Because you seem genuinely interested, I wrote you a paper (I haven't proofread though). If you read it like you will be tested, you will better understand my position. In time, you might even agree.

(Bold is highlighting and All caps is inflection.)

I'm going to try to further "bridge the gap" in understanding, but I can promise you it won't lead to a compromise on hard forks. Not because my side is totally unwilling to compromise, but because we fundamentally believe that we cannot—literally cannot without severely harming Bitcoin.

Reasonable minds can definitely differ on how to interpret the actions and motives of Gavin and Hearn. Again, I only have suspicions. Implicit within your post (certainly inferred in my reading), however, is that you think my suspicions developed my technical perspective. In actuality, it is my technical beliefs that most give rise to my suspicions about the two.

In reading your post, it would seem as though you think we have a technical disagreement over one matter: you think that Bitcoin is best of its block size can grow "organically," while you think I think Bitcoin is best off if its block size is arbitrarily capped at 1MB. I can understand why you see this as the primary technical disagreement. After all, in arenas where the block size is most often "debated," finding the "optimal" block size is typically the subject.

If that were our only disagreement, it would seem that we should be able to "bridge the gap," and come to some compromise. And because we have not done that, I can see why you guys might see our side as totally unreasonable. But the truth is, before we could even get to debating the "optimal" block setting (including unlimited), we have to get through at least three fundamental beliefs that you guys don't realize are **truly fundamental**.

(1) We really believe that a contentious hard fork will split the chain and destroy value.

(2) We really believe that all hard forks SHOULD be contentious, because we believe immutability is the most important property of Bitcoin.

(3) Even if a hard fork were possible and safe, we really believe that the cost of running a node must remain low—low enough to operate over Tor with normal computers—in order to keep Bitcoin ungovernable.

(4) Even if a hard fork with limit increase were possible and safe, we really believe implementing SegWit first and then deploying the Lightning Network is the best route.

Because most time is spent arguing about (4), which is most easily "bike shedded" and which would seem like a mere negotiable matter of preference, you guys might think we have just been unreasonably hard-trading for a year and a half, completely unwilling to compromise. But the real reason there has been not compromise is because of (1)–(3), which you guys probably think we are only asserting as posture. **With regard to (1)–(3), Core developers and those who understand are not posturing—we truly believe it**. There are, however, quite a few cheerleaders/trolls for "our side" who probably also don't realize how serious Core Developers are about (1)–(3), who probably think Core developers are just posturing; this probably becomes apparent in their arguments. But make no mistake; beliefs (1)–(3) are held sincerely, and they don't allow for us to "bridge the gap," except through understanding —not compromise.

Each Belief explained:

**(1) We really believe that a contentious hard fork will split the chain and destroy value.**

Prior to Ethereum's infamous fork that split the chain, we argued until blue in the face that if Bitcoin had a contentious hard fork, the result would be a chain split. Peter Todd went on Bitcoin shows explaining that exchanges would be placed in legal limbo, because they would need to support both chains. We understood that because of this, if Bitcoin split there will be a market for both chains. We understand that the market for the original chain will not just suddenly switch from the chain that has garnered the market value (the one with the strong network effect and the first-mover advantage) to the forked chain. Accordingly, any attempted fork will likely result in a split chain with both likely having less value than before the split (markets hate uncertainty). All of the same people who argued that this would not happen immediately hit social media after the ETH fork to claim victory. And then, after the old chain was practically dead, it was revived, and there was a market value for the original chain (now the original chain is longer than the forked). All of ETH and most of the Bitcoin pro-forkers were truly shocked by this. Those loudest (Brian Armstrong and Gavin Andresen) had egg on their face over the matter. Ironically, these same people (mostly their followers) try to argue that it could not happen to Bitcoin because of the difficulty timing difference.

While there is some merit to the fact that difficulty changes things, a split chain can definitely happen to Bitcoin. And those who said it would not happen have proven they cannot be trusted. I would suspect that a Bitcoin chain splitting would actually be worse. Because the ETH people did not truly believe that a fork was possible, the market mostly switched. That likely will not happen with Bitcoin. Too many of us know that a split is possible (at 75% hash or 95% hash), and we know that the market is not going to suddenly start valuing the forked chain, **especially not after the ETH debacle**. But what a threatened fork will do is cause a lot of uncertainty and cause the market value to begin to decline even before a hard fork is executed. Because of this, those who have the most invested in Bitcoin—miners, exchanges, and large holders—who could affect such a change will always be deterred from attempting a hard fork because of the prior market response. They are also deterred by the post-fork uncertainty (practical certainty) of a chain split. It was a bit of a mess for ETH, it would be a freaking nightmare for Bitcoin.

