The Dogeshit Manifesto

A meme has simultaneously captured the hearts of the public and billions of dollars – Dogecoin. Wealthy powers of corporate interest have coalesced to leverage the public's love of this technology for their own financial successes: Elon Musk, Mark Cuban, Robinhood, and AMC Theaters.

Where are the advancements in the Dogecoin technology from the massive retail investment driven by these corporate powers? What happened to the founding ethos, to bring the ability to participate in blockchain networks to everyday individuals while rejecting the speculative nature of cryptocurrencies? Where are the organic community contributions that funded the Jamaican bobsled team's trip to the Sochi Winter Olympics, funded building a well in the Tana river basin in Kenya, and raised enough to completely cover all of the stolen funds of Dogewallet users?

Two things result from this fact:

1. Control of Dogecoin's value has already been captured by corporate powers.
2. It is high time that Dogecoin returns to its founding ethos, prioritizing the community of individuals who were passionate about blockchain technology but couldn't participate due to prohibitive cost of entry, before corporate raiders have the opportunity to undermine the aging technology at the expense of the community.

To this end, I've created Dogeshit, a set of Solidity contracts that aim to bring the value of the Dogecoin community into a proof of stake ecosystem based around the following 4 major design choices:

1. 1 Dogecoin → 1 Dogeshit
2. Just as Dogecoin was **not pre-mined**, Dogeshit is **not pre-minted**
3. Keep the numbers –**nice**–
4. "To be clear, I strongly believe in crypto, but it can't drive a massive increase in fossil fuel use, especially coal" [1]
   "Ideally, Doge speeds up block time 10X, increases block size 10X & drops fee 100X. Then it wins hands down." [2]

'Shitcoin' – A Primer

The term 'shitcoin' has been term that has been lobbed at projects for a number of reasons: low market capitalization, a lack of purpose besides financial speculation, or a low effort fork of an existing project. The meaning is pretty straightforward, these projects are 'shitcoins' because they're worthless. It's pretty obvious to say that 'shit' is worthless, right?

Well, not so fast. In the context of consumers buying commercial products, virtually no one is going to want to pay for shit; in fact, many people pay for sewer service specifically to get rid of their shit. Corporate stocks are an extension of this; instead of buying a product though, we're talking about buying

part of a company that sells a product. In this case, something begins to emerge; if the company sold organic fertilizer to farmers, all of a sudden there appears to be a case where shit is valuable.

Shit doesn't hold much value as a commercial product; however, ecologically it appears to have been a vital component in fostering the fertility of the grasslands. Looking specifically at the African grasslands, evidence points to the fact the mobility of herds fostered a rich grassland ecosystem by consuming nutrients from across the plain, only to deposit concentrated amounts of shit into corralled areas during the night. The benefits of those habits are still detectable from as long as 3,000 years ago [3].

All of that might be interesting, but how does that matter to Dogecoin? Dogecoin, as well as other decentralized ledger technologies, are very unique technologies, whose growth and networks more closely resemble a collection of cells that works together to create a living organism, than it does a corporate entity or financial product. If we choose to acknowledge these technologies as complex multi-cellular organisms, then it is important that we step out of the Darwinist framework that is often used when discussing market competition. In a pure competition, winner take all, framework for discussing these technologies, the desired end goal is for one technology to hold all of the value – with the value from all the others going to zero. This thinking works for corporations, as the actions of only a handful of actors in the corporation can often determine the outcome of all actors in the corporation.

That's not the case for Dogecoin. While a corporation going under acts as both a financial death as well as a functional death, there is nothing binding the function of Dogecoin to its financial value. As long as there is a desire, someone can, and likely will continue to operate the network. Exchanges can delist it, third party vendors can stop supporting it, but the technology can continue to function regardless as long as there is someone willing to run a node. This allows the technology of Dogecoin to die as organically as it grew.

This creates a large problem, if corporate actors are the reason for the massive investment in Dogecoin, then opaque actions taken by these corporate actors can just as well drive investment out of Dogecoin. This would bring on a financial death that they would have the foresight to anticipate. If is important that there exists an ability for Dogecoin to die a organic financial death – a death not where a handful of cells are able to take massive amounts of value for their own gain, leaving all other cells with nothing in return – rather a death in which the value of the system are returned to the broader ecosystem, supporting the next organic technological evolution.

Insert Dogeshit. A first of kind experiment where Dogecoin can always be exchanged for an equal amount of Dogeshit, but not the other way around. When Dogecoin is exchanged for Dogeshit, it is burned and removed from circulation. But why burn the Dogecoin? Why not allow Dogeshit to be exchanged back to Dogecoin? Well, just as the original nutrients vital to the fertility of the

grassland ecosystem couldn't be converted from shit back to the plants they came from, Dogeshit shouldn't be able to easily able to converted back to Dogecoin for the benefit of the greater blockchain technology ecosystem. I call this process **digestion**.

