Dogecoin likely needs a wingman to survive

The key ingredient to the success of any decentralized public ledger, such as Bitcoin, is incentivizing its transactional network to simultaneously secure the network from attackers and process transactions.

In the case of Bitcoin, and in the case of virtually all other cryptocurrencies, this incentivization process is handled through seigniorage. Every 10 minutes (or 2.5 minutes for Litecoin, or 1 minute for Dogecoin) a fixed amount of bitcoins is paid to the labor force called "miners." These miners are computational systems that perform never-ending mathematical calculations dubbed hashing. This hashing in turn creates security for the network; so as long as more than 50% of the hashrate is maintained by "good" systems, bad actors are prevented from manipulating the ledger through double-spending attempts. The other key role these miners also fill is processing and including transactions into packages called blocks. Every 10 minutes, one miner is rewarded for processing these blocks with fixed income. Last month David Evans published a good overview (pdf) of how this process looks from a labor input and supply output perspective.

For some advocates, one of the purported advantages of cryptocurrencies is that their money supply creation rate is actually deflationary (or contractionary) in the long run (in the short run, Bitcoin's expansionary rate is quite high, with inflation at 11.1% this year alone). That is to say, it is a hardcoded asymptote, tapering off over a known time period. In the case of Bitcoin, the wage for the labor force (miners) is split in half roughly every 4 years (every 210,000 blocks), for approximately the next 100 years – until its money supply is exhausted at a final 21 million bitcoins. Roughly 12.7 million bitcoins have already been paid to miners. With Dogecoin's 100 billion dogecoins, this process is accelerated, with the mining income dividing in half every two months. While it took about five and a half years for about 60% of bitcoins total monetary base to be distributed, as of today 78.9% of dogecoins reward (income) has already been divvied out to its workforce in less than 6 months.

While this has frenetically fast money supply has provided a psychological motivation for early adopters to partake in the Dogecoin ecosystem, economic law suggests that this network will probably cease to exist in its current form within the next 6 months probably through a 51% attack.

The reason is simple: with every block reward halving (also called "halving day"), the labor force is faced with a 50% pay cut. The contractors (laborers) incapable of *profitably* providing hashrate at this level can and will leave the work force for greener pastures. This same issue has impacted other altcoins in the past, such as MemoryCoin, which died after 9 months due to a combination of factors including diminished block rewards (it attempted to divvy out its entire monetary supply in 2 years).

Early advocate of Dogecoin like to point to outlier events such as the Doge bobsled team or sponsored NASCAR driver at Talladega or even a vaunted tipping economy (which is actually just faucet redistribution) as goal posts for growth and popularity, yet after two halving days the actual Dogecoin blockchain has lost transactional volume each month over the past 4 months and the labor force has also left for new employment elsewhere.

This is visualized in the following two graphs.

Chart 1:

