The Moral Case for Satoshi's Half-Airdrop

This is best for Bitcoin – and Satoshi. Ideally, there'd be new SHAD-hardforks each week.

Paul Sztorc
2/20/2024

---

1. Summary

The *"Satoshi half-airdrop"* (**SHAD**), refers to a hard fork in which *Satoshi alone* gets half his coins (everyone else gets 100% of their coins). This is possible because Satoshi's UTXOs are known publicly (see Patoshi Pattern[1]) and they have never moved. Satoshi is "forced" to transfer half his coins, to the fork creator (ie – to us).

"SHAD" can be interpreted in two ways:

Satoshi will be **pissed off…**	**Satoshi** will be **thrilled…**
…but he can't *complain* without compromising his identity (which makes it worse).	…especially that he can *endorse* SHAD whilst remaining secret and tranquil/passive.

Surely it's the left one?! Right?! Obviously -- Satoshi *wants* his coins. People like money. Satoshi could give us the coins, if we asked. So why don't we just ask Satoshi, instead of taking them ??

But appearances can be deceiving.

---

2. The Basics – Satoshi *can only benefit*, from SHAD.

2.A) We're giving, not taking

For starters: we only take fork-coins, not BTC – so none belong to Satoshi in the first place. SHA *adds* to Satoshi's net-worth. Should SHA gain renown, copycats will likely be inspired – all of these *add* coins to Satoshi's stash, *increasing* his wealth. (A big improvement over the Altcoin-style launch, in which Satoshi gets nothing.)

In fact, the only sense in which SHA *decreases* Satoshi's coin-holdings… is one where *his net worth increases*. Let me explain.

2.B) If we win, Satoshi's net worth increases

First, I will define *"winner-take-all crypto"* (**WTAC**) theory. It means:

(1) In the end, only one network will be left standing.
(2) This network will control the bulk of commerce on the internet, and probably, the World.
(3) Each coin ($\frac{1}{21{,}000{,}000}$the total coin supply) will have a market price of around $20 million per

[1] See https://bitslog.com/2013/04/24/satoshi-s-fortune-a-more-accurate-figure/

coin[2], which will then double every ~10 years; total transaction fees will be about $110 Billion per year, and this figure will double about every ~5 years.
(4) All other coins will fade – they will be displaced. Even VISA, Chase, Venmo, etc – all will be subsumed into the winning coin.

WTAC implies that YES -- the SHAD half-airdrop IS INDEED "stealing Satoshi's coins". All Bitcoin forks compete -- they are mutually exclusive. The fork, overwrites its predecessor. So -- ifwe publish a fork, we aim for it to *replace* Bitcoin.

If we fail?	If we succeed?
Then this whole discussion is moot. It is as if nothing happened. No harm no fowl. (In fact, we all learned something from the experiment.)	If the Fork *replaces* Bitcoin? What does that mean? First, the ForkCoin price must be *higher* than BTC's price today (43,000 $/coin). For that *is* success. If 2x higher, then Satoshi's net worth has *increased* via the Fork's creation. In fact, WTAC implies that the price will be either $0 or $20 M. So, if it is ever to be above 43k, then it will be at $20M.

We can redraw the "Three Scenarios" table (from the pitchdeck), adding a row to indicate Satoshi's fate:

"We Fail"	**"BTC Activates Bip300"**	**"Forkcoin Wins"**
Satoshi's wealth: unaffected. We learn from the experiment.	**Satoshi's wealth improves** , to: 1.2 M coins x $20M = $24 Trillion	**Satoshi's wealth improves** , to: 0.6 M coins x $20M = $12 Trillion

C) As An Insurance Policy Against Failure

I don't stand alone, in endorsing WTAC. Satoshi believes it as well:

> *"I'm sure that in 20 years there will either be very large transaction volume or no volume."* – *Satoshi , 2010-02-14*
> *https://satoshi.nakamotoinstitute.org/posts/bitcointalk/57/*

