Scaling Bitcoin Documentation

Release 1.0.1

Bitcoin Community

December 28, 2015

Contents

Like many people in the community I've spent the past month or so looking deeply into the bitcoin scaling debate. I feel there has never been a fully comprehensive thread on how bitcoin could scale. The closest I have seen is /u/gavinandresen's medium posts back in the summer describing the problem and a solution, and pre-emptively answering supposed problems with the solution. While these posts got to the core of the issue and spawned the debate we have been having, they were quite general and could have used more data in support. This is my research and proposal to scale bitcoin and bring the community back together.

CHAPTER 1

The Problem

There seems to me to be five main fundamental forces at play in finding a balanced solution;

- node distribution
- mining decentralisation
- network utility
- time
- adoption

1.1 Node Distribution

Bandwidth has a relationship to node count and therefore node distribution. This is because if bandwidth becomes too high then fewer people will be able to run a node. To a lesser extent bandwidth also effects 'mining decentralisation' as miners/pool owners also need to be able to run a node. I would argue that the centralisation pressures in relation to bandwidth are negligible though in comparison to the centralisation pressure caused by the usefulness of larger pools in reducing variance. The cost of a faster internet connection is negligible in comparison to the turnover of the pools. It is important to note the distinction between bandwidth required to propagate blocks quickly and the bandwidth required to propagate transactions. The bandwidth required to simply propagate transactions is still low today.

New node time (i.e. the time it takes to start up a new node) also has a relationship with node distribution. i.e. If it takes too long to start a new node then fewer people will be willing to take the time and resources to start a new node.

Storage Space also has a relationship with node distribution. If the blockchain takes up too much space on a computer then less people will be willing to store the whole blockchain. Any suitable solution should look to not decrease node distribution significantly.

1.2 Mining Decentralisation

Broadcast time (the time it takes to upload a block to a peer) has a relationship with mining centralisation pressures. This is because increasing broadcast time increases the propagation time, which increases the orphan rate. If the orphan rate it too high then individual miners will tend towards larger pools.

Validation time (the time it to validate a block) has a relationship with mining centralisation pressures. This is because increasing validation time increases the propagation time, which increases the orphan rate. If the orphan rate it too high then individual miners will tend towards larger pools.

Any suitable solution should look to not increase mining centralisation significantly.

1.3 Network Utility

Network Utility is one that I find is often overlooked, is not well understood but is equally as important. The network utility force acts as a kind of disclaimer to the other two forces. It has a balancing effect. Increasing the network utility will likely increase user adoption (The more useful something is, the more people will want to use it) and therefore decreasing network utility will likely decrease user adoption. User adoption has a relationship with node count. i.e. the more people, companies and organisations know about and use bitcoin, the more people, companies and organisations that will run nodes. For example we could reduce block size down to 10KB, which would reduce broadcast time and validation time significantly. This would also therefore reduce mining centralisation pressures significantly. What is very important to realise though is that network utility would also be significantly be reduced (fewer people able to use bitcoin) and therefore so would node distribution. Conversely, if we increased the block size (not the limit) right now to 10GB, the network utility would be very high as bitcoin would be able to process a large number of transactions but node distribution would be low and mining centralisation pressures would be high due to the larger resource requirements.

Any suitable solution should look to increase network utility as time increases.

1.4 Time

Time is an important force because of how technology improves over time. Technology improves over time in a semi-predicable fashion (often exponential). As we move through time, the cost of resources required to run the bitcoin network (if the resource requirements remained static) will decrease. This means that we are able to increase resource requirements proportional to technological improvements/cost reductions without any increase in costs to the network. Technological improvements are not perfectly predictable though so it could be advantageous to allow some buffer room for when technological improvements do not keep up with predictions. This buffer should not be applied at the expense of the balance between the other forces though (i.e. make the buffer too big and network utility will be significantly decreased).

1.5 Adoption

Increasing adoption means more people using the bitcoin/blockchain network. The more people use bitcoin the more utility it has, and the more utility Bitcoin has the more people will want to use it (network effect). The more people use bitcoin, the more people there that have an incentive to protect bitcoin.

