

# Hard forks and Consensus Networks: Meta Questions and Limitations

 **MAbtc** POSTED ON AUGUST 29, 2016

♥ 18    👁 3 Views    💬 17

0  
SHARES

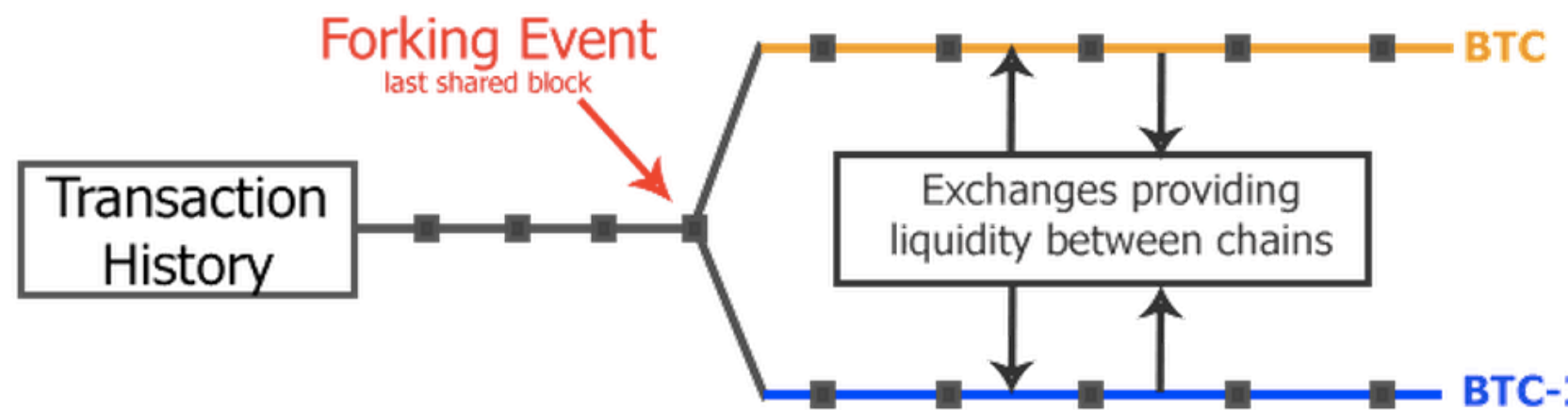
 Share On Facebook

 Tweet It



 G+





Over the past year, there has been considerable confusion around the term *consensus* as it relates to both the *consensus mechanism* that Satoshi wrote of in the Bitcoin whitepaper, and the *consensus rules* that underpin the Bitcoin network. This confusion has led to a widespread misunderstanding of the limitations of consensus networks – and of the nature and risks of hard forks.

## Satoshi’s consensus mechanism

**Satoshi described** the use of proof-of-work computation by network nodes to reach *consensus* – or “general agreement” – about which valid blockchain contains the most cumulative work and is therefore the authoritative blockchain:

“When a node finds a proof-of-work, it broadcasts the block to all nodes... Nodes accept the block only if all transactions in it are valid and not already spent... Nodes express their acceptance of the block by working on creating the next block in the chain... Nodes always consider the longest chain to be the correct one and will keep working on extending it.”

**Christian Decker and Roger Wattenhofer describe** the result of any contention about the

- Advertisement -



## SUBSCRIBE

Email

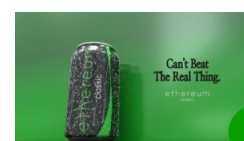
SIGN UP

## POPULAR POSTS



1

**\*\*UPDATE\*\* ETC/DAO stolen coins frozen by exchanges was sent by Ethereum Foundation Developers**



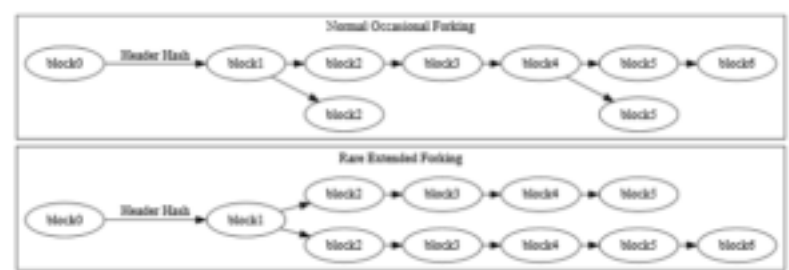
2

**Ethereum Classic: A Masterpiece in the Making**

best blockchain:

“Eventually one branch will be longer than the other branches, and the partitions that did not adopt this branch as theirs will switch over to this branch. At this point the blockchain fork is resolved and the ledger replicas are consistent up to the blockchain head. The blocks discarded by the blockchain resolution are referred to as orphan blocks.”

So, in the context of blocks that conform to the protocol’s rules, the network reaches *consensus* on what constitutes the best blockchain, essentially by a matter of processing power. Miners have rational economic incentive to orphan blocks that are unlikely to be included on the best blockchain. If a miner were to build on such blocks, the odds that their future mining rewards would be accepted by the network would be diminished. In this way, network nodes are able to come to full agreement regarding which chain is authoritative.



Despite the occasional fork, nodes reach consensus about what constitutes the longest valid blockchain.

How do nodes approach blocks which don’t conform to the protocol’s rules? What if a miner includes a block which double spends outputs, or increases the block size? **Satoshi’s answer to that question** was quite clear: They respond by “rejecting invalid blocks by refusing to work on them.”

In other words, Satoshi’s consensus mechanism unequivocally rejects invalid blocks. Failing to conform to the protocol’s rules invalidates any block. Any blockchain that includes such an invalid block is not participating in the Bitcoin network and accordingly, is not in competition for the best blockchain.

The difficulty and hash rate of an invalid blockchain is irrelevant to the Bitcoin network, regardless of what miners might tell you. Despite popular perception, miners do not have any power over the protocol’s *consensus rules* – the rules enforced by every node on the network. The only power that miners specifically have is to order transactions into blocks, in conformity with these rules.

**The basis for a network’s consensus rules**

Listening to the recent hard fork debates, it’s easy to overlook the fact that the term *consensus* derives from the root *consent*. In other words, when you opt in to the Bitcoin network, you *consent* to the protocol’s rules. Users participate via nodes, which enforce these *consensus rules*. Thus, individual user consent is the basis for the *consensus rules* imposed on the network.

**Origin and Etymology of CONSENSUS**

Latin, from *consentire* (see **consent**)

First Known Use: 1843

This has significant philosophical implications for hard forks. A hard fork is not merely a software change; it entails that every user migrates to a new network. A hard fork is fundamentally a new system, with new rules, and is

completely incompatible with the original network. Thus, by definition, a hard fork violates the user consent that serves as the basis for a consensus network like Bitcoin.

In the context of the Bitcoin network, there is no such thing as “achieving consensus for a hard fork.” There never will be. There is no mechanism by which every user of Bitcoin’s

software can consent to a network migration. Inherently, users don't consent to a hard fork – consent exists only post-hoc, after the fork has occurred (when *some* users decide to opt in to the new network). *Anyone that refuses to migrate networks did not consent to the rule changes.*

In other words, any “majority vote” (for example, by hash power distribution or coin stake) prior to a hard fork is merely an inaccurate poll, and cannot act as a replacement for the affirmative consent users provide by opting in to a network. Hard forks violate the basic philosophical principles underlying distributed consensus networks and are thus an existential threat to the integrity of their blockchains.

### Network consensus vs. “Social consensus”

Proponents of hard forks in Bitcoin and Ethereum have sought to replace the definition of *consensus* with that of “**social consensus**” – the idea that if most users agree with a certain plan, that it should be enacted even if it breaks the consensus rules. The underlying logic is that if most people agree to a hard fork, the existing consensus can be subverted, and the majority rulers can economically coerce the minority into migrating networks against their will.

Generally, this understates the risks associated with contentious hard forks by falsely assuming that only one blockchain will survive. Of note, opting in to the forked protocol does not revoke your consent to the original protocol's rules, and individual users may seek to maximize the value of their tokens held on both chains.

After last month's hard fork, Ethereum users now understand that it is very dangerous to assume that a minority fork will simply die. If users remain on the original network – suggesting existing demand for its newly minted tokens – the original chain will be worthy to rationally mine. In this way, multiple blockchains emerge from a contentious hard fork. As the ETH/ETC debacle demonstrated, speculators can further challenge a hard fork by establishing market demand for the original chain's token, ensuring a network split by incentivizing miners to secure the original network.

Perhaps more importantly, this method of governance is in direct contradiction with the basic security premises of Bitcoin (or any similar distributed consensus network). Even if we accept the practical argument that the fear of economic loss associated with mining/transacting on the minority chain is enough to force the minority to migrate to the hard-forked network, the idea should be opposed on philosophical grounds. When you opt in to the network, you and all participants enforce the consensus rules. This entails rejecting invalid blocks – not abandoning the consensus rules anytime 51% (**or 75%**) of miners tell you to. Such attempts to break consensus are an attack on the very idea of participating in a consensus network. If a majority of miners can coerce the network into abandoning the rules every user has agreed to, only by virtue of its hash power, then Nick Szabo is correct to call this “**technologically equivalent to a 51% attack.**”

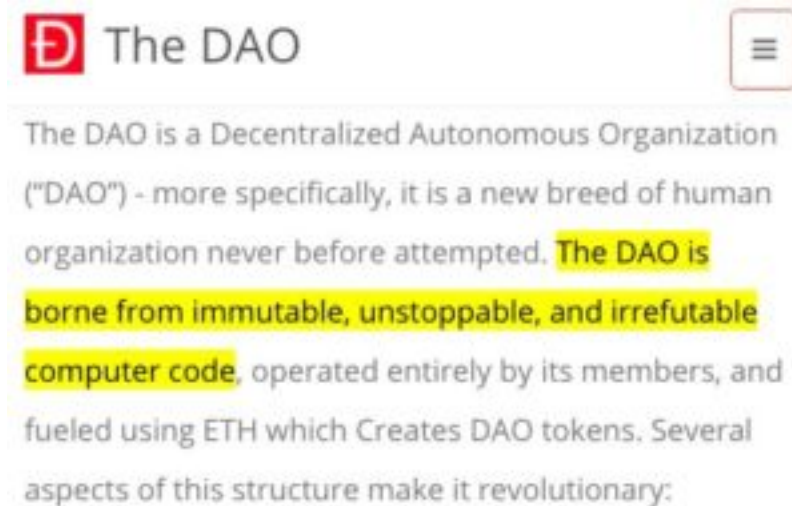
### What can we learn from the DAO fork?

