap análisis de cadena



Dos pizzas, 10.000 bitcoin

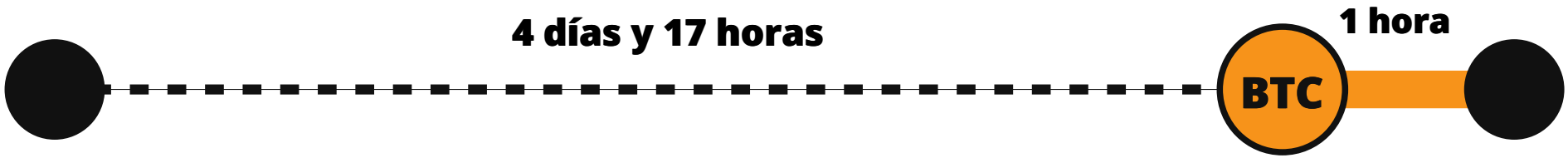
22 de mayo de 2010 · 131 monedas en un pago

131 entradas · de 0,01 a 3.754 BTC

LA HISTORIA

01

Una oferta, un pago y un aviso



18/05/2010
00:35 UTC · la oferta, en el foro

22/05/2010
18:16 UTC · el pago, en la cadena

19:17
el aviso

La oferta 1

Laszlo Hanyecz escribe en el foro Bitcoin Talk que paga **10.000 bitcoin** por dos pizzas.

El pago 2

En el bloque 57.043, una transacción junta **131 monedas** y paga 10.000 BTC en una sola salida.

El aviso 3

Laszlo cuenta en el foro que cambió 10.000 bitcoin por pizza, y le agradece a **jercos**.

La oferta y el aviso están en el foro y el pago está en la cadena. Con este pago, el análisis de Satsumap se equivoca (hojas 05 y 12).

Seis palabras para leer la cadena

Entrada
La moneda que una transacción gasta. Se gasta **entera**, como un billete.

Salida
Una moneda nueva que crea la transacción, con su monto y su candado: quién la puede gastar.

Dirección
Una forma corta de escribir un candado, como 1XPTg…. En 2010 muchas monedas no tenían dirección, y su candado era la clave pública entera.

Coinbase
La primera transacción de cada bloque. **Crea bitcoin nuevo** para quien lo minó. En 2010, 50 BTC.

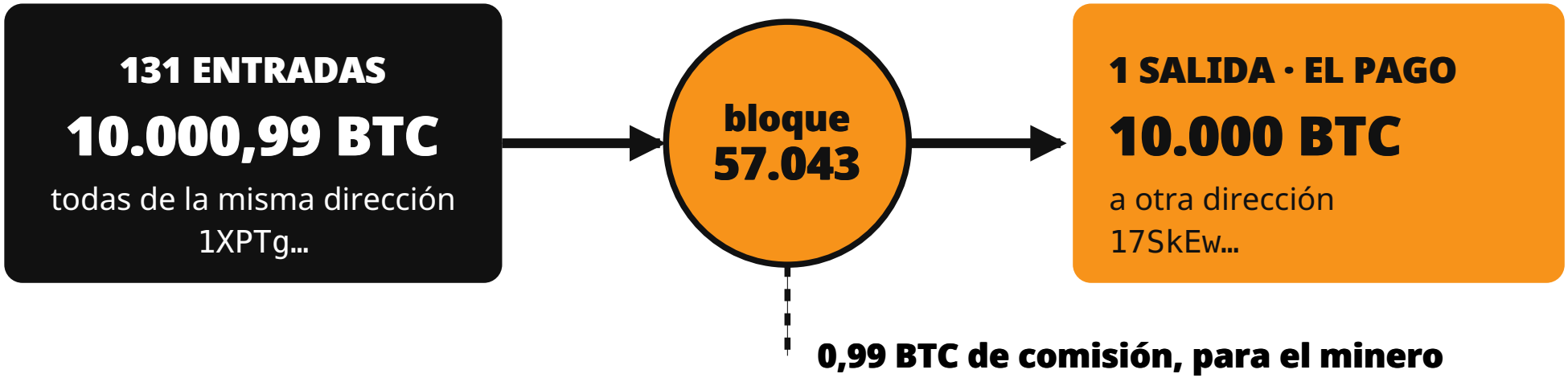
Vuelto
Lo que sobra del billete, que vuelve al que paga en una salida aparte. **Este pago no tiene.**

Consolidar
Juntar muchas monedas propias en una sola. Tiene la misma forma que un pago sin vuelto.