Any suitable solution should look to increase adoption as time increases.

CHAPTER 2

The Lightning Network

2.1 Proposed Solutions by Some Bitcoin Developers

The Lightning Network (LN) is an attempt at scaling the number of transactions that can happen between parties by not publishing any transaction onto the blockchain unless it is absolutely necessary. This is achieved by having people pool bitcoin together in a “Channel” and then these people can transact instantly within that channel. If any shenanigans happen between any of the parties, the channel can be closed and the transactions will be settled on the blockchain. The second part of their plan is limit the block size to turn bitcoin into a settlement network. The original block size limit of 1MB was originally put in place by Satoshi as an anti DOS measure. It was to make sure a bad actor could not propagate a very large block that would crash nodes and increase the size of the blockchain unnecessarily. Certain developers now want to use this 1MB limit in a different way to make sure that resource requirements will stay low, block space always remains full, fees increase significantly and people use the lightning network as their main way of transacting rather than the blockchain. They also say that keeping the resource requirements very low will make sure that bitcoin remains decentralised.

2.2 Problems with the Lightning Network

The LN works relatively well (in theory) when the cost and time to publish a set of transactions to the network are kept low. Unfortunately, when the cost and time to publish a set of transactions on the blockchain become high, the LN’s utility is diminished. The trust you get from a transaction on the LN comes only from the trustless nature of having transactions published to the bitcoin network. What this means is that if a transaction cannot be published on the bitcoin network then the LN transaction is not secured at all. As transactions fees rise on the bitcoin blockchain the LN utility is diminished. Lets take an example:

- Cost of publishing a transaction to the bitcoin network = $20
- LN transaction between Bob and Alice = $20.
- Transaction between Bob and Alice has problem therefore we want to publish it to the blockchain.
- Amount of funds left after transaction is published to the blockchain = $20 - $20 = $0.

This is also not a binary situation. If for example in this scenario, the cost to publish the transaction to blockchain was $10 then still only 50% of the transaction would be secure. It is unlikely anyone really call this a secure transaction.

Will a user make a non-secured/poorly secured transaction on the LN when they could make the same transaction via an altcoin or non-cryptocurrency transaction and have it well secured? It’s unlikely. What is much more likely to happen is that transaction that are not secured by bitcoin because of the cost to publish to the blockchain will simply overflow into altcoins or will simply not happen on any cryptocurrency network. The reality is though, that we don’t know exactly what will happen because there is no precedent for it.

Another problem outside of security is convenience. With a highly oversaturated block space (very large backlog of transactions) it could take months to have a transaction published to the blockchain. During this time your funds will simply be stuck. If you want to buy a coffee with a shop you don't have a channel open with, instead of simply paying with bitcoin directly, you would have to wait months to open a channel by publishing a transaction to the bitcoin blockchain. I think your coffee might be a little cold by then (and mouldy).

I suggest reading this excellent post HERE for other rather significant problems with the LN when people are forced to use it.

The LN is currently not complete and due to its high complexity it will take some time to have industry wide implementation. If it is implemented on top of a bitcoin-as-a-settlement-network economy it will likely have very little utility.

2.3 Uses of the Lightning Network

The LN is actually an extremely useful layer-2 technology when it is used with it's strengths. When the bitcoin blockchain is fast and cheap to transact on, the LN is also extremely useful. One of the major uses for the LN is for trust-based transactions. If you are transacting often between a set of parties you can truly trust then using LN makes absolute sense since the trustless model of bitcoin is not necessary. Then once you require your funds to be unlocked again it will only take a short time and small cost to open them up to the full bitcoin network again. Another excellent use of LN would be for layer-3 apps. For example a casino app: Anyone can by into the casino channel and play using real bitcoins instantly in the knowledge that is anything nefarious happens you can instantly settle and unlock your funds. Another example would be a computer game where you can use real bitcoin in game, the only difference is that you connect to the game's LN channel and can transact instantly and cheaply. Then whenever you want to unlock your funds you can settle on the blockchain and use your bitcoins normally again.