We can further modify the table as follows:

Can "Bitcoin" fail? More specifically: Can *Today's BTC* be ***REPLACED*** by **a Bip300 coin**?					
No			*Yes*		
We Fail	**BTC Activates Bip300**	**Forkcoin Wins**	*We Fail*	*BTC Activates Bip300*	*Bip300 Altcoin wins*
"	"	**Impossible**	"	"	***Satoshi -100%***

[2] In this "hyperbitcoinization" future, there won't be any dollars. Nonetheless, you can imagine how much "stuff" you could buy, as a percentage of GDP, with $20 M USD. That is how much "stuff" you could buy with 1 BTC in this hypothetical future. See here https://www.truthcoin.info/files/bitcoin-mgaw.pdf .

The left side of the table refers to the *Immaculate Conception* thesis. It goes like this: "Bitcoin has already won". It cannot be repeated. Nor replaced. There is nothing to do… but wait. We will all soon be rich – there is nothing left to do, but stack and wait. And perhaps preach the gospel of Bitcoin. (And lead other away from the temptation of shitcoining.)[3]

If that thesis is True, then SHAD cannot harm Satoshi. The ForkCoin will never succeed, so it doesn't matter who owns it. The ForkCoin will be a nice Demonstration – a testnet, and nothing more. It demonstrates Bip300 and why it is good – and therefore it hastens Bitcoin's activation of Bip300. Perhaps, then it hastens Bitcoin's victory. And so we are *good* for Satoshi. Else it is irrelevant.

If that thesis is False (which it is), then Satoshi is vulnerable. He can lose 100% of his Bitcoin wealth at any moment. An Altcoin with Bip300 might come out, and it might win. So, Satoshi should be grateful that we are *cleaning up his mistake* , we are releasing a winning version *that credits him with $*.

I repeat: the fork can only succeed, at all, in a world where BTC's price *has gone to zero*. So, the question "is it morally correct to take half of Satoshi's forkcoins?", can be re-written as "Is it morally correct to ensure that, in *a world where BTC has gone to $0* , Satoshi's net worth *increases* from $0 to *a value much higher than his current net worth* today in 2024?". Obviously, the answer is YES.

---

3. "Selfless" Satoshi Doesn't Want the Patoshi Coins – Not Now, Not Then.

Satoshi used his Patoshi SuperMiner *to keep the network running smoothly*, and NOT *to obtain coins*. Almost certainly, he mined *additional different coins* on the side, with a non-Patoshi miner – and it is *those coins* he relies on for $$ financial remuneration – not the Patoshi coins. The Patoshi coins are either abandoned property, or trapped property.

For one thing, Satoshi programmed the SuperMiner altruistically. It took a 5 minute break after finding each block[4]. This makes no sense for a "greedy miner" – it only makes sense if someone wants to keep the block arrival times on schedule. Furthermore, Satoshi *intentionally slowed* the SuperMiner down, over 2 years, as new people joined the network. The entire thing was a *"selfless" act to ensure a 10 minute interblocktime* , not a selfish act to obtain coins.

But second -- Satoshi never spent (or otherwise used) *any* Patoshi coins.

Perhaps Satoshi is so bullish, that he thinks the coins are undervalued? Satoshi's hoard is worth $52 billion+, so we are being asked to believe that he would not sell even (1/1000th) of it for tens of millions of dollars. That is just not plausible. "Selfish" Satoshi would have sold *some* of the Patoshi coins by now.

Either Satoshi *can't* access them, or else he has *renounced ownership* of them (perhaps on principle, or perhaps out of guilt of using his unique SuperMiner). Either way, SHAD has no negative effect on Satoshi.

---

[3] I have argued many times why the Immaculate Conception thesis is wrong – most recently here x.com/Truthcoin/status/1696994275282636965 and x.com/Truthcoin/status/1704853397269053602 .

