Phenomenal World *August 1st, 2019*

Decentralize What?

— Francis Tseng

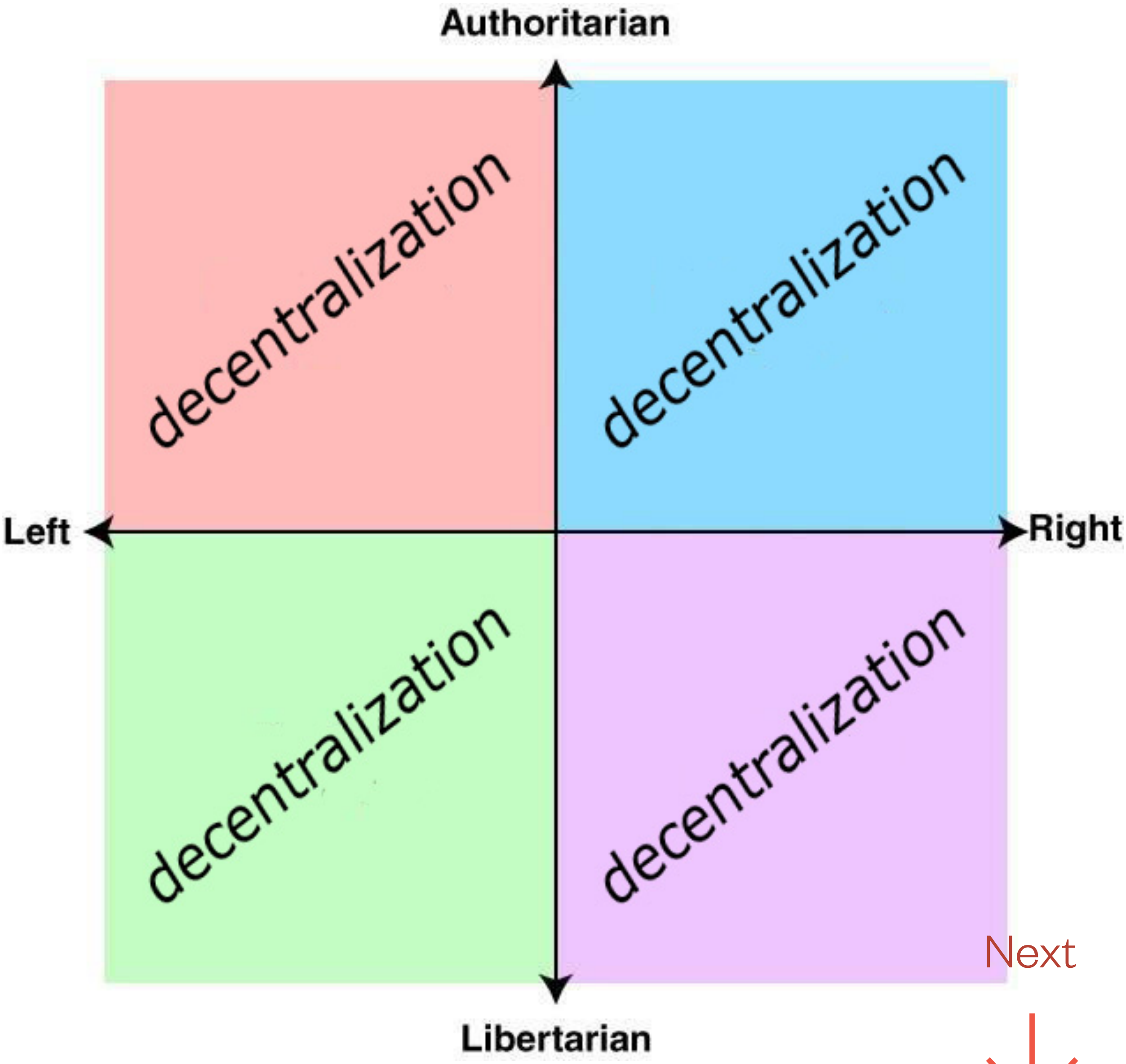


Image credit: Sarah Friend

Next

The internet's early proliferation was steeped in cyber-utopian ideals, which predicted that networking technology would usher in an era of free-flowing information and global emancipation from oppression. The circumvention of censorship and gatekeeping, digital public squares, direct democracy, revitalized civic engagement, the "global village"—these were all anticipated characteristics of the internet age, premised on the notion that digital communication would provide the necessary conditions for the world to change. In a dramatic reversal, we now associate the internet era with eroding privacy, widespread surveillance, state censorship, asymmetries of influence, and monopolies of attention—exacerbations of the exact problems it portended to fix.

