Twitter Thread by Andreas M. Antonopoulos



Andreas M. Antonopoulos
@aantonop



A more detailed explanation of the whole

"A double-spend broke Bitcoin" FUD that was circulated by an irresponsible publication.

1/

There was a chain re-organization in the Bitcoin blockchain. This is a common occurrence that is part of Bitcoin's normal operation. It is a result of decentralized consensus under Proof-of-Work. All PoW chains do this.

2/

Two blocks were mined almost simultaneously, competing for the same height, meaning that they had the same parent block and were trying to extend the chain of the same block

3/

Only one can ever succeed in the long run. It is possible that different nodes and miners see one or the other block first and assume it is the winner. This is also normal in a decentralized consensus algorithm

4/

Eventually, within an average of 10 minutes another block is mined. This new block has as its parent *one* of the two competing blocks. Which one? Whichever one the miner saw first and assumed to be the winner.

The new block extends the chain, resolving the issue.

5/

Of the two originally competing blocks, one is now a parent and the other is the last descendant of a shorter chain. The chain with the greatest cumulative difficulty is selected by all. This "orphans" any descendants from the other chain because it is discarded.

6/

Again, all of this is normal. A 1-block reorganization happens every couple of weeks on average as a consequence of decentralized PoW.

A 2-block reorganization happens less often, maybe a few times a year

A 3-block reorg is extremely rare. I don't think we've ever seen one

7/

What happens to any transactions in the discarded block? If they are also in the winning block then all is well. If they are not in the winning block, each node puts them back into its mempool as "unconfirmed" and they wait for another opportunity

8/

During a re-organization, there is a chance for someone to attempt a "double spend". This is not a double spend from the perspective of the blockchain as a whole. Only one spend survives, therefore no double spends happen. That's the whole point of PoW consensus.

9/

But from the perspective of the recipient of a payment, they may see a transaction that appears to have 1 confirmation (it is in a block), then disappears when that block is discarded.

10/

Very rarely, the sender will sneak a *different* transaction in the competing/winning block. Let's say this is a payment for a lesser amount (more change back), or to a different address.

11/

Because the original transaction is gone (discarded block), the new transaction (winning block) is the only "real" transaction. The blockchain has prevented a double spend by discarding one and only recording the other.

12/

From the perspective of the recipient, they thought they were "paid" after 1 block, then they... weren't. This is why "confirmations" provide /probabilistic/ immutability. The chance of a reorg drops with each subsequent confirmation

13/

This is described in the Satoshi whitepaper on page 8. In fact, it's the only math equation in the paper and it describes the declining probability of a re-org, showing why "6 confirmations", though arbitrarily chosen is a good basis to consider a

transaction finalized

14/

Here's page 8. As you can see the chance of a block getting discarded from a reorg declines /exponentially/ as more blocks are added to the chain. Finality is based on probability.

15/

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012
```

So when do you consider a transaction finalized and when is it safe to give your customer the TV or the fiat or whatever value you are exchanging? It depends on the amount!

I waited 3 confirmations after selling my car for $11,000 USD (IIRC). Was enough for me.

16/

It also depends on the risk of the buyer going away. I'd sell a house on 0-conf, *because I know where they live!*. They can't run away with it. Some things are more dangerous: I'd wait 6 confs to exchange for cryptocurrency, because once I give it I can't get it back.

17/

During this most recent re-org, a transaction of $22 was in both competing blocks as two competing transactions. We don't know why. We don't know who. But there's nothing "impossible" about this. It is part of the protocol

18/

Now, for $22 many would accept 1 confirmation. Worst case, you're out $22 of something you gave in return that was delivered instantly and irreversibly. Not a big deal.

19/

Many credit card vendors don't take a signature for amounts under $25 for the same reason: while it can be disputed without a signature, it's not worth the extra time and delay to get one for such an amount. Same risk model here.

20/

In fact, we do not know that the recipient of that payment lost money. They may have been waiting for 2 confirmations and not delivered the other part of the value. So in that case, they lost nothing - they consider this "unpaid" because it didn't get 2+ confirmations

21/

Someone article quoted the lie "it could've been $22 million". Well, no, it couldn't. If you accept a $22m payment on bitcoin, I would assume you understand how Bitcoin has worked since 2008, exactly as specified in the paper. You don't "deliver" on that payment after 1 conf

22/

Several other incorrect statements are also made in that and other articles about RBF and Segwit. Here's the truth: this is a normal function of any PoW blockchain. A re-org with two different versions of a transaction can occur in every other PoW chain.

23/

Nothing weird or outside the consensus algorithm happened. Bitcoin continues to work exactly as it should. The only thing that happened is bad "journalism" if it can even be called that. In a bubbly market, a rumour can circle the globe before it is debunked.

24/

Consider it debunked.