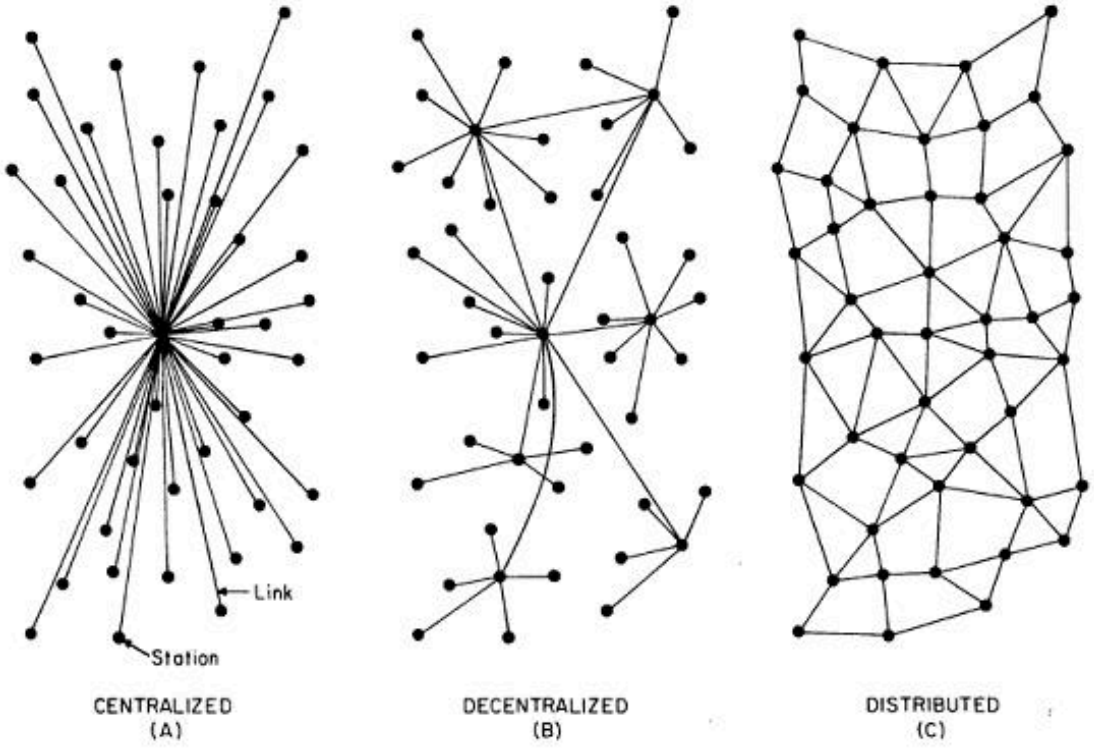
How does distributed web system work?
What would the distributed web network look like?

1. Peer-to-peer (P2P)



For example, the Amazon Cloud. The Amazon Cloud is made up of computers in Amazon.com data centers all over the world. The data stored in this cloud can be copied from computer to computer in these different places, avoiding machines that are not working, as well as getting the data closer to users and replicating it as it is increasingly used. This has turned out to be a great idea. What if we could make the next generation Web work like that, but across the entire Internet, like an enormous Amazon Cloud? This system would be based on peer-to-peer technology — a system that

isn’t dependent on a central host or the policies of one particular country. In a peer-to-peer model, those who are using the distributed Web are also providing some of the bandwidth and storage to run it. Instead of one Web server per website we would have many. The more people or organizations that are involved in the distributed Web, the more redundant, safe, and fast it will become.