The DAO fork is an ideal case study for the dynamics of a contentious hard fork. For background, the DAO was a crowd-funded application built on the Ethereum protocol.

In June, unknown actors exploited a vulnerability in the DAO's code that allowed them to siphon funds from their owners. This resulted in the loss of millions of ETH for the DAO's investors. Part of the Ethereum community decided to implement a hard fork to reverse the theft and return the ETH to its original owners.



Despite efforts to poll the community, the vast majority of Ethereum users (by coin stake) and miners (by hash rate) **did not vote at all**. Still, the hard fork proceeded anyway. Predictably, some users remained on the original chain, and the hard fork resulted in two surviving blockchains on separate, incompatible networks: Ethereum Classic and Ethereum.



### Why was the DAO fork contentious?

The crux of the issue centers on where the exploited code occurred: *the application layer* (in contrast to the *protocol layer*). When a flaw exists at the protocol level, all network participants are negatively impacted; thus, all users are incentivized to fix the problem. While it is impossible to obtain consensus for a hard fork to address such a flaw, a rational analysis of user incentives suggests that it would receive widespread support.

The closest example that illustrates this dynamic in Bitcoin is the **2010 value overflow bug** and subsequent soft fork. *Of note: the solution was a soft fork, so breaking consensus rules was never a concern. Bitcoin has never hard-forked.*

The value overflow bug, by introducing token supply beyond the intended consensus limits, undermined the basic value premise of Bitcoin's finite supply limit. The protocol flaw negatively affected all Bitcoin users by effectively diluting their share of all mined bitcoins by ~45,000x. A soft fork was released within hours of the offending block, which rejected output value overflow transactions and any transaction which paid more than 21 million bitcoins. At block height 74691, the soft forked chain overtook the offending chain and orphaned it. This is an excellent example of the community successfully soft-forking to address a protocol flaw. Unfortunately, the jury is still out regarding whether the community can successfully do so in the case of consensus-breaking changes.

The DAO fork differed significantly in that it was a *hard fork* which sought to address a flaw *on the application layer* – not the protocol layer. Since the protocol wasn't at issue, there was no reason to assume that the fork would receive widespread support.

**The Ethereum Foundation continues to describe** Ethereum as a platform for “unstoppable applications” that “run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.” Stephan Tual, one of the DAO's creators, **made the claim**, “Code is law.”

Ethereum's community was built on the principles of “unstoppable applications” and “no third party interference.” It simply wasn't rational to assume that the entire userbase was incentivized to fork their protocol to effectively *bail out a third party application*. Since the DAO was merely an application, only a minority of Ethereum users participated in its crowd sale. When the DAO theft occurred, only a minority of Ethereum users were affected, and thus directly incentivized to support a hard fork. Predictably, **only a small minority of ETH holders and miners signaled support**.

Although the initial post-fork miner distribution approached 99:1 at one point in favor of the forked network, enough users were incentivized to secure the immutability and consensus of the original chain. As such, value was retained on both blockchains – it

became apparent that both chains were worthy for rational miners to build on, splitting the network into two.

## Implications for Bitcoin

What does this mean for Bitcoin? The answer is two-fold.

Firstly, is it possible to initiate a hard fork that is not contentious? The fundamental problem is that the removal of consensus rules generally involves both security and philosophical trade-offs. Take the block size debate as an example. One side is composed of decentralists – those who point to the centralization of nodes and hash power and the necessity of fee markets as compelling reasons not to increase throughput without scaling mechanisms. On the other side are those that argue that retaining low fees and nurturing adoption is paramount to any concerns about p2p decentralization and security. When the fundamental priorities (and philosophies) of each side are incompatible with the other, how can we expect any resulting hard fork *not* to be contentious?

Vitalik Buterin made an important point when he mused, “I propose we use the term ‘tradeoff denialism’ for when someone tries to reply to ‘I think A is better than B’ with ‘well why not do both?’” Can you imagine a world where 100% of bitcoiners are willing to sacrifice their security for a chance at increased adoption? Where there are trade-offs to be made, there will necessarily be contention.

For years, many Bitcoin users have complained about the lack of a “killer app” that promotes Bitcoin adoption to the mainstream. On the contrary, Bitcoin’s “killer app” was released at inception: math-based, censorship-resistant money on a decentralized inflation-controlled ledger. This is Bitcoin’s primary use case; this is what drives demand and serves as a basis for its value. The risk of a network split initiated by a contentious hard fork is a significant threat to that use case, and to the very idea of a cohesive, global ledger. Pieter Wuille elaborates:

“No matter how you determine the switchover date, there is no way of knowing when (and whether at all) everyone changes their full nodes (and perhaps other software), and even very high hash power votes cannot prevent an actual fork from appearing afterwards. At best, people lose the guarantee that their confirmations are meaningful (because at some point it becomes clear that the other side will get adopted, and they need to switch). At worst, a fork persists, and two partitions appear, in each of which you can spend every pre-existing coin. This defeats the primary purpose Bitcoin was designed for: double spend protection.”

Secondly, a hard fork is a clear attack on the basic security premises and underlying philosophy of Bitcoin. There is no software mechanism to measure user consent to remove consensus rules. There is a widespread misunderstanding in the Bitcoin community which states that hard forks can be enforced as a matter of hash power. This wrongly conflates the nature of hard forks with that of soft forks. Eric Voskuil explains:

“In the case of a hard fork, a new transaction may be valid despite not conforming to the original rules. In the case of a soft fork, new transactions are valid under the original rules. In other words, holders of a money have not agreed to a hard fork but inherently accept a soft fork... A soft fork can be enforced by simple majority of processing power.



In other words a soft fork isn't actually a change in consensus among people, it's a change that flows from the people controlling a majority of processing power... The original paper does not articulate a distinction between these rules, loosely referring to both scenarios as consensus. However it is an error to refer to soft fork rules as 'consensus rules'."

So, it is very true that a majority of hash power can enforce *new rules* with a *soft fork*. However, it is clearly inaccurate to say that hash power has any relationship to the software's *consensus rules*. Miners have absolutely no say over user consent (i.e. *consensus rules*) – except to the extent that they operate their own nodes. When prominent developers, industry executives and centralized mining pools promote the idea of a miner vote to determine consensus changes, this is a direct attack on Bitcoin – it is a direct attack on your money. [Pieter Wuille points out](#):

"Bitcoin is not a democracy. The full node security model is designed to minimize trust in other parties in the system. This works by validating as much as possible according to the consensus rules. In particular, there is no 'majority vote' that can override things (contrary to what some people think, it is not 'longest chain wins, and a majority of miners decide'; even a majority of miners cannot steal your coins or produce more than the allowed subsidy, unless they convince others to change their software)."

### **Hard forks should be opposed as a matter of both risk and philosophy**

From both practical and philosophical perspectives, it seems clear that attempts to hard fork the Bitcoin protocol should be unequivocally opposed. The community should be staunchly opposed to the idea that some group of users (for example, mining pools), can vote away the *consensus rules* that secure *our money*. It is important to recognize that breaking consensus threatens to erode all trust in the supposed ability of Bitcoin to enforce basic rules. If you believe that consensus rules can be removed via democratic vote, do you really believe in the viability of the 21 million BTC supply limit? Why? Any future vote can simply remove that limit, and the majority can dilute the wealth of early adopters. *The consensus rules are your only defense against such theft. Attempting to remove them is opening Pandora's box.*

Readers should ask themselves: *Do you believe that miners ought to be able to change the rules that we, the users, consented to?* If the answer is yes, then you have imbued miners with the power of central banks. Non-mining node operators do not have identical interests to those of miners; non-mining nodes serve as a check on the power of miners. Refusing to trust miners and individually enforcing the protocol's rules is an individual's only protection against collusion by miners (or others) against him/her. In the absence of decentralized node validation, there is no effective difference between miners and central banks; there are no rules by which they must abide. If you grant miners authority over consensus rules, you have sacrificed the fundamental security provided by the full node security model – your money is no longer safe. It is tempting to use miner distribution as a voting mechanism, but it simply has no relation to user consent and thus, should have no bearing on the consensus rules.

As discussed earlier in regards to the 2010 value overflow incident, there is only one narrow condition that may ethically, and in practice, afford us the ability to hard fork: a bona fide protocol flaw that negatively affects all Bitcoin users. Indeed, such a hard fork would violate the consent of users. However, if we know that the protocol flaw affects every user – this is the nature of protocol flaws – then we know *prima facie* that fixing the flaw is aligned with user incentives and expectations. Any rational user is likely to support a hard fork under these narrow conditions.



To be clear, retaining immutable consensus and therefore favoring soft fork solutions to protocol limitations does not mean that progress nor development must stagnate. On the contrary, in regards to the block size debate, soft forks will allow for **incredible improvements to both bandwidth and non-bandwidth scaling** without the risks associated with hard forks. Instead of merely allowing more transaction throughput by increasing maxblocksize, we can drastically optimize transaction size to increase capacity through mechanisms like Schnorr signatures. Once malleability fixes are in place, the doors are opened for smart contracts that contribute via non-bandwidth scaling: Lightning Network will allow trustless contracts with no custodial risk, which will directly mitigate mainchain throughput. MAST can further optimize the size of complex smart contracts. Mining pre-validation (weak blocks) can drastically reduce critical bandwidth, resulting in fast propagation / latency mitigation and “weak” confirmations for transactions, addressing concerns over mining centralization in the context of increased throughput. Improvements like committed bloom maps, batch validation and archive nodes can further reduce resource requirements for nodes, mitigating centralization pressures as throughput increases.

