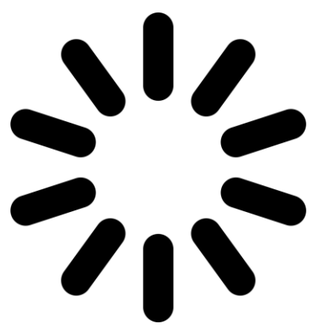
Decentralized File Storage

↓

Decentralizing the Internet



UNIVERSITY of STIRLING

IPFS + Blockchain

Yash Vikhankar
MSc FinTech

The Internet at present:

The current internet works on a protocol called the hyper-text-transfer-protocol also known as the http. It is a framework that depends on a client-server method to retrieve data. When you enter the address of a webpage on your browser, the browser points it to the server that hosts the data and thus the data is fetched to you. Hence, it is said that the http follows a location-based address.

Existing Vulnerabilities:

Centralization: Although the internet is not 100% centralized since no single corporation owns it; relatively few large, physical servers (Amazon, Google, Microsoft, IBM), host the important elements that we call as the internet. There is a lot of diversity in the content that is stored but the control over hosting is concentrated. This makes these servers vulnerable to DDOS attacks as this centralization leads to a single point of failure.

Data Privacy: While your internet experience is censored, your data sits on a central server and it is exposed to serious threats. Social media sites hold the records of at least 2 billion people which has sensitive information like user's full name, date of birth, location, photos, work details, friends, contacts etc. Such stores of information can be often breached by hackers, who either sell the information or commit crimes.

Secure Decentralized File Storage using the IPFS and the Blockchain:

To solve the issue of privacy and censorship, blockchain based file storage has been a potential solution. But Blockchain is terrible at handling large data as it is not scalable (example: Cryptokitties).

Also, having a decentralized secure file storage is a vital step to decentralizing the internet.

The IPFS (Inter Planetary file system) is a method of storing a file in a distributed manner using cryptography. It does so by storing files by fragmenting it into blocks and storing their unique fingerprints(cryptographic hashing) within a network. The fragmented parts of the file are indexed and can be retrieved by asking the network for these files by their unique fingerprints(address-based storage). These fingerprints can then be stored on the blockchain which in turn secures these files with a time stamp. Thus we have a very elegant of 'storing', encrypting and sharing large data and files on the blockchain

Immediate beneficiaries:

- Healthcare
- Financial Institutions
- Cloud sharing companies

For further information contact: *Yash Vikhankar*

yash2410@gmail.com