UNFINISHED
DRAFT!

Slepak's Triangle

The fundamental user limit of decentralized consensus systems

Greg Slepak

October 17, 2016

Abstract. We introduce, and later attempt a proof of a triangle relationship whereby any *single system* can have at most two of the following three properties: *Consensus*, *Mainstream*, and *Decentralized*.

Choose Two: Consensus, Mainstream, Decentralized

When considering *systems* (implementations of protocols), we observe that any single system may possess, at most, two of three properties:

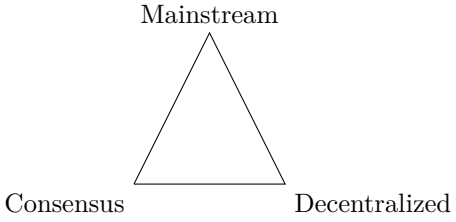

Fig. 1: Slepak's Triangle

- **Consensus** means the system's participants regularly come to agreement about changes to the system's state, thus creating a *shared resource*. The interval at which the system comes to agreement is its *period*, π.
- **Mainstream** means the system is, *by itself*, capable of meeting the transactional demands placed on a leading centralized competitor.[1]
- **Decentralized** means the system meets two related notions of *decentralization*:
    1. *The system has no single point of failure.* This first notion of decentralization, D_1, is measured by counting the number of "doors" to

[1] For example, we could compare Bitcoin's transaction rate to VISA's, or BitTorrent's ability to stream movies to Netflix.

knock on to compromise the *intended behavior* of the system,[2] where each "door" can be an individual or a technical component of the system. By this notion, a system is decentralized when:

$$D_1 \Rightarrow \texttt{doors\_to\_compromise}(\textit{system}) \geq 2$$

2. *The system's behavior is not dictated by a small group.* Whereas D_1 focuses on the ability to compromise the intended behavior of a system, D_2 focuses on *who defines and controls the intended behavior in the first place.* Redefining a protocol is a type of system compromise if it is done against the interests of the users of the system, therefore D_2 is a superset of D_1 that says not only must there not be a central point of failure, but there must also not be a central point of control that can change the system without the consent of its users.

$$D_2 \Rightarrow \texttt{redefinition\_threshold}(\textit{system}) > 75\%$$

We use 75% as a **minimum** threshold for modifying decentralized consensus protocols. See Appendix A for how to choose a safe threshold.

Characteristics of decentralized systems

To understand the proof, we must understand the characteristics of decentralized systems.

Low-cost of participation

Decentralized systems typically have a low-cost of participation. In other words, little effort is needed to use the system, and anyone can play any role.

High costs usually point to the existence of a privileged entity with the power to exclude others from participation (a form of censorship). Such an entity represents a single point of failure (D_1) that could prevent the system from fulfilling its intended purpose for most of its users.

Permissionless and inclusive

Our definition for decentralization means there is no trusted third-party deciding who can or cannot participate. Anyone around the world can join the system as long as they meet very basic resource requirements (e.g. an Internet connection).

[2] Video: "Deconfusing Decentralization"

Gatekeepers represent a central point of control, a violation of D_1 and D_2.

Most importantly, decentralized systems do not exclude inefficient participants. Rather, they go out of their way to ensure the most amount of participation. This is what keeps decentralized systems decentralized, as otherwise economies of scale will push the cost of participation up until a controlling group emerges, creating a single point of failure (D_1), along with the ability for that group to dictate behavior to the rest of the system (D_2).

This does not imply that decentralized systems are slow, but it does mean that decentralized **consensus** systems are *always* significantly slower than their centralized counterparts.

Censorship-resistant

The permissionless nature of decentralized systems, and their lack of a central point of control or failure, means they inherently resist all attempts at censorship.

Can centralize over time

Protocols and *live systems* are two different things. A protocol can only provide *the ability* for a decentralized system to exist; it cannot guarantee its decentralization.

All decentralized systems can be centralized if steps are not taken to combat their centralization. Single points of failure are likely to emerge as the system gains more users and interacts with the systems around it.

If a decentralized system involves *consensus*, then an increase in the number of users represents two fundamental obstacles for keeping the system decentralized:

1. The system becomes more valuable as it gains users, which increases the reward for successfully compromising it. Furthermore, the system will likely disrupt established centralized players who are extracting value out of some resource they've monopolized. Combined, these factors incentivize attackers to either find or create a single point of failure in the new system.
2. More users means more diversity of opinion over the system's future direction and the fate of its shared resource. Simultaneously, it becomes more difficult to distinguish real users from fake sybils or deliberate attempts at sabotage. As the distance between the system's maintainers and its average user increases, so too do misunderstandings. It becomes increasingly likely that *any* decision over the fate of the system will result in the alienation of a significant fraction of users.

Proof

We will construct our proof by proving three assertions:

1. At any point in time, *decentralized consensus systems* have an upper user limit, which, if exceeded, makes the system increasingly centralized.
2. That *decentralized consensus systems* cannot process as much information as their centralized counterparts.
3. That if the previous two assertions are true, Slepak's Triangle holds *for that system alone.*

We also want to make very clear what we **are not** saying:

- We *are not* saying that it's impossible for a decentralized consensus system to reach mainstream adoption. It is certainly possible. For example, one could create a *system of systems*, where most user communication touches only a subset of the system as a whole and does not represent the *shared state* that the entire system is managing.[3]
- Nor are we implying that the system can't, at some distant point in the future, be competitive with centralized systems of the present. Certainly as technology progresses, it improves the performance of all systems, centralized and decentralized. But even if you went to the future and brought back some amazing technology, those advances would quickly be applied to centralized systems just as well.

To Be Finished: At Or After Rebooting Web of Trust 3!

Thank you for reading this draft!

Hopefully you can see where I'm going with this. :-)

[3]It is also possible through more extreme measures, for example by reducing the world's population to the point where the difference between decentralized consensus systems and their centralized counterparts is negligible.