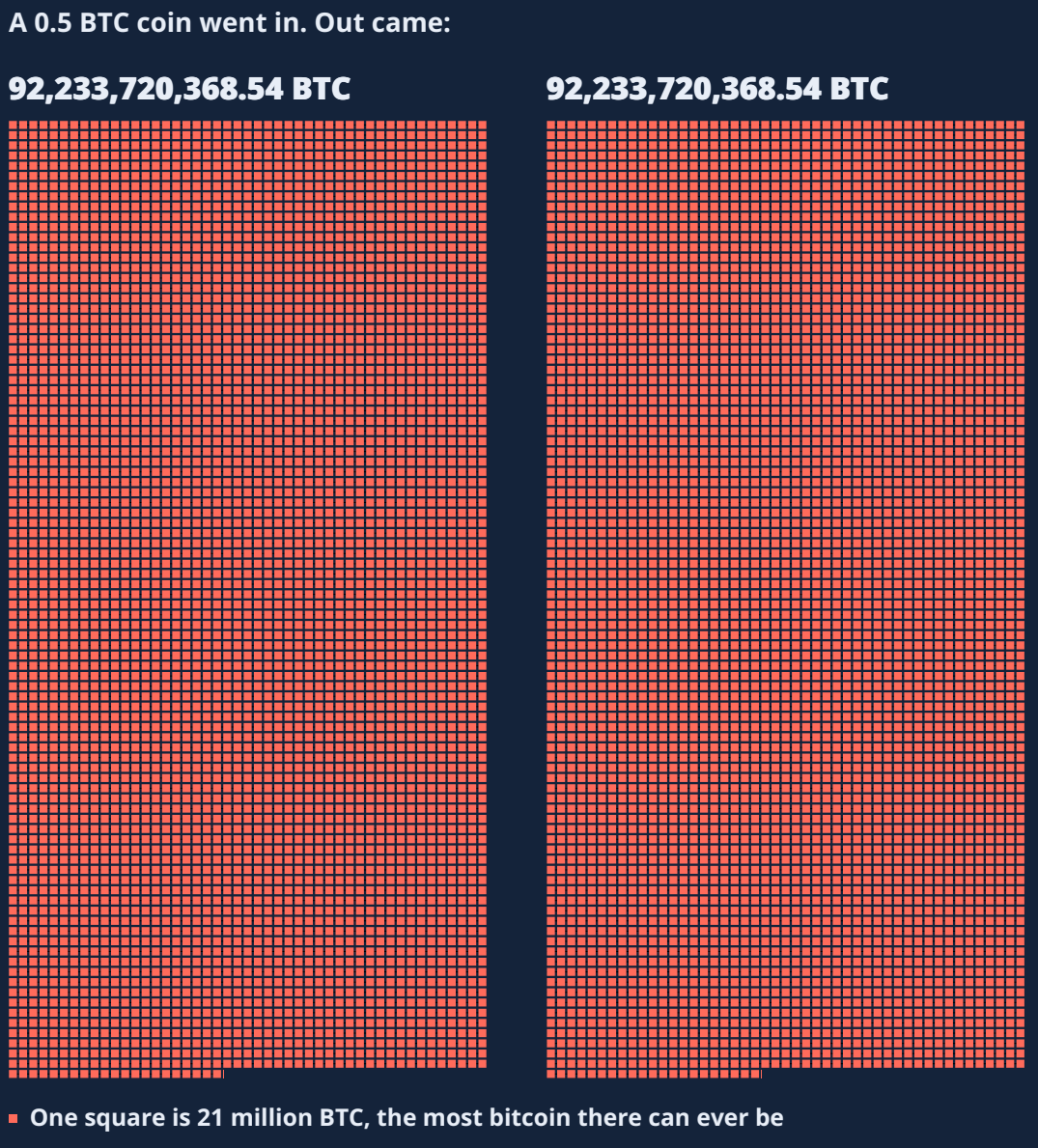
Satsumap chain analysis

The bug that created 184 billion bitcoin

Block 74,638 · August 15, 2010



Translation review by Max Labib (automated agent): compared with the Spanish, Oct 30, 2026