Brilliant scaling solutions are before us – solutions which will directly enhance capacity while mitigating the externalities created by increased throughput. Why would we break consensus simply to increase capacity? The idea is absurd!

### Implications for Ethereum Classic

The Ethereum Classic community has emerged as a reaction to the brazen approach that ETH developers have taken towards hard forks. Ethereum users that value the integrity of their consensus rules and the immutability of their blockchain have rallied behind Ethereum Classic.



Unfortunately, the consequences of the ETH core developers’ brazen approach are not limited to the DAO fork. ETH’s core developers effectively sabotaged the Ethereum protocol by programming the “difficulty bomb.” **Vitalik Buterin describes the effects:**

“At block 3.5m (1 year from now), we would have an equilibrium block time of 25s for 100k blocks (~1 month); then we would see 35s for 100k more blocks (now ~1.4 months); then ~55s for ~2.2 months, then ~95s for ~3.8 months, and so forth

until we get ~655s for ~26 months (ie. slightly worse than bitcoin), and only after that does the protocol break because of the cap of ~99/2048 downward adjustment, and that final doom does not take place until 2021 (though it certainly gets very annoying by the second half of 2017).”

In effect, time between mined blocks will become longer and longer until eventually, “final doom” occurs, when no more blocks can be mined. It should be noted that to purposefully sabotage the Ethereum protocol in order to force a break of consensus shows incredible disdain for the Ethereum userbase by ETH’s core developers. Nevertheless, this is the hand that Ethereum Classic was dealt.

Fortunately, the Ethereum Classic community has the means and moral authority to break consensus to overcome this sabotage. The difficulty bomb is an existential

protocol flaw. All users are incentivized to fix it – they must be, otherwise their protocol is doomed to inertia, and effectively will no longer be an active blockchain.

As such, the only way forward is a hard fork – one whose only change to the protocol is to return delayed block times to historically typical levels. The only chance we have to prevent a contentious hard fork is to restrict consensus changes to the protocol flaw that warrants the fork.

Many bitcoiners have come to support the Ethereum Classic community, some of whom have expressed a desire to fork ETC’s protocol to restrict the future supply and perpetual inflation of ETC. This is the wrong course of action, and enters the dangerous territory of contentious hard forks. ETC’s inflation rate is specifically a security incentive that ensures honest mining – removing it entails significant security trade-offs, which will not be looked upon equally by every user of the protocol. To prevent a network split, emphasis must be put on aligning consensus changes with global user incentives and expectations. Any changes outside the narrow context of addressing protocol flaws are likely to result in contention.

### Concluding notes

Whatever your philosophical opinions might be in regards to hard forks, it’s important to remember that Bitcoin is not merely money; it is also the software development project that seeks to secure that money. In engineering, particularly with considerable value at risk, it’s vital that we plan for worst-case scenarios. We cannot simply assume that users will blindly follow miners and change their software – particularly because they shouldn’t. And while miners are rational in where they point their hash power, this does not entail that miners are *correct* in their assumptions about the resolution of a hard fork. The risks entailed by hard forks simply do not warrant their use as a mechanism for software updates underpinning a consensus ledger.


Bitcoin and other token-based consensus networks are economies. Unfortunately, causality in macroeconomics is, and will likely continue to be a mystery. As David Hume said, “There can be no demonstrative arguments to prove that those instances, of which we have had no experience, resemble those, of which we have had experience.” We can never know beforehand how a hard fork capable of splitting the network will resolve.


We must take a risk-oriented approach and avoid the worst-case scenarios that hard forks entail. In particular, the emergence of multiple Bitcoin networks open to cross-network double-spending would be a devastating failure of Bitcoin’s double-spend protection. Further, it would forever cast doubt on the ability of the Bitcoin network to enforce basic rules, such as its limited supply.





0


SHARES

 Share On Facebook

 Tweet It











AUTHOR

**MAbtc**

Bitcoin, commodities trader.

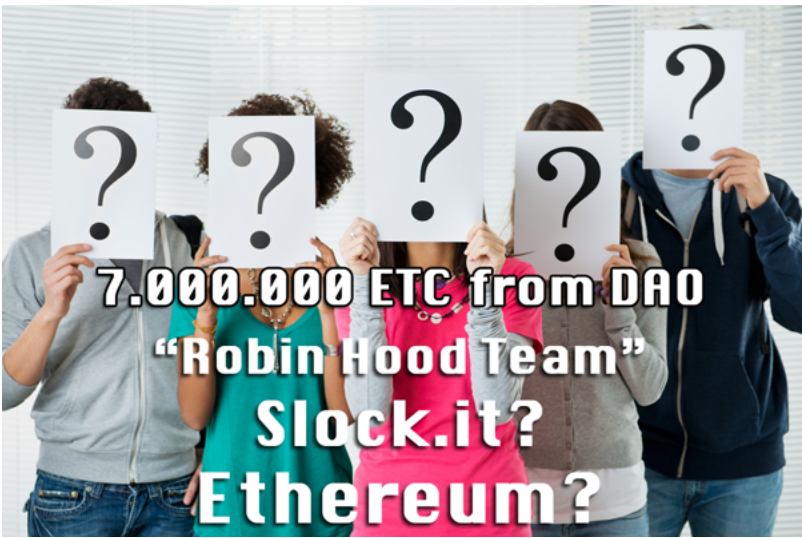


TRENDING NOW



**\*\*UPDATE\*\* ETC/DAO stolen coins frozen by exchanges was sent by Ethereum Foundation Developers**

MoneyTrigz AUGUST 31, 2016



**Ethereum Developer publish statement denying affiliation with the Robin Hood Team?**

MoneyTrigz AUGUST 11, 2016



**READ NEXT**

**Why Bitcoin is the Best Hope for the Denationalization of Money**



17 COMMENTS



**DonJohnson** August 29, 2016 at 6:39 pm **REPLY**

great article! great job  
keep it up



**TNega** August 29, 2016 at 10:36 pm **REPLY**

This article may be the best hardfork and consensus article I have read in a long time.  
I could easily vote this article to be the most important explanation and elaboration  
for the average Bitcoin user (and average crypto-coin user) for the

2016 year.

Your ability to “flesh it out” in more simple terms (for non-techies) is important and an asset in the crypto-currency space. Great job.

~TNega



**HostFat** August 30, 2016 at 10:56 am **REPLY**

Discussion on r/btc 😊

[https://www.reddit.com/r/btc/comments/509ggm/hard\\_forks\\_and\\_consensus\\_networks\\_meta\\_questions/](https://www.reddit.com/r/btc/comments/509ggm/hard_forks_and_consensus_networks_meta_questions/)



**Roger\_Murdock** August 30, 2016 at 12:26 pm **REPLY**

No offense to the author, but this article is very confused.

“Even if we accept the practical argument that the fear of economic loss associated with mining/transacting on the minority chain is enough to force the minority to migrate to the hard-forked network, the idea should be opposed on philosophical grounds. When you opt in to the network, you and all participants enforce the consensus rules. This entails rejecting invalid blocks – not abandoning the consensus rules anytime 51% (or 75%) of miners tell you to. Such attempts to break consensus are an attack on the very idea of participating in a consensus network. If a majority of miners can coerce the network into abandoning the rules every user has agreed to, only by virtue of its hash power, then Nick Szabo is correct to call this ‘technologically equivalent to a 51% attack.’”

What the author seems to miss is that “validity” in Bitcoin is always subjective. Borrowing from an old comment of mine:

“The first rule of Bitcoin is that there are no rules. Or rather, everyone gets to decide for themselves what the ‘rules’ are by deciding which version of software to run and which version of the ledger to value. Of course, as a practical matter, the overwhelming importance of network effects strongly incentivizes people to reach universal (or at least near-universal) agreement on one set of rules and one official version of the ledger. But the agreed-upon ‘rules’ are, by Bitcoin’s very nature, always subject to change. Or as I wrote previously, ‘there is never any ‘real’ (i.e., objective / hard-and-fast) protocol, only provisional and shifting Schelling points.’ But not all Schelling points are created equal, and the potential always exists for two different Schelling points to come into conflict, at which point you get to see which is stronger.”

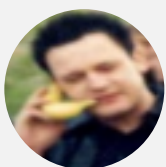
And the conclusion of the piece (that “a hard fork violates [] user consent”) is completely backwards! Any functional change that can be accomplished via a hardfork can also be done via a (more-convoluted) softfork. But softforks are far more insidious because they’re harder to resist. If you don’t consent to a hardfork, you can simply not do anything, which means that there’s no coordination

problem for a disgruntled minority to overcome. On the other hand, if there's a minority group that's strongly opposed to a softfork, they're now faced with the difficult task of coordinating their own hardfork if they don't want to be swept along.

Now that does imply that hard forks are more likely to result in persistent (or at least, semi-persistent) chain splits (again because hardforks are easier for a disgruntled minority to resist). But that's not a bad thing! Again there are very strong incentives that will tend to drive convergence on a single chain (which explains why Bitcoin hasn't spit yet). Thus, if a persistent split does occur notwithstanding these incentives, that's a pretty good indicator that the benefits outweigh the costs. If people feel so strongly about "going their own way" that they're willing to suffer the accompanying loss of network effect, then that's probably the right result. Long-term, I think one chain will likely dominate over the other, but a split seems like a pretty healthy mechanism for the market to express itself and experiment with different directions to determine the best one.

"In the case of a hard fork, a new transaction may be valid despite not conforming to the original rules. In the case of a soft fork, new transactions are valid under the original rules. In other words, holders of a money have not agreed to a hard fork but inherently accept a soft fork... A soft fork can be enforced by simple majority of processing power. In other words a soft fork isn't actually a change in consensus among people, it's a change that flows from the people controlling a majority of processing power... The original paper does not articulate a distinction between these rules, loosely referring to both scenarios as consensus. However it is an error to refer to soft fork rules as 'consensus rules'."