En la cadena, consolidar y pagar sin vuelto se ven igual. Este pago es un ejemplo.

22/05/2010, 18:16 UTC · BLOQUE 57.043

131 monedas, un solo pago



131
entradas, cada una de una transacción distinta

1
dirección de la que salen todas

0
salidas de vuelto. Lo que sobra queda como comisión

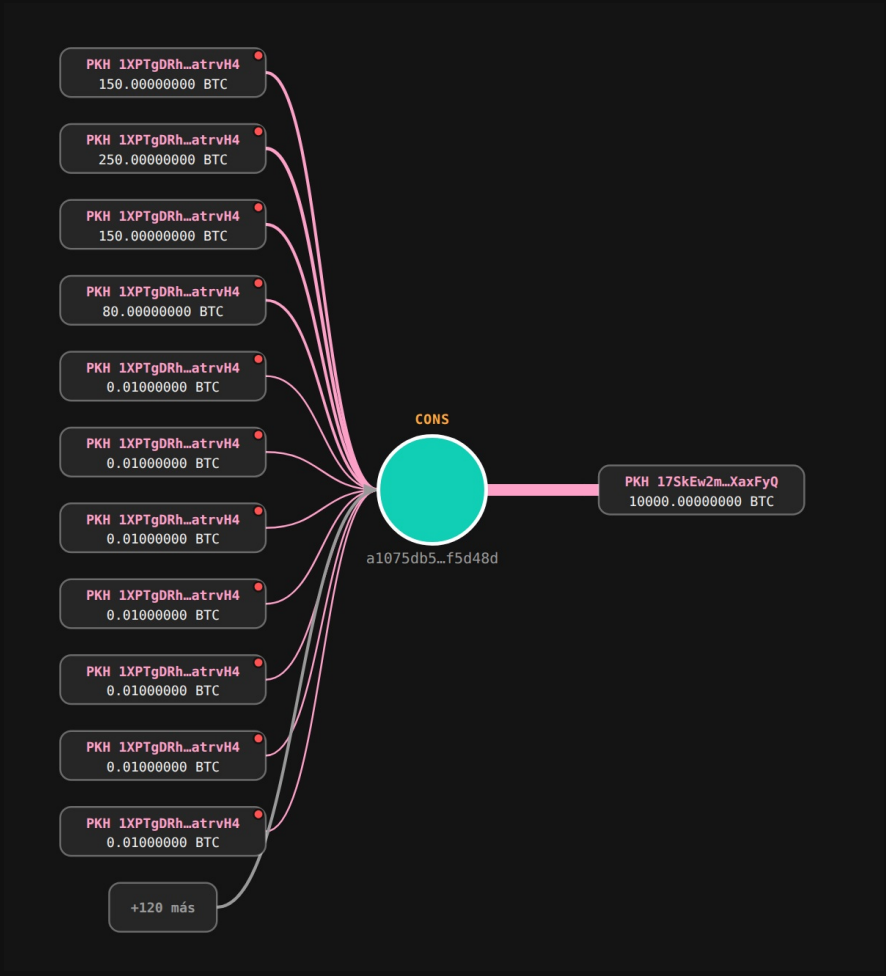
2
transacciones en el bloque: la coinbase y esta

TXID `a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d`. Por qué se pagaron 0,99 BTC de comisión, la cadena no lo dice.

CÓMO SE VE

04

El pago en Satsumap



A la izquierda, las monedas que entran
Todas dicen 1XPTgDRh…atrvH4: la misma dirección. Se ven once; las otras 120 esperan en «+120 más».

En el medio, la transacción
El círculo es el pago. Arriba, la etiqueta CONS, de consolidación.

A la derecha, la única salida
10.000 BTC a 17SkEw…. Ninguna salida vuelve a la dirección que pagó.