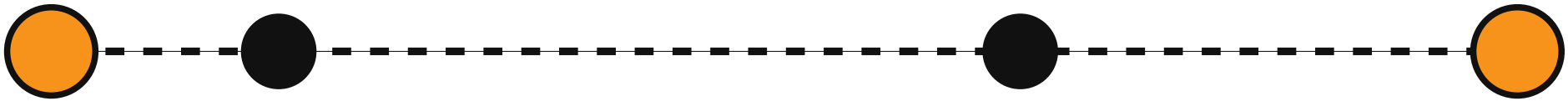
data from Oct 29–30, 2026

THE STORY

01

Seven hours in August 2010

Aug 15, 2010, UTC time



17:05 the block

18:08 the warning

21:35 the fix

23:53 the new chain

The block 1

Block 74,638 carries a transaction that creates **184 billion** bitcoin. Only 21 million can ever exist.

The warning 2

A user of the Bitcoin Talk forum reads the block and posts that the number is “quite strange”.

The fix 3

Satoshi adds a cap to the software. From the new version on, a transaction cannot create more than 21 million bitcoin.

The new chain 4

Nodes with the rule reject the block and mine again from the one before it.

The transaction is no longer on the chain.

Six words for this case

Output
A new coin created by a transaction. What goes out **cannot be more** than what goes in.

Fee
What goes in minus what goes out. The miner who puts the transaction in a block keeps it.

Satoshi
One hundred millionth of a bitcoin. The software stores amounts in satoshis, as whole numbers.

Overflow
A number stored in a fixed space has a maximum. If a sum goes past it, it **wraps around** and shows up negative.

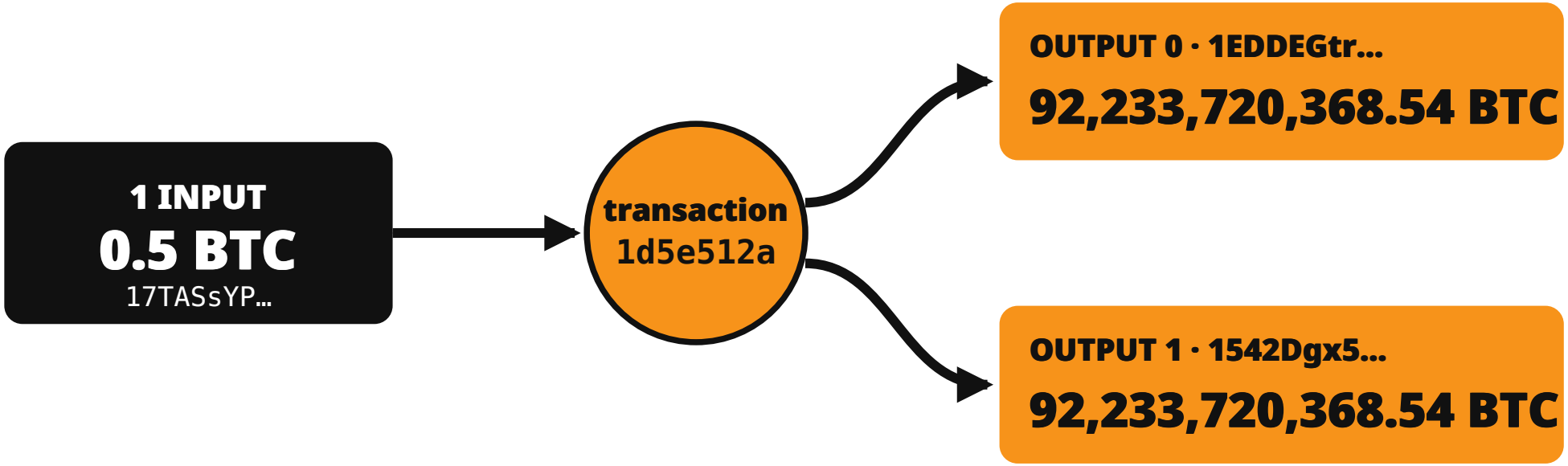
Branch
If two blocks point to the same previous block, the chain splits in two. The network keeps one and drops the other.

Consensus rule
What every node checks in every block. If a block breaks it, that node rejects it.

A node is a computer that runs the Bitcoin software and keeps its own copy of the chain.