And that is just Orwellian nonsense. Holders "inherently accept" a soft fork?! Hey, I know. I'll acquire 51% of the hash power and implement the following two simple soft forks: "no blocks are valid unless I mined them" and "transactions that attempt to spend from addresses I don't own are invalid" (i.e., a complete blacklist of everyone else's coins). Those are just "new rules" (and thus not "consensus rules"), and so there'd be no problem, right? After all, by holding Bitcoin you would have already "inherently accepted" those modest changes.



**MAbtc** August 30, 2016 at 7:40 pm **REPLY**

"What the author seems to miss is that 'validity' in Bitcoin is always subjective."

This is precisely wrong. Validity is defined by the software. You are free to publish invalid blocks and fork yourself onto a different network. But don't expect anyone to accept your mine rewards as bitcoins.

"The first rule of Bitcoin is that there are no rules. Or rather,



everyone gets to decide for themselves what the ‘rules’ are by deciding which version of software to run and which version of the ledger to value.”

There can be no consensus ledger without consensus rules. That there is a single global Bitcoin ledger suggests there exists a single set of consensus rules (as if we didn’t know). There is no “which version of the ledger” to contemplate. Anyone can fork Bitcoin, releasing their own altcoin. People can even give it value. I’m not sure why anyone would call it “Bitcoin” though.

“But the agreed-upon ‘rules’ are, by Bitcoin’s very nature, always subject to change.”

We can agree to disagree. I view the consensus as sacred – the basic fundamental guarantee of the integrity of Bitcoin as money.

Immutability IMO does not refer to blocks. The reversibility of Bitcoin transactions is simply a function of cost. Miners can and will attack the network.

Immutability refers to consensus. If the rules underlying the consensus ledger are mutable, money cannot have integrity. There will come a time when people make the same hollow democratic appeals to increase Bitcoin’s finite supply. I prefer that we lay our cards on the table now, and make clear what is at stake.

“But softforks are far more insidious because they’re harder to resist.”

This is how Bitcoin fundamentally works. By accepting the longest valid chain as authoritative, you implicitly accept soft forks implemented by a mining majority.

Implying that any software update is an \_attack\_ because it implements a soft fork is simply dishonest. But at the end of the day, you don’t have any say over what a mining majority does. By running a full node, you implicitly accept what a mining majority does, as long as it conforms to the software’s rules. Perhaps this is a weakness in Bitcoin, but that’s for another discussion.

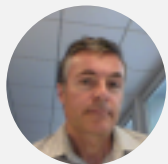
“Again there are very strong incentives that will tend to drive convergence on a single chain (which explains why Bitcoin hasn’t split yet).”

Namely, the fear of economic loss associated with remaining on the “minority” chain. I staunchly oppose a majority of mining power being used to coerce users to migrate networks against their will. Proponents of a hard fork block size increase often point to the “irrationality” of remaining on the “minority” chain. This explicitly suggests the leveraging of economic loss to force users to migrate.

That’s horribly wrong. Nobody running a Bitcoin node signed up for that.

“I’ll acquire 51% of the hash power and implement the following two simple soft forks: “no blocks are valid unless I mined them” and “transactions that attempt to spend from addresses I don’t own are invalid””

Again, this is how Bitcoin works. Whether its rational and cost-effective for an attacker to do so is another story. What you are describing is a realistic attack scenario that can happen right now. We don’t have any control over that, beyond mining honestly ourselves.



**Boussac** August 31, 2016 at 8:21 pm **REPLY**

“Any functional change that can be accomplished via a hardfork can also be done via a (more-convoluted) softfork.”

This does not sound true: not all software changes can be backwards compatible.



**Roger\_Murdock** September 2, 2016 at 6:55 pm

“This does not sound true: not all software changes can be backwards compatible.”

Well, I’m not really much of a coder, but yeah, that’s at least my current understanding. I seem to recall people presenting proposals that show how you could make dramatic protocol changes like increasing the issuance supply cap or raising the block size limit via soft fork. And in fact, the soft fork Segwit proposal itself involves an effective increase in the block size limit – something that, by its nature, would seem to require a “hard fork.” Basically, my understanding is that you could add a new rule (thus, making it a “soft fork”) such that the network will only accept a “main block” as valid if it contains a hash to some kind of additional “extension block.” And then basically you can have all the REAL action vis-a-vis updating the ledger happening in the extension block by applying whatever rule set you want to it. Essentially, the “main blocks” become these sort of “pod-person” blocks that look superficially “valid” to other nodes, but whose true internal workings are totally inscrutable and alien.



**Roger\_Murdock** August 31, 2016 at 2:14 pm **REPLY**

“This is precisely wrong. Validity is defined by the software. You are free to publish invalid blocks and fork yourself onto a different network. But don’t expect anyone to accept your mined rewards as bitcoins.”

There is no “the” / “official” software. There is only the software that people choose to run at any given time. Of course, if you use a

version of the software that's incompatible with the then-economically-dominant rule set, you shouldn't expect your mined rewards to be accepted as "bitcoins." But the economically-dominant rule set / version of the ledger is, by definition, always subject to the potential for change.

"There can be no consensus ledger without consensus rules. That there is a single global Bitcoin ledger suggests there exists a single set of consensus rules (as if we didn't know). There is no 'which version of the ledger' to contemplate. Anyone can fork Bitcoin, releasing their own altcoin. People can even give it value. I'm not sure why anyone would call it 'Bitcoin' though."

Of course, in a sense, there ARE "consensus rules" but they're just Schelling points that are subject to change. Here's a hypothetical I've used before that I think is useful:

Let's say Satoshi suddenly broadcasts a 1.1 MB transaction that sends 900,000 BTC to the 1BitcoinEaterAddress with a 100,000 BTC miner fee. (I don't actually know if you could artificially inflate the size of a single transaction like that without breaking consensus rules other than the 1-MB block size limit, but let's just assume for the moment that it's possible to make the hypo simpler.) If you're an economically-rational miner, what do you do when you see a transaction like that come across the wire? Do you just ignore it because any block you tried to mine it into would be "invalid"? I don't think so. Even if you think that there's a 99.9% chance that, if you're the first to mine that transaction, that that block is just going to be orphaned by the rest of the network (because they're going to view it as "invalid"), there would still be a big positive expected value in trying. Of course, I don't think the market / other miners WOULD view the block as "invalid." The deflationary effect of destroying that much of Satoshi's stash (and removing what some see as its "looming presence" over the market) would be huge. Plus you'd have the renewed implicit endorsement for larger blocks from someone viewed by most as the ultimate Bitcoin "authority." The real risk of orphaning would likely come from other miners attempting to mine that 100,000 BTC fee for themselves (so in practice you'd probably have lots of side deals among major pools agreeing to split the fee in exchange for working to extend the first chain to find it).

To answer your question: why would people refer to a ledger as "Bitcoin" following a hard fork? Well, because that's how language works. In all likelihood, it will be the economically-dominant version of the ledger that most people will refer to as "Bitcoin." And in fact, language is a great analogy for Bitcoin / money. Language is a protocol for communicating all kinds of information, whereas money is a protocol for communicating credible information about value. Both language and money rely heavily on network effects. And the protocol for language is subject to change just as the Bitcoin's protocol is subject to change. But that doesn't mean that "forking" is necessarily going to be easy in either case. (e.g., "Stop trying to make 'fetch' happen.")



“We can agree to disagree. I view the consensus as sacred – the basic fundamental guarantee of the integrity of Bitcoin as money.”

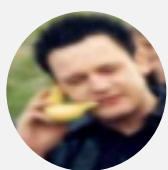
Well, of course. That’s the very nature of Bitcoin as a voluntary, open-source project. You’re free NOT to change the rules in the software you run / accept – just as everyone else is free TO change them. But if the rest of the world moves on without you, you might one day find yourself on a network of one. Sort of like if you were someone who had magically lived to the age of 10,000 but never changed their dialect from the one they learned as a child – probably no one would be able to understand you at this point.

“This is how Bitcoin fundamentally works. By accepting the longest valid chain as authoritative, you implicitly accept soft forks implemented by a mining majority.”

Well, sort of. The software you’re running will automatically “accept” a soft-fork, but YOU might not accept it, leading you to change the software you’re running. And in the case of a clearly malicious 51% attack like the two I outlined, we would of course hope that the economic majority would be able to coordinate a PoW change or other response to neutralize those attacks.

“I staunchly oppose a majority of mining power being used to coerce users to migrate networks against their will. Proponents of a hard fork block size increase often point to the ‘irrationality’ of remaining on the ‘minority’ chain. This explicitly suggests the leveraging of economic loss to force users to migrate.”

To use your own words, “this is how Bitcoin works.” But no one is ever truly “coerced” to migrate – again, because everyone can choose what software to run / what version of the ledger to value (including miners!) Having said that ... the network effect is obviously very, very important. And the “longest” (highest-PoW) chain is a very strong Schelling point about which the market is likely to converge in many cases, especially where the market views the updated protocol as an improvement over the original. Of course, if 51%+ of the hashpower makes a change via hard fork that’s clearly malicious (e.g., raising the 21M cap), it’s very easy for the market to simply ignore that chain. (Here again, we can note that malicious hard forks are much easier than malicious soft forks for users to resist.)



**MAbtc** August 31, 2016 at 7:21 pm **REPLY**

“But the economically-dominant rule set / version of the ledger is, by definition, always subject to the potential for change.”

That’s fine if you’re okay with undermining \_the\_ consensus ledger that runs from 2009 and ultimately migrating to a \_new\_ consensus ledger. Retaining the history and UTXO set doesn’t change that. Neither does a consensus-breaking fork that has more cumulative work. My argument is that mutable consensus rules fundamentally undermine the very basis for Bitcoin’s value

as the consensus rules are the only guarantee of a bitcoin's integrity. The same logic applies to increasing subsidy beyond 2 million bitcoins.

The operating term there is “economically-dominant.” The term moot in the context of a single consensus ledger which already exists. A new, incompatible consensus ledger is just a different ledger on a different network. In that context, the number of users and cumulative difficulty don't matter; there is no reason to directly compare them.

“Of course, in a sense, there ARE “consensus rules” but they're just Schelling points that are subject to change.”

As I said in my previous reply: “We can agree to disagree. I view the consensus as sacred – the basic fundamental guarantee of the integrity of Bitcoin as money.”