Para recorrerlo: satsumap.citadellhost.com, buscar el TXID a1075db5…f5d48d.

Satsumap se equivoca

Lo que dice la app
«Consolidación», con «confianza alta». Y el «?» agrega que es «un hecho leído directo de los datos, no una deducción».

Lo que es un hecho
Que tiene 131 entradas y una salida. Se lee directo en la cadena.

Lo que es una deducción
Que alguien junta lo suyo y los 10.000 siguen siendo de quien pagó. La app tenía un dato en contra, porque la salida va a una dirección que no está entre las entradas.

Lo que pasó
Fue un pago a otra persona. Lo dicen el foro y la entrevista a jercos.



Hasta el 20/10/2026, la técnica «Reconocer una consolidación» del Inspector se practicaba con este mismo pago. Qué pasa si se le cree a la etiqueta, en la hoja 12.

¿Por qué esta transacción?

LO QUE SE VE EN LA CADENA

El monto
Exactamente 10.000 BTC, en una sola salida.

El día y la hora
22/05/2010, 18:16 UTC, una hora antes del aviso del foro.

Ningún nombre
Solo la dirección que paga y la que cobra.

LO QUE SE SABE POR FUERA

«Quiero contarles que pude cambiar 10.000 bitcoin por pizza. [...] ¡Gracias, jercos!»

«I just want to report that I successfully traded 10,000 bitcoins for pizza. [...] Thanks jercos!» Laszlo, Bitcoin Talk, 22/05/2010.

Laszlo **no da el TXID**. Lo da una entrevista a jercos de 2015, que también dice qué dirección usó cada uno. Eso lo escribe el entrevistador, no jercos. La Bitcoin Wiki da el mismo TXID.

La cadena es compatible con esa atribución y no la prueba. Todas las fuentes usan esta transacción, y ninguna propone otra.

De dónde vienen las 131 monedas

GRUPO	MONEDAS	SUMAN	LLEGARON A 1XPTg...
Grandes, de 80 a 3.753,88 BTC	20	9.999,88 BTC	del 15/04 al 22/05/2010
Chicas, de 0,01 BTC cada una	111	1,11 BTC	el 18/04/2010, en menos de dos horas

Ninguna es una coinbase 1

Las 131 le llegaron a esa dirección por una transferencia. Ninguna se creó minando ahí mismo. Por eso se mira **un salto más atrás**.

Un salto más 2

Las grandes llevan a coinbases (hoja siguiente). Las chicas llevan a 111 direcciones distintas, y ahí se corta.

La regla del caso es seguir un salto más cuando una moneda viene transferida. Si ahí tampoco hay coinbase, se para y se dice.

6.100 BTC salen de 122 coinbases



Monedas creadas minando

16 de las 20 grandes salen de envíos que solo juntan coinbases: 5.750 BTC. Otras tres mezclan coinbases con transferencias.

122 claves distintas

Cada coinbase le paga a la clave que elige quien mina. Quien armó cada envío tenía las claves de sus coinbases.

Lo que no llega a una coinbase

3.899,88 BTC vienen de transferencias. Ahí se para.

INFERENCIA

El 04/08/2010 Laszlo escribió que ya no podía seguir pagando pizzas «porque ya no puedo generar miles de monedas por día». **Es compatible** con que esas coinbases las haya minado él. La cadena muestra claves que cobraron recompensas y envíos que las juntaron, no a una persona.

Las cuentas cierran: 6.100 de coinbases + 3.899,88 de transferencias + 1,11 de las monedas chicas = 10.000,99 BTC, lo que entra en el pago.