The free-flow of information is surprisingly easy to impede (as evidenced by China's persistent internet censorship and Egypt's internet shutdown in 2011) and surveil (as is the case with the US's Room 641A). There is a technical explanation for this: Most traffic is routed through a small number of services that rely on a few key architectural points. Consequently, targeted attacks or outages have a disproportionately widespread effect. The Mirai botnet launched a DDoS attack on the Dyn DNS in 2016 that hindered access to many major sites, including Amazon, GitHub, Slack, Squarespace, and Netflix. Because of how the internet is structured, people who were in the same building couldn't communicate over Slack—a service that relies

Next ↓

on passing messages through a geographically distant server before delivering it to the recipient. These attacks are expected to become more frequent as poorly-secured internet-of-things devices continue to proliferate.

The same structure that makes these attacks so effective also contributes to a more general brittleness, even in the absence of hostility. Amazon Web Services (AWS), which controls 40% of the cloud market (it's unclear how much of the internet this actually is, but it’s safe to assume that it's a large amount), similarly takes out a large set of popular services during its various outages.

These issues are frequently understood as falling into two categories of centralization: *Infrastructural centralization* accounts for the fragility that enables DDoS attacks, and *political centralization* motivates oppositional institutional behavior like mass surveillance and censorship. The two are obviously mutually reinforcing; for example, mass surveillance is made easier with infrastructural centralization.

If these are problems of centralization, then decentralization looks like a natural remedy. In the context of the internet, decentralization generally refers to peer-to-peer (p2p) technologies, which have recently regained interest in the form of blockchains and federated applications like Mastodon. Reminiscent of cyber-utopianism, this new technological paradigm presages similar social and political change. But what are we decentralizing exactly, and to what ends? There are

Next ↓

many parts of the internet that could be decentralized—physical infrastructure, the protocols by which computers communicate, the end-user applications we spend our time on—each yielding different outcomes. Discussions about decentralization and the internet tend to conflate these different possibilities, indicating only a vague, monolithic end rather than recognizing the distinct and various means for achieving particular goals.

In this post, I consider whether infrastructural decentralization is an effective way to counter existing regimes of political centralization. The cyber-utopian dream failed to account for the exogenous pressures that would shape the internet—rosy narratives of infrastructural decentralization seem to be making a similar misstep.

Mesh networks

If we were to conceive of an alternative to the centralized internet, we might start by decentralizing the topology and ownership of its physical infrastructure. As it stands, communication over the internet is mediated by relatively few ISPs over a tree-like structure. Points along the trunk of this tree, where many branches come together, can be easily monitored to surveil large amounts of traffic. An alternative to this structure, mesh networks focus instead on direct connections between devices, such that the network looks more

Next ↓

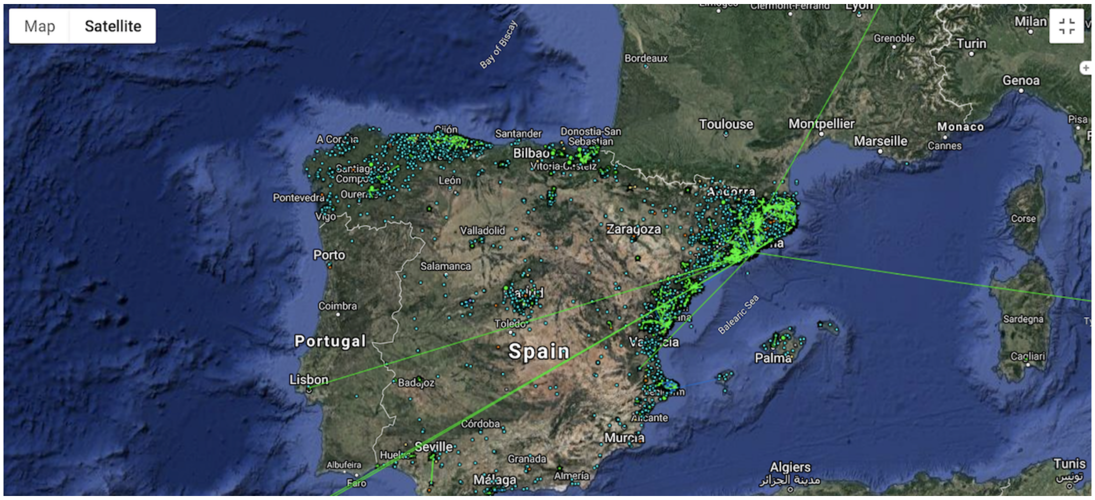
like a fishing net and less like a tree. Communication on a mesh network is not necessarily mediated by an ISP; information can theoretically pass through anyone participating in the network. Rather than having just a few exit points for traffic, a country might have hundreds or thousands of them, all operated by different parties. Accordingly, closing the country off from the internet becomes much more complicated, as there are virtually no single failure points that can collapse in inclement weather, or be shut down, monitored, or filtered by a hostile state.