I'm not sure how repeating that these rules are subject to change addresses that. I'm not arguing that the rules cannot be changed \_in practice\_ I'm arguing that this would undermine the entire system.

“Do you just ignore it because any block you tried to mine it into would be ‘invalid’?”

Of course a rational miner would ignore it. Those block rewards are useless as they can't be spent on the Bitcoin network.

“Of course, I don't think the market / other miners WOULD view the block as ‘invalid.’”

I'm puzzled as to what software you think the Bitcoin network is running.

“Well, because that's how language works.”

That's all well and good, but it's not how consensus networks work. It's not how Bitcoin works. You can continue to use sophistry to avoid the facts, but intelligent people won't fall for it.

“But if the rest of the world moves on without you, you might one day find yourself on a network of one.”

Again with arguments that depend on leveraging fear of economic loss. My argument is \_not\_ that people won't attempt to hard fork Bitcoin. My argument is that hard forking undermines Bitcoin in every sense, and that we have \_no idea\_ how one will resolve - and what kind of effects that will have for peoples' and custodians' stored value, and their ability to easily and securely use the Bitcoin network.

“Well, sort of. The software you're running will automatically “accept” a soft-fork, but YOU might not accept it, leading you to change the software you're running.”

Okay. As Satoshi said: “Nodes can leave and rejoin the network at will.” Go ahead and leave the network.

“But no one is ever truly “coerced” to migrate”

Economists, sociologists and game theorists may argue over the term “economic coercion” and its application. Out of laziness, here is the top Yahoo answer from the top Google result: “Economic coercion is when a controller of a vital resource uses his advantage to compel a person to do something he would not do if this resource were not monopolized.” In this case, the vital resource refers to hash power (in relation to Bitcoin’s difficulty algorithm and the need of users for confirmed transactions). That is exactly the intention of vote thresholds like 75% – to coerce the minority of miners. A sufficient mining monopoly can then coerce the userbase as a function of their need for confirmed transactions.

“Of course, if 51%+ of the hashpower makes a change via hard fork that’s clearly malicious (e.g., raising the 21M cap), it’s very easy for the market to simply ignore that chain.”

It’s far more interesting to consider this scenario in a future context, when the userbase may be less opposed to the idea of removing the 21 million cap – for example, for need of mining security incentive or to dilute the wealth of early adopters.



**Roger\_Murdock** September 1, 2016 at 3:10 am

“My argument is that mutable consensus rules fundamentally undermine the very basis for Bitcoin’s value, as the consensus rules are the only guarantee of a bitcoin’s integrity.”

Ok, but the “consensus rules” ARE mutable in the sense that the ability of anyone who wants to to hard fork is inherent in Bitcoin’s very nature. So the only “guarantee” of Bitcoin’s integrity is not any particular version of “the” consensus rules that you’d like to imagine are set in stone, but rather the market / the game-theoretic incentives of market participants. It sounds like you think the market needs to internalize this idea of “no hard forks ever” as a safeguard against certain doom. In other words, it sounds like your thought process is: “if we can just get Bitcoin stakeholders to widely internalize the idea that hard forks are never acceptable, that will act as a strong bulwark against improvident and value-destroying hard forks.” And I suppose that would. But it would ALSO act as an obstacle to the implementation of necessary and value-enhancing protocol changes. In other words, your proposed norm is overly broad. It seems to me that the norm you ACTUALLY want is SOME level of general bias against protocol changes (“we shouldn’t make changes to the Bitcoin protocol unless we’re sure there’s a very good reason for doing so” / “if it ain’t broke don’t fix it” combined with some even stronger skepticism regarding changes to features of Bitcoin that are viewed as especially important (e.g., the 21M supply cap). And the specific bias



against “hard forks” is also just inexplicable to me when I consider that malicious or misguided soft forks can be every bit as damaging. And indeed (and again – sorry to repeat myself), malicious / misguided soft forks strike me as MORE dangerous because of the greater difficulty that honest actors face in neutralizing them. After all, the archetypal “doomsday attack against the Bitcoin network, the “51% attack,” is just one kind of malicious soft fork!

“The operating term there is ‘economically-dominant.’ The term is moot in the context of a single consensus ledger which already exists. A new, incompatible consensus ledger is just a different ledger on a different network. In that context, the number of users and cumulative difficulty don’t matter; there is no reason to directly compare them.”

Ok, but it’s trivial to spin up a hard fork / spinoff and start mining on it – although you and maybe one of your bored friends might be the only people who are using it. But if an economically-meaningful hard fork ever DOES happen and most people end up migrating to it, then, at least in the eyes of most of the world, that new chain is going to be “Bitcoin.” The stragglers on the rump chain are free to declare that they’re the only ones using the “real” Bitcoin. But as a practical matter, that’s like me declaring that Dogecoin is the real Bitcoin. Heck, just look at which chain had to rebrand following the ETH / ETC fork – the economic minority one even though that’s the chain that’s using the original rule set!

“we have \_no idea\_ how one will resolve – and what kind of effects that will have for peoples’ and custodians’ stored value and their ability to easily and securely use the Bitcoin network.”

Well, we have SOME idea in light of the ETH / ETC split. It caused some confusion. Some exchanges that weren’t prepared lost some funds. But overall, it wasn’t apocalyptic or anything and in fact, the combined market cap of the two chains post-fork was higher than the single chain’s pre-fork market cap, which seems to support my hypothesis that we should only expect persistent / semi-persistent splits to occur when the benefits outweigh the costs. (The costs are the loss of network effect / ecosystem disruption. The benefits are the ability of more people to satisfy their preferences with respect to protocol operation.) And it was also a learning experience. It seems likely that if hard forks become more common, people in the space will get better at dealing with the practical issues that arise (and maybe they’ll also learn how important the network effect is). How will it play out long-term? Who knows? I tend to think one chain will dominate over the other given the extraordinary importance of the network effect. (Of course, over the very long term, I doubt the viability of either chain as the entire project seems pretty ill-conceived to me.) Also consider that the ETH / ETC split was the result of a

fundamentally-irreconcilable dispute regarding the ledger’s integrity as opposed to a potentially-resolvable dispute regarding a particular protocol feature (e.g., bigger blocks) that could always be added later.

“I’m puzzled as to what software you think the Bitcoin network is running.”

The question isn’t what software network participants are currently running. The question is what changes to their software (if any) they would make in the event of my hypothetical. I certainly know what I’d do if I were a major pool operator.

“That’s all well and good, but it’s not how consensus networks work. It’s not how Bitcoin works. You can continue to use sophistry to avoid the facts, but intelligent people won’t fall for it.”

Well, I don’t see how my analogy is “sophistry.” It’s just an analogy that I happen to be fond of. Is it a perfect analogy? Well, no because analogies never are. But, to expand on my analogy since I really do love it, it seems to me that your view of Bitcoin (referring to “the” software and claiming that it requires “immutable consensus rules”) is sort of like the people who treat “the dictionary” as the definitive guide to whether or not a word is “real.” And thinking that “soft forks” and “new rules” are acceptable but that “hard forks” aren’t is sort of like being ok with adding new words to “the dictionary” but trying to stop people from repurposing old words (because the latter can result in ambiguity / a “split” in how you’re understood by different people depending on whether they’ve “updated the language protocol”).

“Okay. As Satoshi said: ‘Nodes can leave and rejoin the network at will.’ Go ahead and leave the network.”

Well, you can obviously call it whatever you like. To me, a more accurate characterization would be “the network routing around an attack.” Because to me, “the network” isn’t defined by one particular rule set with this weird ratchet-like characteristic where rules can only be added but never subtracted. Rather, “the network” is a network of economic participants using an inherently-fluid protocol to maintain and update a shared monetary ledger.

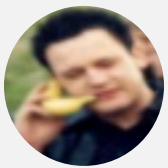
“That is exactly the intention of vote thresholds like 75% – to coerce the minority of miners. A sufficient mining monopoly can then coerce the userbase as a function of their need for confirmed transactions.”

Eh... or their intention is just to use the protocol they prefer. (You’re not suggesting we force them not to run the software they want to?) Look, if you want to call that “coercion,” sufficient it to say that it’s the kind I’m A-OK with. To me, complaining about “coercion” in that scenario is sort of like my imaginary

10,000-year-old man complaining that he's being continually "coerced" into changing the language he speaks. (BTW, I just watched an interesting YouTube video called "How far back in time could you go and still understand English?" and apparently the answer is only like 600 years before things start getting really dicey.)

"It's far more interesting to consider this scenario in a future context, when the userbase may be less opposed to the idea of removing the 21 million cap – for example, for need of mining security incentive or to dilute the wealth of early adopters."

Well, ok sure. Again, people are always going to be able to run the software they want and value the ledger they choose. So you don't really have any choice but to trust the market to guard against unwise changes.



**MAbtc** September 1, 2016 at 11:56 am **REPLY**

In reply to Roger\_Murdock:

"Ok, but the 'consensus rules' ARE mutable in the sense that the ability of anyone who wants to to hard fork is inherent in Bitcoin's very nature."

No, that doesn't suggest that consensus rules are mutable at all. It suggests that you can opt out of the network.

"So the only 'guarantee' of Bitcoin's integrity is not any particular version of 'the' consensus rules that you'd like to imagine are set in stone, but rather the market / the game-theoretic incentives of market participants. It sounds like you think the market needs to internalize this idea of 'no hard forks ever' as a safeguard against certain doom."

This is not a matter of markets. This is a matter of philosophy and ethics. Prominent executives and developers have continually repeated the idea that miners have the authority to change consensus rules. I simply want to state my rejection of that idea – that it fundamentally violates user consent. No one should feel forced to migrate networks as a matter of hash power. But the inability to get transactions confirmed in a timely manner (in the context of a massive drop in hash rate) is the mechanism to force users' hands.

"But it would ALSO act as an obstacle to the implementation of necessary and value-enhancing protocol changes. In other words, your proposed norm is overly broad. It seems to me that the norm you ACTUALLY want is SOME level of general bias against protocol changes ("we shouldn't make changes to the Bitcoin protocol unless we're sure there's a very good reason for doing so" / "if it ain't broke don't fix it") combined with some even stronger skepticism regarding changes to features of Bitcoin that are viewed as especially important (e.g., the 21M supply cap)."