HACIA ATRÁS · LAS CHICAS

09

111 monedas de 0,01: no se sabe

18/04/2010
el día que llegaron todas, entre las 17:57 y las 19:46 UTC

111
envíos, cada uno desde una dirección distinta

0,01 BTC
a 1XPTg... en cada envío, y el resto a otra dirección

2
envíos gastan la otra salida de un envío anterior

Lo que muestra la cadena

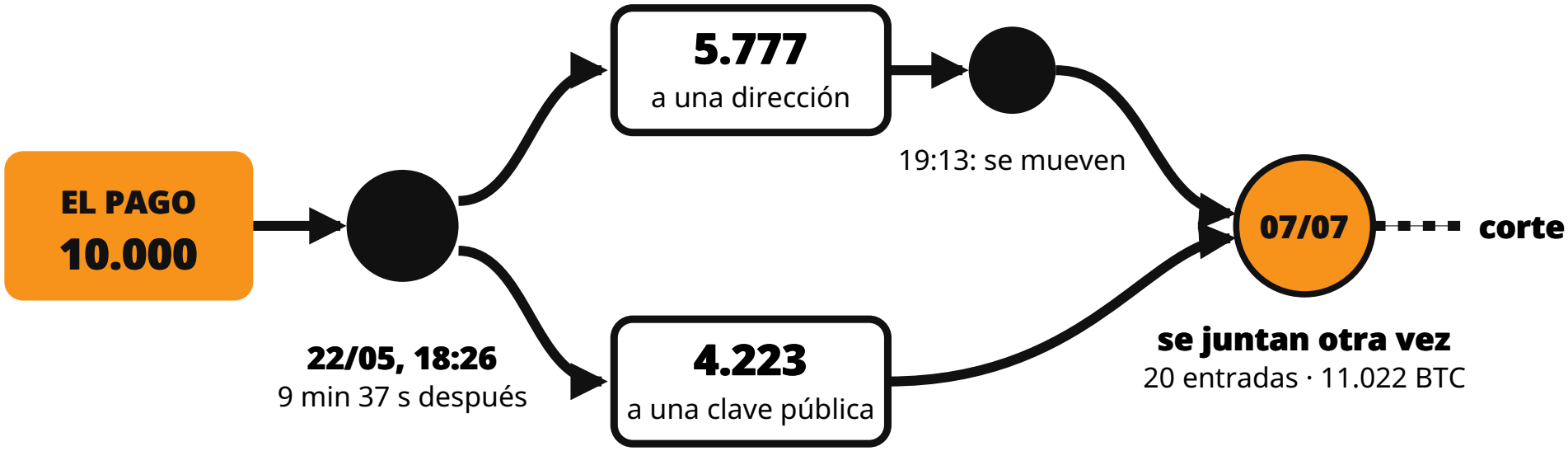
En dos casos, un envío usa lo que quedó de otro. Que cada pareja sea de una misma billetera es inferencia. Del resto no dice si fue una sola persona o muchas.

Lo que no muestra

Quién las mandó y para qué. Este caso no lo especula. Un mes después, esas 111 monedas entraron en el pago de las pizzas.

Sumadas, las 111 monedas chicas son 1,11 BTC de los 10.000,99 que entran en el pago.