[4] See https://blog.lopp.net/was-satoshi-a-greedy-miner/

A final possibility is that SHAD will *help* Satoshi. The Patoshi List is already "out there" and being watched. Perhaps, Satoshi fears to touch these coins, lest he dox himself. Bip-300 SHAD would bail Satoshi out of this situation, by providing for him a zCash sidechain for him to use – the only way for him to get the coins. Half is better than zero! In this case, we aren't **-50%**ing him, we are **+50%**ing him.

---

4. "In Contempt of Activation" – Who's responsible for this mess??

In law, if you refuse to cooperate with a court, then the court puts you in jail *until you do*. This is called "contempt of court". It happened to Chelsea Manning, for example.

> US District Court Judge Anthony Trenga ordered that Manning be remanded in custody and fined $500 (£390) a day after 30 days if she still refuses to testify, rising to $1,000 after 60 days.
>
> She will **remain in custody until she agrees to testify** or until the term of the grand jury expires in 18 months, according to the Post.

The phrase "until she agrees to testify" refers to a legal doctrine where "The contemnor…possesses the "keys to his own cell"." As far as the court is concerned, it is *you* putting *yourself* in jail. And you can stay there, as long as you like. (Manning was ultimately there for 1 year.)

This lens is how we should view SHAD. It is *the miners* putting *the ForkCoin* ahead of BTC. After all: **at any time, 51%-hashrate could activate drivechain.** Unilaterally, they could kill the Fork. By declining to activate Bip300, they favor SHAD – this alerts people to the problem (and *that* there is a problem at all).

---

5. What You Are Really Betting On

Sometimes I'm asked: "if BTC activates Bip300, then what? Will you just abandon the fork?".

As if I had a choice! The Fork *must* be abandoned, in that case. Should BTC activate 300 quickly, the Fork is superfluous. The Fork can only survive, if 300-activation is *unfairly slow*. That is the Column 3 "we all get rich" outcome. It is out of our hands – we need to hope that the miners make a mistake, and fail to act in their collective best interests. **We are betting on *miner's stupidity*.**

		Is Bip300 a good idea?	
		Yes	**No**
Will BTC Reject Bip300? (Are Miners Stupid?)	**Yes**	*Column 3*	*Column 1*
	No	*Column 2*	*Column 1*

Some people say: miners don't control activation. This is false. For Bip300 it is, at any rate. Miners are wrong if they say this, and negligent if they don't look into it. They have bad researchers, if they look into it themselves and conclude this; or alternatively they are deferring to the wrong experts. Either way, they are responsible.

BTC activation process is either defective, or it isn't.

BTC Activation is Defective	**BTC Activation is NOT Defective**
Current BTC activation process is broken. It wrongly pulls in low-merit ideas (such as Taproot), and wrongly rejects high-merit ideas (such as Bip300).	Everything in BTC is going perfectly.
The existing crop of BTC miners is doing something wrong. They are running the wrong software; they are deferring to the wrong technical experts; they are negligent lazy and mistaken.	Everything in BTC is going perfectly.

But, more importantly is *why* it might be defective. Will 51%-hashrate *come around later, in time*, or do they need to be replaced?

51% Miners Will Come Around (Slow Learners)	**51% Miners Will Not Come Around (Corrupt)**
Well, then – when they come around, they will just activate Bip300 – this is **Column 2. No harm done.**	In this case, it is a *moral imperative* that these miners be replaced, as quickly as possible. **Fire the miners. Column 3.**

---

6. Enslaving Our Critics – ("Hidden Gem" Theory)

Column 2 and Column 3 are both great – we win! However, Column 3 we win *more*.

This is the genius of SHAD: it turns every *opponent* of Bip300-on-BTC, into a *supporter* of our *best* financial outcome. People who would normally be our biggest *enemies* are in fact our de facto strongest supporters.

This has two benefits:

1) Our enemies have been neutralized, and are instead helping use earn more money.
2) The *stigma* of the hardfork is obliterated. No one actually knows, which Fork-Critics are genuine, and which are Secret Column-3ers. Anyone who appears to be bullying us, or criticizing us, may actually be helping us: a Column-3-er.

