Submission to DIN RG Workshop on the Centralization in the Internet

How We Got from There to Here: Searching for the Root Cause

Lixia Zhang (lixia@cs.ucla.edu), May 16 2021

Recent years have witnessed a growing number of efforts and activities in developing solutions to "decentralize the Internet" – clearly the Internet today is no longer what it is used to be. However, in order to find effective means to move forward, the first step is to understand how we got here.

Unprecedented Internet growth took most, if not all, people by surprise and unprepared. Only in retrospect, one gets to see a bit clearly what has happened. It seems to me today's centralization resulted from an imbalance among the three factors: economy, network architecture, and regulation.

If we look at the architecture first: the original Internet was distributed because anyone could communicate with anyone else with an IP address, with a basic client-server app model. Anyone could pull off new stuff when others find it useful. *That is no longer the case today*. Communication has moved up to app-layer using names/identities; no app developers dealing with IP addresses. But more importantly, communication today must be secured. Unfortunately, people in general don't have identities that can be used to *reach them directly*, don't have tools to secure such directly communications (obviously, sine security is tied to identity). So they really don't have the means to write or deploy truly peer-to-peer apps. Note that users today do have identities, just that everyone's identity is assigned and managed by the big guys running the cloud (e.g. single-sign-on using gmail addr. or Facebook ID). Therefore, users can only communicate THROUGH the cloud, not independent of it. Given the success of Internet's is really the success of its applications, a decentralized internet means running decentralized apps. The **architecture**, that the Internet started with, no longer offers its users to communicate peer-to-peer *directly* and *securely*. As a result, truly decentralized apps do not have a ground to get started (and blockchain does not solve this problem; see more below).

Economy: the market missed no time in grabbing the opportunity of controlling the *server end* of the client-server model, when few people paid attention, and quickly turned *all clients* to revenue-generating eyeballs. Not knowing better, together with no technical alternatives, the user community at large was powerless, while a few companies rode on economy-of-scale to become cybergiants and took over everything. Economy-of-scale is not now, has always been a big factor driving centralization (maybe bigger & faster this time). In the past it was counter-measured by **regulation**. However, this time not only the regulation is falling behind, it would not be effective by itself in countering market centralization, if that is the only means apps can be built – now we circle back to the **architecture** inefficacy.

Today's Internet is insecure, the only place that seems secure is inside the cloud. As a side note and supporting evidence: all the three examples (email, DNS, Wen) cited by the IAB DEDR workshop report RFC8980, which started being distributed and now centralized, share the same root cause: (lack of) security. The report even mentioned this point, but fell short to see it as the common cause of all:

1. Under email: "need for coordination to defend against spam and other attacks."
2. Under DNS: "Future developments in DNS may see concentration through the use of globally available common resolver services, which evolve rapidly and can offer better security"
3. Under Web: "Their services provide scaling, distribution, and prevention of denial of service in ways that new entrants and smaller systems operators would find difficult to replicate".

Steering Internet away from today's consolidation should start from establishing a basic framework on how to improve Internet security, in particular *at edge*, *enabling direct, secure user-user communication*. There seems a lack of shared understanding on how such a framework would look like. Consequently, efforts on securing Internet (there are lots of them) seem scattered/isolated. There is also much misconception floating around, confusing necessary coordination in running a global-scale system with centralization, and security with anonymity (which leads to all the high hopes in blockchain direction). I would further add that the *real privacy* should be by-products of a truly *secured distributed system*; isolated privacy solutions at component levels may not help much; when someone can see every key click one makes, running DoH to hide DNS lookup from local ISPs does little in improving user privacy.