Distribution Fairness

Besides the symbolism, this digestion process was chosen as a method to promote fairness over the initial distribution of Dogeshit. When a new token is created, it's common to see the account that deploys the token mint an amount and allocate it all to themselves. Then it is distributed through some form of presale, airdrop, or a self funded liquidity pool. All of these methods give a large amount of control, and oftentimes a massive financial windfall to the developer. This process is not necessarily malicious, but it relies on the trust of the initial developer. This ability to control such a large portion of the tokens can lead to the infamous behavior known as **'rug-pulling'** – when someone who controls a massive amount of the token supply sells their tokens on the market[4]. Since the token holder had basically no vested financial risk in their position, this behavior can completely undermine the value of the token at the expense of those who chose to invest in the project.

This is not how Dogeshit works. There are only 2 ways that Dogeshit is minted:

1. When Dogecoin is digested into Dogeshit.
2. As staking rewards that are distributed to those who chose to lock their Dogeshit in the staking contract.

Instead of the unfair advantage being allocated to myself simply for writing some code, the only advantage that has been created is for those who either:

1. Already own Dogecoin.
2. Digest Dogecoin into Dogeshit and stake it.

Just as Dogecoin was released with no premine, it is essential that any evolution to Dogecoin is released with no premint. It is also essential that the community that formed around and supported Dogecoin isn't forced into competition with a new token just because it is on a new blockchain. No matter the price of Dogeshit, even if it is worth more than Dogecoin, Dogecoin can always be digested into Dogeshit. This choice was made to avoid creating any 'fear of missing out'. The goal of Dogeshit is to allow Dogecoin owners time to choose to migrate over if they wish. Blockchain technologies are complicated; it is important that Dogecoin owners can have time to evaluate their choice and not feel pressured to digest their Dogecoin before they feel comfortable with the choice.

Staking Rewards – nice.

To reward the early adopters who are some of the first to digest their Dogecoin into Dogeshit, Dogeshit will emit staking rewards on a schedule that mimics the

mining reward payout schedule of Dogecoin.

Dogecoin initially rewarded miners a random amount between 0 and 1,000,000 DOGE per block. This was designed to halve 5 times after a little more than 69 days before rewarding a fixed 10,000 DOGE per block until a supply cap of 100 billion DOGE was reached [5], This meant that, the expected date, assuming a truly random distribution should have stopped rewarding miners after less than a year and a half, sometime around June 2015. It turned out that this wasn't the case, and the 100 billion supply cap was never enforced, so after the mining rewards moved to the fixed 10,000 DOGE, Dogecoin continued to reward 10,000 DOGE per block indefinitely [6].

This rewards schedule looks as such:

Block	Days Since First Block	Rewards Per Block (DOGE)	Expected Supply (DOGE)
1	0	0 - 1,000,000	0
100,001	69	0 - 500,000	50 B
200,001	138	0 - 250,000	75 B
300,001	208	0 - 125,000	87.5 B
400,001	277	0 - 62,500	93.75 B
500,001	347	0 - 31,250	96.875 B
600,001	416	10,000	98.4375 B

Dogeshit was designed to mint 69 billion dSHT in a similar time frame to the initial Dogecoin staking rewards before it reached a constant 10,000 DOGE per block.

Block	Days Since First Block	Rewards Per Block (dSHT)	Total Rewards Distributed (dSht)
1	0	9696	0
3,000,001	69	6969	29.088 B
6,000,001	138	3693	49.995 B
9,000,001	208	1337	61.074 B
12,000,001	277	969	65.085 B
15,000,001	347	420	67.992 B
17,400,002	402	69	69 B
34,800,001	805	42	70.2 B
55,000,001	1273	13	71.049 B
75,000,001	1736	9	71.309 B
100,000,001	2314	6	71.534 B
125,000,001	2893	4	71.684 B
150,000,001	3472	2	71.784 B
200,000,001	4629	1	71.884 B

Instead of running expensive specialized hardware like you have to mine Dogecoin, anyone who owns dSHT can stake it. Staking rewards are distributed proportionally, meaning that if you have staked 50% of the total amount staked, then if it were in the first 3,000,000 blocks, you would receive 4848 dSHT per block.

