

Le web décentralisé

TOURAINETECH 2018



@AntoineCailly



acailly



zenika



**Il était une fois le web
en 2017...**

Censure



Sat Apr 29 2017 08:02:55 GMT+0300 (+03)
<https://en.wikipedia.org> 5005 DOWN
<https://tr.wikipedia.org> 5009 DOWN
<https://az.wikipedia.org> 5009 DOWN
<https://fr.wikipedia.org> 5007 DOWN
<https://www.wikipedia.org> 5007 DOWN



Turkey Blocks

@TurkeyBlocks



Suivre

Confirmed: All editions of the [#Wikipedia](#) online encyclopedia blocked in [#Turkey](#) as of 8:00AM local time turkeyblocks.org/2017/04/29/wik...

07:22 - 29 avr. 2017



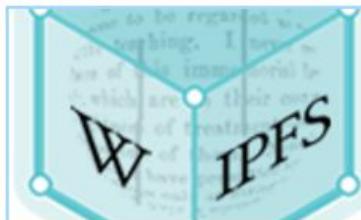
86



2 875



1 015



Vikipedi'ye hoş geldiniz

Herkesin katkıda bulunabildiği Özgür Ansiklopedi

Türkçe madde sayısı: 288.931

9 Ocak 2017, Pazartesi

- Bilim

- Coğrafya

- Din

- Fizik

- Matematik

- Sanat

- Spor

- Tarih

- Tüm portaller

Haftanın seçkin maddesi



Mars, Güneş Sistemi'nin Güneş'ten itibaren dördüncü gezegeni. Roma mitolojisindeki savaş tanrıları Mars'a ithafen adlandırılmıştır. Yüzeyindeki yaygın demir oksitten dolayı kızılımsı bir görünümü sahip olduğu için *Kızıl Gezegen* de denir. İnce bir atmosferi olan Mars gerek Ay'daki gibi meteor kraterlerini, gerekse Dünya'daki

gibi volkan, vadi, çöl ve kutup bölgelerini içeren çehresiyle bir *yerbenzeri gezegendir*. Ayrıca dönme periyodu ve mevsim dönemleri Dünya'ninkine çok benzer.

<https://ipfs.io/ipfs/QmT5NvUtoM5nWFfrQdVrFtvGfKFmG7AHE8P34isapyhCxX/wiki/Anasayfa.html>

Güneş Sistemi'nde bilinen en yüksek dağ ve *Marineris Vadisi* adlı kanyon en büyük kanyondur. Ayrıca Haziran

2008'de *Nature* dergisinde yayımlanan üç makalede

Günün seçkin resmi





Referèndum 2017

Inici

Normativa electoral

Sindicatures electorals

Sala de premsa

Com s'ha de votar

On votar



Col·laboradors del referèndum

El més destacat

- Material per descarregar
- Calendari electoral
- Call for international monitoring

Preguntes més freqüents

Electors

Calendari electoral

Mesos electorals

Suppression des données



Donald J. Trump 
@realDonaldTrump



Suivre

It's freezing in New York—where the hell is global warming?

21:37 - 23 avr. 2013



397



470



281



Trump Just Deleted Obama's Climate Change Webpages



By Brian Kahn

Follow @blkahn

9,117 followers



Published: January 20th, 2017

At the exact hour when the presidency transferred hands, the Obama administration's climate and energy webpages became some of the first casualties of the new Trump administration.

In their place is an "["America first" energy plan](#)", which talks at length about tapping fossil fuel resources in the U.S. but makes no mention of climate change or renewable energy. Investing in the latter will be crucial to avert catastrophic changes to the world.



<http://www.climatecentral.org/news/trump-delete-climate-change-webpage-21091>

Obama's climate page has been sent off to the archive.

Building refuge for federal climate & environmental data

DataRefuge helps to build refuge for federal data and supports climate and environmental research and advocacy. We are committed to fact-based arguments. DataRefuge preserves the facts we need at a time of ongoing climate change.

This site is one part of the project. The vast majority of the government information gathered through this project is available from the Internet Archive through the [End of Term project](#). This data catalog is a place to store data that is difficult or impossible to harvest through web crawlers. Data was added to this site by volunteers at [Data Rescue events](#). You can see the [workflow](#) used at many of these events on the Data Refuge project site, however this workflow is no longer supported.



<https://www.datarefuge.org/>



maxwell ogden
@denormalize

 Suivre

Today Trump removed all open data (9GB) from the White House open.whitehouse.gov/browse but I grabbed it all Jan 20! Will distribute soon

21:12 - 14 févr. 2017

288 8 854 12 877

Shared with Dat

Explore public data shared with Dat.



EXECUTIVE OFFICE OF THE PRESIDENT

Archive of open.whitehouse.gov

Backup of the open data released by President Barack Obama
before being deleted in February, 2017.

