IPFS

TL;DR

- P2P distributed filesystem where files are adressed by their content (hash)

/ipfs/XLHBNmRQ5sJJrdMPuu48pzeyTtRo39tNDR5

High throughput.
High capacity.
Low latency.

PLANETARY SCALE

IPFS

BIGCHAIN DB

FULLY DECENTRALIZED

Anyone can join as validator.

bitcoin ethereum

CONSISTENT

All nodes see same data at same time.

Filesystem objects

type: **blob**


```
{
 "data": "c2Rhc2Rhc2RhUw0KREENCnNkYXMNCmZzZA0KZg0KY
  XNkZg0KYXMNCmRmDQphc2RmDQpzYWRmc2Zkc2ZzZGYNCnNhZA0
  KZnNkDQpmcw0KZGYNCmFzZA0KZnNhDQpkZmENCnNkZg0KYXNkZ
  g0Kc2FkDQpmc2ENCmRmDQpzYWRmDQphc2QNCmZhcw0KZGZzZGY
  NCnNhZA0KZmENCnNkZ…"
  links: {}
}
```


sha1

XLYkgq61DYaQ8NhkcqyU7rLcnSa7dSHQ16x

type: **tree**


```
{
  "data": ["blob", "tree", "blob"],
  "links": [
    { "hash": "XLYkgq61DYaQ8NhkcqyU7rLcnSa7dSHQ16x",
      "name": "less", "size": 189458 },
    { "hash": "XLHBNmRQ5sJJrdMPuu48pzeyTtRo39tNDR5",
      "name": "script", "size": 19441 },
    { "hash": "XLWVQDqxo9Km9zLyquoC9gAP8CL1gWnHZ7z",
      "name": “template/icon.png", "size": 5286 }
  ]
}
```


sha1

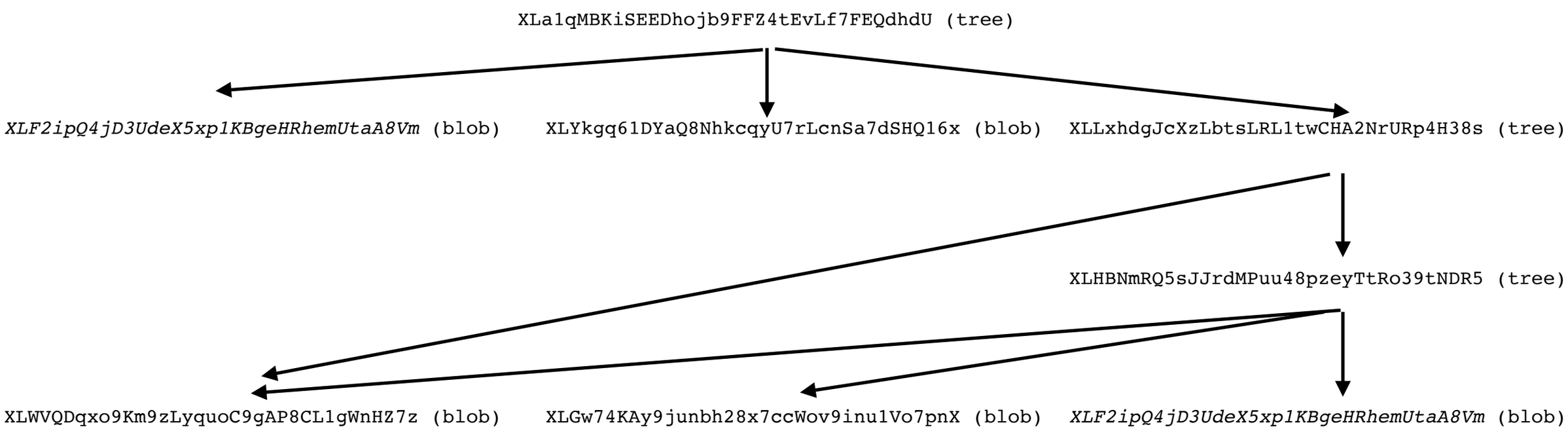
XLGw74KAy9junbh28x7ccWov9inu1Vo7pnX

/ipfs/XLGw74KAy9junbh28x7ccWov9inu1Vo7pnX/less (content+name)