AUG 15, 2010, 17:05 UTC · BLOCK 74,638

From 0.5 BTC to 184 billion



4,392
times the 21 million that can exist, in each output

2
transactions in the block, the miner's and this one

50.51
BTC for the miner: the block's 50 and 0.51 in fees

0.01
BTC too much in that fee. The input was 0.5

TXID 1d5e512a9723cbef373b970eb52f1e9598ad67e7408077a82fdac194b65333c9. The amounts as they were posted on the forum that afternoon.

THE SOFTWARE'S MISTAKE

04

The sum wraps around

Each output passes on its own

The software checked that no output was negative. Both were positive.

The sum does not fit

Together they add up to 18,446,744,073,708,551,616 satoshis. The software added them in a space that goes up to 9,223,372,036,854,775,807.

It ends up at −0.01 BTC

Past the maximum, the number wraps around and shows up negative, like an odometer going from 99999 to 00000.

The rule lets it through

What goes out (−0.01) is not more than what goes in (0.5). The fee comes to 0.5 − (−0.01) = 0.51.

EACH OUTPUT

2^{63} − 500,000 sats

BOTH TOGETHER

2^{64} − 1,000,000 sats

WHAT THE SOFTWARE SAW

−1,000,000 sats

That someone chose those amounts on purpose is not recorded on the chain. It is deduced from the shape, because the sum comes out just barely negative.

AUG 15, 2010 · BITCOIN TALK FORUM

An hour later, on the forum

18:08 UTC · JGARZIK, “STRANGE BLOCK 74638”

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

He posts the whole block, as text, **an hour after** the time the miner put on it.

18:55 UTC · LFM, IN THE SAME THREAD

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

And asks people to shut down what they can and not to send or accept payments.

jgarzik copied the block from his node. theymos showed it from his own, 20 minutes later.

WHAT IS GONE

06

How to check an erased transaction

It cannot be looked up today

On today's chain, the transaction and its block do not exist. Search for it on mempool.space and it answers that it cannot find it.

The forum kept all of it

jgarzik posted the signature, the key, the coin it spends and the two outputs.

It is rebuilt, byte by byte

With that data, its fingerprint (the TXID) comes out **exactly** 1d5e512a…65333c9. A single different byte would change the whole fingerprint.

The key owns the coin

The signing key is the one for the 0.5 BTC coin it spends, which is still on the chain.

What it proves

That the forum dump is faithful. The exact amount of each output and the two addresses come from it.

The signature itself. The 2010 nodes accepted it, and today's chain no longer keeps it. **NOT CHECKED**

The 2010 software printed the script data with its bytes reversed. Turned around, the fingerprint matches.

A new rule in four and a half hours

```
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");
}
```

In green, what is new, summarized. No output, and no sum of outputs, can go past 21 million bitcoin.

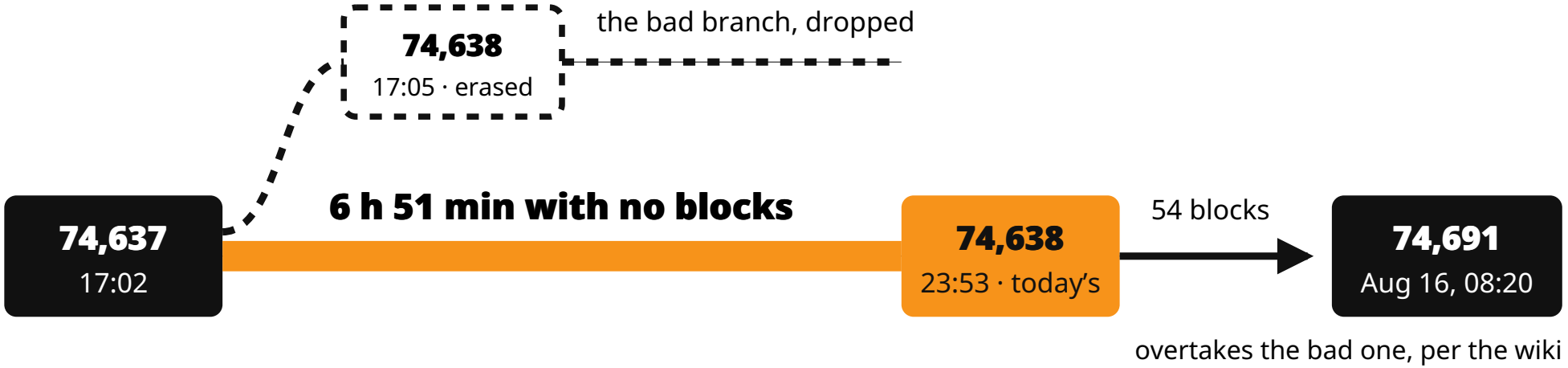
UTC	WHAT HAPPENED
17:05	The block with the overflow
18:08	The warning on the forum
20:39	Gavin Andresen posts a first patch
21:06	Satoshi asks people to stop mining: “We will probably need to re-do a branch”
21:35	The fix goes into the code (SVN 132)
23:48	Satoshi announces version 0.3.10

