



**Vitalik Buterin**  
@VitalikButerin

Thread Reader App  
14 tweets  
22 Jan 2018 16:50

My conclusion from yesterday's polls: people have very underdeveloped intuitions about how bad various kinds of 51% attacks on blockchains are and how easy or hard they are to recover from, and tradeoffs between security margin and cost.

Exhibit 1: people are apparently willing to accept basically exactly the same failure rate to avoid 1% issuance as they are to avoid 5% issuance.



**Vitalik Buterin** ✓  
@VitalikButerin



Blockchain security/cost tradeoff poll #2.

Suppose you had to choose between:

- (i) a blockchain/cryptocurrency with a failure rate  $X$ , and no issuance
- (ii) a bc/ccy with zero failure rate, but 1% annual issuance

What is the highest failure rate for which you would choose (i) ?

1:47 AM - Jan 22, 2018

17% >1 per year

24% 1 per 1-10 years

16% 1 per 10-100 years

43% <1 per 100 years

11,425 votes • Final results

♥ 307 💬 275 people are talking about this



**Vitalik Buterin** ✓  
@VitalikButerin



Blockchain security/cost tradeoff poll #3.

Suppose you had to choose between:

- (i) a blockchain/cryptocurrency with a failure rate  $X$ , and no

issuance

(ii) a bc/ccy with zero failure rate, but 5% annual issuance

What is the highest failure rate for which you would choose (i) ?

3:05 AM - Jan 22, 2018

16% >1 per year

24% 1 per 1-10 years

17% 1 per 10-100 years

43% <1 per 100 years

9,357 votes • Final results

♥ 185 💬 193 people are talking about this



I will make the usual behavioral economics caveat that what people say they want in surveys and what people can be deduced to actually want from their actions are very different, but that just means that the public discourse on this topic is warped and doesn't reflect reality.

To be clear: I define a blockchain failure as any situation that causes the blockchain to not fulfill its basic guarantees that is bad enough and unrecoverable in-protocol, and so requires out-of-band coordination among users to move on.

For example, if a 51% attack on PoW happens, then the attacker likely has enough hardware to keep doing it forever ("spawn camp attack"), so the community has to change the PoW algorithm to "delete" everyone's ASICs.

In PoS, you can recover from 51% attacks by coordinating a minority UASF, and the community can do this an unlimited number of times, but out-of-band coordination is still required.

And yes, in either PoW or PoS, this WILL happen. The idea that if a 51% spawn camp attack happens, all \$190b of bitcoin's users will just pack up their bags and leave is absurd; way too much incentive to coordinate and try to continue the ledger.

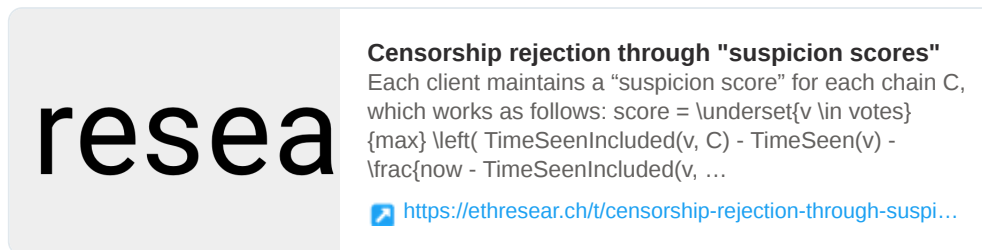
Though an important question is, how easy or hard is this? IMO it's much harder in PoW than PoS, and so PoS can achieve the same level of reliability in practice with a higher frequency of attacks, and hence can survive with a quite low cost of consensus

Now the second question. Now that we know 51% attacks are survivable, can we try to estimate the cost of one? I see two main factors:

1. Cost of loss of service during the attack itself
2. Cost of giving the social layer too much power by over-actively using it

After all, minimizing use of the social layer *is* what blockchains are about. But reducing it to zero has infinite cost, and so there are real tradeoffs between minimizing the social layer and minimizing cost.

There are opportunities to improve things with better technology, for example things like



The image shows a tweet from the account 'ethresear'. The tweet title is 'Censorship rejection through "suspicion scores"'. The text of the tweet explains that each client maintains a 'suspicion score' for each chain C, and provides a mathematical formula for the score: 
$$\text{score} = \underset{v \in \text{votes}}{\max} \left( \frac{\text{TimeSeenIncluded}(v, C) - \text{TimeSeen}(v)}{\text{now} - \text{TimeSeenIncluded}(v, \dots)} \right)$$
. Below the text is a blue link icon followed by the URL 'https://ethresear.ch/t/censorship-rejection-through-suspi...'. The 'ethresear' logo is visible on the left side of the tweet card.

<https://ethresear.ch/t/censorship-rejection-through-suspicion-scores/305>

can do 80% of the work of social coordination automatically, making it easier to use against attacks and harder to abuse for other ends.

Reminder: if a blockchain fails and recovers, you still have all your assets, unless they were in channels and loss of liveness during the attack enabled an attack on the channel. It's not 100% truly fully yours unless it's on-chain; channels are already a security/cost tradeoff.

Though with long withdrawal times and well-designed gadgets (bonded service providers, insurance markets, etc) they can be quite a good security/cost tradeoff.

So accepting a 1% issuance rate to avoid a 1% chance of attack per year is actually really not that smart a choice to make, at least if your use of a blockchain is for a cryptocurrency to store your value.