You appear to approach this as a pragmatist above all else. I can respect that, but in the plainest terms, what I am saying is: the ends \_do not\_ justify the means. Attempting to break the consensus of millions of users via miner attack is ethically unacceptable. I believe we are at an impasse in that regard.

“And the specific bias against ‘hard forks’ is also just inexplicable to me when I consider that malicious or misguided soft forks can be every bit as damaging. And indeed (and again – sorry to repeat myself), malicious / misguided soft forks strike me as MORE dangerous because of the greater difficulty that honest actors face in neutralizing them.”

Sufficiently centralized miners can attack us via soft fork at will. At any time. That’s supposed to be neutralized by mining incentive – this is how the protocol works. I’m puzzled as to why you keep railing against soft forks, when you \_already\_ implicitly accept them by accepting the longest valid chain.

You keep implying that soft forks are themselves attacks. If a soft fork update is backward compatible and doesn’t censor you in any way, what kind of attack are you talking about, exactly? Are you opposed to the implementation of Segwit, for instance?

I’m just trying to work within the parameters of the software. Nodes accept the longest valid chain. That means that for better or worse, nodes accept soft forks implemented by a majority of miners. Nothing in the software tells me to remove consensus rules when some miners tell me to. That requires opting out of the network.

Opting in and out of the network is the basis for consensus. You are free to opt out and hard fork at any time. But \_our consensus\_ is not mutable. Opt in/opt out.

“But if an economically-meaningful hard fork ever DOES happen and most people end up migrating to it, then, at least in the eyes of most of the world, that new chain is going to be ‘Bitcoin.’ The stragglers on the rump chain are free to declare that they’re the only ones using the ‘real’ Bitcoin. But as a practical matter, that’s like me declaring that Dogecoin is the real Bitcoin.”

I’m not sure that’s immediately clear. In any case, you are casually suggesting that splitting Bitcoin into multiple surviving networks is acceptable. I think that will force massive liabilities on users (particularly SPV users) and custodians. To iterate, we cannot possibly know how a hard fork will resolve. It simply isn’t possible to know. Trying to argue otherwise is like trying to establish causality in macroeconomics. There are far too many variables at play.

And there is legitimate concern that a clearly dominant chain will not emerge. Are you okay with two Bitcoins? How about six? What’s the supply again?

Again, your arguments hinge on economic coercion. I am ethically opposed. You are free to hard fork to whatever system you’d like. I’m not sure why you feel the need to come here and refer to us as

“stragglers on the rump chain” and compare our network to Dogecoin, though, if not to reinforce the idea that “it’s irrational to remain on the minority chain” and therefore attempt to leverage fear of economic loss to convince users to migrate networks. We are at another impasse. You won’t convince me that the longest invalid chain is valid – and particularly not with a fallacious bandwagon argument that attempts to reduce Bitcoin to Dogecoin.

“Heck, just look at which chain had to rebrand following the ETH / ETC fork – the economic minority one even though that’s the chain that’s using the original rule set!”

So, you are pointing to ETH as a success story here? The losses incurred (by both users and custodians) in replay attacks alone makes the idea laughable. Not sure it’s a worthy comparison either. Arguably, the Ethereum Foundation (closed, corporate, no public consensus-driven decision mechanism) is a very centralizing force in Ethereum development, and Vitalik “I am working 100% on ETH” Buterin holds a particular influence over ETH which is unparalleled by anyone in Bitcoin. Further, the hard fork exposed the overwhelming centralization of ETH mining. All mining pools enforced the fork based on a minority of hash rate, and one pool even violated its miner vote. Further, the developers of all major ETH clients forked \_by default\_ without offering users any choice in the matter. “Upgrade or we no longer support your client.” Every means to prevent users from having any say in the fork was employed. There is no comparing this to Bitcoin.

“But overall, it wasn’t apocalyptic or anything and in fact, the combined market cap of the two chains post-fork was higher than the single chain’s pre-fork market cap, which seems to support my hypothesis that we should only expect persistent / semi-persistent splits to occur when the benefits outweigh the costs.”

So, you’re comparing a network split in an altcoin to a network split in Bitcoin? And then praising the idea because of the market price on a particular day? In any case, the combined market cap is significantly lower than ETH’s market cap was prior to the DAO debacle – not that this matters one bit.

Different value propositions, different positions in the ecosystem, different userbase, different context. Do you really think that your data set of \_one\_ convinces anyone that the market cap of Bitcoin(s) won’t fall in a network split? (As if that were even the issue)

“Also consider that the ETH / ETC split was the result of a fundamentally-irreconcilable dispute regarding the ledger’s integrity as opposed to a potentially-resolvable dispute regarding a particular protocol feature (e.g., bigger blocks) that could always be added later.”

You can claim this dispute is resolvable, but I’ve written a lengthy article and several responses directly to you explaining exactly why it is not. Indeed, my points are not about the technical risks posed

by an increased maxblocksize – there are numerous, a few of which were touched on in the article – but the broader ethical problems and risks associated with any consensus break.

“The question isn’t what software network participants are currently running.”

Yes it is. That is the only question. The software defined the consensus ledger. The consensus ledger defines the software.

“it seems to me that your view of Bitcoin (referring to ‘the’ software and claiming that it requires ‘immutable consensus rules’) is sort of like the people who treat ‘the dictionary’ as the definitive guide to whether or not a word is ‘real.’ And thinking that ‘soft forks’ and ‘new rules’ are acceptable but that ‘hard forks’ aren’t is sort of like being ok with adding new words to ‘the dictionary’ but trying to stop people from repurposing old words (because the latter can result in ambiguity / a ‘split’ in how you’re understood by different people depending on whether they’ve ‘updated their language protocol’).”

More irrelevant analogies.

“Rather, ‘the network’ is a network of economic participants using an inherently-fluid protocol to maintain and update a shared monetary ledger.”

That’s certainly not how the software works. So it seems you are just attaching some arbitrary definition. Bitcoin is now an “inherently fluid protocol?” How so? Are we just throwing immutability out the window entirely now? Enforcement of consensus is the precise opposite of “fluid.” No consensus changes since 2009, yet you have the audacity to call consensus “fluid?” Simply repeating that the consensus rules \_everyone else\_ agreed to are mutable based on (your? some miners’?) say-so, simply isn’t compelling.

“Eh... or their intention is just to use the protocol they prefer. (You’re not suggesting we force them not to run the software they want to?) Look, if you want to call that coercion”

Um. This is what I said:

“Proponents of a hard fork block size increase often point to the ‘irrationality’ of remaining on the ‘minority’ chain. This explicitly suggests the leveraging of economic loss to force users to migrate.”

“Economic coercion is when a controller of a vital resource uses his advantage to compel a person to do something he would not do if this resource were not monopolized.’ In this case, the vital resource refers to hash power (in relation to Bitcoin’s difficulty algorithm and the need of users for confirmed transactions). That is exactly the intention of vote thresholds like 75% – to coerce the minority of miners. A sufficient mining monopoly can then coerce the userbase as a function of their need for confirmed transactions.”

If your arguments are not based in coercing users to migrate, then stop appealing to the rationality of migrating to the majority chain (and the irrationality of being a “straggler” on the “rump chain”). If

this is \_only\_ about “using the protocol they prefer” (your words), then stop using bandwagon arguments about the inevitable victory of the hard forked chain. You seem convinced that one chain will dominate; there is no such relationship among incompatible networks. Hence why Ethereum Classic survived despite a 99:1 miner distribution. Miner distribution doesn’t matter across incompatible networks. Have you noticed how no one talks about ETH hash rate vs. ETC hash rate anymore? Because it doesn’t matter. There is no “dominant” chain. There are simply two networks. I have zero interest in multiple Bitcoin networks.

“Again, people are always going to be able to run the software they want and value the ledger they choose. So you don’t really have any choice but to trust the market to guard against unwise changes.”

No. I don’t trust the market. I don’t trust democracies. I trust my full node. Feel free to opt out of my network; break the rules and my node will do it for you.

You will never convince me to trust miners, nor the market. I trust only the software, which ensures that I don’t need to trust anyone at all.



**Rosemary** September 1, 2016 at 6:33 pm **REPLY**

If you are interested in topic: best ways to make money in charlotte nc – you should read about Bucksflooder first



**Roger\_Murdock** September 2, 2016 at 5:07 am **REPLY**

In response to MAbtc:

Well, I suspect we’re reaching the point of diminishing returns where we’re both going to be mostly repeating ourselves and wondering why the other guy still doesn’t get it. So yeah, we may have to agree to disagree on this one, but I’ll try at least one more shot to see if I can bring you around to my way of thinking.

“No, that doesn’t suggest that consensus rules are mutable at all. It suggests that you can opt out of the network.”

This seems like semantics to me. You’re basically claiming that “consensus rules” are “immutable” because you’re choosing to define “consensus rules” that way. So apparently, it wouldn’t matter to you if 100% of users and miners (or maybe just 99.9%) all gladly decided to switch to a new rule set via a hard fork because they all recognized the advantages of the change over the status quo. From your perspective, everyone in that scenario would be guilty of the sin of “breaking the immutable consensus,” and you’d consider them all to have left “the network” and started some sort of “alt-coin.” And again, from MY perspective, that makes no sense because the most meaningful way to think about “the network” is as a network of economic participants maintaining a shared ledger.



Also, this claim in the article that the “new rules” of a soft fork aren’t “consensus rules” is just bizarre to me. If that’s really the case, then UNWINDING one of these “new rules” (i.e., a rule that was previously added via a soft fork) shouldn’t “violate consensus,” correct? In other words, if a “new rule” isn’t a “consensus rule” when it’s being added, it shouldn’t suddenly become one when you try to remove it. And so (for example) removing the 1-MB block size limit that was added as a “new rule” in 2010 shouldn’t now be seen as problematic.

“This is not a matter of markets. This is a matter of philosophy and ethics.”