When nothing is at stake, people *pontificate*. Not so, when their money is on the line. Everyone is a bag-holder. In the investment world, it is never a popularity contest – rather the reverse: everyone hopes to find a ***hidden gem***. Something that *has potential* but that *everyone else has overlooked*.

So, we can summarize it like this:

No fork = It is ***very bad*** for us to have stupid critics… because we have to fight through them.
Fork = It is ***irrelevant*** for us to have stupid critics… because people know to be skeptical and DYOR.
SHA Fork = It is ***good*** for us to have stupid critics… because they harm Column 2 and help Column 3.

> *Great investment = a great idea + a competitive moat + you figure it out early*

---

7. Sabotaging Column 2

Since we actually want Column 3 (or do we), I will briefly comment on how to give C3 the edge over C2.

Background: BIP-activation is a *collective action problem*. That's the issue. Instead, if Bip300 made *individual miners* more profitable than *rival miners*, then campaigning would not be necessary. Miners would be "beating a path to the front door". Bip300 makes *all miners* more profitable. Hence, no individual miner has any fear, of being a late adopter. So, to win, **we must transform the collective action problem into something else**. Luckily, this is exactly what SHAD does.

Ultimately, which is easier? Build a coalition via…	
↓	↓
…convincing 51%-hashrate to activate Bip300 (all at once, *as a group*). *(collective action problem)*	…convince *each individual miner* to move their hashrate (**one at a time**, with earlier defectors *benefitting* disproportionately). *(capitalism)*
Outcome: ***Column 2***	Outcome: ***Column 3***

See this article[5] for more.

---

8. Some lesser reasons.

a) Academic Independence

Interestingly, we often get the *opposite* question (from point #5): "How will your company make money, if Bip300 fails to activate? Doesn't your business model *depend* on Bip300 activating?".

Thanks to SHAD, the answer is no. Our 2nd road to financial success, unbiases us.

Which is good. It is morally wrong for Bip300 supporters to influence Bitcoin Development.

[5] https://www.truthcoin.info/blog/imex/

b) As A Sieve

Network effects are the top priority. We *want users*.

However, some people are *odious* – they repel others. They are a net bad. They are anti-social, free-loaders and bullies. Sociopaths and parasites. We must repel these people, if we want to optimize our chances of winning.

SHAD does exactly this. Neurotic, "hung up" people – people who are too deep in the cult – they will hate SHAD. They will sell the ForkCoin and criticize it. This is exactly what we want. Plus, it looks like *we* are paying *them* in order to get them to *sabotage* Bip300 activation on BTC.

We want to only attract people who are focused on getting 8 billion people to use "Bitcoin" ASAP.

c) Are You Kidding Me

Satoshi doesn't need all that money. Even after SHAD, he would still have more coins than anyone else. He is still in *the #1 spot*.

d) As A Scapegoat if we Fail

If this investment fails, we can always blame SHAD. We can say "it would have worked, except for SHAD".

e) Decentralization

Legally, one criteria for decentralization is 'concentration of ownership'. Every little bit helps!

f) As Reverse Psychology / "engagement farming" / marketing / Hate-marketing

(Self Explanatory).

---

9. What's the Alternative?

I'll start with some examples:

a) First, consider the case where our investors just ***gift*** us the money. **Investors** are the victim. This has the most perverse effect of all: the *people who financially supported Bip300, did the* ***worst, out of everyone,*** if and only if Bip300 succeeds. That doesn't make sense!
b) Second, consider the case where we **premine treasury** 600k extra coins. **All Bitcoin-holders** are the victim, not just Satoshi. We violate 21M coin limit (and lose that meme). The number 600k now appears arbitrary, so any who follow us may set their premine to +2m , +5mm, or +21mm. There is an incentive for Rich Bitcoiners to soft fork a descruction of the premined coins, or start a competing project.
c) We might try to **swap the PoW + be an early miner**. This requires us to get into the hardware business – which we know nothing about. It requires us to drop Sha256D, thus making **all present Bitcoin miners** the victims, and natural enemies of the project --- which is disastrous to the overall strategy. Also, it would take 200k blocks to mine 600k coins (since the 3.125-halving is already upon us) – this would require us to hit every single block, straight, for about 3.5 years – this is impossible. Horrible idea.

