Jug Summer Camp

-enjoy it-

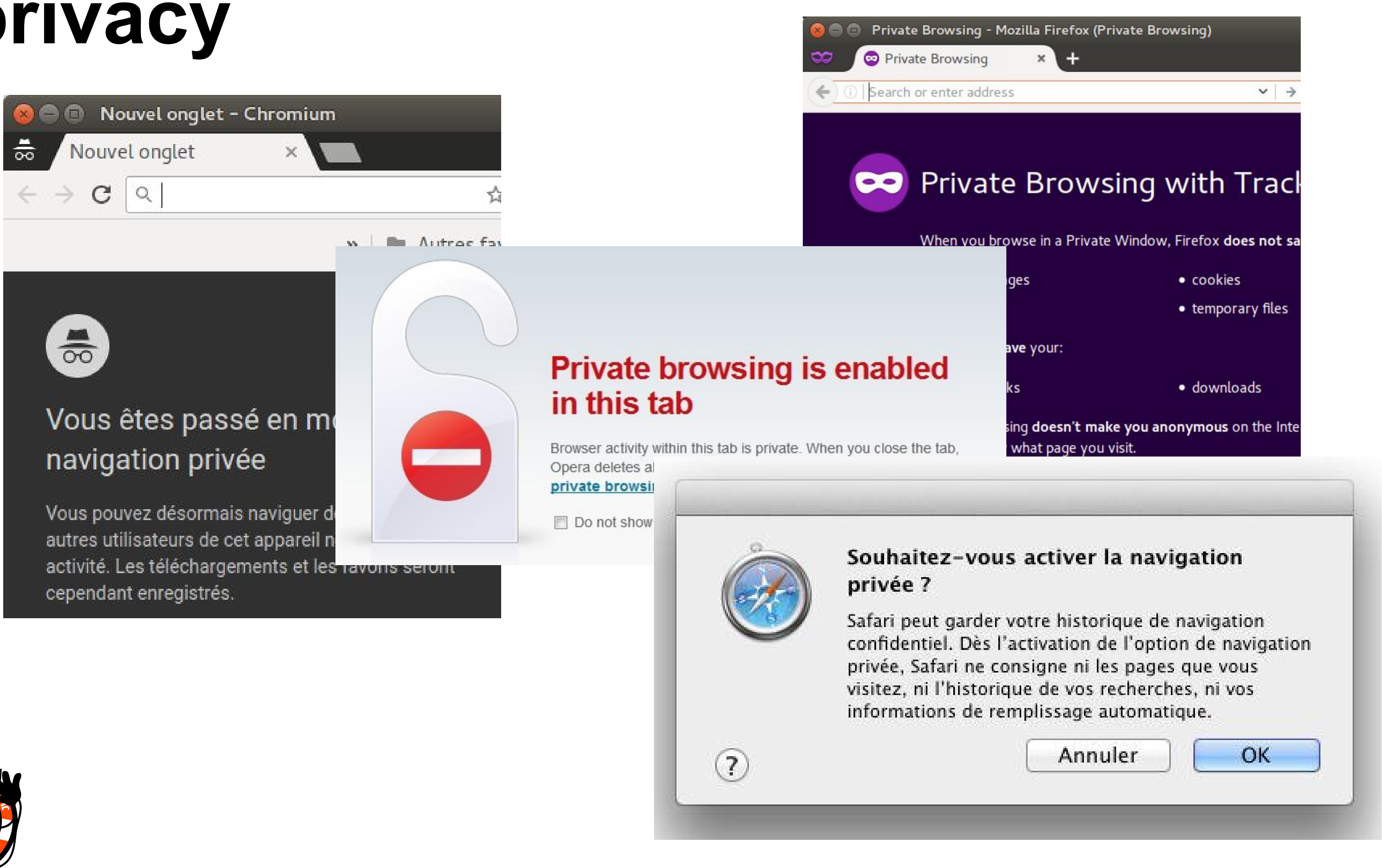
Du P2P dans vos applications

Speaker : Jérôme Creignou - @jcreignou

Pourquoi des applis P2P ?

privacy

privacy



Nouvel onglet - Chromium

Nouvel onglet

Autres fav

Vous êtes passé en m
navigation privée

Vous pouvez désormais naviguer d
autres utilisateurs de cet appareil n
activité. Les téléchargements et les favoris seront
cependant enregistrés.

Private Browsing - Mozilla Firefox (Private Browsing)

Private Browsing

Search or enter address

Private Browsing with Track

When you browse in a Private Window, Firefox **does not sa**

ges

- cookies
- temporary files

ave your:

ks

- downloads

sing **doesn't make you anonymous** on the Inte
what page you visit.

Private browsing is enabled in this tab

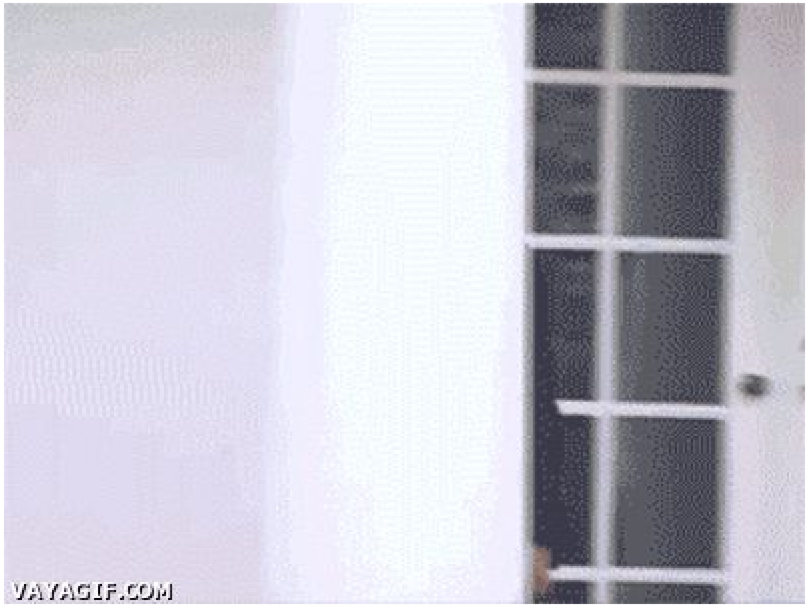
Browser activity within this tab is private. When you close the tab,
Opera deletes al
private browsi