Preview

<https://datproject.org/explore>

Centralisation des services



Recherche



Maps



YouTube



Play



Actualités



Contacts



Drive



Agenda



Docs



Traduction



Photos



Inbox



WhatsApp



waze



Instagram



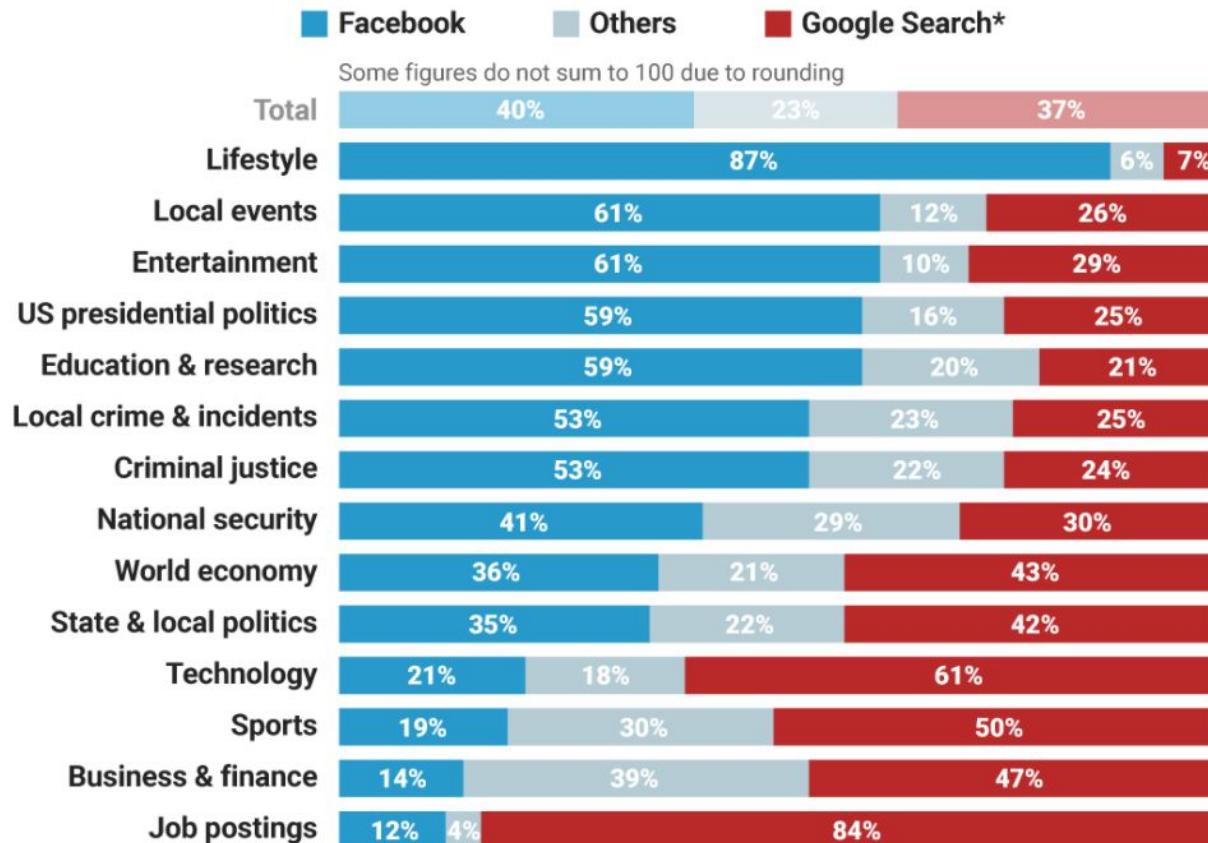
ANDROID



chrome

Centralisation du trafic

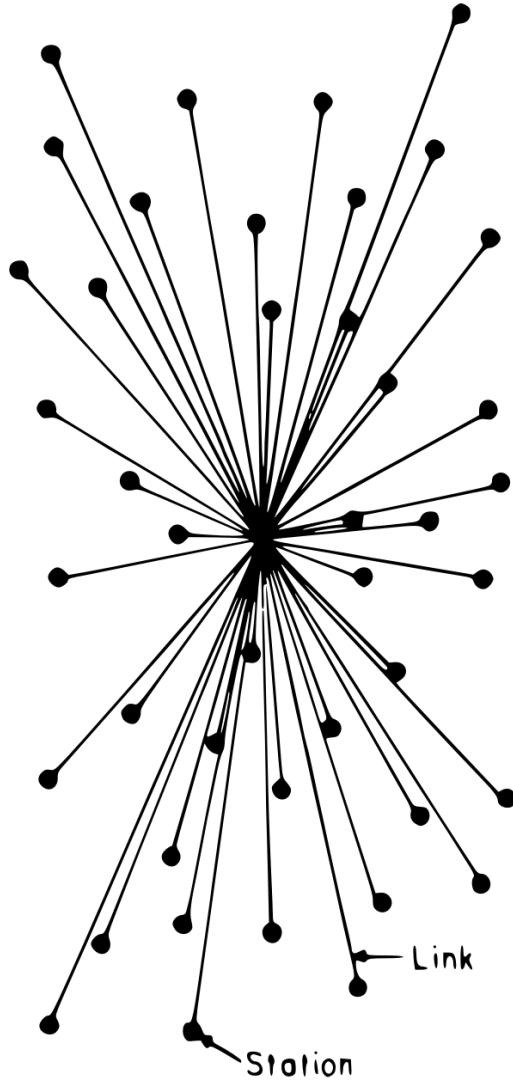
DISTRIBUTION OF REFERRAL TRAFFIC SOURCES BY TOPIC