/ipfs/XLHBNmRQ5sJJrdMPuu48pzeyTtRo39tNDR5 (only content)

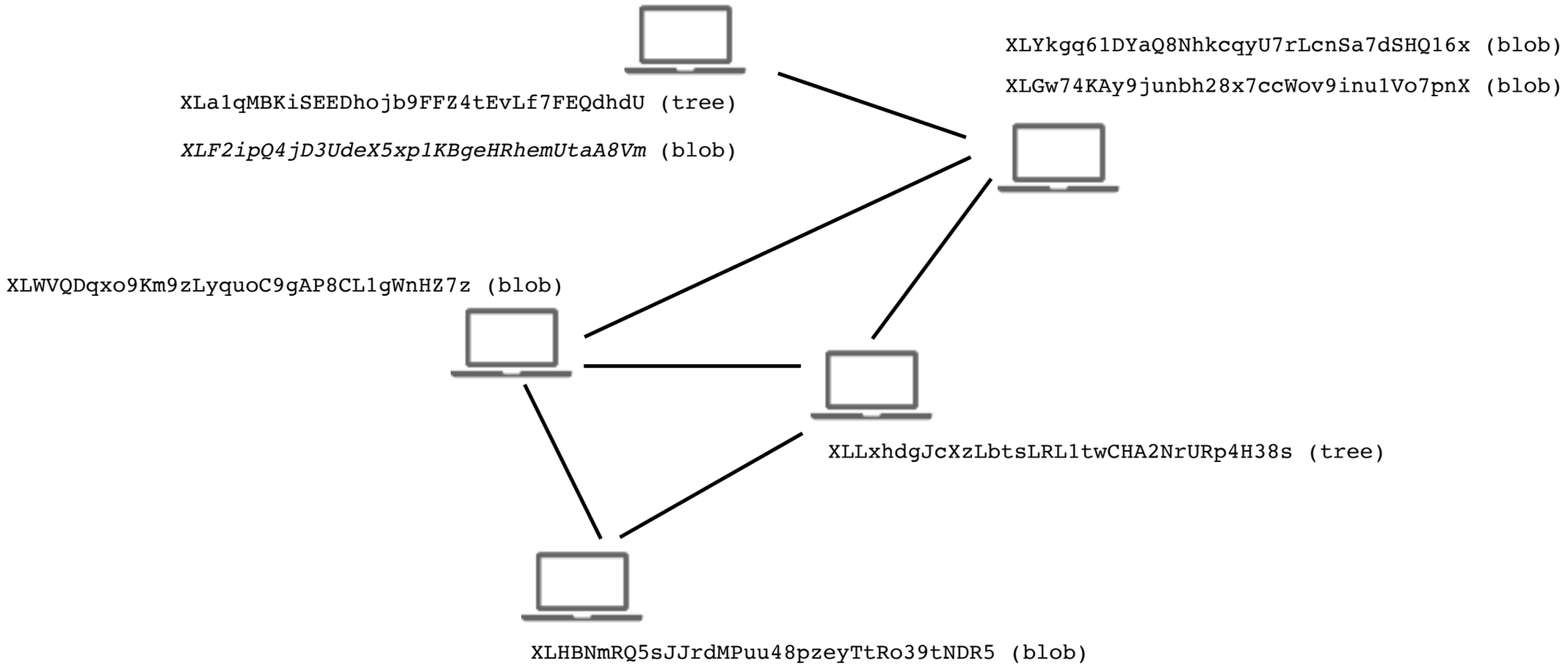
multihash : <function code><digest length><digest bytes>

Logical view



Each object is a entity, there’s no “unix-fs hard links”
Object Merkle DAG (Directed Acyclic Graph)

Deployment view



S/Kademlia Distributed Hash Table Protocol (DHT)
BitSwap for P2P transmition beteen nodes

The permanent web

DAG. Consider the properties of IPFS that fall out of the Merkle DAG: objects can be (a) retrieved via their hash, (b) integrity checked, (c) linked to others, and (d) cached indefinitely. In a sense:

Objects are **permanent**

These are the critical properties of a high-performance distributed system, where data is expensive to move across network links. Object content addressing constructs a web with (a) significant bandwidth optimizations, (b) untrusted content serving, (c) permanent links, and (d) the ability to make full permanent backups of any object and its references.