□ Do not show

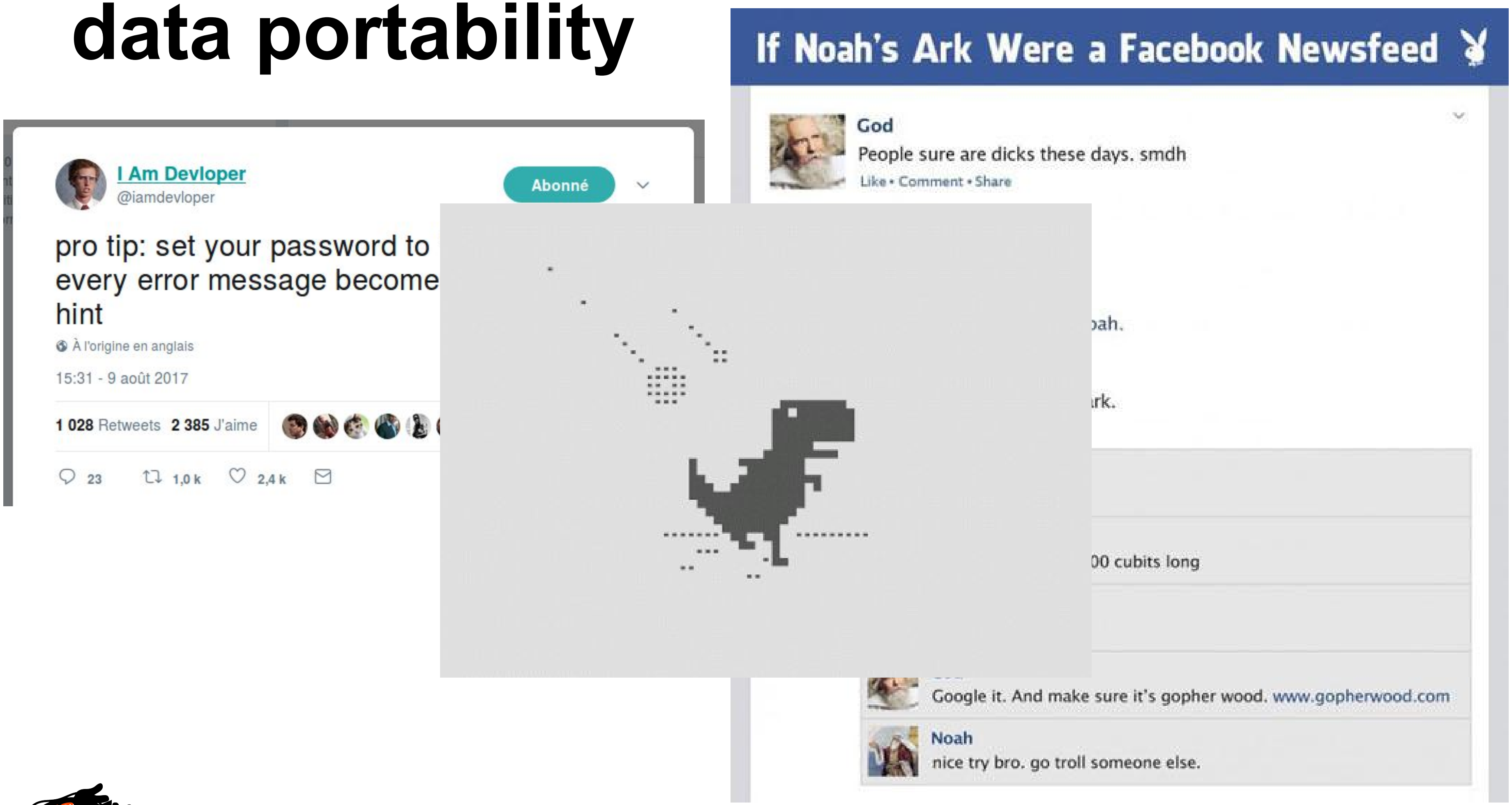
Souhaitez-vous activer la navigation privée ?

Safari peut garder votre historique de navigation confidentiel. Dès l'activation de l'option de navigation privée, Safari ne consigne ni les pages que vous visitez, ni l'historique de vos recherches, ni vos informations de remplissage automatique.

data portability



data portability



I Am Devloper
@iamdevloper
Abonné

pro tip: set your password to
every error message become
hint

À l'origine en anglais

15:31 - 9 août 2017

1 028 Retweets 2 385 J'aime

23 1,0 k 2,4 k

If Noah's Ark Were a Facebook Newsfeed

God
People sure are dicks these days. smdh
Like • Comment • Share

oah.

rk.

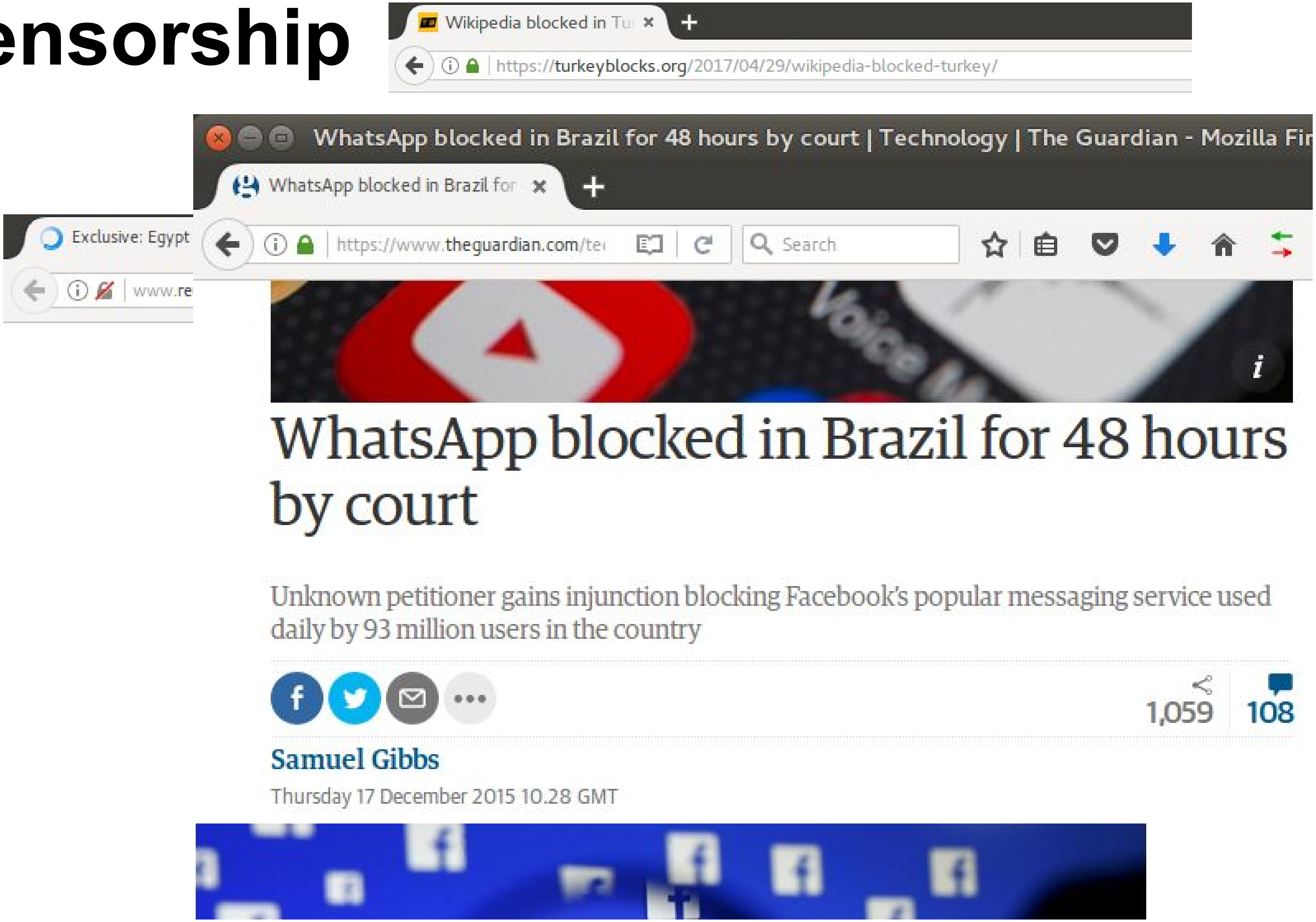
00 cubits long

Google it. And make sure it's gopher wood. www.gopherwood.com

Noah
nice try bro. go troll someone else.