LN is hugely more powerful, the more powerful bitcoin is. The people making the LN need to stick with its strengths rather than sell it as an all-in-one solution to bitcoin's scaling problem. It is just one piece of the puzzle.

CHAPTER 3

Improving Network Efficiency

The more efficient the network, the more we can do with what we already have. There are a number of possible efficiency improvements to the network and each of them has a slightly different effect.

3.1 Pruning

Pruning allows the stored blockchain size to be reduced significantly by not storing old data. This has the effect of lowering the resource requirements of running a node. a 40GB unpruned blockchain would be reduced in size to 550MB. (It is important to note that a pruned node has lower utility to the network)

3.2 Thin Blocks

Thin blocks uses the fact that most of the nodes in the network already have a list of almost all the same transactions ready to be put into the blockchain before a block is found. If all nodes use the same/similar policy for which transactions to include in a block then you only need to broadcast a small amount of information across the network for all nodes to know which transactions have been included (as opposed to broadcasting a list of all transactions included in the block). Thin Blocks have the advantage of reducing propagation which lowers the mining centralisation pressure due to orphaned blocks.

3.3 libsecp256k1

libsecp256k1 allows a more efficient way of validating transactions. This means that propagation time is reduced which lowers the mining centralisation pressure due to orphaned blocks. It also means reduced time to bootstrap the blockchain for a new node.

3.4 Serialised Broadcast

Currently block transmission to peers happens in parallel to all connected peers. Obviously for block propagation this is a poor choice in comparison to serial transmission to each peer one by one. Using parallel transmission means that the more peers you have, the slower the propagation, whereas serial transmission does not suffer this problem. The problem that serial transmission does suffer from though is variance. If the order that you send blocks to peers in is random, then it means sometimes you will send blocks to a peer who has a slow/fast connection and/or is able to validate slowly/quickly. This would mean the average propagation time would increase with serialised transmission but depending on your luck you would sometimes have faster propagation and sometimes have slower propagation.

As this will lower propagation time it will also lower the mining centralisation pressure due to orphaned blocks. (This is just a concept at the moment but I don't see why it couldn't be implemented).

3.5 Serialised Broadcast Sorting

This is a fix for the variance that would occur due to serialised broadcast. This sorts the order that you broadcast a block to each peer into; fastest upload + validation speed first and slowest upload speed and validation speed last. This not only decreases the variance to zero but also allows blocks to propagation to happen much faster. This also has the effect of lowering the mining centralisation pressure due to orphaned blocks. (This is just a concept at the moment but I don't see why it couldn't be implemented).

Here is a table below that shows roughly what the effects these solutions should have.

Name	Bandwidth	Broadcast Time	Validation Time	New Node Time	Storage Space
Pruning	1	1	1	1	0.014
Thin Blocks	0.42	0.1	0.1	1	1
libsecp256k1	1	1	0.2	0.6	1
Serialised Broadcast	1	0.5	1	1	1
KYN	1	0.75	1	1	1
Segregated Witness	1	1	1	0.4	1
TOTAL	0.42	0.0375	0.02	0.24	0.014
Multiplier	2.38	26.7	50	•	70

CHAPTER 4

Finding a Balanced Solution

At the beginning of this post I detailed a relatively simple framework for finding a solution by describing what the problem is. There seems to me to be five main fundamental forces at play in finding a balanced solution; 'node distribution', 'mining decentralisation', 'network utility', 'time' and 'adoption'. The optimal solution needs to find a balance between all of these forces taking into account a buffer to offset our inability to predict the future with absolute accuracy.

To find a suitable buffer we need to assign a set of red line values which certain values should not pass if we want to make sure bitcoin continues to function as well as today (at a minimum). For example, percentage of orphans should stay below a certain value. These values can only be a best estimate due to the complexity of bitcoin economics, although I have tried to provide as sound reasoning as possible.

4.1 Propagation time

It seems a fair limit for this would be roughly what we have now. Bitcoin is still functioning now. Could mining be more decentralised? Yes, of course, but it seems bitcoin is working fine right now and therefore our currently propagation time for blocks is a fairly conservative limit to set. Currently 1MB blocks take around 15 seconds to propagate more than 50% of the network. 15 second propagation time is what I will be using as a limit in the solution to create a buffer.