Commit d4c6b90 in the Bitcoin repository: “fix for block 74638 overflow output transaction”. The times come from the forum and the repository.

ON TODAY'S CHAIN

08

6 h 51 min with no blocks



23:53
the time of today's 74,638. Block 74,637's is 17:02

35.6 min
the next-longest gap among the 90 blocks around it

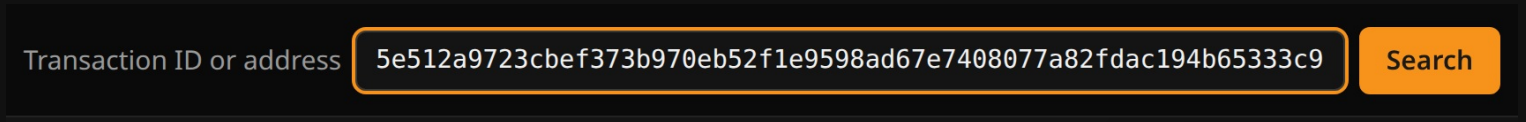
5 min 37 s
between the 0.3.10 announcement and the first block of the good branch

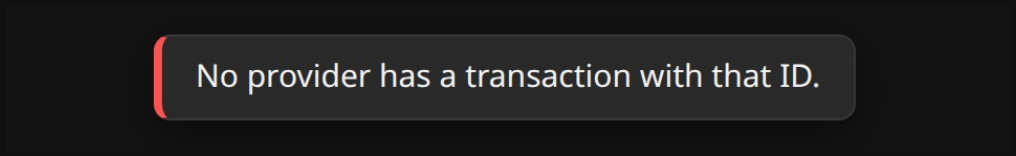
8 h 26 min
to mine the 54 blocks up to 74,691

The bad branch is not on the chain. How many blocks it had, or at which block the good one caught up, comes from the Bitcoin Wiki. The times are the ones each miner wrote.

HOW IT LOOKS

Satsumap says it does not exist





What is searched for

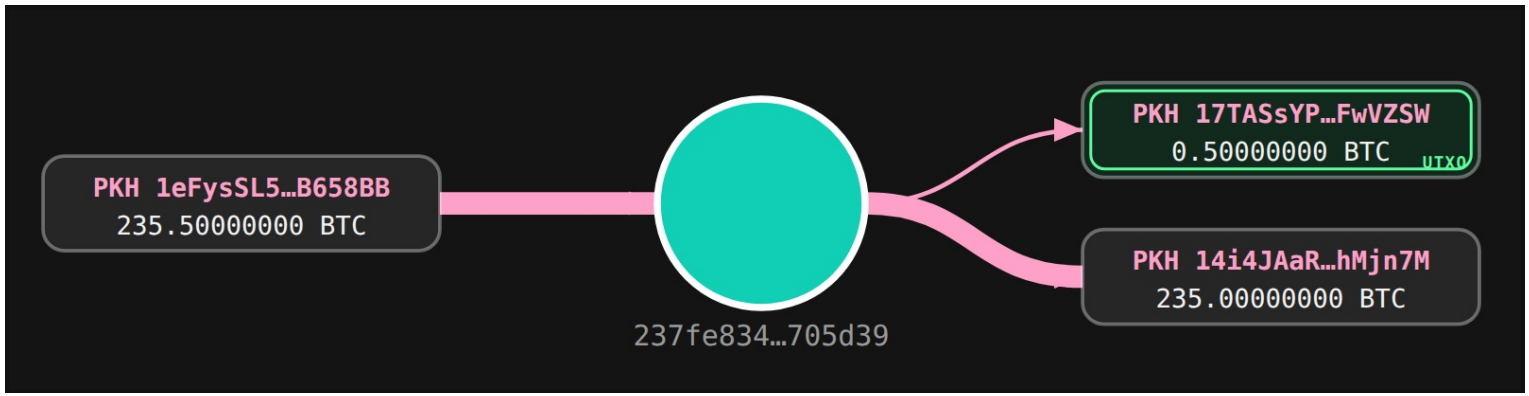
The TXID of the overflow transaction, typed into the search box.

