Twitter Thread by Lucas Nuzzi



Lucas Nuzzi
@LucasNuzzi



1\ There is an alarming amount of misinformation (fueled by the media) on what exactly happened to Bitcoin yesterday, and whether funds were "double spent"

Here's everything you need to know ■

2\ On the 18th, a user broadcast a transaction with very low fees.

When users underpay fees, their transactions gets stuck because miners have more profitable opportunities.

Users are left with 2 options:

a) wait until fee levels drop
b) tell miners they will increase fees

3\ The most popular way to (b) increase fees of an already-broadcast transaction is through a "Replace By Fee (RBF)" transaction.

Put simply, RBF is a copy-and-paste of the original transaction with higher fees and an explicit instruction to favor the new transaction instead.

4\ Nearly a day passed after our infamous user broadcast the original transaction and miners did not include it.

So the user decided to issue an RBF on the 19th with higher fees... but not high enough!

And the transaction was again stuck...

5\ A couple of hours later, the user decided to bump fees up again via a second RBF!

This time around the user paid enough fees.

6\ So, to recap, the user broadcast a total of 3 transactions:

1) Dec 18th 22:11 UTC (1 sat/b)

2) Dec 19th 21:22 UTC (9.4 sat/b)
3) Dec 20th 00:32 UTC (14.3 sat/b)

And here's where things get a bit more complex

7\ At around 1:18AM the blockchain split into 2 versions, which is an entirely normal occurrence; a fundamental part of how Bitcoin works.

When this happens (1+ times per month), miners need to converge on a single version of events, which often takes around 1 block, or 10 min.

8\ However... by the time the user broadcast the third transaction, fee levels had quieted down and the chain was split:

-One miner picked the first (low fee) transaction for their version of the chain
-The other miner picked up the third (highest fee RBF transaction)

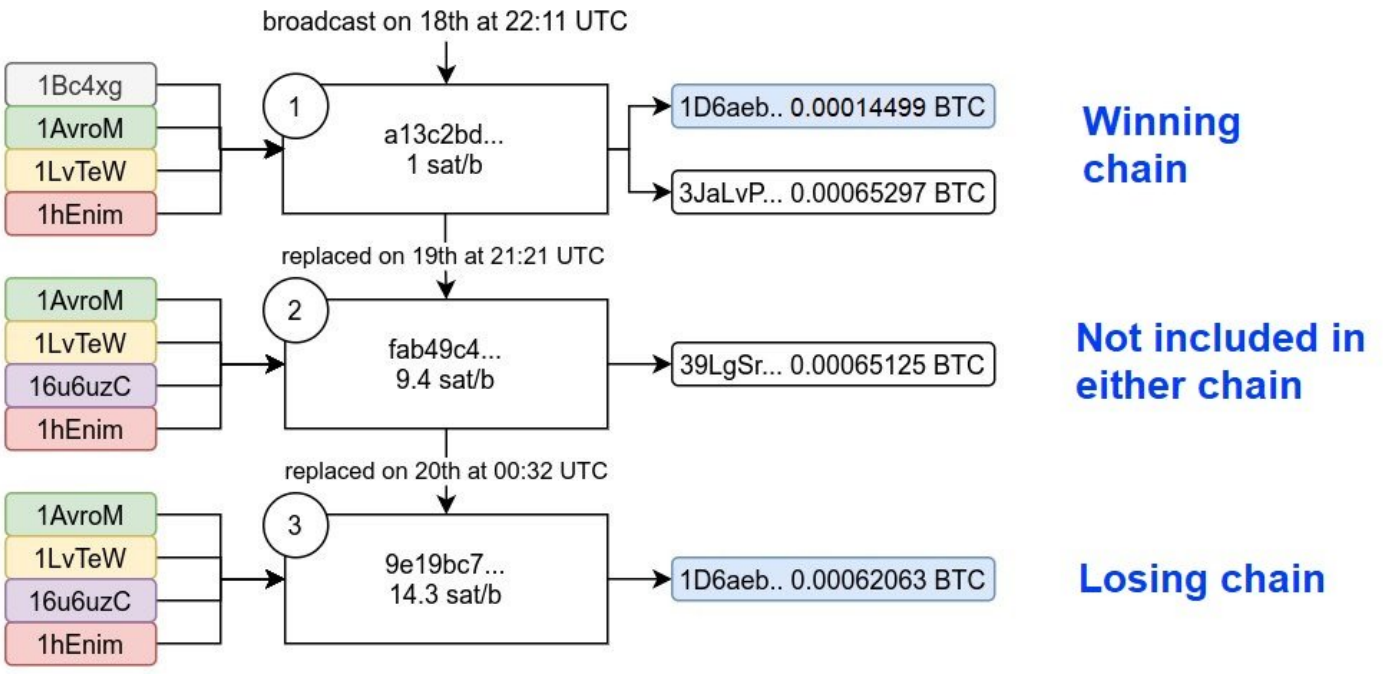
9\ The thing about RBFs is that they're entirely optional. Miners decide which transaction to pick.

In this occasion it might have looked like a malicious "double spend" (inflation), but it is a completely normal event.

10\ The chain was split for 1 block (again, normal), but ultimately the miner on the branch with the low fee transaction ended up winning.

The important thing to know is that, yes, there might be different versions of the same transaction, but ONLY 1 will ultimately be accepted.

11\ @0xB10C (follow this man) made a helpful timeline of events using @coinmetrics data:



12\ Again, RBFs in stale blocks is business as usual.

No reason to freak out. No inflation, no "double-spend" was actually confirmed. Just a ton of loud ignorance and misinformation.

13\ This is a wake up call for crypto media. Looking at you @crypto and @Cointelegraph

You benefit by serving crypto adds. I urge you to at the very least understand your responsibility and step up your technical game.

How about sponsoring a bitcoin developer?

14\ Another clarifying point: @BitMEXResearch is doing an amazing job for the community with https://t.co/k9MhseACnP and https://t.co/0gjizyXMy7

Their depiction of what happened was accurate. Unfortunately, their post was grossly misrepresented misrepresented for clickbait...