Signed anchors

- Local server has RSA4096 key
- One DAG object can be published a /ipns/<hash-of-server-public-key>
- Published object is signed by server private key
- Published object can be changed so, /ipns/… is mutable

Signed anchors

/ipns/lAksja92

signature

/ipfs/XLa1qMBKi (tree)

hash

/ipfs/*XLF2ipQ4jD* (blob)

hash

/ipfs/XLGw74KAy (blob)

/ipns/i19hjc9

signature

/ipfs/XLLxhdgJcX (tree)

hash

/ipfs/XLHBNmRQ5s (tree)

hash

hash

/ipfs/*XLF2ipQ4jD* (blob)

Use cases

- Mounted global filesystem, under /ipfs (permanent) and /ipns (mutable)
- Blockchain data structures
- Versioned package manager for all software
- Booting a virtual machine from the network from a hash
- Integrity-checked CDN for large static files (without SSL)
- The Permanent Web, where links do not die
- MaaD : Mars as a datacenter

Versioning

- “commit” node type under discussion
- go-ipfs using secure references for importing packages

```
package fsrepo

import (
  ...
  logging "gx/ipfs/QmSpJByNKFX1sCsHBEp3R73FL4NF6FnQTEGyNAXHm2GS52/go-log"
  util "gx/ipfs/QmZNVWh8LLjAavuQ2JXuFmuYH3C11xo988vSgp7UQrTRj1/go-ipfs-util"
  "gx/ipfs/QmeqtHtxGfcsfXiou7wqHJARWPKUTUcPdtSfSYYHp48dtQ/go-ds-measure"
)
```

Sybil attack

S/Kademlia based IPFS identity generation:

```
difficulty = <integer parameter>
n = Node{}
do {
  n.PubKey, n.PrivKey = PKI.genKeyPair()
  n.NodeId = hash(n.PubKey)
  p = count_preceding_zero_bits(hash(n.NodeId))
} while (p < difficulty)
```

Upon first connecting, peers exchange public keys, and check: `hash(other.PublicKey) equals other.NodeId`. If not, the connection is terminated.

Sybil attack: the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence.

- Sybil Isabel Dorsett (1923), the main personality
- Victoria Antoinette Scharleau (1926), nicknamed Vicky, self-assured a
- Peggy Lou Baldwin (1926), assertive, enthusiastic, and often angry
- Peggy Ann Baldwin (1926), a counterpart of Peggy Lou but more fear
- Mary Lucinda Saunders Dorsett (1933), a thoughtful, contemplative, a
- Marcia Lynn Dorsett (1927), an extremely emotional writer and painte
- Vanessa Gail Dorsett (1935), intensely dramatic, fun loving, and a tal
- Mike Dorsett (1928), one of Sybil's two male selves, a builder and a c
- Sid Dorsett (1926), the second of Sybil's two male selves, a carpente
  Mason's personality would have been named Sam (**S**hirley **A**rdell **Ma**
- Nancy Lou Ann Baldwin (date undetermined), interested in politics as
- Sybil Ann Dorsett (1928), listless to the point of neurasthenia
- Ruthie Dorsett (date undetermined), a baby and one of the less devel
- Clara Dorsett (date undetermined), intensely religious and highly criti
- Helen Dorsett (1929), intensely afraid but determined to achieve fulfil
- Marjorie Dorsett (1928), serene, vivacious, and quick to laugh
- The Blonde (1946), a nameless perpetual teenager with an optimistic

Demo time

gràcies

adria@codecontext.io
@codecontext