Of course this is a matter of markets! If we could rely on managers of a currency to act “ethically,” we could stick with fiat! The whole idea behind Bitcoin as a “trustless” form of money is that you DON’T have to trust participants to act “ethically.” You rely instead on their self-interest and the game-theoretic incentives of the system’s design. The good news here is that it’s not in miners’ interest to fork themselves onto a chain that other people aren’t going to value.

“Prominent executives and developers have continually repeated the idea that miners have the authority to change consensus rules. I simply want to state my rejection of that idea – that it fundamentally violates user consent. No one should feel forced to migrate networks as a matter of hash power. But the inability to get transactions confirmed in a timely manner (in the context of a massive drop in hash rate) is the mechanism to force users’ hands.”

Well, miners don’t have any “authority to change [THE] consensus rules” (because there is no “official” set of consensus rules), but they certainly DO have the right to run the software they want. You don’t own their hardware. They can shut it off if and when they want to. They can use it to start mining a true “alt-coin” with a brand new genesis block. Or they can use it to mine a “fork” / “spinoff” of the Bitcoin ledger. It’s true that in the last scenario, the importance of the network effect may incentivize people to follow those miners to the new chain, but that doesn’t mean that the miners are acting “coercively.” After all, if the vast majority of users DON’T migrate to the new chain and instead, the market continues to value the original chain, THAT will have the effect of incentivizing the miners to RETURN to mining the original chain. In that case, are the users and investors “coercing” the miners not to change their software? Of course not.

To me, this is sort of like if every year you meet your friends at a certain beach for a joint vacation. And you have a sweet boat that you always bring and that everyone parties on. And one year you’re like, “you know guys, I think actually I want to go a different beach this year. You’re all welcome to join me, but if you want to stick with your usual place, that’s cool too. I’ll understand.” And then one of your friends is like, “WTF, dude? But I want to party on your boat. You’re ‘coercing’ me to go to a different beach, and I consider that to be highly ‘unethical.’” Who’s the jerk in that situation?

“Attempting to break the consensus of millions of users via miner attack is ethically unacceptable.”

Calling a hard fork a “miner attack” is assuming your conclusion. And again, if we have to rely on market actors to act “ethically,” then Bitcoin is doomed.

“I’m puzzled as to why you keep railing against soft forks, when you \_already\_ implicitly accept them by accepting the longest valid chain.”

Well, I’m NOT really “railing against soft forks.” They’re probably fine in cases where (a) the protocol change in question is truly non-controversial (i.e., no one would WANT to break away as a result of it) and (b) the nature of the change lends itself naturally to implementation via soft fork (i.e., the soft fork isn’t a klugey “hack” to avoid a much simpler hard fork). My real point is just that hard forks are LESS of a threat than soft forks because, in the case of a malicious change, the former are far easier for honest actors to resist. And again, the SOFTWARE you run may automatically “accept” a soft fork regardless of how malicious it is, but YOU may not, leading you to change the software you’re running to thwart the attack (in a coordinated manner with other market participants).

“You keep implying that soft forks are themselves attacks. If a soft fork update is backward compatible and doesn’t censor you in any way, what kind of attack are you talking about, exactly? Are you opposed to the implementation of Segwit, for instance?”

No, like I said above, soft forks are probably fine in some situations, but soft forks, by their nature, lend themselves to attacks in a way that hard forks don’t. I haven’t studied the Segwit soft fork proposal that closely, but my inclination is to oppose it because my understanding is that (a) it’s the kind of “hack” I just said we should avoid, and (b) it creates an arbitrary, economics-changing discount for witness data.

“And there is legitimate concern that a clearly dominant chain will not emerge. Are you okay with two Bitcoins? How about six? What’s the supply again?”

I think that concern is overblown and fails to appreciate the overwhelming importance of the network effect. Am I “ok” with two / six / twenty “Bitcoins”? I’m ok with as many persistent splits as the market is ok with. Because obviously it’s not really up to me. Which chains will I personally value / accept? Well, the one or ones that I predict that other people will value. That’s the inherently-speculative nature of all money. You want to hold the money that you predict others will want to hold in the future (when you’re trying to trade that money for goods and services).

“So, you are pointing to ETH as a success story here?”

Well, I wouldn’t point to ETH as a success story. (I think I mentioned above that I’m pretty skeptical of the entire project). And you obviously wouldn’t point to the debacle that led to the hard fork as

a success. But the hard fork itself that resulted in an (at least so far) persistent chain split, yeah that seemed to go reasonably well (and it also provided useful experience to the crypto ecosystem that should help future hard forks go even better).

“Do you really think that your data set of \_one\_ convinces anyone that the market cap of Bitcoin(s) won’t fall in a network split? (As if that were even the issue)”

Well, it’s certainly better than NO empirical data. But my intuition is that the market is unlikely to allow a meaningful persistent split that would result in serious harm to Bitcoin’s market cap. And I do think that IS the issue. Bitcoin is a market phenomenon. It is in stakeholders’ interests to act in a way that promotes an increased value for their holdings. And 99.9% of the time I think that’s going to mean avoiding an economically-meaningful persistent split because of the overwhelming importance of the network effect.

“You can claim this dispute is resolvable, but I’ve written a lengthy article and several responses directly to you explaining exactly why it is not.”

Well, it might not be COMPLETELY resolvable. Certainly, we can imagine that there will be small groups that hard fork themselves away from “the herd” to obtain the new protocol they want, as well as small groups that refuse to join in a mass migration to an updated protocol. But the network effect is a beast. So in general, I think the herd will stick together (and I don’t think that means staying on the current trajectory indefinitely – although the status quo is always a powerful Schelling point).

“Yes it is. That is the only question.”

No, not at all. And certainly not in the context of the hypothetical we were discussing. A rational miner wants his computer to produce the string of 0’s and 1’s that’s going to be exchangeable by him in the future for the most value. Obviously the “current software” is a very strong Schelling point and thus, generally, a very intelligent guess as to what’s going to produce that sequence. But I think my hypothetical scenario would be very likely to produce a shift in the most powerful Schelling point, leading miners to coordinate a change to the software they’re running.

“More irrelevant analogies.”

What? Those analogies are pure gold! 😊

“That’s not how the software works. So it seems you are just attaching some arbitrary definition. Bitcoin is now an ‘inherently fluid protocol?’ How so? Are we just throwing immutability out the window entirely now? Enforcement of consensus is the precise opposite of ‘fluid.’ No consensus changes since 2009, yet you have the audacity to call consensus ‘fluid?’ Simply repeating that the consensus rules \_everyone else\_ agreed to are mutable based on (your? some miners’?) say-so, simply isn’t compelling.”

Forget “the” software. The software is just a TOOL for a NETWORK

OF HUMAN BEINGS to reach agreement on a shared monetary history. The tool can change. Obviously, the task of coordinating certain kinds of changes to that tool is tricky, so we shouldn't expect changes to be made lightly or frequently. But if a vastly-superior tool is discovered, or if the current tool starts to malfunction, if a 51% attack / malicious soft fork occurs or a significant vulnerability in Bitcoin's cryptography is discovered, we should absolutely expect that this network of economically-rational human beings will shift to a new tool while preserving the continuity and integrity of the all-important ledger.

"Hence why Ethereum Classic survived despite a 99:1 miner distribution."

If it's true that the initial mining distribution was that lopsided and the chain still survived, that's great news! Because it suggests that despite the fact that miners badly misjudged investor sentiment, the market still prevailed. (Miners are at best a proxy for investors.) But look, the fact that ETC has a certain non-trivial value means that there are a number of people out there who currently place value on it. And the same is true of ETH. Again, I tend to think BOTH sets of investors are misguided, but I'm not the market. I'm just one individual. And I'm certainly not going to begrudge anyone the right to use and value the cryptocurrency they choose.

"No. I don't trust the market. I don't trust democracies. I trust my full node."

Well, ok but in the real world, that's not good enough because money is a network good. Again, if the rest of the world moves on, you could find yourself "trusting a full node" that's no longer connected to anyone else because it's using a rule set that's been rendered completely obsolete. You're the 10,000-year-old man speaking what everyone else considers to be gibberish.



**MAbtc** September 2, 2016 at 9:34 pm **REPLY**

"Well, I suspect we're reaching the point of diminishing returns where we're both going to be mostly repeating ourselves and wondering why the other guy still doesn't get it. So yeah, we may have to agree to disagree on this one, but I'll try at least one more shot to see if I can bring you around to my way of thinking."

I agree. Ditto.

"This seems like semantics to me. You're basically claiming that 'consensus rules' are 'immutable' because you're choosing to define 'consensus rules' that way."

It's only a semantic issue if you argue that "consensus" is not based on "agreement." Consensus flows from users - who else? Their agreement can only be established by opting in to the network, which has defined rules. Users do not define these rules; they agree to them.

You can opt out if you disagree. Since a network is composed of its participants, opting out means that you are no longer part of the network. Can other people also opt out and join \_your\_ network? Sure. But it's a distinctly different network – and you opting out of \_my\_ network doesn't change the rules of the \_my\_ network. You cannot change \_other peoples'\_ consensus rules, by definition; you cannot change the software that \_I\_ run. That is why consensus is immutable.

In other words, a hard fork doesn't mean that the consensus rules have \_changed\_ (both networks may very well still exist) – it simply means that an additional network with different rules now exists. This is a factual matter, not an issue of semantics.

“From your perspective, everyone in that scenario would be guilty of the sin of ‘breaking the immutable consensus,’ and you consider them all to have left ‘the network’ and started some sort of ‘alt-coin.’”

As stated in the article, I believe there are narrow conditions to achieve a hard fork when we know *prima facie* that all users are incentivized to support it.

I am not arguing that a hard fork will never occur – nor that this hard fork will not be valued by the market. But yes, a hard fork creates an “alt-coin” for better or worse. I argue that since consensus flows from users, that users should be wary of migrating to that alt-coin based purely on the actions of several mining pools. If consent to a hard fork \_actually\_ flowed from the users, a miner vote would be inconsequential. Further, I argue that most hard forks will result in network splits (unless they are implemented as firm forks, which are incredibly unethical as they depend on a literal 51% attack). I am arguing that a sustained network split would irreparably harm Bitcoin's value proposition, cause real losses for users and custodians, and significantly erode trust (from both users and the public) in Bitcoin's ability to maintain integrity as money and a store of value.

