

Inoculating Against
Social Attacks on Decentralization

@ALYSEKILLEEN



breaking bitcoin

September 2017

This is a long term game.



breaking bitcoin

September 2017

Decentralization

Most fundamentally: Decentralization makes the bitcoin blockchain and bitcoin itself less vulnerable to attack.

2014 example: “The point of decentralization is that the system cannot do evil or be hijacked to do evil (e.g. a government agency may not come in and stop Person X's transactions/freeze their account by "partnering" with a mining pool - this could be possible today through GHash). The point of decentralization and of the bitcoin network is SIMPLY: anyone can process transactions without having to trust anyone else. Today, you have to trust GHash. Big problem.”



breaking bitcoin

September 2017

A Predisposition to Social Attacks on Decentralization

- The way we've known things to be – *centralized* – tends to be most comfortable for most because it's familiar.
- We are at the start of this new paradigm shift, and all we can know is our current and historical world.
- Even members of the community may struggle with the familiar paradigm, and various stakeholders (both from within and external to the ecosystem) will push to centralize the way bitcoin works, how consensus is achieved, and how technical decisions and prioritizations are made.

Note: From a participant's perspective, decentralization is in part measured by the freedom allowed for joining in consensus-making. Freedom of decision-making, including the power to participate, as well as to quit.



breaking bitcoin

September 2017

Everyone agrees that decentralization is important 🤔

- Stakeholders with different goals competing and collaborating with one another.
- Ideally, we hope for mutual understanding and an appreciation that parties will act on their own time lines, accepting that other peoples goals are different from their own.
- **Problems and tensions may arise in when businesses and venture capital investment based on business models that are inconsistent with decentralization or that are not timed to match the maturation rate of the bitcoin blockchain.**



breaking bitcoin

September 2017

Key Disagreements

How to measure consensus?



breaking bitcoin

September 2017

Key Disagreements

Who is to say what Bitcoin should be and what gives Bitcoin value?



breaking bitcoin

September 2017

Key Disagreements

How to measure different variables exposed to tradeoffs?

Nick Szabo: “Easy to measure performance, but not easy to measure security until it’s too late.”



breaking bitcoin

September 2017

Social Attack

- ❖ **Jamming the Process:** Dividing the community through tiring and contrived debates, often while targeting the developers and engineers in the process. aka “wearing people down”.
- ❖ e.g. One timely example could include turning technical issues into political issues.



breaking bitcoin

September 2017

Social Attack

- ❖ Pushing “fake news”, creating a high noise to signal ratio: A battle for perception
 - ❖ Resulting problems –
 - ❖ Impossible to evaluate every piece of knowledge, argument, or data for veracity.
 - ❖ Many community members, especially newer members or non-technical members, are unable to discern fact from propaganda (especially in bulk or on the “how to” of technical issues).
 - ❖ Compounding problems –
 - ❖ Tribalism – Who do I identify with mostly closely; I’ll follow what their lead.
 - ❖ Most people will not evaluate things themselves and defer to real or perceived experts.
- ❖ If you can’t fact check, how do you transition away from trust & tribalism? – HINT: Understand decentralization!



breaking bitcoin

September 2017

Social Attack

- ❖ **Assumptions of Authority:** Declaration of authority and the justification to make decisions for other stakeholders.
- ❖ Including – Assuming that you as an individual represents a common group of stakeholders (or that you as a resource provider represent those you provide resources to), and that you as a business owner represent and make community decisions on behalf of your users. In a decentralized ecosystem, users and individual entities represent themselves.
- ❖ Including – Assuming the authority to curate the group who forms “consensus.”
- ❖ Note: Business represent shareholders, and particularly large shareholders (by % ownership), not user or customers. (See Equifax, Wells Fargo, etc.).



breaking bitcoin

September 2017



*"Yes, the planet got destroyed. But for a beautiful moment
in time we created a lot of value for shareholders."*



breaking bitcoin

September 2017

Inoculating Against
Social Attacks on Decentralization

@ALYSEKILLEEN



breaking bitcoin

September 2017