d) We could also just **proceed slowly, as academics**. No fundraising, no stakes, no winners-and-lowers. Here, the victims are the **end user** , and the BIP300 supporters (including us) – they get useful stuff *at a slower rate*. Sociopaths, bullies, and other anti-social/anti-prosperity voices succeed. This punishes people for doing the right thing, and rewards wrongdoing.

Of all moral abominations, one of the worst is the "Bail Out" -- "heads I win; tails I break even". This is *wrong*. Everyone should pay a *price* for any mistakes they make.

If BIP300 wins, it must be a punitive win. Everyone who supported it must do well – everyone who opposed it must suffer.

SHAD creates a community that has $$, pride, is not beholden to financial backers, has real independence. It is *a reward for fighting through* the stigma

People who complain about SHAD, seem to want two things:

• Invest in a Bip300 company/project… • …be *rewarded* if it succeeds.	• Launch a "fair fork" with no "victim"… • …such that *no one is harmed* if it succeeds.

Unfortunately, you can't have both! The harm = the success.

If one person is "climbing the totem pole", then others are falling down. There is no way for a Bip300 investor to *do well,* without someone else doing worse.

Ultimately, someone will have to take a financial risk. In our case, it is *our investors* who take the risk. And it is them who gets the **reward**. This is appropriate! (Remember, that Satoshi only "loses" in a world where his net worth *increases* from where it is today – and a world where *we* defeat the specter of BTC-failure).

Anyone who dislikes SHAD, should *first and foremost tell us who **their** victim would be*. Otherwise, frankly, they are just bullsh**ters. SHAD is the optimal business model, for this problem-scenario.

---

10. The Plan

(1) Advise laypeople to own BTC and ForkCoin in equal amounts. (Ie, if you own 7 ForkCoin you should own 7 BTC, and vice-versa). Force people to take responsibility for their private investment decisions.
(2) Aggressively blame 51%-hashrate on BTC for not activating Bip300. We *back up this rhetoric*, by making it as easy as possible for BTC miners to activate. This helps everyone see that we are telling the truth – which of course we are. (It also triggers people's defensiveness.)
(3) Maximize the suffering of the Priest Class, to minimize their support for Column 2. This maximizes our financial return. On top of that we get to do the right thing – since the way to maximize their suffering is just to *hold them accountable*. That is what they hate more than anything else. Plus our supporters will love it, and it will cause engagement.

(4) Replay all the txns from one chain, onto the other. Thus both will appear to have equal usage – the two chains will be identical in almost every way, just that one has Bip300 enforced and the other has it *unenforced*.
(5) Pick a completely new name, so there's no "Bitcoin" name drama (nor the related stigma).

---

11. Conclusion.

What makes something moral? Kant answered that question by asking: should *everyone* do this thing?

Clearly, *theft* is immoral. After all, rampant, universal theft produces a nasty world – one where no one bothers to make anything valuable enough to be worth stealing. That would be hell.

However, *SHAD* is moral. Everyone should make a SHAD BTC hard fork. Even if they half-airdrop Satoshi; or even if they half-airdrop other people! This is the kick in the pants that Bitcoin needs. It needs **competition**. It needs *fear* of being replaced by a rival. Only the threat of a *viable competitor* is enough to keep today's Bitcoiners honest. We need more people "attacking" Bitcoin this way… by giving everyone more money.

SHAD is the victory of economics and commerce, over the forces of politics and tyranny. Not only is SHAD morally permissible, it is in fact a moral imperative.