censorship

censorship



Wikipedia blocked in Tu

https://turkeyblocks.org/2017/04/29/wikipedia-blocked-turkey/

Exclusive: Egypt

www.re

WhatsApp blocked in Brazil for 48 hours by court | Technology | The Guardian - Mozilla Fi

WhatsApp blocked in Brazil for

https://www.theguardian.com/te

Search

WhatsApp blocked in Brazil for 48 hours by court

Unknown petitioner gains injunction blocking Facebook's popular messaging service used daily by 93 million users in the country

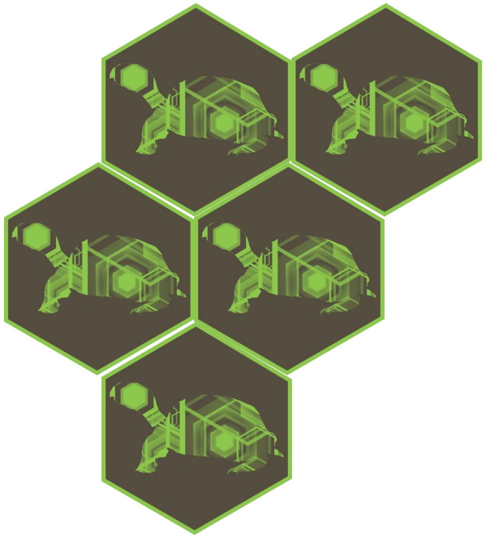
1,059 108

Samuel Gibbs

Thursday 17 December 2015 10.28 GMT

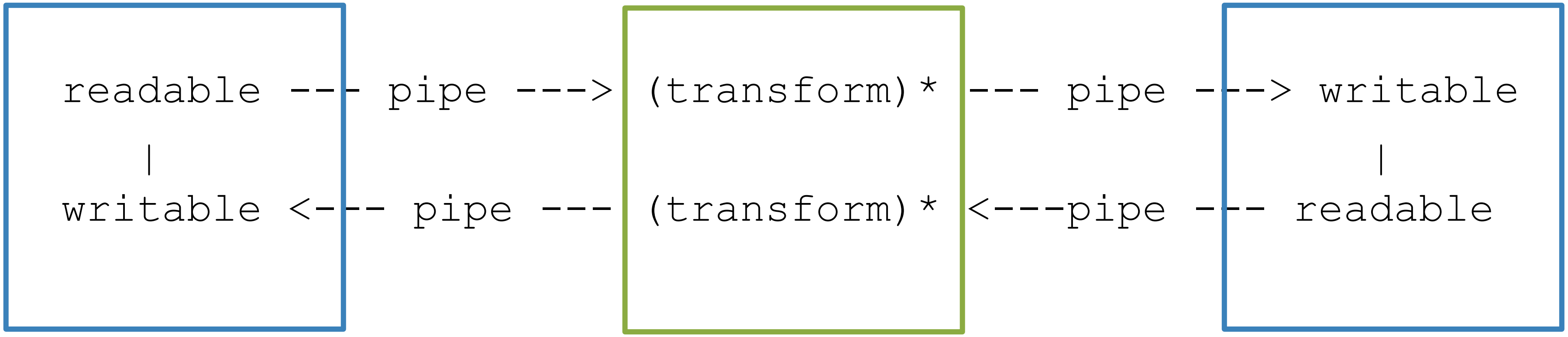
security

c’est parti !



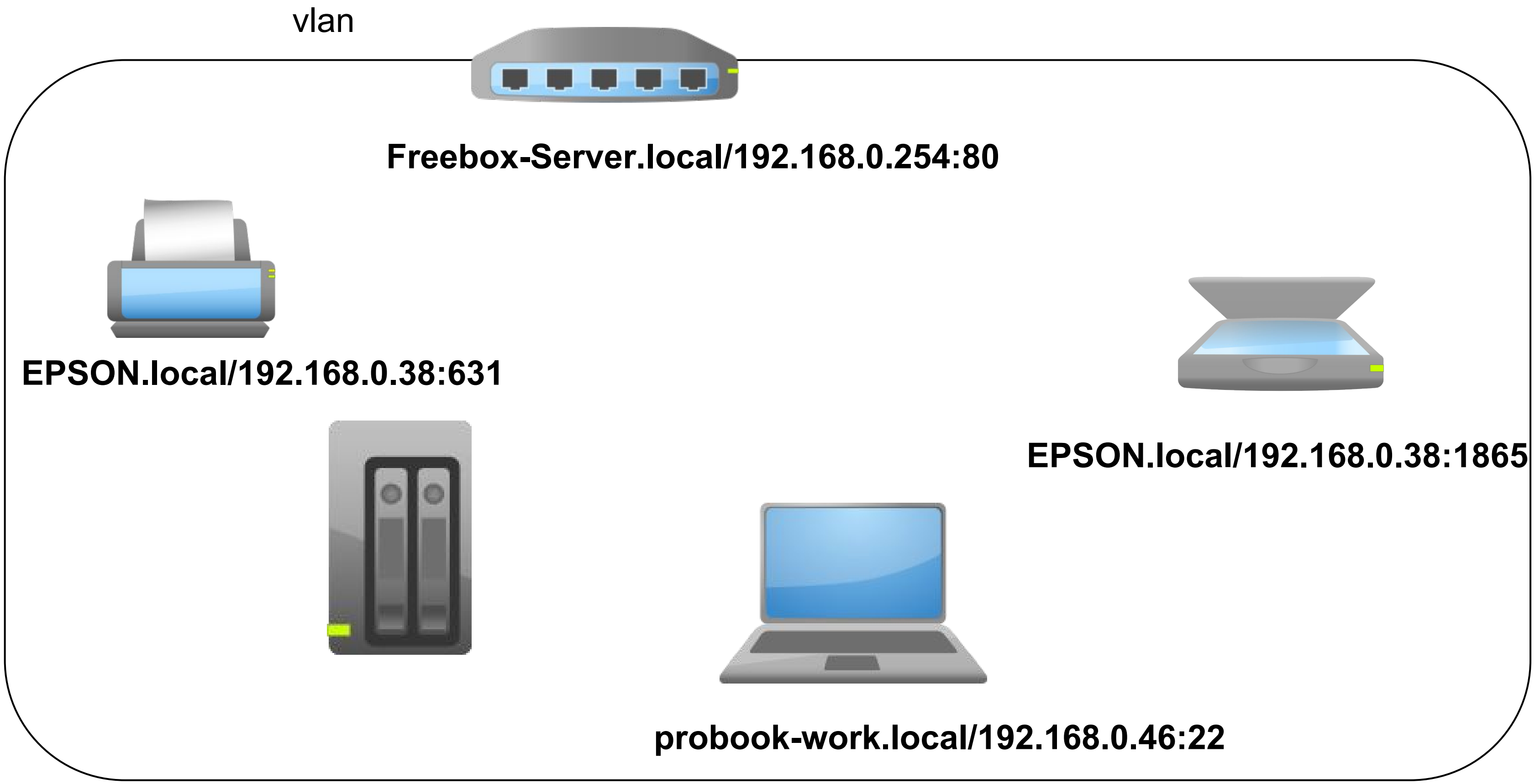
connectivité :
nodejs streams

```
process.stdin.pipe(process.stdout);
```



```
  readable --- pipe ---> (transform)* --- pipe ---> writable
     |                                                 |
  writable <--- pipe --- (transform)* <---pipe --- readable
```

découverte des pairs :
multicast dns / dns-sd / bonjour



vlan

Freebox-Server.local/192.168.0.254:80

EPSON.local/192.168.0.38:631

EPSON.local/192.168.0.38:1865

probook-work.local/192.168.0.46:22

découverte des pairs :