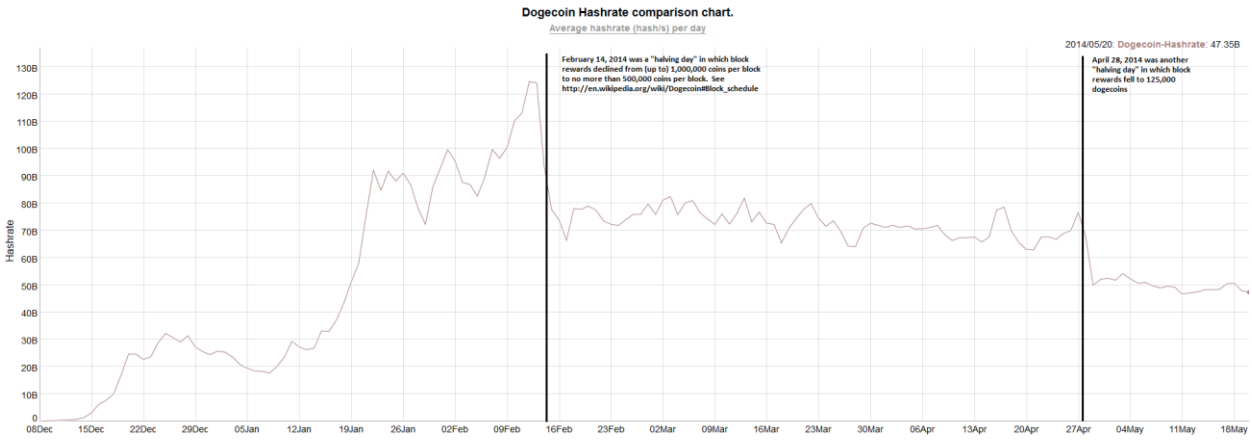
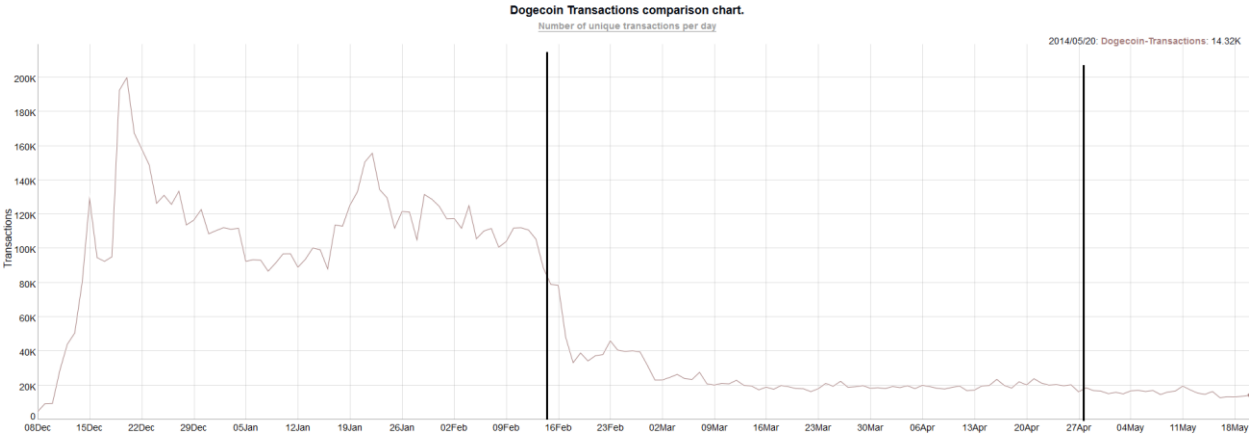


Chart 2:



The first chart shows Dogecoin's collective hashrate. The black lines indicate when the "halving day" or rather "income-halving day" occurred. Because the price level of a dogecoin remained relatively constant during this time frame, there was less incentive for miners to stay and provide labor for the network. If token values increased once again, then there may be incentives in the short-term for laborers to rejoin the network. Yet based on this diagram, roughly 20-30% of the labor force left after each pay cut.

The second chart shows on-chain transactional activity. The first three months are erratic because of how mining pools (similar to lottery pools) paid their workforce (miners). Following the first halving day in February, the network transaction rate fell to roughly 40,000 transactions per day and then leveled off to around 20,000 until April 28, 2014. Another halvingday occurred on April 28th and the subsequent transactional volume remained relatively flat to negative -- it is currently at 14,320 transaction per day,