SOURCE: Parse.ly *Not including Google AMP

statista | BUSINESS INSIDER

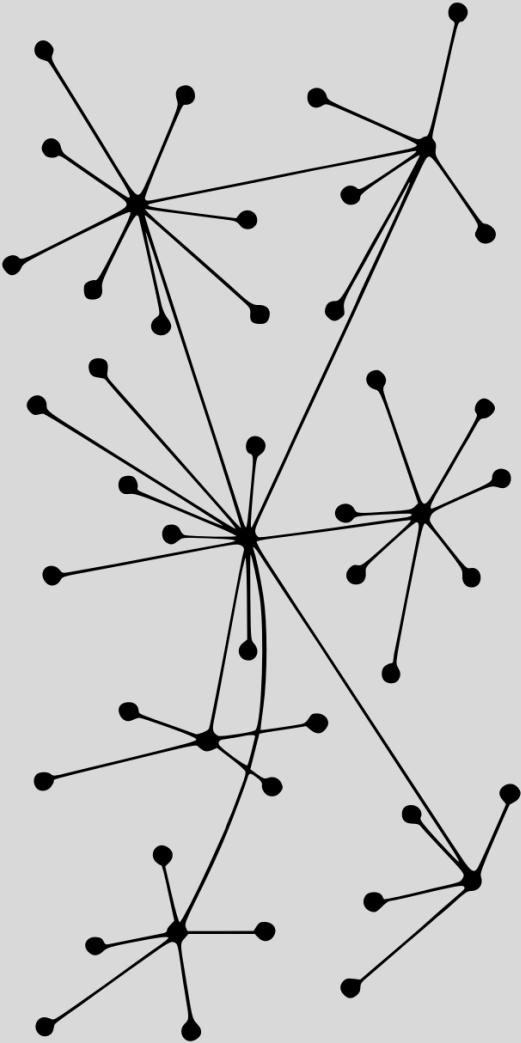
**Un point
commun ?**



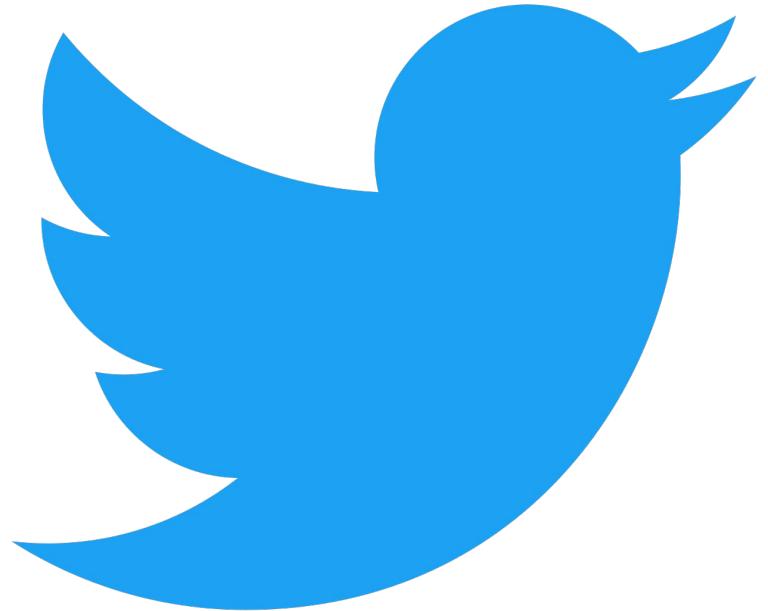
**Single
point of
failure**

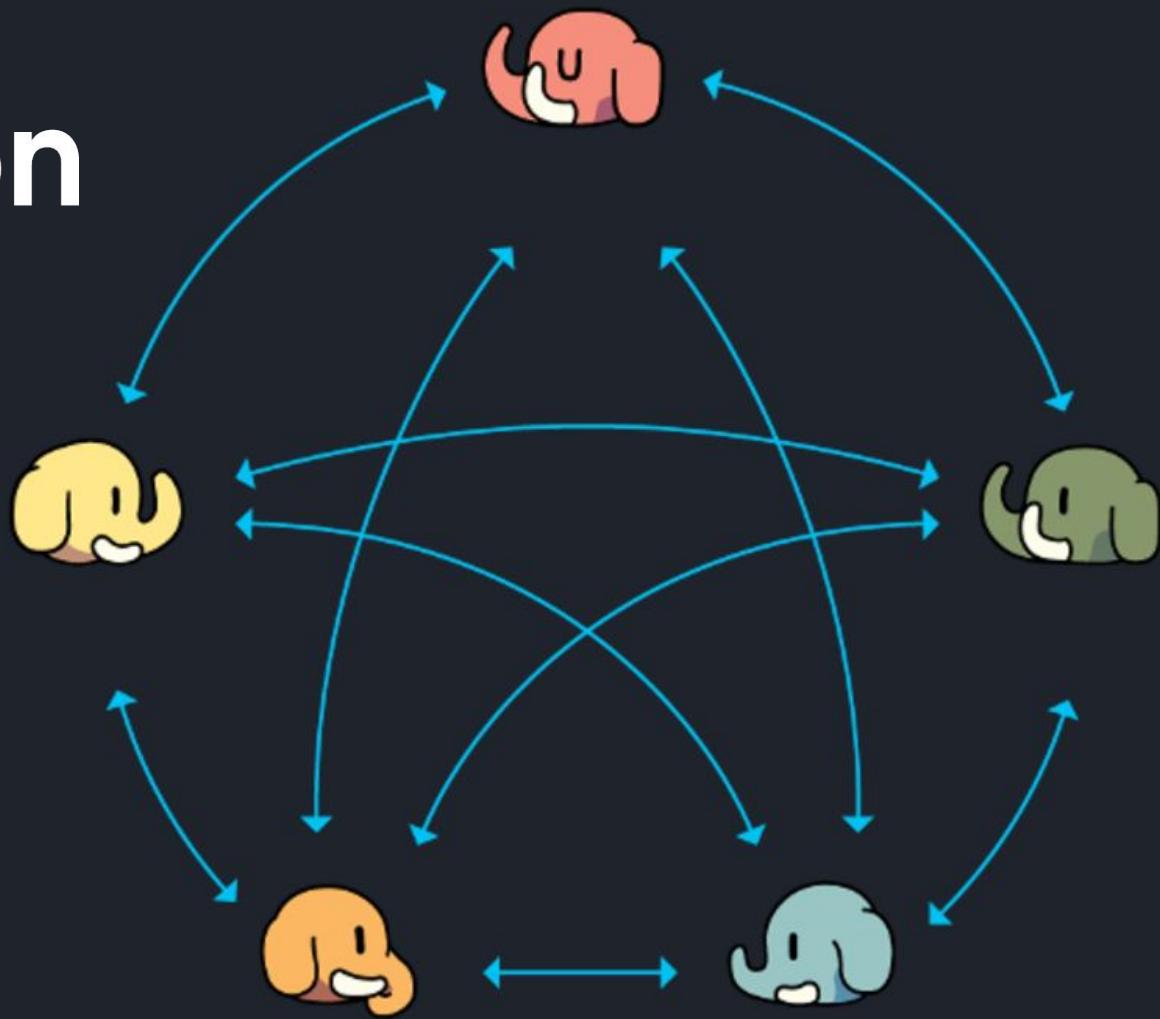
**Single
point of
control**

Une solution ?



