THEME 02

The emergence of the decentralized stack

BLOCKCHAIN DECENTRALIZATION FIXING THE INTERNET

Many of the issues of the internet we encounter today, such as vendor lock-in, platform feudalism, large-scale internet black-outs, hacks or leaks, are in one way or another related to its increasingly centralized structure. On the one hand, governments are trying to reduce these risks through legislative measures and policies, on the other hand, computer scientists are looking into technical means that can help (re-)decentralize parts of the internet with the aim of dissolving central points of failure that are currently vulnerable to malfunction, coercion and corruption. Here we take a closer look at what decentralization means and how it can help resolve some of the current issues of the internet.

Our observations

- On May 9th Chris Hughes, co-founder of Facebook published an opinion piece in which he calls for the break-up of Facebook due to its disproportionate concentration of power. Similarly, democratic presidential candidate Sen. Elizabeth Warren has already called for the break-up of big tech and is gaining more support from other candidates like Sen. Kamala Harris and Joe Biden.
- In the last few years, quite a few projects (e.g. Solid, IPFS, Freenet, Zeronet, Blockstack, SAFE Network) have been developing open-source protocols, conventions and tools which try to realize data ownership, open data, privacy and decentralized applications.
- Microsoft announced their decentralized identifier (DID) system called Identity Overlay Network (ION), which allows for a decentralized digital identity that users own and control, backed by self-owned identifiers that enable secure, privacy preserving interactions. By running on top of the Bitcoin blockchain and IPFS users do not have to rely on trusted third parties.
- As written before, Facebook is also looking into the potential of decentralized tech. Mark Zuckerberg has mentioned that a decentralized identity management system could be achievable in the short term, whereas a decentralized alternative of Facebook is further away due to scalability issues. Furthermore, Facebook is presumably working on a crypto stablecoin named 'Libra' with the aim of facilitating all transactions on their platform.