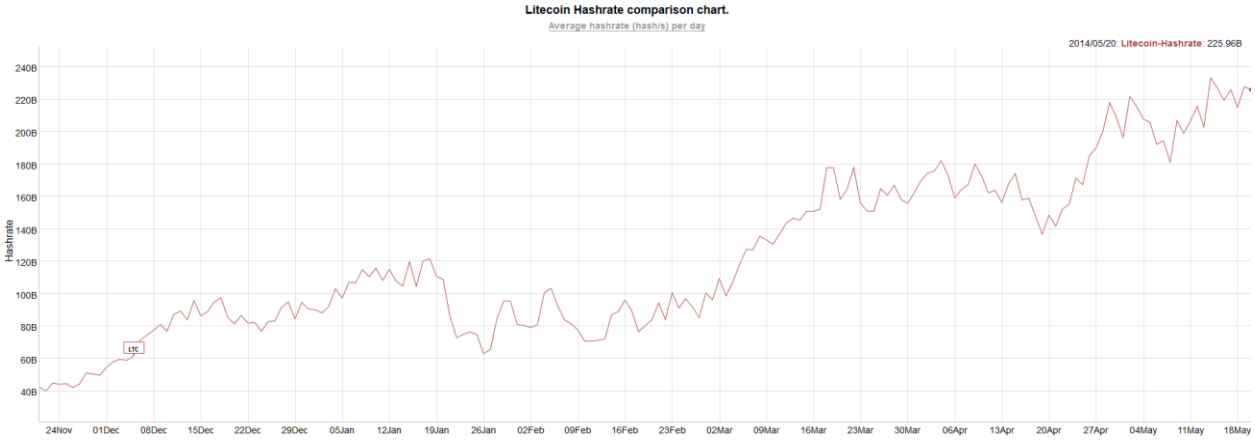
or roughly the same level it was during the first week of its launch five months ago (most of it is mining payouts from pools).

Now some readers may claim that a lot of the transactional volume such as tip services and tip bots are being conducted off-chain and thus the total number of transactions is likely higher. And they would be correct. But that would completely defeat the purpose of having a blockchain in the first place – a trustless mechanism for bilateral exchange that negates the need for "trust-me" silos (as Austin Hill calls them). Also, while this topic deserves its own series of articles, but there is little literature that suggests that tipping can grow an economy; it is *not* a particularly good signaling mechanism or way to cultivate a developing economy (i.e., "China, you need more tipping activity to grow and prosper").

However the key issue is this: if the trend continues and the network hashrate continues to fall 20-30% after each halvingday, then within the next 2-4 months it will be increasingly *inexpensive* for competing mining pools on other ledgers to conduct a 51% attack on Dogecoin's network, destroying its credibility and utility.

For instance, the chart below is the Litecoin hashrate over the past 6 months. Litecoin is Dogecoin's largest competitor based on its proof of work (PoW) mechanism called scrypt:

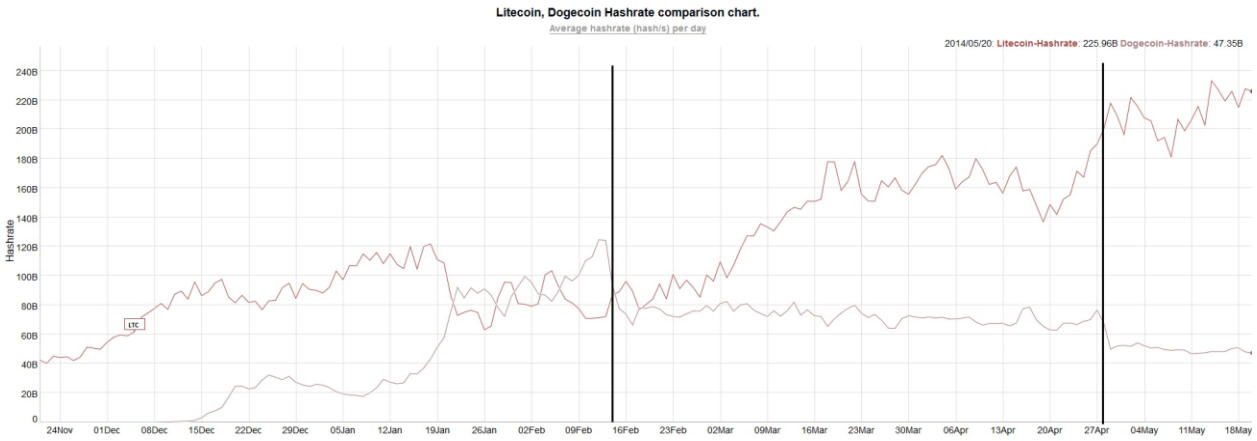
Chart 3:



One of the reasons the Litecoin hashrate is not rising or falling at a constant rate but is instead jumping and down erratically is that miners as a whole are economically rational actors. When the cost of producing security is more than the reward (block reward income), the labor force turns towards a more profitable process such as another alternative scrypt-based "coin" (note: Bitcoin's PoW method uses SHA256d whereas Litecoin and Dogecoin uses scrypt). The same phenomenon of hashrate jumping up and down occurs with the Bitcoin network (see Securing Information).

For the sake of simplicity, the Litecoin network can be viewed as roughly 200 gigaghashes/second versus the Dogecoin network which is roughly 50 gigahashes/second. To conduct a 51% attack on Dogecoin today, an entity would need to control roughly 25-26 gigahashes/second which is roughly 1/8th the processing power of the Litecoin network. The current 'market cap' for Dogecoin is $35 million, assuming MV=MC (see pdf), *ceteris parebis* on paper it could cost $17.5 million in capital and operating expenses to successfully attack the Dogecoin network.

Chart 4:



The chart above shows both the hashrate of Litecoin (in red) and Dogecoin with the vertical black lines representing the dogecoin "halvingday." What this shows is that while Dogecoin, for roughly one month in early 2014 was more profitable to mine than Litecoin, the halvingday led to an exodus of labor.

If current prices and trends continue (which they may not), in two months the Litecoin collective hashrate may hit 240 gigahashes/second and Dogecoins hashrate shrinks due to halvingday by another 20% to 40 gigahashes/second. At this rate a successful 51% attack on Dogecoin would require just $1/12^{th}$ of the hashing power of Litecoin which at the same prices levels would entail less than $10 million in capital and operating expenses to do.

Will dogecoin survive?

While the development team could theoretically switch its proof of work algorithm (to X11 as used in Darkcoin), the doge community is really faced with six options:

- Merge mine. Namecoin was (and is) an independent blockchain, but since block 19,200 about 80-85% of its network hashrate (and block rewards) are tied to Bitcoin mining pools through a process called "merged mining." The new sidechains project from Blockstream is attempting to do the same process. Charlie Lee, creator of Litecoin explained how Dogecoin could be "merged mined" with Litecoin in a series of posts last month.
- Transaction fees. Both the development team and mining community could agree to float or raise transaction fees on the doge network (similar to what Mike Hearn has been discussing for Bitcoin). In practice however, even if approved, very little actual commerce (and therefore transactions) is conducted on the dogecoin network thus it is unlikely that this will compensate the large drop in mining income. Similarly, as Gavin Andresen pointed out in Amsterdam last Friday, increased transaction fees reduces the participation rate (note: the actual transaction costs are much higher than stated, block rewards (token dilution) are usually not factored in).
- Proof of stake. There are several variations of proof of stake. Whereas Bitcoin, Litecoin, Dogecoin and most other cryptocurrency experiments use a proof of work mechanism to protect the network from malicious entities, a proof of stake (PoS) system, such as that used in NXT, will randomly assign a "mining node" (called a "forger" a poor marketing term for

sure) to process all the blocks for the next minute. Because all of the other nodes in the network know which miner to trust, this lowers the amount of infrastructure needed to protect the network. In theory this sounds amazing. In practice however, most proof of stake systems end up almost immediately centralized in one manner or the other (Andrew Miller, Andrew Poelstra and Nicolas Houy call it "proof of nothing"). Perhaps Stephen Reed's version can work in the future.