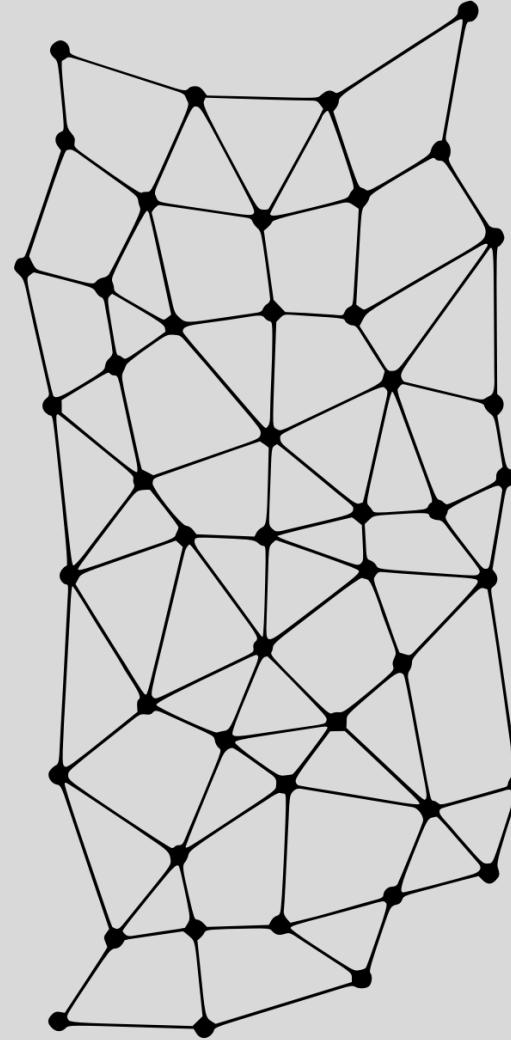
Décentralisé

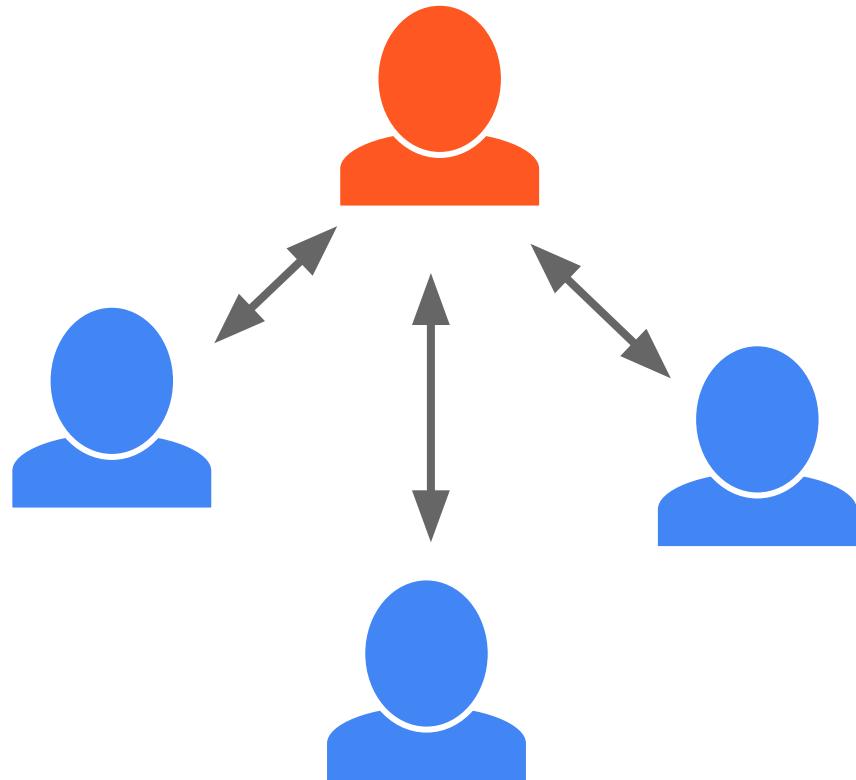




<https://joinmastodon.org/>