Mesh networks are praised for their resiliency to such failures, their capacity to generate alternative models of internet infrastructure ownership and stewardship, and the challenge they pose to the commodification of digital communication. With such "community networks," access to the internet is no longer contingent on the business interests of a private ISP, but rather on people's communication needs. When neighborhoods are subject to "digital redlining" or overlooked because of low density, they can deploy local mesh networks and form an intranet among members of those communities. Active community network projects in the US include the Detroit Community Technology Project, NYC Mesh, and Red Hook Wifi.

Community networks outside the US are more common and mature. guifi is the largest community network in the world, composed of some 35,000 nodes that cover most of Catalonia and large parts of Valencia and Asturias. As of 2015, the

Next

network required about €7.3 in capital expenditure and costs about €3 million per year. The throughput can vary quite a bit—in 2015, one analysis found the mean throughput to be 17.4Mbps to the internet gateway and 6.2Mbps through it. Compared to other ISPs operating in the area, a study from the same year found the network to rank first in median latency, but the network has been transitioning to fiber infrastructure, which has improved speeds. The service is priced at cost, leading to considerably lower prices: in 2016, a guifi gigabit fiber connection cost around $20–$37 a month. In comparison, Xfinity's gigabit service costs $105 a month today. guifi seems successful in expanding affordable and high-speed digital connectivity.



guifi nodes, as of 05/23/2019. See: https://guifi.net/maps

Next

This setup doesn't provide complete autonomy, however. An ISP is still required to communicate to the broader internet beyond the mesh network. This is a limitation of scale: if mesh networks grow in popularity, ISPs will become less and less necessary as various local mesh networks can merge into larger aggregate networks.

That the architecture of a mesh network consists of physically decentralized components does not mean that it's managed in a decentralized way, nor does it imply particular values guiding the decision-making or application of the network. Mesh networks may be deployed exclusively for their fault tolerance—a quality that appeals to a range of political actors, including the military. And they don't necessarily need to be priced at cost or made accessible—it's easy to conceive of an ISP that operates a mesh network, owning a majority if not all of its nodes (for example, this startup in Philadelphia which requires that users watch ads to access the network). Community networks such as guifi take a decentralized technical architecture and extend that notion of decentralization to its social and political meanings—ensuring access, participation, and ownership are central to the network's development.

Networking protocols

Networking protocols define how computers find and talk to one another, and centralization at the network level can contribute to the effectiveness of the DDoS attacks described above. In the present client-server paradigm, the vast majority of computers (clients) are looking for and talking to a much smaller subset of

Next ↓

computers (servers). For example, 2.3 billion people access Facebook's servers every month. The content and data that those people are interested in are more or less exclusively located on Facebook's servers. If an interested attacker can wrangle enough bandwidth, they could attack some key part of Facebook's infrastructure to disrupt access for many of those 2.3 billion people.

p2p networking protocols, on the other hand, seek to distribute data (and the traffic that accesses it) across the very computers that are looking to access it. This tit-for-tat structure is key to p2p networking protocols and is part of the more horizontal structures that these protocols are built around. Using and contributing to the network are essentially the same act. This sharing of network load can lessen the impact of DDoS attacks—because there is no longer a piece of key infrastructure that can be targeted, every computer becomes equally (un)important.