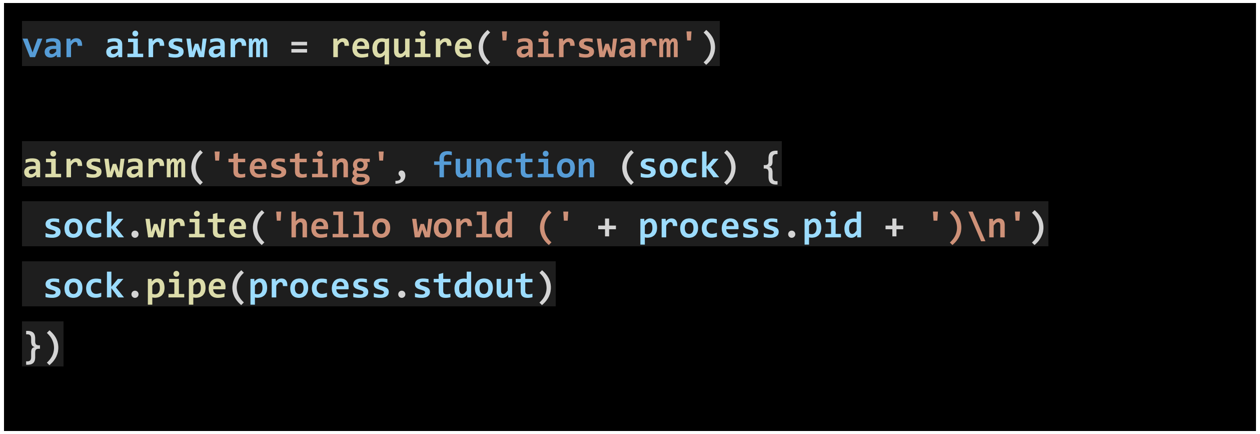
Exemple :

Airpaste

https://github.com/mafintosh/airpaste

découverte des pairs :
exemple

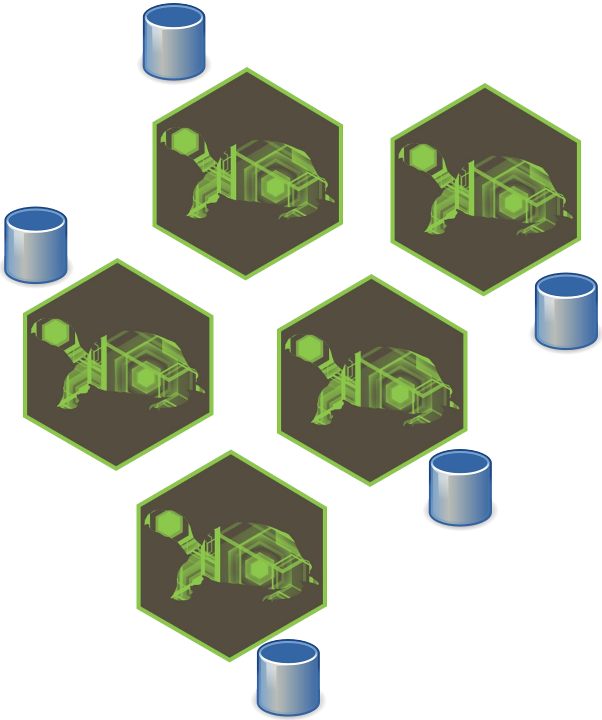
airswarm :



```
var airswarm = require('airswarm')

airswarm('testing', function (sock) {
 sock.write('hello world (' + process.pid + ')\n')
 sock.pipe(process.stdout)
})
```

github.com/mafintosh/airswarm

Persistance / réplication



Persistance / réplication
structures de données

Eventual consistency

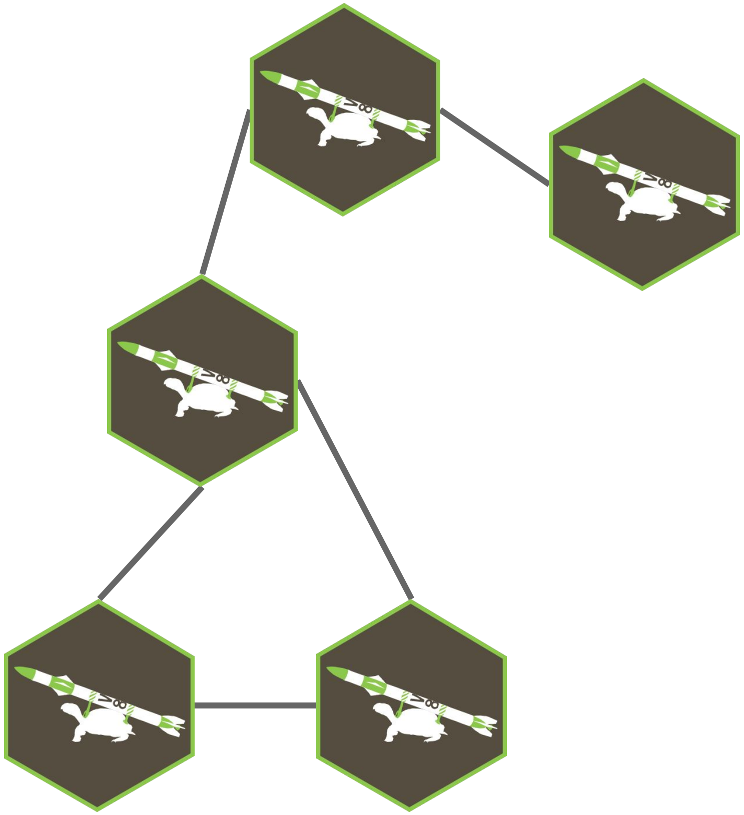
Conflict-free Replicated Data Type
data structure which can be ***replicated across multiple computers*** *in a network, where the replicas can be* ***updated independently and concurrently without coordination*** *between the replicas, and where it is always* ***mathematically possible*** *to resolve inconsistencies which might result.*