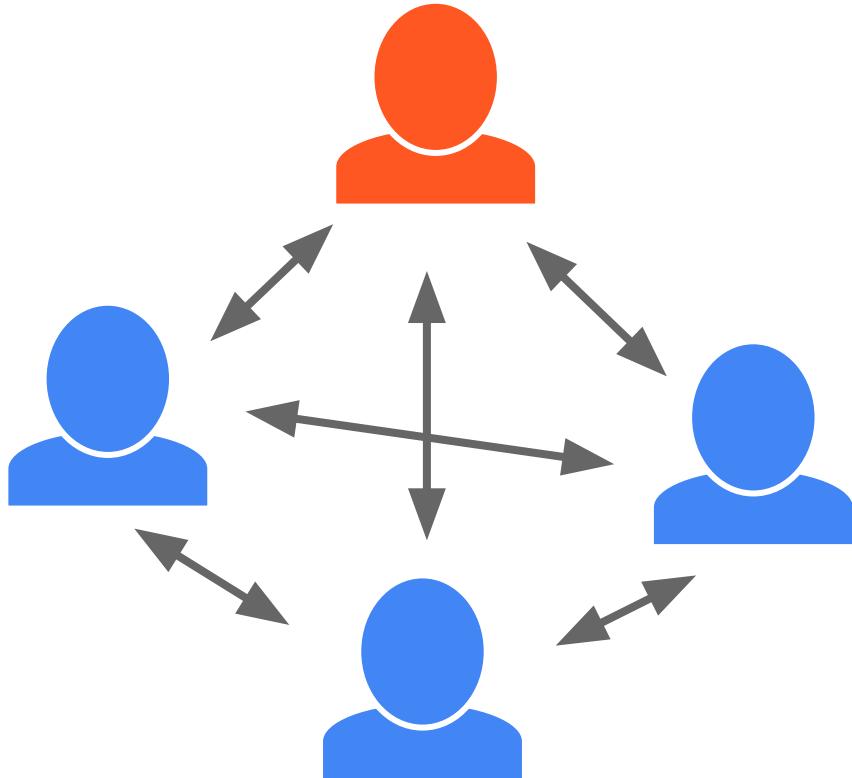
Distribué





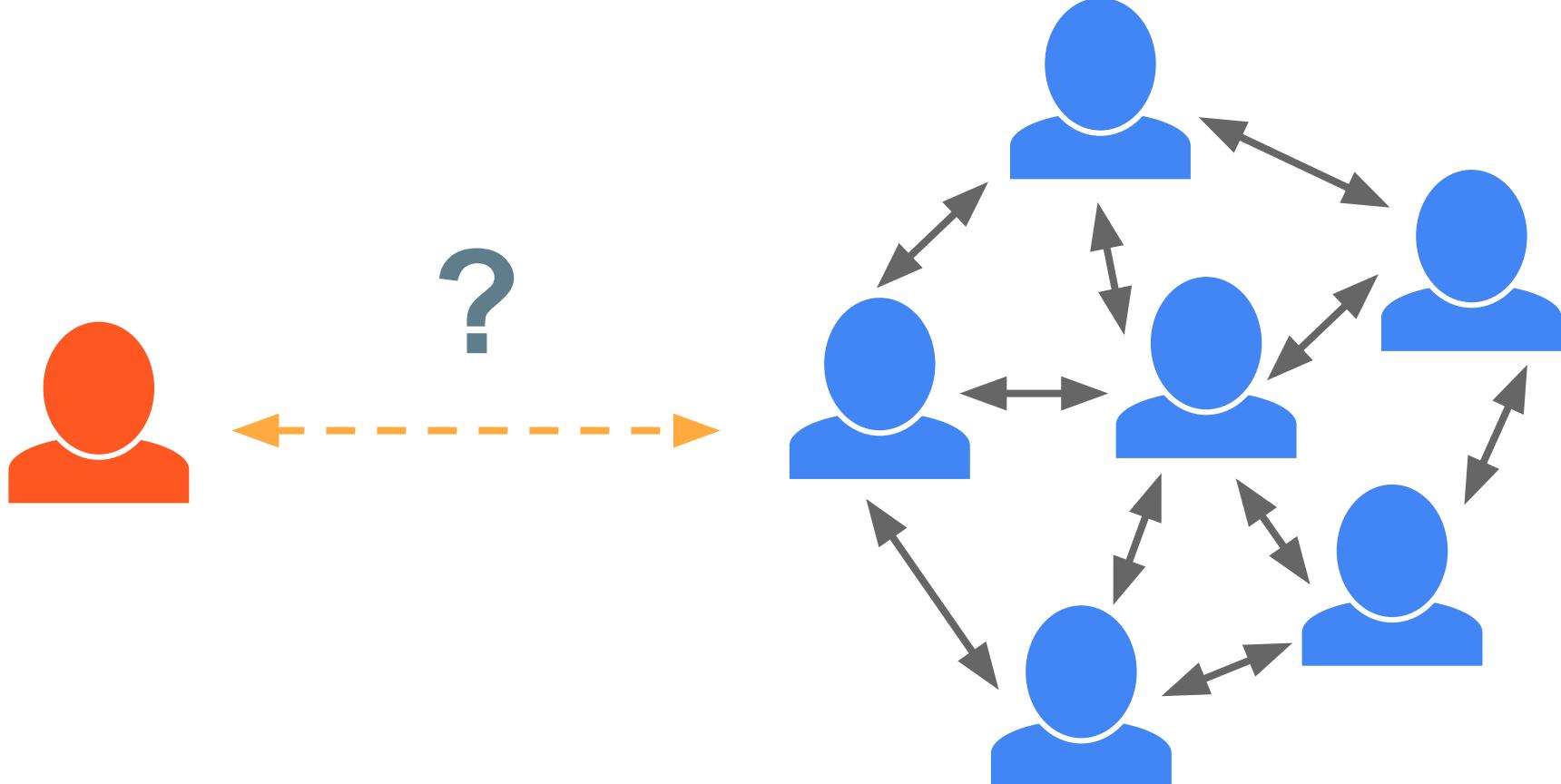


git



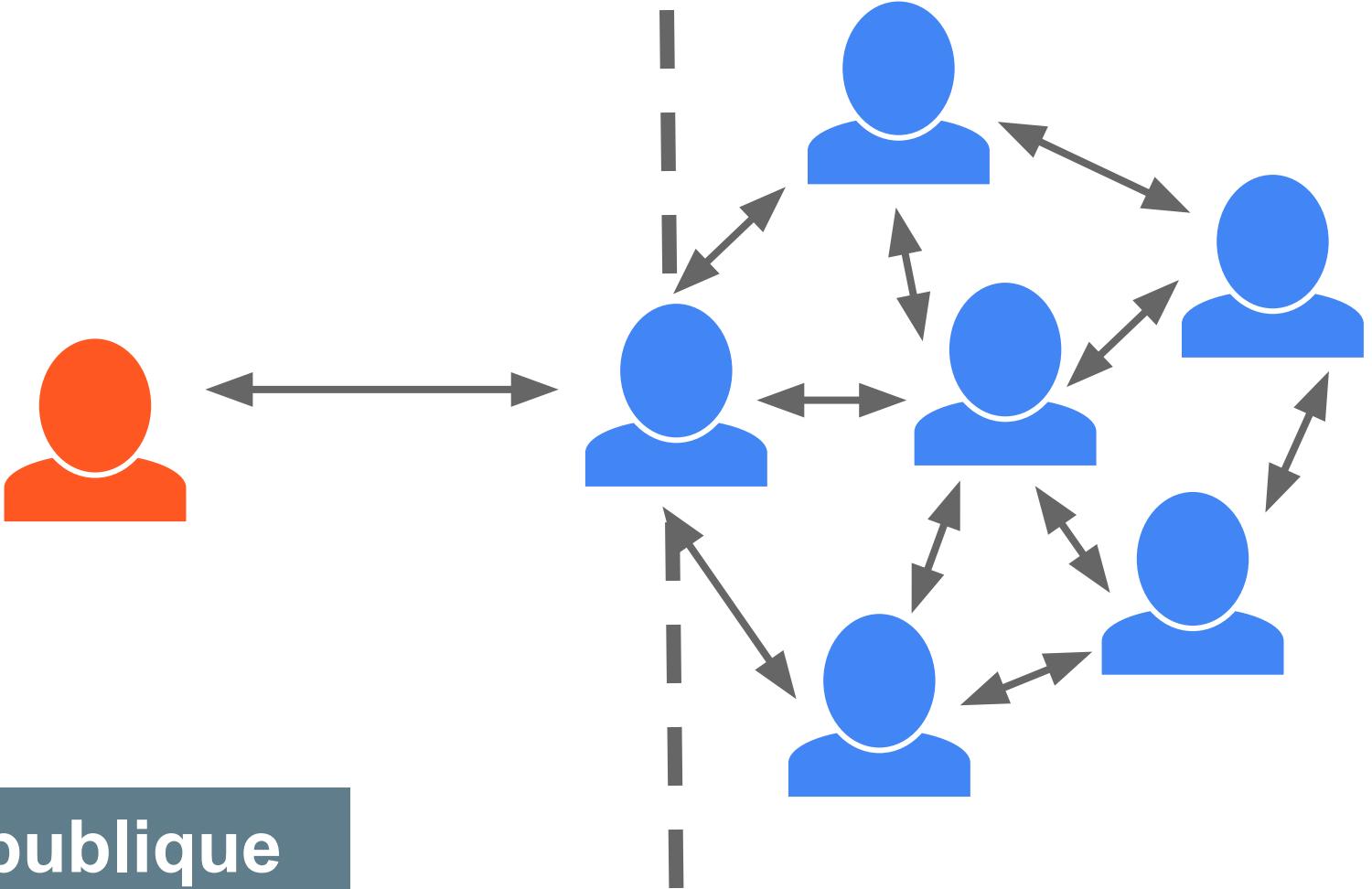
Comment ça marche ?