**(2) We really believe that all hard forks SHOULD be contentious, because we believe immutability is the most important property of Bitcoin.**

While you guys might look at the above and try to find a way to make hard forks possible. We don't see the value. We think Bitcoin's most important property is its immutability. Accordingly, we think hard forks should always be contentious, because they are a threat to immutability. I am part of the crowd of true believers that would extend that even to soft forks. Hard forks remove rules, while soft forks add them. I am glad to see that Bitcoin has progressed to the point where hard forks are practically impossible. **I want to see the political contention within Bitcoin factions grow to the point where even soft forks are impossible**. We may already be there. While I think that SegWit is fantastic and am fine with its implementation. But if it is blocked, Bitcoin will have reached another milestone towards achieving true immutability. **We don't want to "bridge the gap," because contention secures immutability**. This is, I think, the essence of so-called Nakamoto consensus. As diversity in usership grows, consensus becomes impossible, and THIS is what ultimately secures Bitcoin. Compromise and agreement are the enemy to immutability.

You guys will often argue that Bitcoin will be replaced by one that is "better," if we don't compromise. But those seeking a secure store of value outside the purview of government don't care about any other features if the coin lacks immutability. The first-mover with true immutability will be hard—damn near impossible—to catch. The market will move to Bitcoin and as it does, it will the market less and less likely to move to another. There is a very strong network effect. The only way we are presently willing to compromise is to delay immutability for soft forks like SegWit. But make no mistake, that is a compromise—I will make more money faster if SegWit is "blocked"/"ignored"/"not voted for"/"whatever." The market will value the benefit of true immutability more than any features added by SegWit.

**(3) Even if a hard fork were possible and safe, we really believe that the cost of running a node must remain low—low enough to operate over Tor with normal computers—in order to keep Bitcoin ungovernable.**

Until we overcome the above two beliefs, discussing this one serves little purpose. But for the purpose of bridging the gap in understanding I am discussing.

Bitcoin has become controllable by far fewer people than intended. Right now miners and exchanges could almost collusively force any change that they want. But there is one check: ordinary users can run nodes that validate the blocks of even a few dissenting miners. That is a BIG check. That's the check that kept the original Ethereum chain (ETC) running. When the miners and the exchanges essentially colluded to perform a 51% attack on Ethereum, the original chain survived, because ordinary users could run nodes and validate the blocks of only a few miners. This allowed the establishment of a market value, which lead to all exchanges having to pay people the ETH/ETC they deposited on the chain they deposited. If this is not possible, the control of the protocol is left in the hands of a few. **And anything left in the hands of a few is governable**.

We want Bitcoin to remain ungovernable. Government governs at choke points. If the cost of node operation increases to where ordinary users cannot participate, the government has a choke point. In fact, the governments already has choke points with only a few thousand nodes. But as long as nodes can be ran over Tor, governance is least likely. Once ordinary users can no longer run nodes, they have no ability to resist changes (by running nodes and mining the original chain) they disagree with.

We want to see Bitcoin become less governable by decentralizing mining. But increasing node cost beyond a certain point will result in a governable Bitcoin with no turning back. When the Core developers looked at SegWit, they were not posturing when they said that the only downside was that it increased block size. This is not viewed as a positive. It is viewed as a move in the wrong direction.

**Your preference to have an "organically" determined block size is diametrically opposed to our position**. Removing the cap Satoshi placed will result in removing nodes from individuals, and that is unacceptable to us. We could accept the 1–4 MB SegWit allows, but that is pushing it.

Of course, once we start talking about this, this is where your side wants to start arguing. That's the pull of bike-shedding. All of this is barely even worth discussing because of (1) and (2) above.

**(4) Even if a hard fork with limit increase were possible and safe, we really believe implementing SegWit first and then deploying the Lightning Network is the best route.**

There is probably most room to compromise here. It seems clear to me that SegWit/Lightning first would be better, because then we could know how to change the block cap limit to fit the needs under Lightning, which will certainly be less than without. But I guess it is "arguable." Regardless, because of (1)–(3), arguing about it is pretty much pointless. **We don't like compromise, because we love immutability. Our compromise on change has been to allow soft forks. Our compromise on the block size is SegWit. But eventually contention will block soft forks. And if that happens now, then Great! As it turns out, we did not have to compromise at all (although the benefits of SegWit are nice)**.