4.2 Orphan Rate

This is obviously a value that is a function of propagation time so the same reasoning should be used. I will use a 3% limit on orphan rate in the solution to create a buffer.

4.3 Non-Pruned Node Storage Cost

For this I am choosing a limit of $200 in the near-term and $600 in the long-term. I have chosen these values based on what I think is a reasonable (maximum) for a business or enthusiast to pay to run a full node. As the number of transactions increases as more people use bitcoin the number of people willing to pay a higher price to run a node will also increase although the percentage of people will decrease. These are of course best guess values as there is no way of knowing exactly what percentage of users are willing to pay what.

4.4 Pruned Node Storage Cost

For this I am choosing a limit of $3 in the near-term (next 5 years) and $9 in the long-term (Next 25 years). I have chosen these values based on what I think is a reasonable (maximum) for normal bitcoin user to pay. In fact this cost will more likely be zero as almost all users have an amount of storage free on their computers.

4.5 Percentage of Downstream Bandwidth Used

This is a best guess at what I think people who run nodes would be willing to use to be connected to the bitcoin network directly. I believe using 10% (maximum) of a users downstream bandwidth is the limit of what is reasonable for a full node (pruned and non-pruned). Most users would continue to access the blockchain via SPV wallets though. Downstream is generally a much more valuable resource to a user than upstream due to the nature of the internet usage.

4.6 Percentage of Upstream Bandwidth Used

This is a best guess at what I think people who run nodes would be willing to use to be connected to the bitcoin network directly. I believe using 25% (maximum) of a users downstream bandwidth is the limit of what is reasonable for a full node (pruned and non-pruned). Most users would continue to access the blockchain via SPV wallets though. Upstream is generally a much less valuable resource to a user than downstream due to the nature of the internet usage.

4.7 Time to Bootstrap a New Node

My limit for this value is at 5 days using 50% of downstream bandwidth in the near-term and 30 days in the long-term. This seems like a reasonable number to me for someone who wants to start running a full node. Currently opening a new bank account takes at least week until everything is set up and you have received your cards, so it seems to me people would be willing to wait this long to become connected. Again, this is a best guess on what people would be willing to do to access the blockchain in the future. Most users requiring less security will be able to use an SPV wallet.

It is important to note that we only need enough nodes to make sure the blockchain is distributed across many places with many backups of the full blockchain. It is likely that a few thousand is a minimum for this. Increasing this amount to hundreds of thousands or millions of full nodes is not necessarily that much of an advantage to node distribution but could be a significant disadvantage to mining centralisation. This is because the more nodes you have in the network, the longer it takes to propagate >50% of it.

4.8 Storage cost

Storage cost follows a linear logarithmic trend. Costs of HDD reducing by 10 times every 5 years, although this has slowed over the past few years. This can be attributed to the flooding in South East Asia and the transition to SSD technology. SSD technology also follows the linear logarithmic trend of costs reducing 10 times every 5 years, or roughly decreasing 37% per year.

4.9 Average Upload and Download Bandwidth Increases Over Time

Average upload and download bandwidth increases in a linear logarithmic trend. Both upload and download bandwidth follow the same trend of doubling roughly every two years, or increasing 40% per year.

4.10 What should be the acceptable limit? What would be the growth over time?

- Github Issue 1

I propose 200GB and 20% annually for pruned nodes. iirc comcast caps at 300GB, so 200GB seems like a good upper limit. In my country it hasn't increased 20% annually, but consumer demand for lots of data-usage is increasing a lot, so I think we can be optimistic.

For full nodes it should be a limit where limit+ 'more than average usage' will start to raise red flags with providers. If I had to pick a number I'd pick 1TB +20% annually, but I don't have any data to back that up.

To estimate the total bandwidth usage after IBLT and for pruned nodes (as they don't serve historical blocks) it would be great to have some data on transaction relaying and block relaying separately, so if anyone has some data on this that would be great.