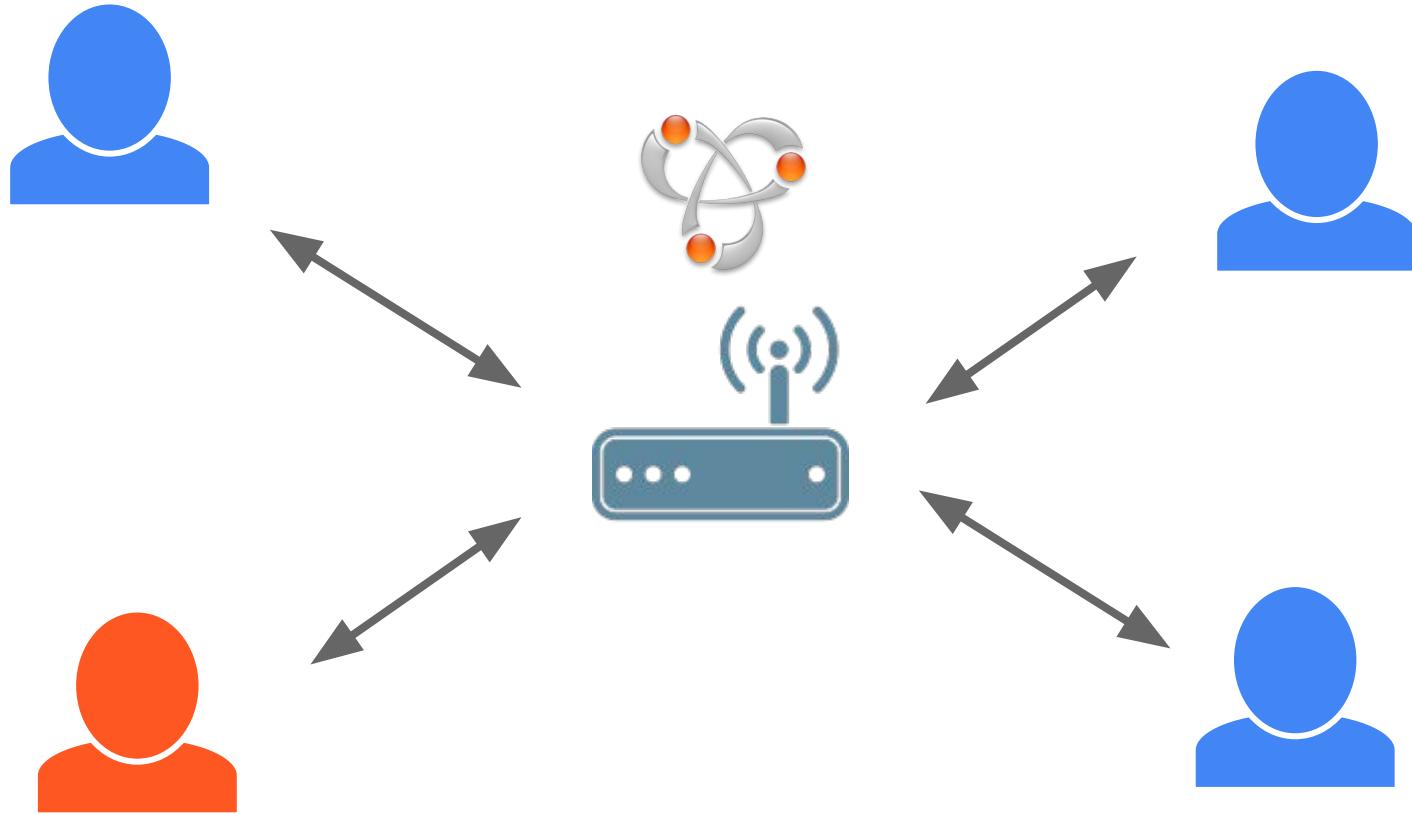


Comment on entre ?

Bootstrapping



Node publique



Multicast DNS (ZeroConf, Apple Bonjour)

Démo

Trouver une node publique Bitcoin

PS C:_Projets\Perso\doc> nslookup bitseed.xf2.org

Serveur : dns2.proxad.net

Address: 212.27.40.241

Réponse ne faisant pas autorité :

Nom : bitseed.xf2.org

Addresses: 24.52.35.44

50.177.196.160

68.48.214.241

76.111.96.126

85.214.90.1

94.226.111.26

96.2.103.25

97.117.255.48

99.242.230.163

162.243.194.210

173.69.49.106

198.38.93.227

209.208.110.92

PS C:_Projets\Perso\doc> nslookup bitseed.xf2.org

Serveur : dns2.proxad.net

Address: 212.27.40.241

Réponse ne faisant pas autorité :