Précédence: “causal ordering"
Horloge de Lamport

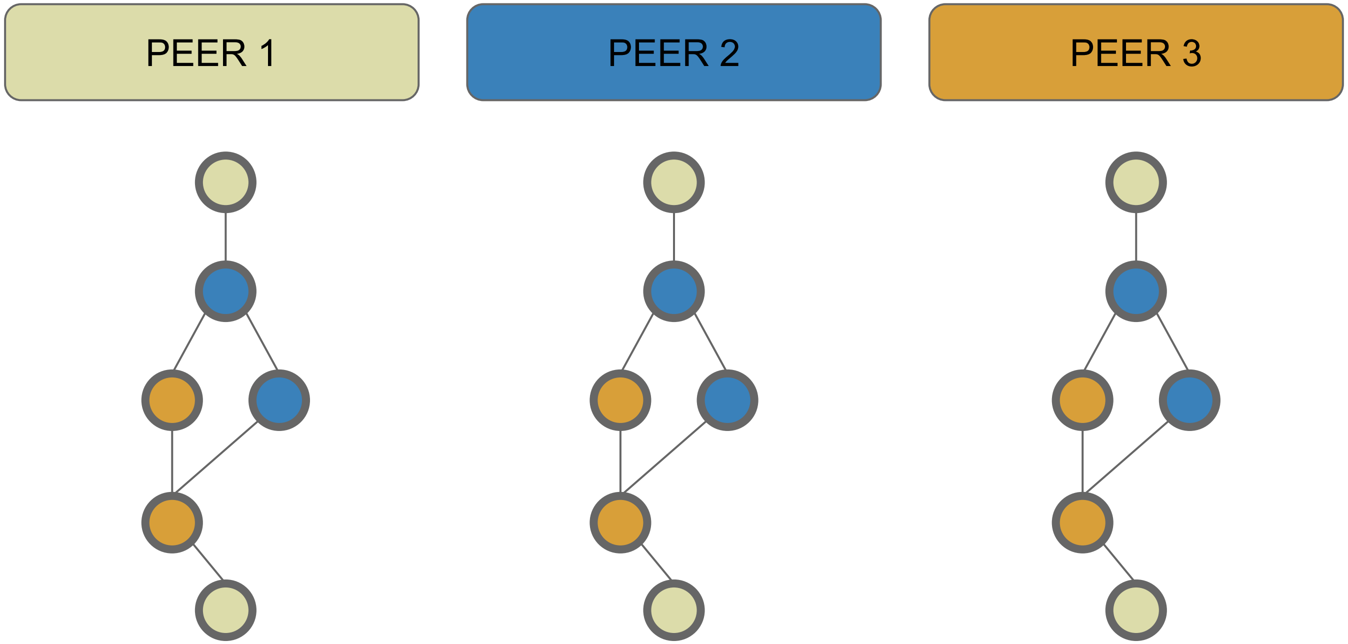
Intégrité: Merkle graph

Persistance / réplication:

- Amazon (S3)
- Bittorrent
- BGP



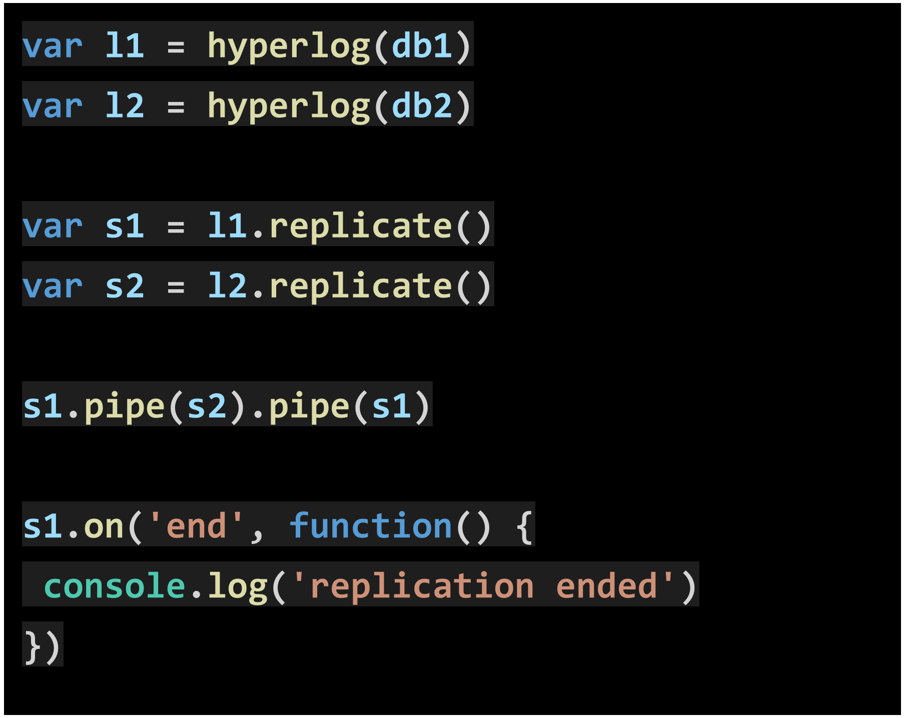
Persistance / réplication:



Persistance / réplication:
exemple

Hyperlog :

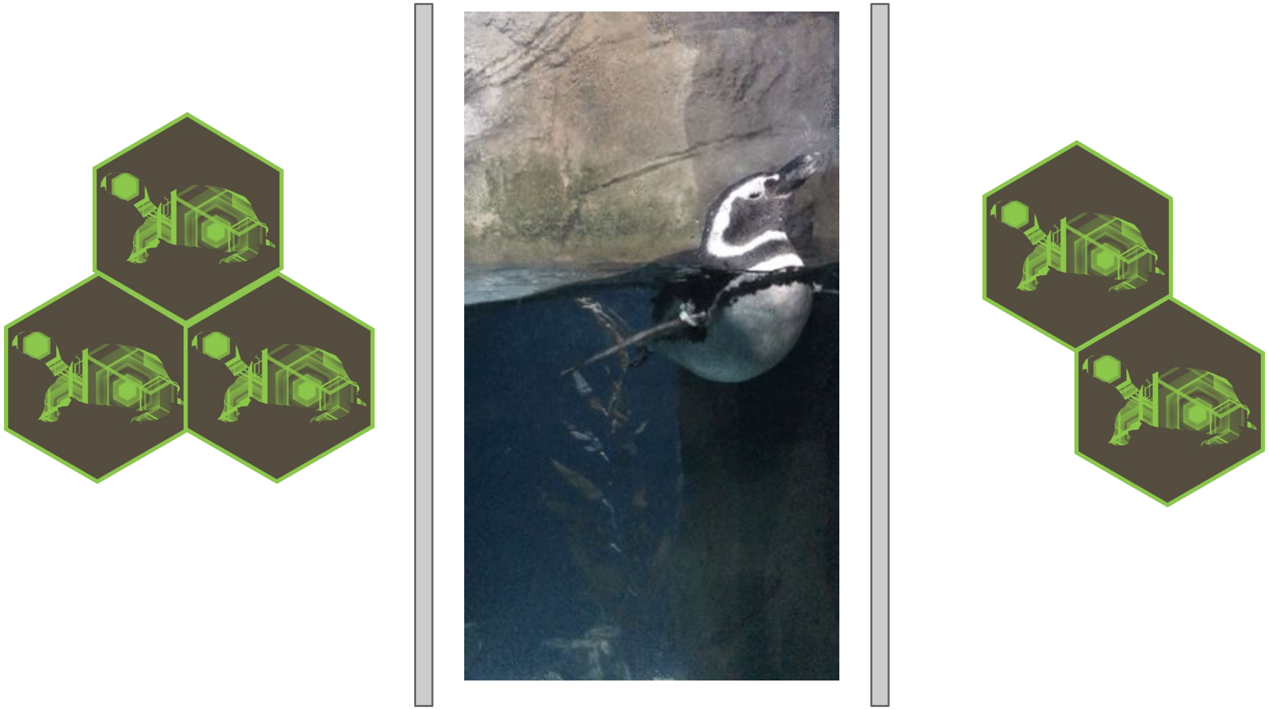
- Merkle graph
- scuttlebutt (gossip)
- leveldb



```
var l1 = hyperlog(db1)
var l2 = hyperlog(db2)

var s1 = l1.replicate()
var s2 = l2.replicate()

s1.pipe(s2).pipe(s1)

s1.on('end', function() {
 console.log('replication ended')
})
```

github.com/mafintosh/hyperlog

Firewalls



Firewalls :
Signaling / STUN

Session Traversal Utilities for NAT STUN	NAT STUN	IETF RFC 5389
Universal Plug-and-Play	UPnP	UPnP.org
Port Control Protocol	PCP	RFC 6887
Hosted NAT Traversal	HNT	Draft MMUSIC-Latching
Traversal Using Relays around NAT	TURN	IETF RFC 5766
Jingle Relay Nodes	XSF	XEP-0278
Interactive Connectivity Establishment	ICE	IETF RFC 5245
Interactive Connectivity Establishment for ICE	Trickle ICE	IETF DRAFT MMUSIC-Trickle-ICE

