Dear Bitcoin Community,

I'd love to get some feedback on my BIP-Idea. Both technically and content-wise. I acknowledge that I might be wrong with my allegations on Bitcoin. If so, I would be more than happy to get some input. This is **not** meant to be a scientific paper, I just tried to provide enough explanations.

TLDR: I have highlighted the key points in bold.

Issue

You are all aware of the security, scalability and decentralization triangle. A problem which will not be solved soon or more likely will never be solved in my opinion. Most people in the Bitcoin community I meet seem to think that the Lightning Network (LN) is a sufficient solution. Which to a certain extent I agree with. The concept of a LN node providing infinite self-custodial sub wallets is truly awesome. However, the small commitment of trust in this is only negligible when the user can withdraw his funds onchain in case of **malicious behavior. I believe we will have a huge problem in the future closing those channels.**

We need to look at this from the perspective that Bitcoin will grow in value over time. Therefor the actual fees paid to the miners measured in sats/vbyte[1] might stay the same, but its value becomes higher and higher. **With the minimum fee of 1 sat/vbyte there is a minimum amount that can be (economically) transferred onchain**.

A P2TR[2] address with 2 inputs and outputs takes up 211.5 vbytes[3], which makes any transaction amount of 1000 sats or less senseless to go onchain. With a current value of 0,91 USD[4] this seems laughable today. **However, that means that with the growing adoption of Bitcoin (& increase in value), the value a person can own on the LN "trustlessly" decreases. This means that the LN as scaling solution and transaction method of the future forces its not so wealthy users into trusting the infrastructure provider.** Destroying one core value of Bitcoin. And every year the number of people that will be forced to trust trusted parties increases with the increase of Bitcoins value.

Also

- The long-term problem of coins that get lost forever will worsen this issue mentioned above.
- Many small UTXO's become stranded. Even though the keys are maintained, the minimum fee doesn't allow them to be moved.
- At some point Bitcoin might become too expensive for everybody to use.

---

[1] Or BTC/kvB
[2] Taproot address
[3] https://bitcoinops.org/en/tools/calc-size/
[4] March 06, 2025

Solution

My idea would be to bring **smaller decimal units to the Bitcoin main chain and lower the minimum fee** rate. This would allow users to own Bitcoins trustless onchain regardless of how wealthy they are. As easy as this solution sounds it's also bringing a lot of new issues. Let's go through them:

1. Profitability of miners

In the future miners will primarily rely on transaction fees. They will obviously not agree to an infinite decrease in their profits by cutting the transaction fee. This could be solved by **halving the minimum fee every 210.000 Blocks**. Like the block subsidy the absolute reward gained by transactions fees will decrease over time, but since the value of the already gained coins increases their business stays profitable. The finetuning will be done by the difficulty adjustment.

2. **Time pressure** on the decision-making process

More and more people will suffer from the issue mentioned above, while at the same time mining is becoming more and more profitable because the minimum fee that needs to be paid can't be lowered.

Forcing miners to suddenly accept way less will not be accepted by the miners. A late user driven request of change might lead to a network split in a highly centralized infrastructure system. A transparent agile rule, as mentioned above, allows miners and LN nodes to plan their businesses way ahead in time. And with the greater good of Bitcoins core values in mind its more likely the miners will agree, if the decision is presented early.

I estimate that the mining subsidy of 0.0244..BTC **in the year** 2052 or 0.0122.. BTC in **2056** will be equal to the transaction fee of blocks with an average of 1 sat/vbyte. I assumed this based on current transaction fees in **1 sat/vbyte blocks** of ~ 0.017BTC[5]. This would make the minimum transaction fees an important part of the miner's payout. Obviously they become important before **reaching 50% of their income**.

2028	2032	2036	2040	2044	2048	2052
1.5625 BTC	0.7812 BTC	0.3906 BTC	0.1953 BTC	0.0976 BTC	0.0488 BTC	0.0244 BTC
1.08%	2.13%	4.17%	8.01%	14.83%	25.84%	41.06%

6 7

[5] See Block: 886692 (0.018BTC) , 886687 (0.011BTC), 886422 (0.015BTC), 886297 (0.023BTC)
[6] https://github.com/RealCocoArdo/BitcoinOverview/blob/main/pictures/Overview4.PNG
[7] 0.017BTC is 1.08% of 1.5795 BTC (1.5625+0.017)

3. Technically adjustment

Since computer-wise, **we can't go lower than 1 Satoshi**[8] we need to **instead increase everything by a magnitude**. For example: 1000x. So, the maximum amount of Bitcoin wouldn't be 21 million[9] Bitcoins, but instead 21,000 million Bitcoins. We should still own the same amount times the magnitude. Changing nothing about the limited supply or the ratios owned by people.

4. Hard fork

Changing the supply of Bitcoin as well as the minimum fee rate requires a **hard fork**.

Hardfork without Miner support:

In my opinion this change should be supported by all users. If the users decide to implement this change and split the network that would leave the majority of miners with a fork without transactions. This empty network would become worthless, forcing the miners to join the fork of the users.

5. Transition

We can't just change the amounts of Bitcoins in old Blocks by the ratio to allow smaller units than 1 Satoshi since it would mess up the block hashes. So, we would instead need a certain Block height on which we agree to make the changes and agree on the set ratio. That would mean that if you owned 1 single satoshi (pre-update) you would "technically" own 1000 satoshis after the update, but we would handle it as still only 1.000 satoshi, but with decimal places. The value wouldn't change since everyone still owns the same percentage of the total supply.

I believe block height 1,350,000 (December 2033) would be a good time to aim for. That should provide plenty of time to discuss and plan out the BIP. It also fits nicely between the block halving's on 1,260,000 and 1,470,000. The minimum fee would only make out 2.13% at that time as mentioned above. Meaning a halving would cost miners only 1.07%. But most importantly I hope the situation doesn't become too bad until then for poor people.

6. Network hashrate limit

Probably the biggest concern about my proposal is that halving the minimum transaction fee could end up in a peak hashrate, which may stop growing. This could mean the security of the Network is in danger, because it becomes easier to acquire sufficient hashrate to attack Bitcoin.

I believe that this is the same concern as when people say that the current supply halving would end up stopping the hashrate to growth. Yes, we did see a decrease in the past, but with the difficulty adjustment we never peaked out.

---

[8] As far as I know it's because places after the decimal point displayed in binary will create inaccuracies.
[9] *20.999.999,97690 BTC

Comments

- Batching:
  To collect transactions and saving on required space offers savings opportunities. But it doesn't change the direction in which we are moving (Higher values per coin and less available coins).

- Bitcoin Optech Newsletter #342[10]:
  Including the closing fee in the channel balance does also not solve the problem mentioned above (Even though it's nice to have). Even if we were able to close the channel, we would end up with a stranded UTXO where the owned amount is too small.

- Storage capacity:
  I did not yet calculate how multiplying the supply by a magnitude would affect the storage capacity to store a Bitcoin amount. Whether in single transactions, in different op-codes or in blocks. Feedback on that would be helpful.

Thanks for reading.

Best regards

Coco Ardo

Contact

Email: CocoArdolo@protonmail.com

Nostr: Coco_Ardo (npub1cj9...syga2tw)

Website (TOR required):
http://d3nmu3ybs6gjwikw6qiwuzbs7d7q5mq3v5c4vlh4dq4eja6x7mngbaad.onion/

[10] https://bitcoinops.org/en/newsletters/2025/02/21/