What it answers

That it does not exist. The answer comes from mempool.space, which keeps today’s chain.

The transaction existed for a few hours on the bad branch. The chain that nodes keep today does not have it.

The attack's coin is still unspent



Top right, the 0.5 BTC

The coin the overflow transaction spent, at 17TASsYP…FwVZSW. Satsumap marks it UTXO: **unspent**.

Why it is still unspent

Its spending was in the erased block. Since 2010 nobody has moved it again.

1

transaction in that address's history, the one that gave it the coin.

TXID 237fe8348fc77ace11049931058abb034c99698c7fe99b1cc022b1365a705d39, output 0. The other output, 235 BTC, was spent 17 minutes later.

183 payments of 0.5 BTC



183
payments up to the one to 1542Dgx5..., each with the previous one's change

173
different addresses receive the 0.5

19
payments together in block 74,642, the first with payments from this chain after the gap

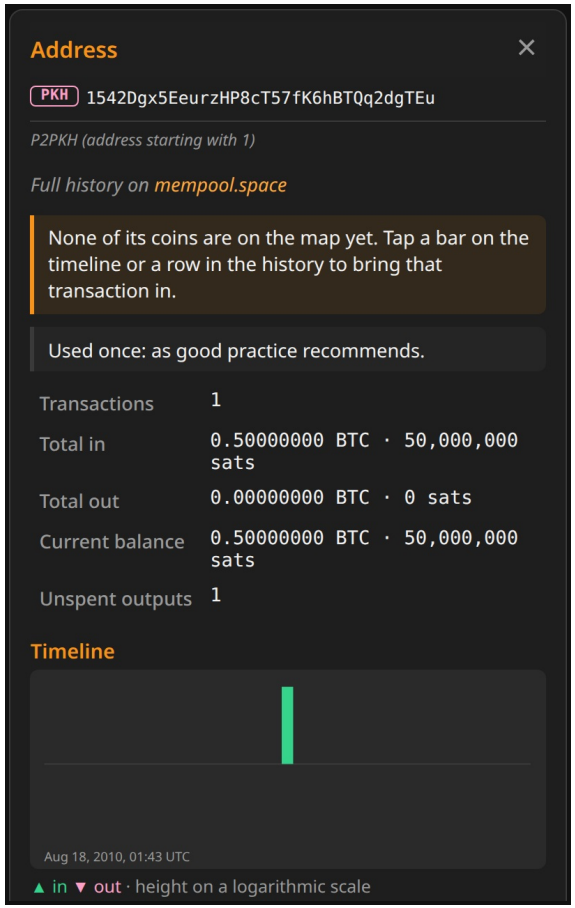
235 → 143.5
BTC of change over those 183 steps, 0.5 less at each step

In the same block 74,642, transaction `fb9c3667…` gathers six coins of 0.5 into a single 3 BTC output. Five are payments from this chain. Spending each coin takes its key, so most likely those five addresses had the same owner.

173 ADDRESSES ARE PROBABLY NOT 173 PEOPLE

The change was followed output by output. The shape is that of a faucet, a site that gave away bitcoin to try it out. Whose it was has not been confirmed.

A payment to an overflow output



What can be read on the chain

Payment 183 of the chain goes to 1542Dgx5…, output 1 of the overflow, 56 hours after the bad block. It is its only transaction, and that 0.5 BTC is still unspent. The chain goes on after that payment.

The other address

1EDDEGtr…, output 0, has no transactions on today's chain.

INFERENCE

It is consistent with the same person having built the overflow and asked for both payments. **It does not prove it.** A faucet sends to whatever address it is given, and anyone who knew how to pull that address out of the forum dump could ask for it.