Firewalls :
découverte des pairs

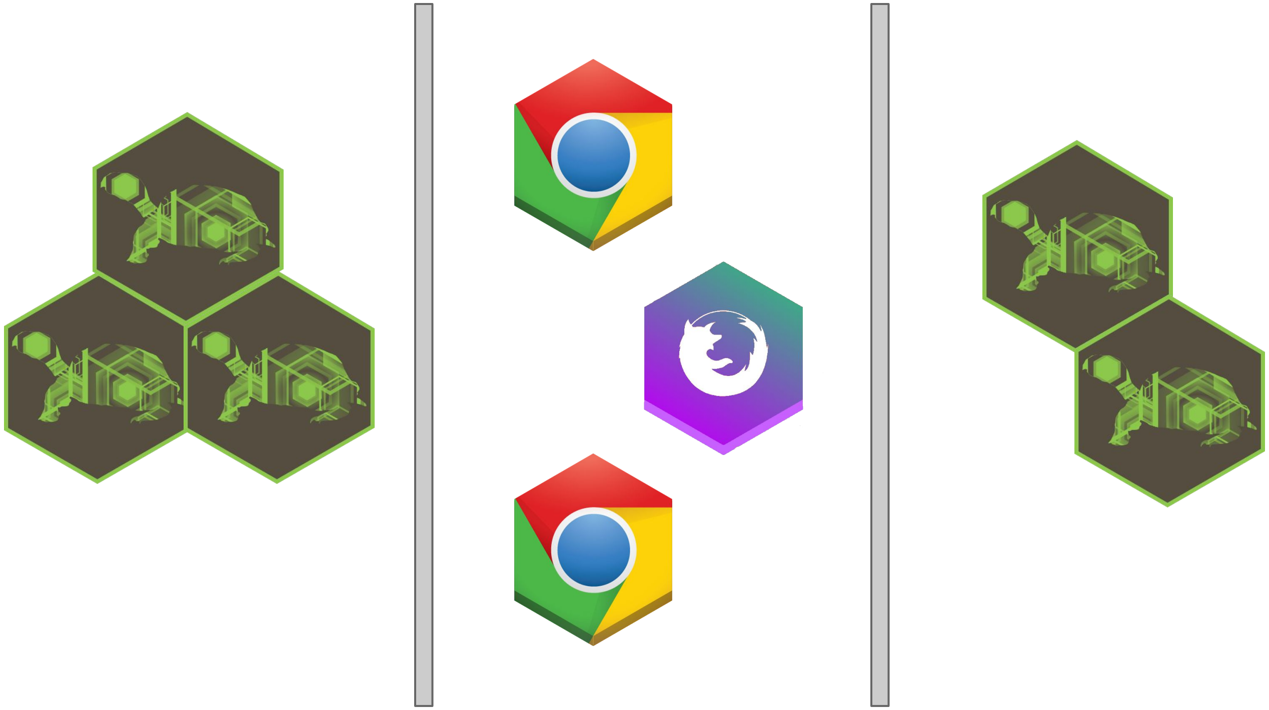
Pairs initiaux :

- dns / ip hardcoded
  - bitcoin : *seed.bitcoin.sipa.be* (dns seed)

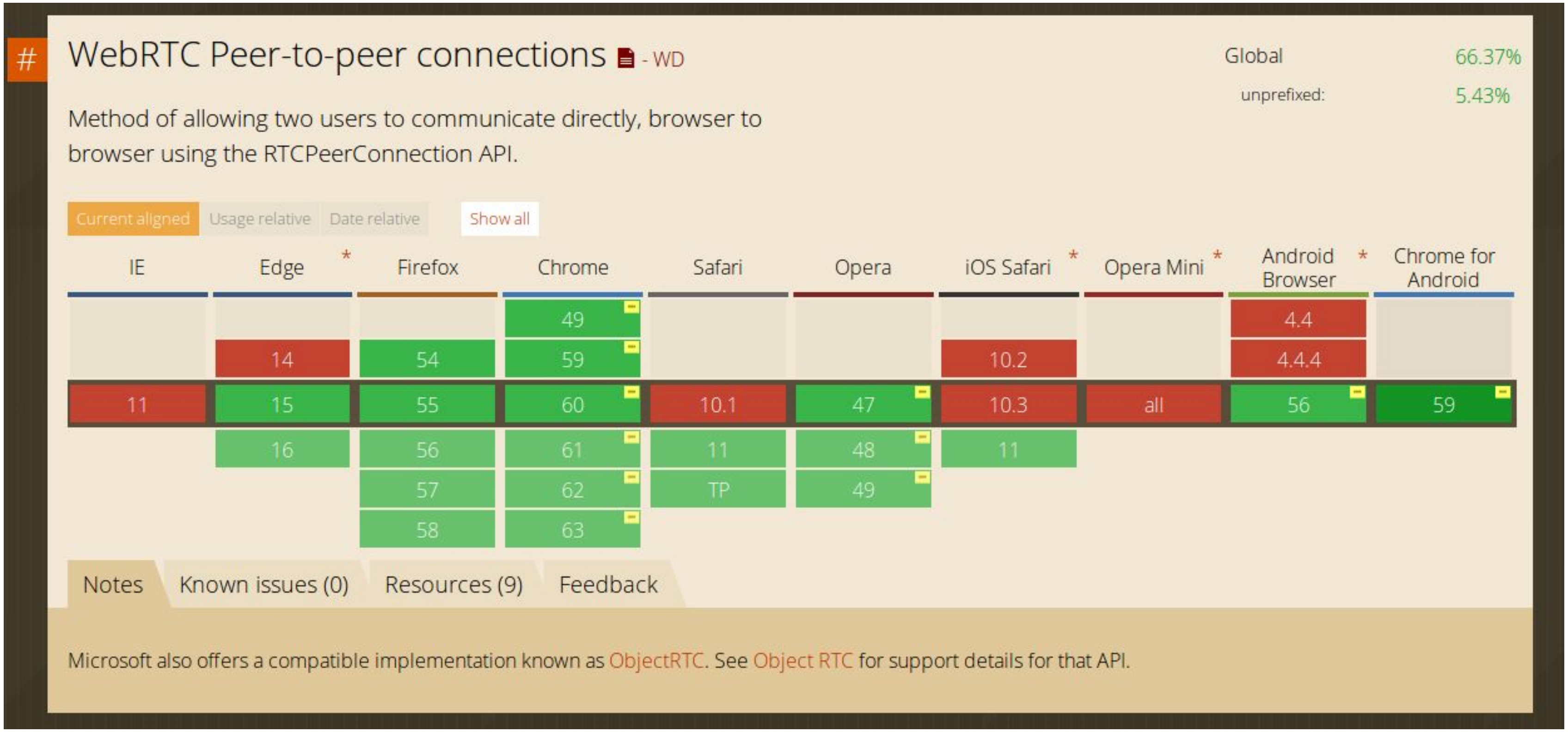
Distributed Hash Table (DHT) :