>> see next page

Connecting the dots

From a systems theory perspective, decentralized systems have the characteristic property of being emergent in nature. In other words, instead of lower-level components falling under the control of a central actor, decentralized systems rely on lower-level components acting on local information which give rise to complex behavior at a collective level. The internet is just one example of such emergent behavior. In the book 'The Starfish and the Spider' by Ori Brafman and Rod A. Beckstrom, many parallels are drawn between digital, social and biological decentralized systems. For instance, the Apache tribe versus the Spanish colonizers shows a similar behavior as peer-to-peer file sharing networks prosecuted by the government. Both lack a central point of attack, are extremely flexible and grow more open, decentralized and resilient under external coercion. From a political perspective, there are generally three reasons why one would choose to decentralize a system, whether digital or physical. The first one is to increase a system's fault tolerance, i.e. to what extent a system fails accidentally. Since decentralized systems offer more redundancy, they are more tolerant when individual components fail. Secondly, decentralization helps improve attack resistance by making a system more costly to attack as it lacks vulnerable central points of attack. Lastly, decentralized systems make it harder for participants to collude, as they have to mobilize a large amount of autonomous actors in order to compromise the system. However, in the case of digital systems, simply running an open-source protocol on as many nodes (i.e. connected computers) as possible, does not necessarily guarantee any of these aforementioned goals. After all, the operating nodes themselves could be owned by one corrupt actor or by a group of collaborating corrupt actors, the software could have a bug, the developers of the software could be corrupt and/or the computers running the node could be faulty. As it appears, one should consider the entire context and the different aspects that can be decentralized. Vitalik Buterin, co-founder of Ethereum, discerns three different dimensions of decentralization, namely to what extent a system is politically, logically and architecturally decentralized. The architectural dimension considers how many physical computers the system consists of. Political decentralization refers to how many individuals control the nodes in the system. Lastly, if the system behaves like an amorphous swarm instead of a large virtual computer, it can be considered logically decentralized. Regarding the centralization of the internet at large, political, architectural and logical centralization can be found at different layers of the stack. Instances of government internet shutdown, ISPs compromising net neutrality and distrust in internet infrastructure (e.g. Huawei) mainly relate to architectural and political centralization of internet communication infrastructures. However, issues surrounding big tech can largely be traced back to political, architectural and logical centralization at the application level. Even though the core protocols of the internet mostly guarantee decentralized data transmission (e.g. TCP/IP protocols), at the application level we see more centralized structures due to client-server protocols (e.g. hypertext transfer protocol) who grant considerable control to the application owner in terms of setting the application rules, controlling application resources and most importantly, having leverage over user data collection. Joel Monégro refers to these applications as 'fat applications running on thin protocols as most of the created value is accrued by the application. In contrast, he expects that permissionless blockchains could flip this model to 'thin applications running on a fat protocol', since user data is not controlled by the application layer, but is captured in a shared data layer at the protocol level, namely the blockchain itself. Furthermore, in order to compensate for the lack of a rent-seeking business model that we have grown accustomed to in centralized applications, permissionless blockchains have an integrated reward and penalty system. The built-in consensus protocol (e.g. Proof-of-Work or Proof-of-Stake) provides individual contributors with a stake in the network (e.g. through energy consumption, staking funds) which drives actors towards honest behavior, while the built-in token facilitates a reward system which incentivizes actors to contribute to the network. Thus, the value of the token is determined by the demand of the token which is a function of its usefulness. The consensus protocol in permissionless blockchain systems is thereby a form of logical centralization at the protocol level which stimulates political and architectural decentralization with the purpose of increasing trust and security in a network. Therefore blockchains are expected to become an important enabling factor in creating decentralized applications (dApps) and data marketplaces. However, it is important to realize that the decision for a client-server architecture has not been an arbitrary one, as it allowed the internet to scale much faster and more efficiently. However, now that we are encountering the repercussions of this approach, users are looking for systems that have different trade-offs. As the blockchain trilemma highlights, blockchain systems compared to centralized ledgers, are sacrificing scalability for the purpose of achieving decentralization and security. After all, in order to become independent from central actors, these decentralized systems rely on enormous redundancy, as many of the resources have to be distributed across the network. However, looking at the many different solutions that are emerging, some willingly choose a less decentralized design in order to allow for more scalability (e.g. Bitcoin vs Bitcoin Cash). Some solutions also choose for more centralized control (e.g. government intervention) to mitigate the disadvantages of decentralization. For instance, censorship resistance is usually seen as an advantage of decentralization (e.g. within the context of dictatorial regimes), however it can also be unwanted in situations where harmful information is distributed (e.g. child pornography, social harassment). This shows that decentralization is not a binary quality and an end itself, but a continuum in which some solutions will make different trade-offs, depending on the specific values and functionalities that are being pursued at the application level. Lastly, the question arises as to why current dominant centralized actors would ever allow this decentralization trend to take place, as it could undermine their current business model. However, as we can already see, society at large is increasingly experiencing the disadvantages of an internet that is too centralized. Consequently, we can already see how big tech companies are pursuing and developing decentralized services to gain an advantage over their competitors (e.g. Microsoft) or they are simply being forced to implement decentralized tech to prevent being disrupted by it (e.g. Facebook).

Implications

- As we rely more on 'fat protocols', the barriers to entry will be lower and will lead to more open innovation since more developers and applications have access to data, instead of a handful of dominant services. This will also have considerable consequences for the development of AI as its development is largely dependent on the large-scale availability of data.
- Taking the blockchain trilemma into consideration, it is likely that we end up with a few complementary blockchains, each having a different trade-off in terms of scalability, security and decentralization, in order to facilitate the different qualities (secure value storage, high transaction density, government intervention) the broad spectrum of applications will need.
- In the long term, with the expectation of peer-to-peer wireless connectivity to become cheaper, more capable and widespread, crypto-driven mesh networks could emerge, which could have considerable consequences for ISPs and governments seeking to control the flow of information at the communication infrastructure level.

>> see next page