4.11 Price

I was hesitant to include this one here but I feel it is unavoidable. Contrary to what people say (often when the price is trending downwards) bitcoin price is an extremely important metric in the long-term. Depending on bitcoin's price, bitcoin's is useful to; enthusiasts->some users->small companies->large companies->nations->the world, in roughly that order. The higher bitcoin's price is the more liquid the market will be and the more difficult it will be to move the price, therefore increasing bitcoin's utility. Bitcoin's price in the long-term is linked to adoption, which seems to happen in waves, as can be seen in the price bubbles over the years. If we are planning/aiming for bitcoin to at least become a currency with equal value to one of the worlds major currencies then we need to plan for a market cap and price that reflect that. I personally think there are two useful targets we should use to reflect our aims. The first, lower target is for bitcoin to have a market cap the size of a major national currency. This would put the market cap at around 2.1 trillion dollars or $100,000 per bitcoin. The second higher target is for bitcoin to become the world's major reserve currency. This would give bitcoin a market cap of around 21 trillion dollars and a value of $1,000,000 per bitcoin. A final, and much more difficult target is likely to be bitcoin as the only currency across the world, but I am not sure exactly how this could work so for now I don't think this is worth considering.

As price increases, so does the subsidy reward given out to miners who find blocks. This reward is semi-dynamic in that it remains static (in btc terms) until 210,000 blocks are found and then the subsidy is then cut in half. This continues to happen until all 21,000,000 bitcoins have been mined. If the value of each bitcoin increases faster than the btc denominated subsidy decreases then the USD denominated reward will be averagely increasing. Historically the bitcoin price has increased significantly faster than subsidy decreases. The btc denominated subsidy halves roughly every 4 years but the price of bitcoin has historically increased roughly 50 fold in the same time.

Bitcoin adoption should happen in a roughly s curve dynamic like every other technology adoption. This means exponential adoption until the market saturation starts and adoption slows, then the finally is the market becomes fully saturated and adoption slowly stops (i.e. bitcoin is fully adopted). If we assume the top of this adoption s-curve has one of the market caps above (i.e. bitcoin is successful) then we can use this assumption to see how we can transition from a subsidy paid network to a transaction fee paid network.

4.12 Adoption

Adoption is the most difficult metric to determine. In fact it is impossible to determine accurately now, let alone in the future. It is also the one of the most important factors. There is no point in building software that no one is going to use after all. Equally, there is no point in achieving a large amount of adoption if bitcoin offers none of the original value propositions. Clearly there is a balance to be had. Some amount of bitcoin's original value proposition is worth losing in favour of adoption, and some amount of adoption is worth losing to keep bitcoin's original value proposition. A suitable solution should find a good balance between the two. It is clear though that any solution must have increased adoption as a basic requirement, otherwise it is not a solution at all.

One major factor related to adoption that I rarely see mentioned, is stability and predictability. This is relevant to both end users and businesses. End users rely on stability and predictability so that they do not have to constantly check if something has changed. When a person goes to get money from a cash machine or spend money in a shop, their experience is almost identical every single time. It is highly dependable. They don't need to keep up-to-date on how cash machines or shops work to make sure they are not defrauded. They know exactly what is going to happen without having to expend any effort. The more deviation from the standard experience a user experiences and the more often a user experiences a deviation, the less likely a user is going to want to continue to use that service. Users require predictability extending into the past. Businesses who's bottom line is often dependent on reliable services also require stability and predictability. Businesses require predictability that extends into the future so that they can plan. A business is less likely to use a service for which they do not know they can depend on in the future (or they know they cannot depend on).

For bitcoin to achieve mass adoption it needs a long-term predictable and stable plan for people to rely on.

CHAPTER 5

Proposal

This proposal is one based on determining a best fit balance of every factor and a large enough buffer to allows for our inability to perfectly predict the future. No one can predict the future with absolutely certainty but it does not mean we cannot make educated guesses and plan for it.