Nom : bitseed.xf2.org

Addresses: 24.52.35.44

50.177.196.160

68.48.214.241

76.111.96.126

85.214.90.1

✓ 85.214.90.1:8333 /Satoshi:0.15.99(UASF-SegWit-BIP148)/

99.242.230.163

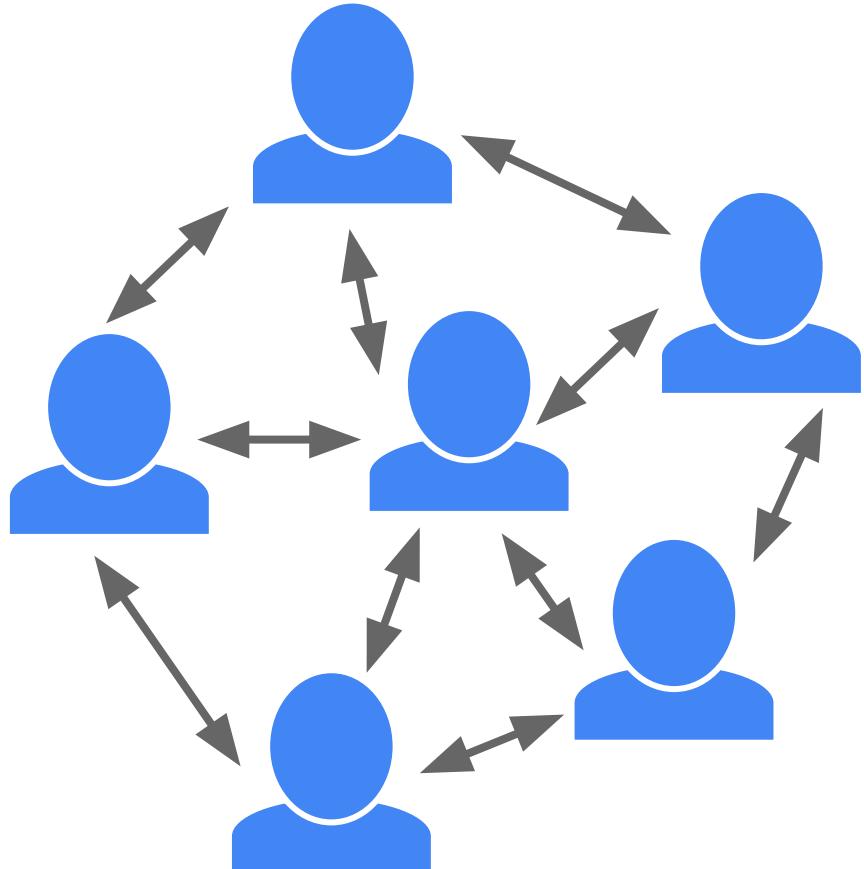
162.243.194.210

173.69.49.106

198.38.93.227

209.208.110.92

foo.txt ?

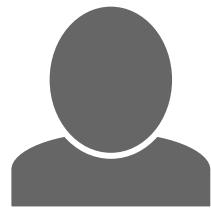


Où est Charlie ?