A los 9 minutos, se parte en dos



9 min 37 s
después del pago, el primer gasto: en el bloque siguiente

5.777 + 4.223
las dos partes en que se divide

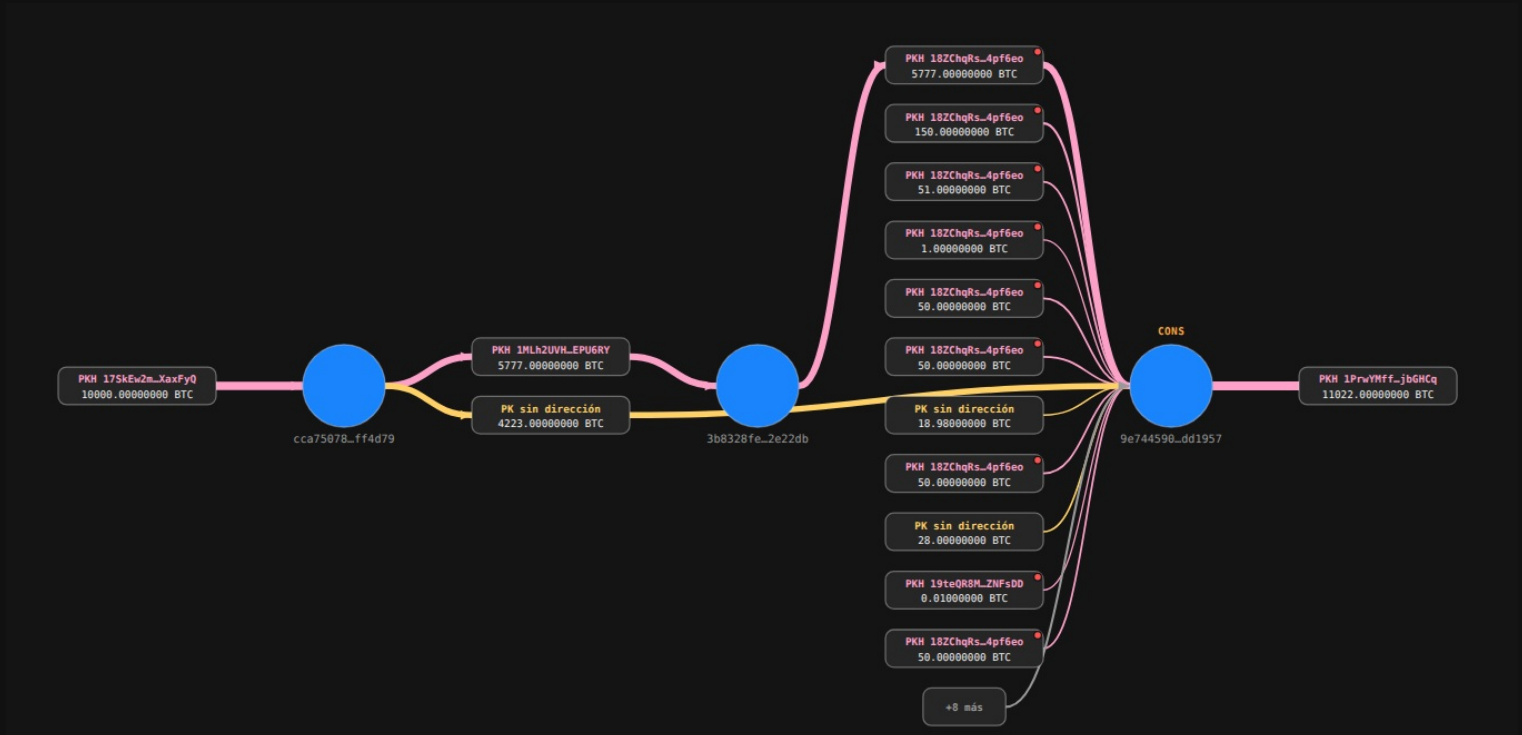
45 días
después, el 07/07/2010, las dos partes vuelven a gastarse juntas

0
de comisión en cada uno de estos pasos

Después de juntarse, los 11.022 BTC se parten en 5.500 y 5.522. Ahí se corta, porque después del que cobró nadie tiene nombre.

07/07/2010 · BLOQUE 64.683

Las dos partes, la misma billetera



Lo que muestra

Para gastar una moneda hay que tener su llave. Si dos monedas entran en la misma transacción, quien la armó tenía las dos, salvo que la armaran varias personas juntas, como en un CoinJoin.

Lo que no muestra

De quién es esa billetera. jercos contó en 2015 que gastó los 10.000 «bastante rápido». La cadena no dice si ya eran de otro.

En amarillo, las monedas con candado de clave pública, sin dirección: los 4.223 y dos de las otras 18. Entran todas con los 5.777 en 9e744590…dd1957.

SI SE LE CREE A LA ETIQUETA

Así falla un análisis de cadena

PASO	LA REGLA	LO QUE CONCLUYE	¿ES CIERTO?
1	Entrada común	Las 131 entradas son de un mismo dueño, 1XPTg…	**Sí**
2	«Consolidación»	La dirección que cobró, 17SkEw…, también es suya	**No**, fue un pago a jercos
3	Seguir la plata	Los 5.777 y los 4.223 en que se partió el pago siguen siendo suyos	**No**, por el paso 2
4	Entrada común	El 07/07/2010, las 20 monedas que entran juntas también: 11.022 BTC	**No**, por el paso 2
5	«Consolidación»	La app también le pone CONS, así que la dirección que la cobra también sería suya	**No**, por el paso 2

EL RESULTADO

El que pagó y el que cobró quedan como el mismo dueño. Las monedas de jercos se le atribuyen a Laszlo, y también todo lo que jercos hizo después con ellas. Eran dos personas distintas.