The first part of the proposal is to spend 2016 implementing all available efficiency improvements (i.e the ones detailed above) and making sure the move to a scaled bitcoin happens as smoothly as possible. It seems we should set a target of implementing all of the above improvements within the first 6 months of 2016. These improvements should be implemented in the first hardfork of its kind, with full community wide consensus. A hardfork with this much consensus is the perfect time to test and learn from the hardforking mechanism. Thanks to Seg Wit, this would give us an effective 2 fold capacity increase and set us on our path to scalability.

The second part of the proposal is to target the release of a second hardfork to happen at the end of 2016. Inline with all the above factors this would start with a real block size limit increase to 2MB (effectively increasing the throughput to 4x compared to today thanks to Seg Wit) and a doubling of the block size limit every two years thereafter (with linear scaling in between). The scaling would end with an 8GB block size limit in the year 2039.

5.1 How does the Proposal fit inside the Limits

TODO: add source links See original Reddit post

5.2 Propagation time

If trends for average upload and bandwidth continue then propagation time for a block to reach >50% of the nodes in the network should never go above 1s. This is significantly quickly than propagation times we currently see.

In a worst case scenario we can we wrong in the negative direction (i.e. bandwidth does not increase as quickly as predicted) by 15% absolute and 37.5% relative (i.e. bandwidth improves at a rate of 25% per year rather than the predicted 40%) and we would still only ever see propagation times similar to today and it would take 20 years before this would happen.

5.3 Orphan Rate

Using our best guess predictions the orphan rate would never go over 0.2%.

In a worst case scenario where we are wrong in our bandwidth prediction in the negative direction by 37.5% relative, orphan rate would never go above 2.3% and it would take over 20 years to happen.

5.4 Non-Pruned Node Storage Cost

Using our best guess predictions the cost of storage for a non-pruned full node would never exceed $40 with blocks consistently 50% full and would in fact decrease significantly after reaching the peak cost. If blocks were consistently 100% full (which is highly unlikely) then the maximum cost of an un-pruned full node would never exceed $90.

In a worst case scenario where we are wrong in our bandwidth prediction in the negative direction by 37.5% relative and we are wrong in our storage cost prediction by 20% relative (storage cost decreases in cost by 25% per year instead of the predicted 37% per year), we would see a max cost to run a node with 50% full blocks of $100 by 2022 and $300 by 2039. If blocks are always 100% full then this max cost rises to $230 by 2022 and $650 in 2039. It is important to note that for storage costs to be as high as this, bitcoin will have to be enormously successful, meaning many many more people will be incentivised to run a full node (businesses etc.)

5.5 Pruned Node Storage Cost

Using our best guess predictions the cost of storage for a pruned full node would never exceed $0.60 with blocks consistently 50% full. If blocks were consistently 100% full (which is highly unlikely) then the max cost of an un-pruned full node would never exceed $1.30.

In a worst case scenario where we are wrong in our bandwidth prediction in the negative direction by 37.5% relative and we are wrong in our storage cost prediction by 20% relative (storage cost decreases in cost by 25% per year instead of the predicted 37% per year), we would see a max cost to run a node with 50% full blocks of $1.40 by 2022 and $5 by 2039. If blocks are always 100% full then this max cost rises to $3.20 by 2022 and $10 in 2039. It is important to note that at this amount of storage the cost would be effectively zero since users almost always have a large amount of free storage space on computers they already own.

5.6 Percentage of Downstream Bandwidth Used

Using our best guess predictions running a full node will never use more than 0.3% of a users download bandwidth (on average).

In a worst case scenario we can we wrong in the negative direction by 37.5% relative in our bandwidth predictions and we would still only ever see a max download bandwidth use of 4% (average).

5.7 Percentage of Upstream Bandwidth Used

Using our best guess predictions running a full node will never use more than 1.6% of a users download bandwidth (on average).

In a worst case scenario we can we wrong in the negative direction by 37.5% relative in our bandwidth predictions and we would only ever see a max download bandwidth use of 24% (average) and this would take over 20 years to occur.

5.8 Time to Bootstrap a New Node

Using our best guess predictions bootstrapping a new node onto the network should never take more than just over a day using 50% bandwidth.