2. Blockchain(database)

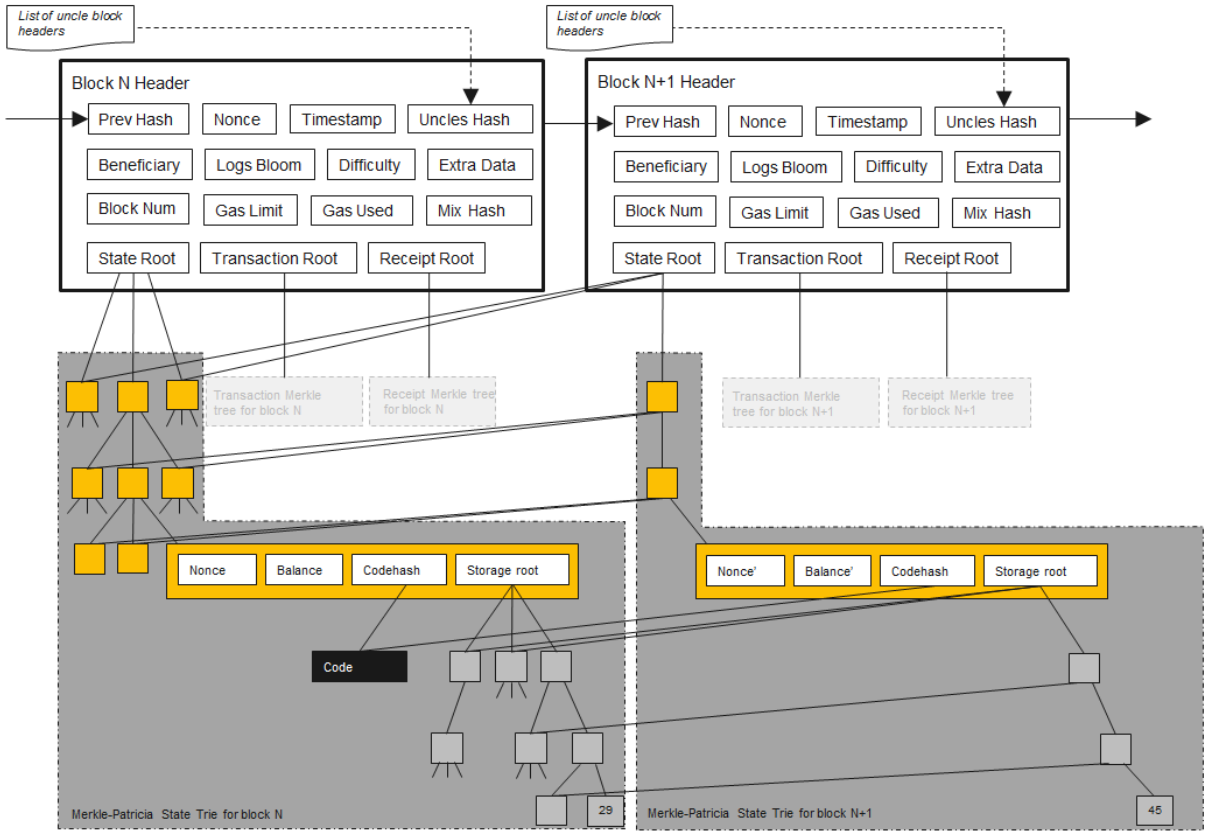
What would the distributed database look like?

Every web application must have databases. For distributed web application, we also have distributed database such as Blockchain system. ~~As we know that Block Chain technology enables the Bitcoin community to have a global database with no central point of control. It can be used in distributed web applications.~~ Imagine how Bittorrent works, it stores and retrieves files in a distributed way. Bittorrent is kind of magic, where typing a long number that is a unique identifier for a file or set of files will cause it to appear on your machine. Pieces of the desired file will come from other computers that had previously retrieved those files and therefore store them on their computers. In this way, the readers of files become the servers of those files. There are millions of users of Bittorrent sharing everything from commercial movies, to free software, to library materials. The Internet Archive, for instance, offers petabytes of files to the public using the Bittorrent protocol so that users have the option to retrieve files from the Internet Archive or from other users who might be closer, which is what the Amazon Cloud is doing.

What does the blockchain structure look like?

That is pretty much how blockchain does.

A blockchain is comprised of unchangable, digitally recorded data in packages called blocks. These digitally recorded "blocks" of data is stored in a linear *chain*. Each block in the chain contains data, is cryptographically hashed. The blocks of hashed data draw upon the previous-block (which came before it) in the chain, ensuring all data in the overall "blockchain" has not been tampered with and remains unchanged.



`

Other backup topics for QA phase:

Easy Names of Distributed Websites

In the implementations described above for both Bittorrent and IPFS, a webpage is an unique, incomprehensible string such as: 88f775eea02293b407e4b22c69d387cb9bbf50b8 or /ipfs/ QmavE42xtK1VovJFVTVkCR5Jdf761QWtxmvak9Zx718TVr.

One distributed naming system that currently exists is called Namecoin, and it is an open source system built on a Bitcoin-like Blockchain, which is in itself a distributed system. People can register a name and address pair in the Blockchain.

Another system that could be used for this is the Distributed Hash Table, or DHT, which is central to the way Bittorrent works. This is another distributed system for looking up a name.

Distributed Identity

To know who is allowed to update a blog, we need a system to register administrators and then to authenticate someone as being that person.

A better system might be one that uses cryptography to allow users to create multiple account credentials and use these without necessarily tying them back to their persons. That way people would have control over who knows what about them, and if they wanted to walk away from an account, that would work as well.This could use what is called public key encryption, which uses special math functions to create pairs of public and private keys. The private key is used to sign documents in such a way that anyone using the public key, which is publicly known, can verify that it was correctly signed. No one else can forge a document. Thus, if posts were signed on a Distributed Web, then the readers can verify that it is the particular user that has the authority to perform that action and the website never needs to

know a user's password or private keys.

Conclusion:

Our new Web would be reliable because it would be hosted in many places, and multiple versions. Also, people could even make money, so there could be extra incentive to publish in the Distributed Web.

It would be more private because it would be more difficult to monitor who is reading a particular website. Using cryptography for the identity system makes it less related to personal identity, so there is an ability to walk away without being personally targeted.

And it could be as fun as it is malleable and extendable. With no central entities to regulate the evolution of the Distributed Web, the possibilities are much broader.

What we need to do now is bring together technologists, visionaries, and philanthropists to build such a system that has no central points of control. Building this as a truly open project could in itself be done in a distributed way, allowing many people and many projects to participate toward a shared goal of a Distributed Web.

Transition to IPFS