LA REGLA QUE SÍ VALE

«Cierta vinculación sigue siendo inevitable con las transacciones de varias entradas, que necesariamente revelan que sus entradas eran de un mismo dueño.» Satoshi Nakamoto, whitepaper de Bitcoin, 2008. Habla de las entradas, y la salida queda afuera.

Los cinco pasos usan reglas razonables, y ninguna regla de la cadena corrige el error. Lo corrige un dato de afuera, el aviso del foro.

EN DÓLARES DE LA ÉPOCA

10.000 bitcoin, 41 dólares

US$ 41
lo que valían los 10.000 BTC el 18/05/2010, según un usuario del foro. Unos 0,4 centavos cada uno

US$ 25
lo que costaban las dos pizzas, según Laszlo, «quizás 30 con una buena propina»

US$ 400
lo que valían cuando jercos los gastó, según contó él en 2015

LO QUE NO COINCIDE

jercos recuerda haber pedido en **Domino's**, pero las fotos muestran **Papa John's**. No se puede saber, y no cambia nada de lo que dice la cadena.

HASTA HOY

La dirección que cobró recibió **50 envíos chicos** desde 2015, 38 de ellos en 2026, y ninguno se gastó. Como en el génesis, suelen leerse como homenajes. La cadena solo muestra los envíos.

No hay precios en la cadena. Los tres salen del foro (mayo y junio de 2010) y de la entrevista a jercos (2015).

Qué dice la cadena y qué no

AFIRMACIÓN	DE DÓNDE SALE
Una transacción junta 131 monedas de una dirección y paga 10.000 BTC a otra	**Cadena**
Esa transacción es el pago de las pizzas	Fuera: la entrevista de 2015 y la Wiki. La cadena es compatible
Pagó Laszlo Hanyecz y cobró jercos	Fuera: Laszlo en el foro y la entrevista
6.100 BTC del pago salen de 122 coinbases, a dos saltos	**Cadena**
Laszlo minó esas coinbases	**Inferencia**, compatible con lo que contó él
Quién mandó las 111 monedas de 0,01 y para qué	**No se sabe**
Las dos partes de los 10.000 se gastan juntas el 07/07/2010	**Cadena**
De quién era esa billetera	**No se sabe**
Es una consolidación, como dice Satsumap	**Falso**: fue un pago a otra persona
Los 10.000 BTC valían 41 dólares	Fuera: el foro, mayo de 2010

Lo que dice la cadena lo puede comprobar cualquiera, con los TXID de la hoja siguiente.

COMPROBALO VOS

Los datos, a la vista

Bloque 57.043 · el pago de las pizzas
`a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d` mempool.space

Bloque 56.343 (18/05/2010) · 18 coinbases juntadas en una moneda de 900 BTC
`07c8b28197c8c84bcb77104e299ee7ae75f3543f74d8d37217de54b6da85c72c` mempool.space

Bloque 57.044 · el primer gasto: 5.777 y 4.223
`cca7507897abc89628f450e8b1e0c6fca4ec3f7b34cccf55f3f531c659ff4d79` mempool.space

Bloque 57.053 · se mueven los 5.777
`3b8328fe7e53a8162cf023738a53c85a3cbf21efe517ab878e8cfecc3a2e22db` mempool.space

Bloque 64.683 · las dos partes, juntas otra vez (07/07/2010)
`9e744590d196b63d02a1dd7ef596fd6082286f84295d66da411a9ffebfdd1957` mempool.space

Dirección que paga · las 131 entradas
`1XPTgDRhN8RFnzniWCddobD9iKZatrvH4` mempool.space

Dirección que cobra · los 10.000 BTC
`17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ` mempool.space

Cada TXID y cada dirección abre **Satsumap** con un clic, y al lado está el enlace a **mempool.space**. También se pueden copiar y pegar en el buscador de los dos.

Fuentes de fuera de la cadena: Laszlo Hanyecz, «Pizza for bitcoins?», Bitcoin Talk (2010) · entrevista a jercos, Bitcoin Who's Who (2015) · Bitcoin Wiki.