Though p2p protocols aspire to have a fully horizontal network topology in which peers are interchangeable, there is a spectrum of hierarchy throughout their designs. Hierarchization can have important effects beyond protocol operation—Napster, for instance, had a high degree of centralization, with an index server coordinating peer connection. The index server was managed by the company and thus, the courts ruled, made them liable for the file-sharing that occurred on the network. At the opposite end, protocols like Gnutella are completely non-

Next

hierarchical and rely on "flooding," in which peers blast all other peers with requests, which is very inefficient and unreliable. Protocols like Kademlia are hierarchically flat like Gnutella but not marred by its problems, with good guarantees on efficiency and reliability. Kademlia's simple design demonstrates that the tradeoff implied by hierarchical networks —between resilience and efficiency—isn't necessary.

p2p networking protocols are often designed to work on existing internet infrastructure, forming a "virtual" or "overlay" network on top of the underlying physical network. Even if the actual packets between computers are routed via conventional ISP infrastructure, they communicate as if they were directly connected. This reliance on the topology of the physical network exposes overlay networks to the same fragility their underlying physical network is exposed to. For example, in the current tree-like structure of internet infrastructure, traffic on an overlay network may still enter and exit a country at only a few points, and those points could be shut off to sever the network. In the case of file-sharing, this is what enables ISPs to prosecute file-sharers.

Mesh networking would of course resolve these ISP issues. Overlay networks are generally portable to mesh networks, so the two would be straightforward to combine in practice. p2p networking protocols complement mesh networks by providing more flexible and efficient routing. They also support decentralized applications like distributed storage, which enables

Next

faster content delivery, file-sharing, and better censorship resistance.

Interestingly, p2p networking is about as old as computer networking in general. ARPANET, the 1960s precursor to the internet, was originally designed as a p2p network. Over time the p2p aspect of the internet faded in favor of the client-server relationship, until the late 90's when file-sharing applications like Napster, Gnutella, Limewire, and Kazaa re-introduced the concept to broader audiences.

p2p networking protocols decentralize the responsibility of storage and routing on a network. Yet there aren't strong guarantees that this decentralization will persist or proliferate—a centralized social networking application could conceivably be built on top of a p2p architecture. While these protocols may provide more reliability than Facebook's current infrastructure, they don't preclude the existence of something with as much influence and power as Facebook. Just as the unprecedented consolidation of wealth and political power by large internet services reflects exogenous system characteristics as much or more than their underlying technical architecture, a p2p social network application could, in practice, lead to a similar centralization of power and influence.

Next

More immediately troubling is that there is an entire class of attack known as Sybil attacks which fundamentally undermine the security of p2p networks. Sybil attacks provide a way for covert centralization to emerge, where a swarm of seemingly distinct peers are actually controlled by a single party. With a large enough set of Sybil peers, that party can effectively shut off parts of the network, serve malicious files, or surveil traffic. In practice, there are several techniques proposed to lessen the effect of such attacks, but there is no way to eliminate them entirely. In p2p networking protocols, as with mesh networking, the realized infrastructural decentralization is contingent on factors exogenous to the protocol.

Blockchains

Blockchain is a relative newcomer to the p2p space and is probably the most well-known. The technology itself focuses on achieving consensus across a set of computers, ultimately taking the form of an append-only ledger. But what other forms of decentralization does this achieve?

On its own, not much. This decentralized consensus mechanism is one component of a much broader system, similar to how mesh networks and p2p networking protocols address problems in different layers of networking infrastructure. A decentralized consensus mechanism is on its own not incompatible with other centralizing tendencies. One key assumption for the security of blockchains is that the pool of miners—participants whose responsibility it is to validate transactions (additions to the ledger)—be as distributed as possible. Over time, however, these

Next

miners have become rather concentrated. Consider Bitcoin: at least 70% of mining is in China, largely owing to factors exogenous to the protocol like access to mining hardware and cheap electricity. In blockchain, acknowledgement of this fact leads to the reintroduction of other forms of decentralization.