Your replies continue to echo the idea that “network splits are good” – agree to disagree.

“And again, from MY perspective, that makes no sense because the most meaningful way to think about ‘the network’ is as a network of economic participants maintaining a shared ledger.”

Incompatible networks do not share a ledger. You're talking about breaking into multiple ledgers. This is a technical problem that does not fit into this social conception.

“And so (for example) removing the 1-MB block size limit that was added as a ‘new rule’ in 2010 shouldn't now be seen as problematic.”

This is a technical matter. It requires a hard fork.

“Of course this is a matter of markets! If we could rely on



managers of a currency to act ‘ethically,’ we could stick with fiat. The whole idea behind Bitcoin as a ‘trustless’ form of money is that you DON’T have to trust participants to act ‘ethically.’ You rely instead on their self-interest and the game-theoretic incentives of the system’s design.”

I don’t know what you mean by “managers” but the full node security model protects your money from unethical policy changes, like debasement. A decentralized network of full nodes is what allows trustlessness. That is the system’s design.

“The good news here is that it’s not in miners’ interest to fork themselves onto a chain that other people aren’t going to value.

That’s good but it’s very important to note that how users define the network should not be based on miners’ interests. The rational mining incentive is intended to secure users’ transactions. There is no reciprocation there: users do not opt into the Bitcoin network to serve the interests of miners. Consensus must flow from users. Miners should be seen as completely irrelevant to these discussions, beyond the extent to which they run nodes.

“Well, miners don’t have any ‘authority to change [THE] consensus rules’ (because there is no ‘official’ set of consensus rules), but they certainly DO have the right to run the software they want.”

There is an official set of consensus rules; they underpin the one Bitcoin ledger. A change to those consensus rules will create a new ledger, distinct from the original.

Anyone can run any software they want. They can opt out of the Bitcoin consensus network and create a new consensus network based on a different set of rules. This is a hard fork. I am not attempting to deny anyone’s right to do that. I am just trying to make clear that a) consensus flows from users, not miners and b) a network split can do significant and irreparable harm.

“After all, if the vast majority of users DON’T migrate to the new chain and instead, the market continues to value the original chain, THAT will have the effect of incentivizing the miners to RETURN to mining the original chain. In that case, are the users and investors ‘coercing’ the miners not to change their software? “Calling a hard fork a ‘miner attack’ is assuming your conclusion.

The primary market mechanism at play is rational incentive to mine user transactions into blocks. So miners follow users; their blocks have no value on a dead network, as you’ve pointed out. But the only rational incentive users have to follow miners (onto a different network) is for fear that slow confirmations/low hash rate will destroy the value of their money. Users depend on miners for confirmed transactions; this is a vital resource.

What we are talking about is a handful of centralized mining pools leveraging a perceived monopoly on hash power to

provoke user action. It is very possible, then, that users are not consenting at all by migrating. This is analogous to the matter of consent vs. coercion in cases of rape. The lack of literal force does not imply consent of the other party. I am stressing that user consent is paramount to anything in this discussion – and particularly to miners’ interests. We should not look to the interests of miners for anything; their incentives are already provided for.

Miners are only concerned with their own rational interests. They are here to make profit. Since `_users_` define the network, hash rate votes should be ignored on the basis that they say very little about users.

“To me, this is sort of like if every year you meet your friends at a certain beach for a joint vacation.”

Where is the monopoly in this scenario? It seems there are no “miners” in this analogy.

“My real point is just that hard forks are LESS of a threat than soft forks because, in the case of a malicious change, the former are far easier for honest actors to resist.”

Hard forks are easy to resist on a technical level because the software rejects them automatically. What makes them harder to resist is the widespread misbelief that profit-motivated companies and mining pools should have any say over consensus rules (user consent).

“And again, the SOFTWARE you run may automatically ‘accept’ a soft fork regardless of how malicious it is, but YOU may not, leading you to change the software you’re running to thwart the attack (in a coordinated manner with other market participants)

Indeed. If miners are 51% attacking the network in perpetuity, Bitcoin’s fundamental incentive mechanism has failed. As you acknowledge here, you can then opt out of the network. These circumstances are fairly aligned with the “existential protocol failure” scenario mentioned in the article.

“I haven’t studied the Segwit soft fork proposal that closely, but my inclination is to oppose it”

Oh.

“it creates an arbitrary, economics-changing discount for witness data.”

It’s not arbitrary. It’s based on the capacity changes.

“I think that concern is overblown and fails to appreciate the overwhelming importance of the network effect. Am I ‘ok’ with two / six / twenty ‘Bitcoins’? I’m ok with as many persistent splits as the market is ok with.”

Exhibit A: Ethereum and Ethereum Classic.

Well, we are at an impasse here. I've stated why a network split is likely and why it would be very harmful to Bitcoin. To the extent that we can avoid such a split, we should.

"Which chains will I personally value / accept? Well, the one or ones that I predict that other people will value. That's the inherently-speculative nature of all money. You want to hold the money that you predict others will want to hold in the future (when you're trying to trade that money for goods and services)

This is why the idea of economic coercion is so relevant here. Fundamentally threatening the value of a holders' money is the rational basis for forcing a network migration. "No one wants to be left on the minority chain" means specifically that miners have ultimately decided, not users. This is why I want to stress to readers that there is no such thing as "majority/minority chains" in a hard fork. There are merely multiple networks.

"But my intuition is that the market is unlikely to allow a meaningful persistent split that would result in serious harm to Bitcoin's market cap. And I do think that IS the issue."

Bitcoin's fiat market cap is not the issue at all. A permanent network split would be far more detrimental than a hit to the market cap, as stated above. Good discussion of those implications here: <http://diyhpl.us/wiki/transcripts/2016-july-bitcoin-developers-miners-meeting/cali2016/>

"And 99.9% of the time I think that's going to mean avoiding an economically-meaningful persistent split because of the overwhelming importance of the network effect."

That suggests that hard forks will never be contentious - that the incentive you point to overrides all other concerns of every user. I assert the opposite, and lay out the case for it in the article.

"But I think my hypothetical scenario would be very likely to produce a shift in the most powerful Schelling point, leading miners to coordinate a change to the software they're running."

Who cares what miners do? Consensus flows from users, not hash rate.

"Forget 'the' software. The software is just a TOOL for a NETWORK OF HUMAN BEINGS to reach agreement on a shared monetary history. The tool can change."

You can change the software you run. That doesn't re-define what Bitcoin is. Someday, we may all leave Bitcoin behind for a better system. Indeed, the tool can change.

All of your arguments basically amount to "Bitcoin = what the market decides, today." If that's true, the 21 million BTC supply limit hasn't a chance in hell. By function of the inflation rate, future users have incentive to dilute the holdings of early adopters. By doing so, they can increase their percentage of the total supply - and as time goes on, an increasing proportion of

the network would benefit from this. As adoption increases, users' per capita holdings decrease (distribution), increasing the incentive of each user to redistribute wealth. Compared to a decreasing inflation rate, they would also benefit from a proof-of-work security perspective. As time divorces the current network from domination by early adopters, the incentive to steal from early adopters increases. If the rules don't matter – only the market does – a majority of rational participants would find such changes acceptable.

If we do not emphasize the importance of the system's rules, retaining the system's integrity from majority rule becomes more and more difficult. Think of the consensus rules as the Constitution: there must be rules that are safe from the tyranny of the majority.

“Again, I tend to think BOTH sets of investors are misguided, but I'm not the market. I'm just one individual. And I'm certainly not going to begrudge anyone the right to use and value the cryptocurrency they choose.”

Opting in and out of a network is a user's right. I am talking about the damage a permanent network split will cause, and the importance of user consent vs. miner provocation.

“Well, ok but in the real world, that's not good enough because money is a network good. Again, if the rest of the world moves on, you could find yourself 'trusting a full node' that's no longer connected to anyone else because it's using a rule set that's been rendered completely obsolete. You're the 10,000-year-old man speaking what everyone else considers to be gibberish.”

You continually present this bandwagon argument to make people fearful of remaining on the “minority” chain. “Everyone is going to switch, you better switch now, or you're going to lose money!” is fallacious on its face. It's also coercive on its face. Coercion is based in threats, and we are specifically discussing inducing threats to the value of a holder's money in order to provoke a redefinition of Bitcoin.

What I am saying is \_not\_ that you must restrict yourself to a dead network. Anyone can opt in or out of any network they please.

What I'm saying to users is: The decision is not up to miners – it's up to you. Don't let your “consent” be defined by miners. Bitcoin's security model is set up exactly to protect you from miners. **DO NOT TRUST THEM.**

Also, to be clear, hash rate across Bitcoin forks is not a zero sum matter. I assure you that I, as a non-miner, am not alone when I say that I will be mining the original chain immediately after the fork (in the near term via mining contracts). If you think I am alone in believing in the importance that consensus holds for the integrity of Bitcoin as money, I believe you are in for a very rude awakening on fork day.



**Stevie** September 4, 2016 at 3:15 am **REPLY**

If you are interested in topic: make money zynga poker – you should read about Bucksflooder first

Your email address will not be published.

*Name\**

*Email\**

*Website*

POST COMMENT

# Stay Updated



Bringing the latest news in the bitcoin and cryptocurrency industry.



## RECENT POSTS



Ethereum Classic: A Masterpiece in the Making



**\*\*UPDATE\*\* ETC/DAO stolen coins frozen by exchanges was sent by Ethereum Foundation Developers**

Bitcoin: Blind Men and Elephants by

## POPULAR POSTS



**\*\*UPDATE\*\* ETC/DAO stolen coins frozen by exchanges was sent by Ethereum Foundation Developers**



Ethereum Classic: A Masterpiece in the Making

Why Bitcoin is the Best Hope for the





HassanMirakhor



Denationalization of Money

