Twitter Thread by Lucas Nuzzi



Lucas Nuzzi
@LucasNuzzi



1/ It's time to have a conversation about #Dogecoin.

If you're invested in $DOGE after @elonmusk's much endorsement (such wow), there are a couple of things that you should probably know■

2/ First, let's talk about network security (I'll try to keep it simple).

Unlike BTC, ETH, or really any other major network, Dogecoin does not have its own miners -- it currently relies on another network, Litecoin, to survive.

So how did this happen and what does it mean?

3/ Back in 2014, Dogecoin was at a tough spot. There weren't enough miners working on $DOGE and there was a real risk that its network would be attacked.

A network attack (like a "51% attack") would likely destroy Dogecoin, so its developers had to do something...

4/ Their solution was to adopt something called Auxiliary Proof of Work (AuxPoW); a way to merge Dogecoin mining with other similar networks.

Put simply, AuxPoW enables miners to work on multiple coins at the same time and reuse the same work.

5/ Back then, it was somewhat of a controversial solution. Some users were concerned that AuxPoW would put the future of $DOGE at the mercy of bigger miners.

While the change likely saved Dogecoin, the concern was valid: ~95% of Dogecoin mining today is done by Litecoin miners.

6/ This dependance carries some nasty security implications when DOGE has a market cap of nearly 10B USD.

When AuxPoW was adopted, not a lot of value was being settled on Dogecoin...

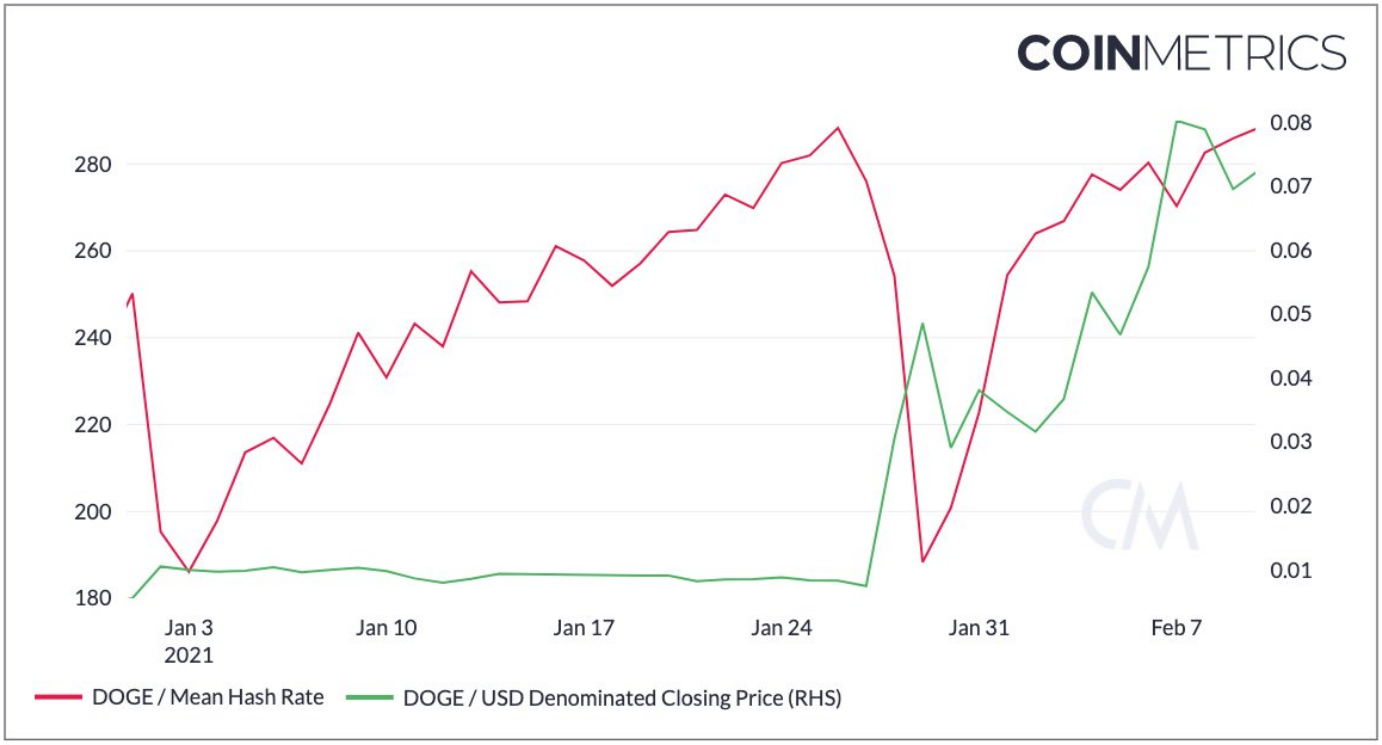
But in the month of January alone, Dogecoin settled the equivalent of over 8 billion USD ■

7/ You see, the thing about AuxPoW is that it's a double edged sword...

While it protects both LTC and DOGE with the same work, it also makes it easier (and considerably cheaper) for an attacker to simultaneously take over both networks.

8/ Consider that the price of $DOGE is up 1200% YTD, while hashrate (a proxy for network security) grew a meek 15% YTD.

This ratio, coupled with the existence of AuxPoW, makes a 51% attack on LTC (and by extension DOGE) incredibly attractive since it would carry a high ROI.



9/ So how could this go down?

Here's a hypothetical attack:

1) Buy large quantities of DOGE+LTC

2) Deposit all of it in a major exchange

3) Trade DOGE+LTC for BTC

4) Withdraw BTC

5) Issue 51% attack on LTC that makes it so that deposit (2) never happened in either chain

10/ It's unfortunate, but DOGE and LTC will have to endure a dangerous period until more miners join in and make this attack harder to pull off

Although it's now 136% more profitable to merge mine LTC+DOGE, it'll take time for more miners to setup farms and bootstrap operations

11/ So what can be done?

The best thing to do is to increase transaction confirmations when receiving LTC or DOGE.

■The 20 confs exchanges and users are currently relying on is not enough■

A full day is what I'd personally require. That puts a ~2M USD cost floor on attacks.

12/ Does this only affect crypto exchanges?

No. Exchanges are primary targets, but if you've received a LTC/DOGE withdraw transaction from an exchange who is subsequently targeted, your withdraw might disappear after the attack takes place.

13/ Now let's talk a bit about maturity.

Is this the only problem affecting Dogecoin?

Such no... much no...

Dogecoin is a fork of Litecoin who hasn't seen much development in the past 4 years.

Networks like Bitcoin evolved and matured, while Dogecoin remained stagnant.

14/ We run 3 dogecoin nodes at @coinmetrics and we can see they're struggling to support all of this activity.

As of now, they're all on different heights and taking time to catch up to the tip of the chain.

15/ This lack of maturity and seriousness is fun, it's part of the meme..

But if a ten-billion-dollar-marketcap Dogecoin is your stepping stone into crypto, you have to be careful. Don't put your life savings in a meme.