- The market price of dogecoin increases, incentivizing the labor force to continue providing security of the network with the expectation that the tokens they are given in return for their labor will continually appreciate in value. This is betting on hope. Charlie Lee pointed out the uphill task this would require beginning next year when rewards fall to less than 1/10th of they are today, stating last month, "At Dogecoin block 600,000, only 10,000 coins will be created per block. So in order for Dogecoin to keep the same amount of security as today, Dogecoin price would need to go up by 25 times. And Dogecoin price would need to gain on Litecoin by 50 times in order to catch up on Litecoin's security. And assuming everything stays the same, the market cap of Dogecoin needs to reach $1.5 billion by January of next year." For comparison, the 'market cap' of Dogecoin today is roughly $35 million (note: it is probably not accurate to call it a 'market cap,' see Jonathan Levin's explanation).
- Migration. Dogecoin could also migrate to a platform like Counterparty and become a fully secured atcoin with a dash of Proof Of Transaction thrown in to inflate the coin with ongoing usage that this particular community likes to embrace. It could be fully protected by the Bitcoin hashrate with no further need to try to acquire miners to protect it.
- Further experimentation. While it is unlikely the Dogecoin has the resources to create secure production code in the shortened time frame, Robert Sams "growthcoin" and Ferdinando Ametrano's "stablecoin" could provide a mechanism that enables the network to live on in a different manner.

While any or all of these may be tried out, it may be too little, too late. With that said, stranger things have happened. A rising tide lifts all boats and thus in the event that "bitlicense" approved exchanges in Wall Street come online this summer and new capital actually flows into Bitcoin and other alternative ledgers, perhaps similar speculative funding will flow into Dogecoin as well. However, this is not something that can be known *a priori*.

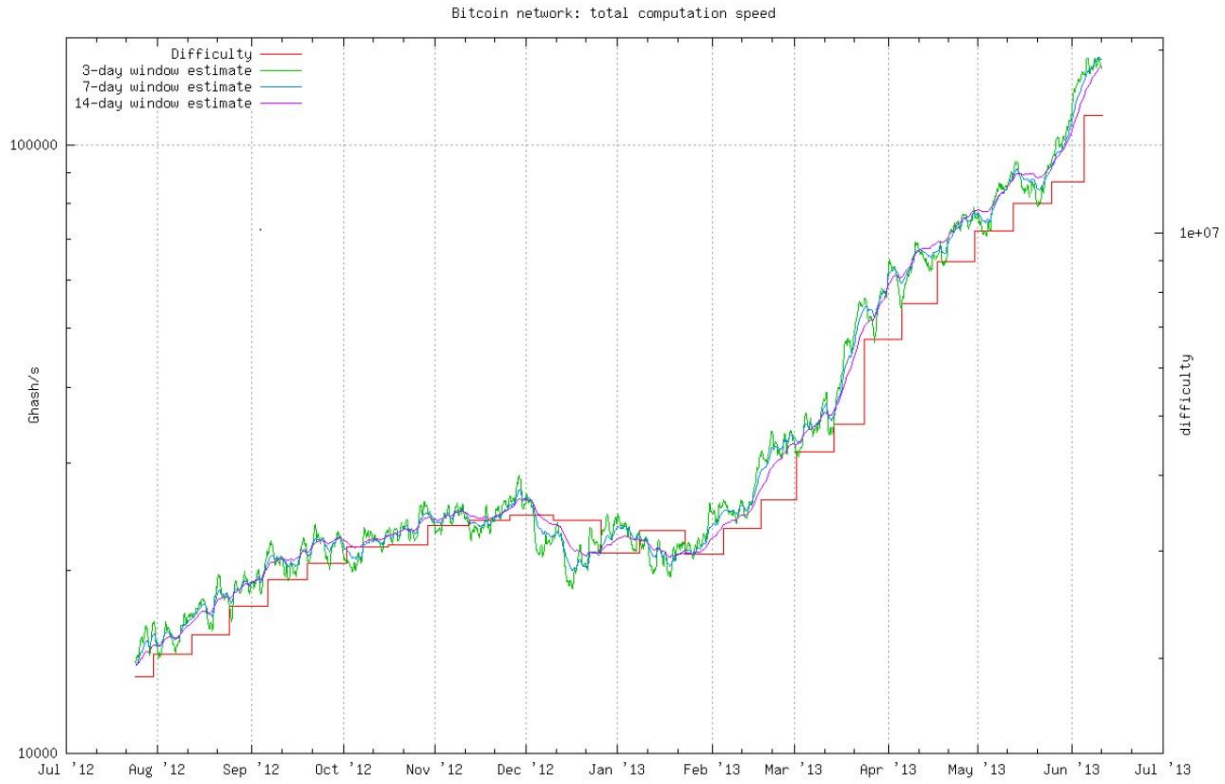
I contacted Jackson Palmer, creator of Dogecoin for his thoughts on the situation. In his view:

> It is definitely a challenge that Dogecoin (and all current-gen crypto currencies) will face in the future. I'm very concerned about the impact of centralized mining and reliance on transaction fees could hold for Bitcoin as it becomes less enticing to mine - really, the network can be held at ransom to attach hefty transaction fees if the mining pools are cherry picking as they create blocks.
>
> At the end of the day, I think the viability of cryptocurrency really hinges on a move away from PoW-based mining to something new and innovative that doesn't just stimulate an arms race and put all the power back into the hands of the fiat-wealthy. I don't have a solution unfortunately, but hopefully someone will find one and bring about a new generation of digital currencies in the coming 5-10 years.

That being said, cryptocurrency as a space is very unpredictable so it wouldn't surprise me at all if Dogecoin beats the odds and overcomes these challenges in some weird, wacky way. It's in the community's hands, and they're certainly passionate about seeing it reach the moon, as am I.

Can this happen to Bitcoin?

To be balanced, below is the network hashrate for the Bitcoin network following its first halvingday on November 28, 2012:



(source: http://bitcoin.sipa.be)

The following two months, from December 2012 through January 2013, the hashrate stayed flat and in some weeks even declined.

There were at least three reasons why the network did not decline precipitously like Dogecoin:

- Despite the fact that very little real commerce actually takes place on the Bitcoin network, there was some amount that did in 2012 and does today (primarily gambling and illicit trading of wares). Thus there was external demand for the tokens beyond miners and tippers.
- The token prices rose creating appreciation expectations. The price rose from $12.35 on November 28, 2012 to $20.41 on January 31, 2012. If miners believe and expect the price to

increase in value, they may be willing to operate at a short-term loss (see Estimated costs of building the infrastructure).

- The first batch of ASICs from Avalon shipped and arrived to their customers at the very end of January. These provided roughly 2-4 orders of magnitude per watt in performance than the top competing FPGAs and GPUs. This is equivalent of miners being given sticks of dynamite instead of pick axes to tunnel through mountains.

While more research will be conducted and published in the following months before the next Bitcoin halvingday (estimated to occur probably before August 2016), the Bitcoin network faces a similar existential hurdle, though perhaps less stark once more ASIC processes hit similar node fabrication limitations. That is to say, in the next couple of years there will no longer be performance gains measured in orders of magnitude (they will likely compete on energy costs a topic for another paper). Since most participants do not like paying transaction fees, incentivizing miners to stay and provide security will likely be problematic for the same income reduction issues. This scenario will likely be revisited by many others in the coming years.

Nothing personal

From a marketing perspective Dogecoin has done more to bring fun and excitement to this sub-segment of digital currencies than most other efforts (remember, USD can also be digitized and encrypted). In turn it brought in a new diverse demographic base to blockchain technology, namely women. While some of the more outlandish gimmicks will likely not be enough to on-ramp the necessary token demand which in turn leads to token appreciation, this project has not gone unnoticed.

For instance, two weeks ago I had coffee with a bank manager in the San Francisco financial district. As we were wrapping up he asked me to explain Dogecoin. I mentioned that what sets doge apart from the rest was its community was much more open towards self-ridicule, self-parody, less elitist and most importantly, women actually attended meetups.

He quickly surmised, “Oh, so it’s the wingman currency. It’s the friend you bring to the bar who is willing to look goofy to help you out.”

That is probably a fair enough assessment and it will likely need a wingman to survive.