IPFS

By Ardalan Razavi

Traditional File Sharing Explained

- HTTP servers
- Request and response
- Centralized!! What happen if a server goes down? problem!!
- Censorship
  - Bahrain: 2012–present.
  - Belarus: 2006–8, 2012–present.
  - China: 2008–present.
  - Cuba: 2006–present.
  - Ethiopia: 2014–present.
  - North Korea: 2006–present.
- Uses HTTP for websites
  - Client send a request to server
  - Content is loaded using URL (Location Based Addressing)
  - Client need to know location
- Why?
  - More control over service quality
  - No alternative that can handle high traffic

InterPlanetary File System (IPFS)

- Peer-to-Peer
- Distributed
- Content Based Addressing
- Client need to just know what file is needed

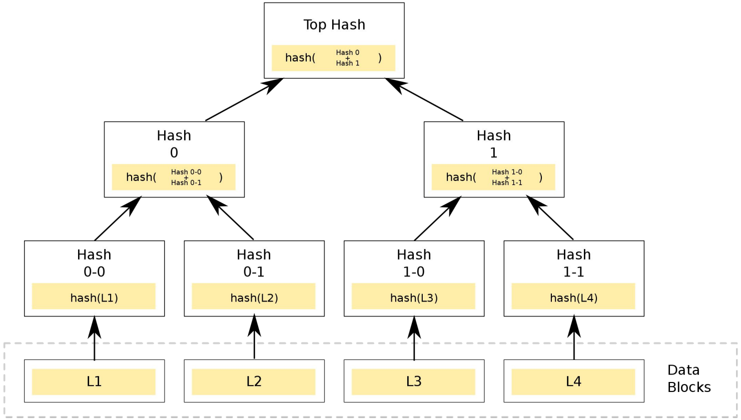
Learned and combined following

- DHT
  - Used for peer to peer addressing and file object address
- Git
  - Learned the versioning from git
  - Using Markle DAG
  - Immutable objects represent Files (blob), Directories (tree), and Changes (commit).
- SFS
  - Self Certified Filesystems
  - Learned the address of the nodes which is hash of public key
- Bittorrent
  - Block Exchanges
  - tit-for-tat

Design

- Identities
    - Hash of node’s public key (NodeId)
- Network
    - Transport: WebRTC DataChannels
    - Reliability: using uTP or SCTP
    - Connectivity: ICE NAT traversal
    - Integrity: optional hash checksum
    - Authenticity: optional HMAC with sender's public key
- Routing
    - Using IPFS’s DHT: small file (less 1kb) saved on table, others stores references of NodeIds
- Block Exchange
    - BitSwap from bittorrent
    - Want_list and have_list

Design Continued



- Object Merkle DAG
  - Directed Acyclic Graph
    - Content Addressing
    - Tamper Resistant
- Paths
  - /ipfs/<hash-of-object>/<name-path-to-object>
- Local Objects
  - Files and blocks stored locally on a node
- Object Pinning:
  - Pinning an object locally and store it locally
- Publishing Objects
  - Adding key to DHT
- Object Level Cryptography
  - Possible to encrypt and decrypt files using peer key (links protected)

Demo