In a worst case scenario we can we wrong in the negative direction by 37.5% relative in our bandwidth predictions and it would take one and 1/4 days to bootstrap the blockchain using 50% of the download bandwidth. By 2039 it would take 16 days to bootstrap the entire blockchain when using 50% bandwidth. I think it is important to note that by this point it is very possible the bootstrapping the blockchain could very well be done by simply buying an SSD with blockchain already bootstrapped. 16 days would be a lot of time to download software but it does not necessarily mean a decrease in centralisation. As you will see in the next section, if bitcoin has reached this level of adoption, there may well be many parties will to spend 16 days downloading the blockchain.

5.9 What if Things Turn Out Worse than the Worse Case?

While it is likely that future trends in the technology required to scale bitcoin will continue relatively similar to the past, it is possible that the predictions are completely and utterly wrong. This plan takes this into account though by making sure the buffer is large enough to give us time to adjust our course. Even if no technological/cost improvements (near zero likelihood) are made to bandwidth and storage in the future this proposal still gives us years to adjust course.

CHAPTER 6

Conclusions and Summary

6.1 What Does This Mean for Bitcoin?

6.2 Significantly Increased Adoption

For comparison, Paypal handles around 285 transactions per second (tps), VISA handles around 2000tps and the total global non-cash transactions are around 12,400tps.

Currently bitcoin is capable of handling a maximum of around 3.5 transactions every second which are published to the blockchain roughly every 10 minutes. With Seg Wit implemented via a hardfork, bitcoin will be capable or around 7tps. With this proposal bitcoin will be capable of handling more transactions than Paypal (assuming Paypal experiences growth of around 7% per year) in the year 2027. Bitcoin will overtake VISA's transaction capability by the year 2035 and at the end of the growth cycle in 2039 it will be able to handle close to 50% of the total global non-cash transactions.

When you add on top second layer protocols(like the LN), sidechains, altcoins and off-chain transactions, there should be more than enough capacity for the whole world and every possible conceivable use for digital value transfer.

6.3 Transitioning from a Subsidy to a Transaction Fee Model

Currently mining is mostly incentivised by the subsidy that is given by the network (currently 25btc per block). If bitcoin is to widely successful it is likely that price increases will continue to outweigh btc denominated subsidy decreases for some time. This means that currently it is likely to be impossible to try to force the network into matching a significant portion of the subsidy with fees. The amount of fees being paid to miners has averagely increased over time and look like they will continue to do so. It is likely that the optimal time for fees to start seriously replacing the subsidy is when bitcoin adoption starts to slow. Unless you take a pessimistic view of bitcoin (thinking bitcoin is as big as it ever will be), it is reasonable to assume this will not happen for some time.

With this proposal, using an average fee of just $0.05, total transaction fees per day would be:

- Year 2020 = $90,720
- Year 2025 = $483,840.00
- Year 2030 = $2,903,040.00
- Year 2035 = $15,482,880.00
- Year 2041 = $123,863,040.00 (full 8GB Blocks)

Miners currently earn a total of around $2 million dollars per day in revenue, significantly less than the $124 million dollars in transaction fee revenue possible using this proposal. That also doesn't include the subsidy which would still play some role until the year 2140. This transaction fee revenue would be a yearly revenue of $45 billion for miners when transaction fees are only $0.05 on average.

6.4 Proposal Data

You can use these two spreadsheets (1 - 2) to see the various metrics at play over time. The first spreadsheet shows the data using the predicted trends and the second spreadsheet shows the data with the worst case trends.

6.5 Summary

It's very clear we are on the edge/midst of a community (and possibly a network) split. This is a very dangerous situation for bitcoin. A huge divide has appeared in the community and opinions are becoming more and more entrenched on both sides. If we cannot come together and find a way forward it will be bad for everyone except bitcoin's competition and enemies. While this proposal is born from an attempt at finding a balance based on as many relevant factors as possible, it also fortunately happens to fall in between the two sides of the debate. Hopefully the community can see this proposal as a way of making a compromise, releasing the entrenchment and finding a way forward to scale bitcoin. I have no doubt that if we can do this, bitcoin will have enormous success in the years to come.

CHAPTER 7

Indices and tables

- genindex
- modindex
- search