- stocke les adresses des pairs dans la DHT

et le web ?



connectivité :
webrtc & datachannels



WebRTC Peer-to-peer connections - WD

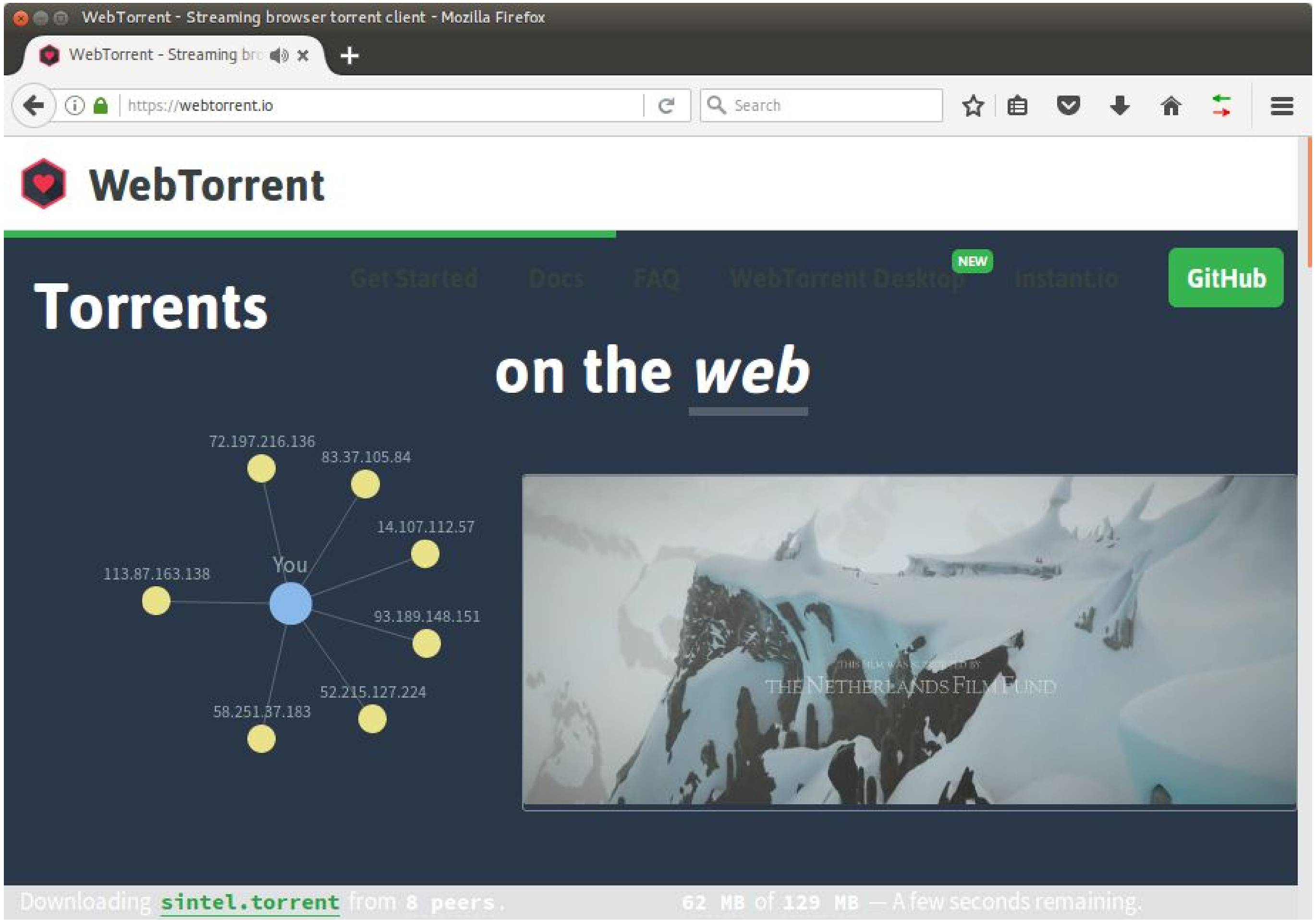
Global 66.37%
unprefixed: 5.43%

Method of allowing two users to communicate directly, browser to browser using the RTCPeerConnection API.

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Android Browser *	Chrome for Android
			49					4.4	
	14	54	59			10.2		4.4.4	
11	15	55	60	10.1	47	10.3	all	56	59
	16	56	61	11	48	11			
		57	62	TP	49				
		58	63						

Microsoft also offers a compatible implementation known as ObjectRTC. See Object RTC for support details for that API.