The address does not appear written on the forum, because the dump had its bytes reversed. The three threads about the incident were searched.

FOR BEGINNERS

What the overflow leaves behind

Each node applies the rule

On Aug 15 the nodes accepted the block because that rule did not exist. With 0.3.10, each updated node rejected it on its own.

The warning came from a node

jgarzik posted the block his node had received. lfm explained it 47 minutes later.

Another branch was mined

Nobody edited blocks. The network mined another branch from 74,637 and kept that one.

How a node decides

It checks each block on its own, with the rules of the software it has installed. It only counts a branch's work if its blocks follow those rules. That is why, after updating, the bad block's branch stopped counting for that node, even if it was longer.

Nodes that did not update

For the old software, both branches were valid, and the node followed the longer one. When the good branch overtook the bad one, the node switched to the good one without anyone touching it.

The rule is still in today's software, Bitcoin Core. A node rejects a transaction if one output, or the sum of the outputs, goes past 21 million BTC.

FOR BEGINNERS

A new rule and old blocks

The 2010 rule had no starting block

The fix applied to the whole chain. That is why it made 74,638 invalid, even though it was already mined.

To clean up, blocks had to be downloaded again

At 21:40, Satoshi asked people to shut down the software, replace their saved blocks with a copy from before 74,000, update and let the rest download. The missing blocks were downloaded with the already updated software.

0.3.10 brought another check

It was added at 22:21 (SVN 133). It rejected a new block if its branch went through the bad 74,638, recognized by its hash.

The next day, updating was enough

On Aug 16 the good branch already had more work. An updated node switched to it on its own, without deleting anything.

Today a new rule starts at a set block

Taproot activated at block 709,632, on Nov 14, 2021. Earlier blocks are still validated with the rules of their time.

Bitcoin Core can verify the saved chain again (-reindex) or mark a block as invalid by hand (invalidateblock).

READ WITH CARE

What can be read on the chain and what cannot

STATEMENT	WHERE IT COMES FROM
The transaction and its block are not on today's chain	**Chain**
The transaction's amounts, signature and addresses	The forum, checked with the rebuilt fingerprint, which gives the TXID
The sum comes to −0.01 and the fee to 0.51	The arithmetic, on those amounts
The miner collected 50.51 BTC	The forum (that transaction is gone too)
The 6 h 51 min gap after block 74,637	**Chain**
The times of the warning, the patch and 0.3.10	The forum and the code repository
The good branch overtook the bad one at block 74,691	Bitcoin Wiki. It cannot be checked on the chain
The 0.5 BTC coin is still unspent	**Chain**
The 183 payments up to the one to 1542Dgx5…, and that the chain goes on	**Chain**
The payments spent together had the same owner	**Inference** from the shape
The payments came from a faucet	**Inference** from the shape, and the wiki says "appears"
Who built the overflow	**Unknown**

CHECK IT YOURSELF

The data, in plain sight

Block 74,421 · the 0.5 BTC coin the overflow spent (output 0)
`237fe8348fc77ace11049931058abb034c99698c7fe99b1cc022b1365a705d39` mempool.space

Today's block 74,638 (23:53 UTC) · its first transaction
`2ae30f63b1507761b5541f7a723f566abb0701e5f8a97927980381341b5d8cbd` mempool.space

Block 74,923 · the 0.5 BTC payment to an overflow address
`672495458201c55cdf4fa47cd40ff0bc8cbbd898b5dd564f84b81b0a87423417` mempool.space

Address of the attack's coin
`17TASsYPbdLrJo3UDxFfCMu5GXmxFwVZSW` mempool.space

Overflow output 1 · received 0.5 BTC on Aug 18, 2010
`1542Dgx5EeurzHP8cT57fK6hBTQq2dgTEu` mempool.space

Overflow output 0 · no transactions today
`1EDDEGtrZ5877WPsLU5o9TwjJDqaUqhvte` mempool.space

The overflow transaction, to search for it and see that it is not there: `1d5e512a9723cbef373b970eb52f1e9598ad67e7408077a82fdac194b65333c9`

Sources off the chain: Bitcoin Talk, threads 822, 823 and 827 (2010) · commit d4c6b90 in the Bitcoin repository · Bitcoin Wiki, "Value overflow incident".