At the blockchain application level, "decentralization" is typically conflated with "markets," which emphasize token economies, mechanism design, and economic incentives. For example, curation markets (e.g. FOAM), prediction markets (e.g. Augur and Gnosis), and data markets (e.g. Ocean Protocol). For Ethereum itself, market and market-inspired structures underlie much of the design and thinking around the protocol. Yet a market structure does not necessarily follow from the underlying distributed consensus mechanism. This tendency towards market mechanisms is likely a bias owing to the technology's financial genesis: blockchain, via Bitcoin, was introduced as a currency and received as a way to abolish central banks. Many early adopters of blockchain were from finance, including Consensys (perhaps one of the most prominent blockchain companies) and Ethereum co-founder Joseph Lubin, who was VP of Technology for Goldman Sachs' Private Wealth Management division. Of course, the ongoing speculative nature of cryptocurrencies contributes to this image as well. "Cryptoeconomics", the primary design practice around blockchain protocol design, is concerned with structuring interactions around idealized economic incentives such that the importance of trust is minimized, often to the point where these

Next

protocols are described as "trustless." To make these protocols viable under such a framework, they usually are built around tokens—quantifiable, exchangeable, and (usually) fungible units. Resulting inequities in accumulation, or token wealth, become part-and-parcel of the protocol. This doesn't seem particularly decentralized: inequities in wealth are tantamount to the consolidation of influence. But that may not be the kind of decentralization these applications are concerned with.

Another way this financial legacy emerges is through the primary contender to replace proof-of-work, the current key component behind the distributed consensus mechanism. The proposed replacement is proof-of-stake which takes on a framing of investment. Rather than devote intensive computational power to validate transactions, one "stakes" some of their wealth and is compensated with a return based on the staked amount. While there is some protection against leveraging wealth to influence the network—if you validate a fraudulent transaction, you lose your stake—this mechanism is a feedback loop where wealth begets wealth, exacerbated by the fact that larger stakes are more likely to be selected to validate (some protocols let smaller stakers pool together so they can compete). This can translate into centralization endogenous to the network, or exogenous centralization that bears upon the network in different ways, such as bribes to influence the governance of the protocol.

Next

Ongoing conversations around governance in blockchain point to another layer in the blockchain stack, where what is meant by decentralization is unclear. Questions of governance in blockchain amount to a reckoning that the blockchain is surrounded by not-so-decentralized structures and processes. In particular, the governance conversation focuses on decision-making around protocols—i.e. the design of blockchain systems. If the protocol needs to be changed, who has what say in that decision? The conversation broadly cleaves into two camps: "off-chain" governance, which privileges a clergy of protocol developers and miners (i.e. informal power with limited accountability), and "on-chain" governance, which institutes some formal mechanism for input from more or less everyone using the platform. On-chain governance subdivides into roughly two further distinctions: one-person-one-vote and one-token-one-vote. One-person-one-vote is complicated by Sybil attacks: if it's cheap to create new identities on a blockchain, then a person can create many identities and vote multiple times. One-token-one-vote, on the other hand, is equivalent to instituting a plutocracy. The more tokens (wealth) you have, the larger your influence. A plutocratic regime is the de facto standard for on-chain governance; it is taken as the lesser of the two evils, a formal endorsement equating wealth with trustworthiness. Because plutocracy looks like the only alternative, off-chain governance—the clergy option—is frequently advocated.

Next ↓

The Sybil attack is the most persistent problem in p2p networking. It constantly plagues the design of p2p protocols, because if an attacker can flood the network with bots or spam they can disrupt or manipulate it. The paper that introduced the attack concluded that there is no guaranteed prevention that doesn't involve a trusted central authority that assigns or verifies identities. Relying on a centralized institution is exactly what these systems don’t want to do! And so the plutocratic option, in one light, looks like the most decentralized option available.

But this conclusion takes for granted that having a voter verification body is more centralized than a plutocracy and a clergy class, and the appropriateness of that conclusion largely depends again on what one thinks decentralization is for. Is it just to ruthlessly eliminate institutions? Or is it to, as much as possible, set up a system of equitable decision-making? If the goal is the latter, it seems that under all circumstances a plutocratic system and a clergy class are going to be unequal, whereas one-person-one-vote, even with the introduction of a mediating authority, has a greater potential of being more equal.

Conclusion

The conversation around decentralization and internet technologies too frequently takes for granted unstated goals around authority, ownership, and governance, conflating infrastructural decentralization with the realization of these less technical goals. This can be read as a failure to account for the

Next

political environment in which a new technical infrastructure will be deployed. The development and deployment of these new technologies must be considered against explicit goals and evaluated against the existing contexts that will influence its development.

Thanks to Arthur Röing Baer, Sarah Friend, and Maksym Rokmaniko for their feedback on the piece.

Title	Decentralize What?
Authors	Francis Tseng
Date	August 1st, 2019
Collection	Miscellaneous
Filed Under	decentralization internet digital ethics blockchain computer science

Next