connectivité :
webrtc & datachannels



WebTorrent - Streaming browser torrent client - Mozilla Firefox

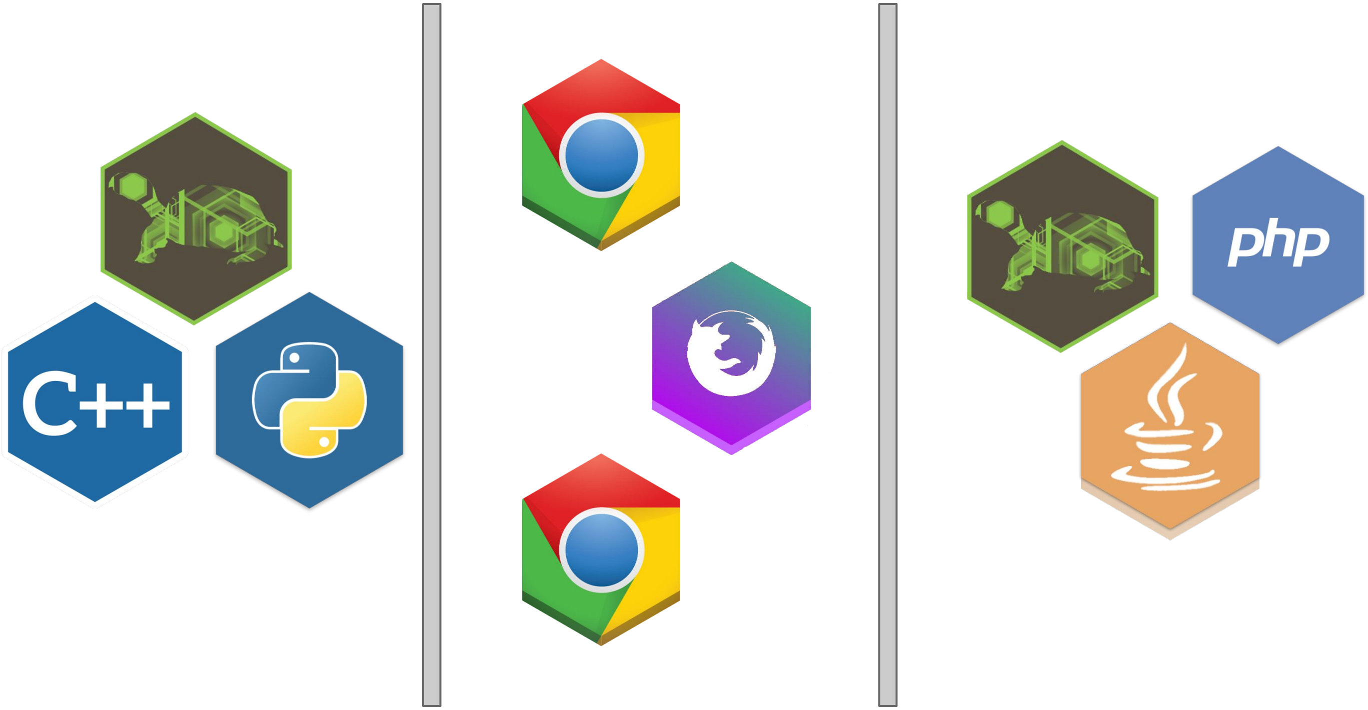
https://webtorrent.io

WebTorrent

Torrents on the *web*

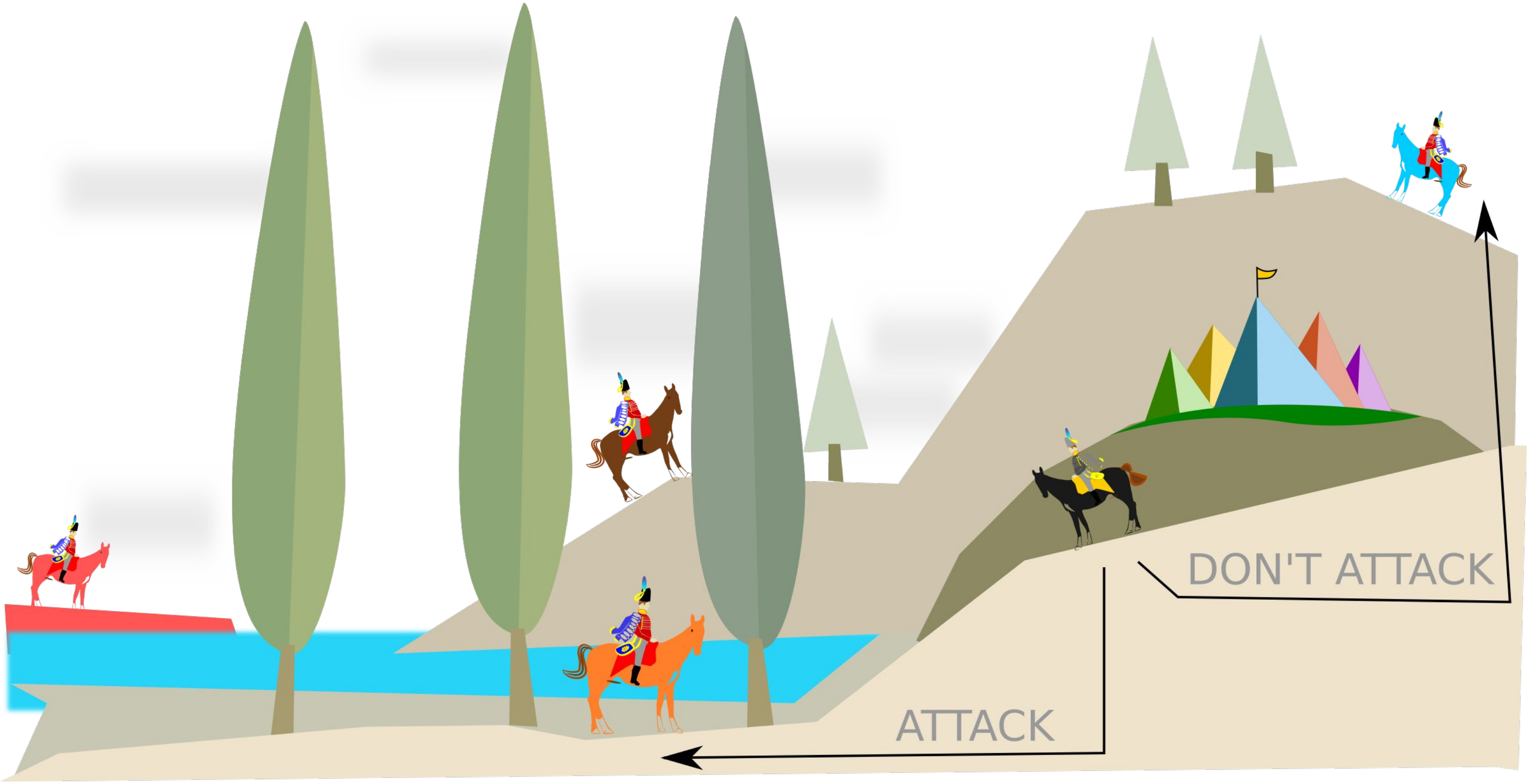
Downloading sintel.torrent from 8 peers. 62 MB of 129 MB — A few seconds remaining.

Ecosystème



Ecosystème : rogue peers

- problème des “généraux byzantins”



Ecosystème :
règles sociales

favoriser le bon comportement des pairs

bittorrent :

- demander les parties de fichier les plus rares
- donner la priorité au pairs ayant échangé le plus de parties de fichiers

=> mais pas d’intéressement pour seeder un fichier qui est fini de télécharger

The web was designed to be decentralised so that everybody could participate by having their own domain and having their own webserver and this hasn't worked out. Instead, we've got the situation where individual personal data has been locked up in these silos.

tim berners-lee

Apps / protocoles

- DAT project : https://datproject.org/
- IPFS : https://ipfs.io/
- Beaker Browser : https://beakerbrowser.com/
- secure-scuttlebutt : https://github.com/ssbc/secure-scuttlebutt
- webtorrent : https://webtorrent.io/

Sources

- https://giphy.com
- https://macwright.org/2017/07/20/decentralize-your-website.html
- https://techcrunch.com/2016/10/09/a-decentralized-web-would-give-power-back-to-the-people-online
- http://www.novaplanet.com/radionova/79531/episode-c-est-la-crise-chez-wikimedia
- https://staltz.com/an-off-grid-social-network.html
- https://github.com/noffle/p2p-handbook
- https://github.com/kgryte/awesome-peer-to-peer
- https://www.html5rocks.com/en/tutorials/webrtc/basics/
- https://ipfs.io/blog/24-uncensorable-wikipedia/
- https://webrtchacks.com/trickle-ice/
- https://en.wikipedia.org/wiki/Gossip_protocol
- http://www.bortzmeyer.org/gossip-protocol.html
- https://en.wikipedia.org/wiki/Merkle_tree
- https://bitcoin.org/en/developer-guide#peer-discovery
- https://en.wikipedia.org/wiki/Conflict-free_replicated_data_type
- http://christophermeiklejohn.com/crdt/2014/07/22/readings-in-crdts.html
- https://fr.slideshare.net/seancribbs/eventuallyconsistent-data-structures

Publications

Gossip/Scuttlebut protocol :

- http://www.cs.cornell.edu/home/rvr/papers/flowgossip.pdf

Merkle Trees :

- http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/becker_1.pdf
- https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/merkleodb.pdf

CRDTs :

- https://run.unl.pt/bitstream/10362/7802/1/Sousa_2012.pdf
- https://hal.inria.fr/inria-00555588/document

Merci