Energy Usage, Speed, and Transaction Fees

Why Litecoin

Dogecoin's core technologies are a fork of Luckycoin, a now defunct fork of Litecoin. Currently, Dogecoin and Litecoin are merged mined, meaning that miners can utilize the same work to mine Litecoin and Dogecoin simultaneously. This initial choice of forking off of Litecoin was based on the fact that Litecoin had faster and cheaper transactions and that at the time, it could still be mined on consumer GPUs. At this point, Bitcoin mining was already controlled by ASICs, expensive custom chips designed with the sole purpose of mining Bitcoin. At the time, this meant Dogecoin was the one of the most accessible ways of interacting with blockchain technologies, both as a user and a miner. Unfortunately, by June of 2014, ASIC miners capable of mining both Litecoin and Dogecoin had hit the market, meaning the Dogecoin mining operations shared the same prohibitive entry costs as Bitcoin.

The initial design choices to base Dogecoin off of Litecoin were well intentioned, but unfortunately, were made moot by technological progression. While the cost of using Dogecoin remained low, the cost of effectively participating in the network became inaccessible to a general audience.

Current Dogecoin Metrics

We're going to look at 4 important metrics when evaluating the current Dogecoin network. Each of these play an important role in what makes a blockchain technology scalable and usable in day to day transactions.

- Transactions per Second
- Finality Time
- Transaction Cost
- Network Energy Usage

Transactions per Second (TPS) The number of transactions that can be processed per second. This number is important, but not as vital as it might seem. The big issue with a low TPS comes from spikes of high demand. For reference Visa claims to be able to handle up to 24,000 transactions per second, but it only appears to average around 1,700 transactions per second. Paypal handles on average 190 transactions per second, but can handle up to 1000 transactions per second during peak periods.

Dogecoin can handle a maximum of **68** transactions per second. This can be calculated by the following:

$$\frac{\text{Block Size Limit}}{\text{Minimum Transaction Size} \times \text{Block Time}} = \frac{1024^2 \,\text{Bytes}}{257 \,\text{Bytes} \times 60 \,\text{seconds}} \approx 68 \,\text{TPS}$$

Finality Time   Finality time describes how long it takes to be sure that the result of a transaction is final. Unfortunately, Dogecoin, as well as Litecoin and Bitcoin, a transaction can never truly be finalized. Instead these protocols rely on a number of additional blocks to verify that the given transaction remains in the longest chain. 6 confirmations is generally what wallet software uses, but exchanges can often require significantly more. Kraken requires 40 confirmations, and Coinbase requires 60 confirmations. Each one of these confirmations takes a minute, so the effective time for a Dogecoin transaction to clear can range from **6-60 minutes** depending upon the context.

Transaction Cost   The transaction fee represents how much it costs to send Dogecoin, regardless of amount. In 2021 the median transaction fee for Dogecoin peaked at just over **$1.25** per transaction, and now currently hovers around **$0.34** (October 2021).

Network Energy Usage

The Importance of Blockchain Literacy

> The Internet is extremely valuable if you know what you're looking for... But you can't pursue any kind of inquiry without a relatively clear framework that's directing your search and helping you choose what's significant and what isn't... If you don't have some sort of a framework for what matters — always, of course, with the provisor that you're willing to question it if it seems to be going in the wrong direction — if you don't have that, exploring the Internet is just picking out the random factoids that don't mean anything... The random exploration through the internet it turns out to be a cult generator — pick up a factoid here, pick up a factoid there, and all of a sudden you have some crazed picture that has some factual basis but nothing to do with the world. You have to know how to evaluate, interpret, and understand... And cultivating that capacity to seek what's significant, always willing to question whether you're on the right track — that's what education is going to be about, whether it's using computers and the Internet, or pencil and paper, or books.

– Noam Chomsky - The Purpose of Education

References

[1] Elon Musk. Tweet. May 15, 2021. https://twitter.com/elonmusk/status/1393738154889338884

[2] Elon Musk. Tweet. May 13, 2021. https://twitter.com/elonmusk/status/1392950720979030019

[3] Marshall, F., Reid, R.E.B., Goldstein, S. et al. Ancient herders enriched and restructured African grasslands. Nature 561, 387–390 (2018). https://doi.org/10.1038/s41586-018-0456-9

[4] CoinMarketCap. "Rug Pull." Alexandria. CoinMarketCap, August 21, 2021. https://coinmarketcap.com/alexandria/glossary/rug-pull

[5] dogecoin. src/main.cpp, commit 1bf59137b, 1124-1184. Github. March 13, 2014 https://github.com/dogecoin/dogecoin/blob/1bf59137bee8bbf4699af8010e1fc2b2f92cef4d/src/main.cpp#L1124

[6] Jackson Palmer. Not actually capped at 100 billion? #23. Github. February 2, 2014 https://github.com/dogecoin/dogecoin/issues/23#issuecomment-33893149