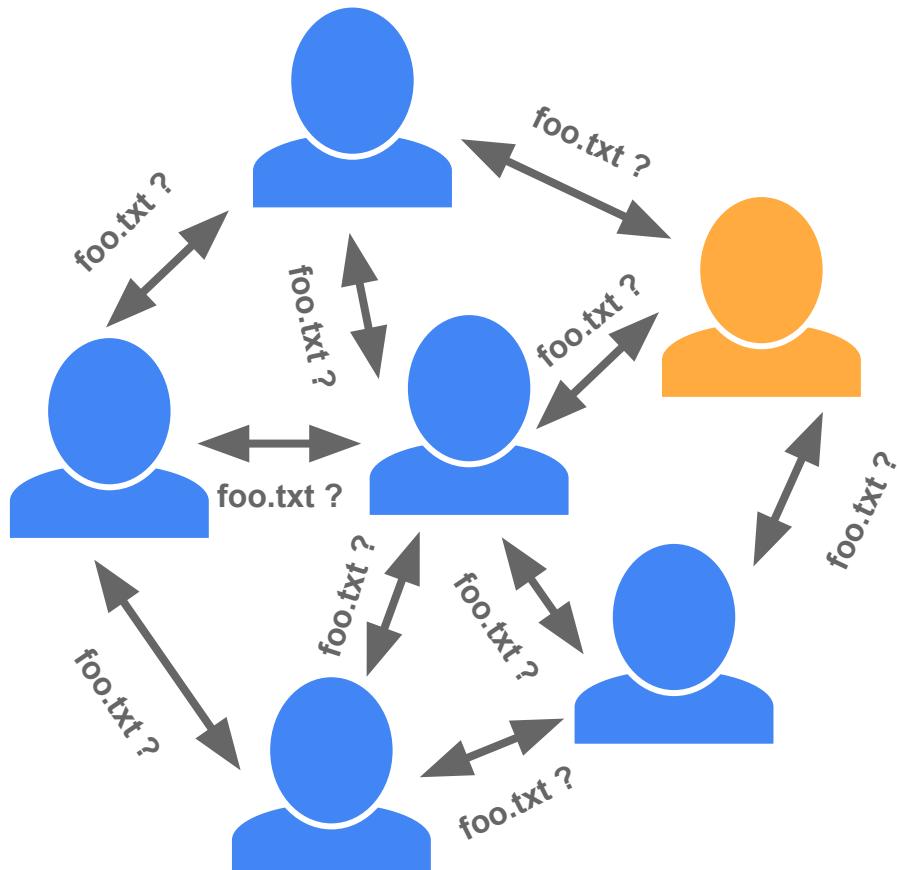
Discovery

**Retour dans les années
2000...**

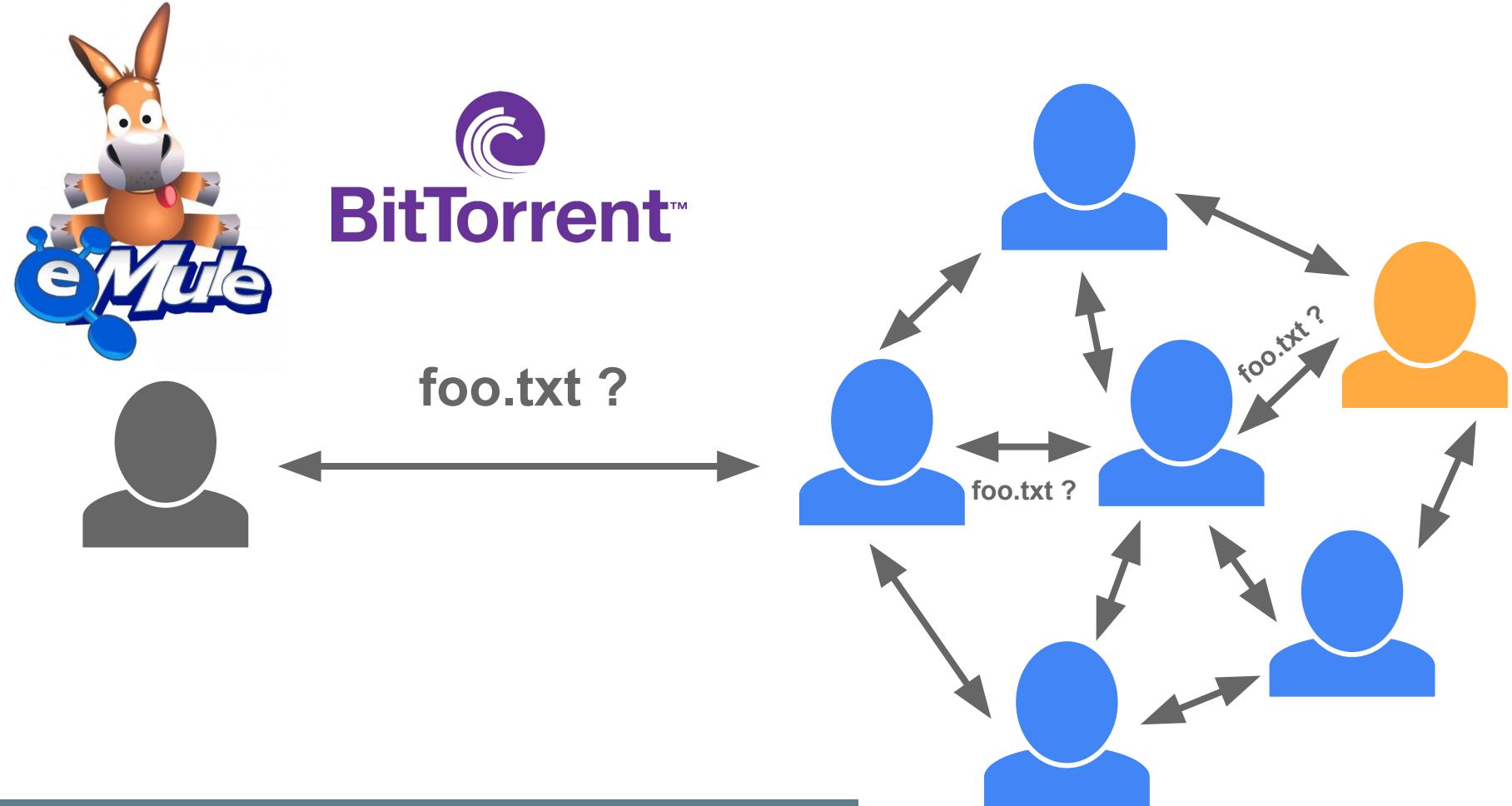
gnutella



foo.txt ?



Query Flooding

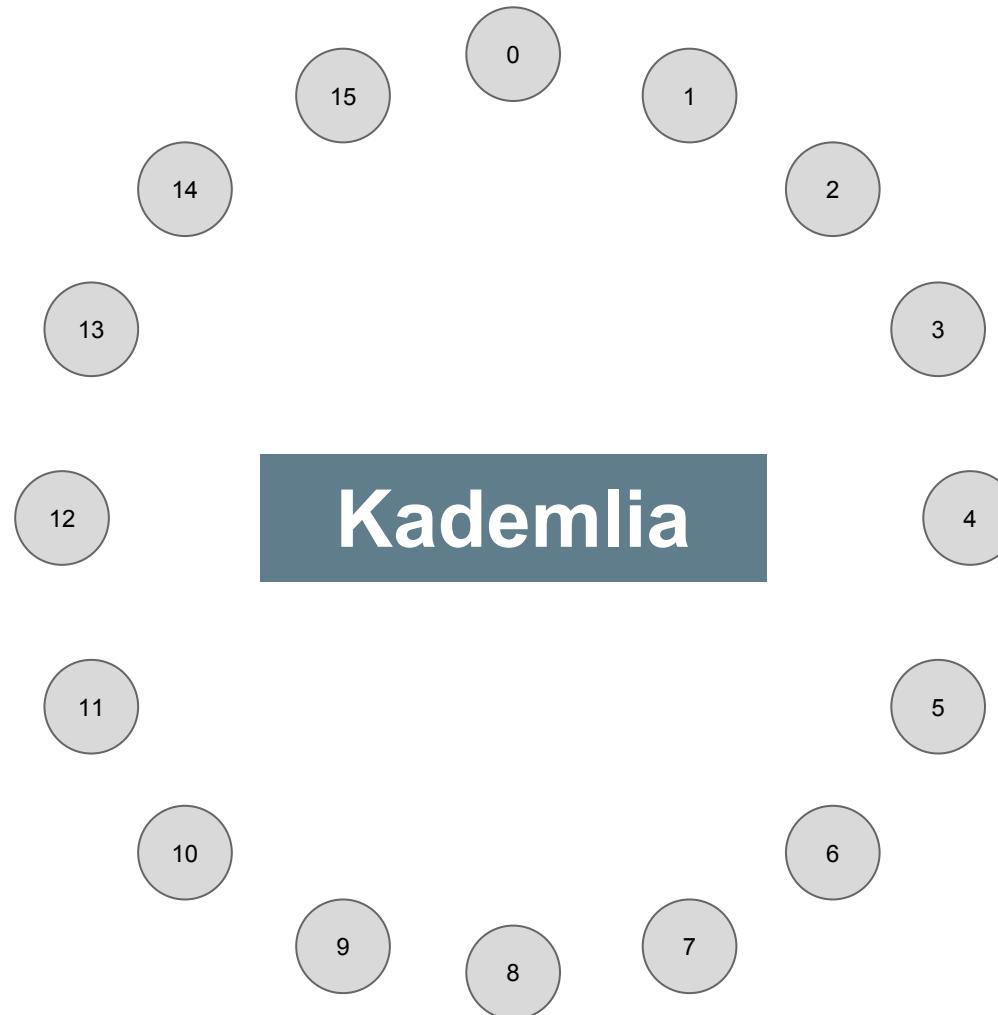


Distributed Hash Table

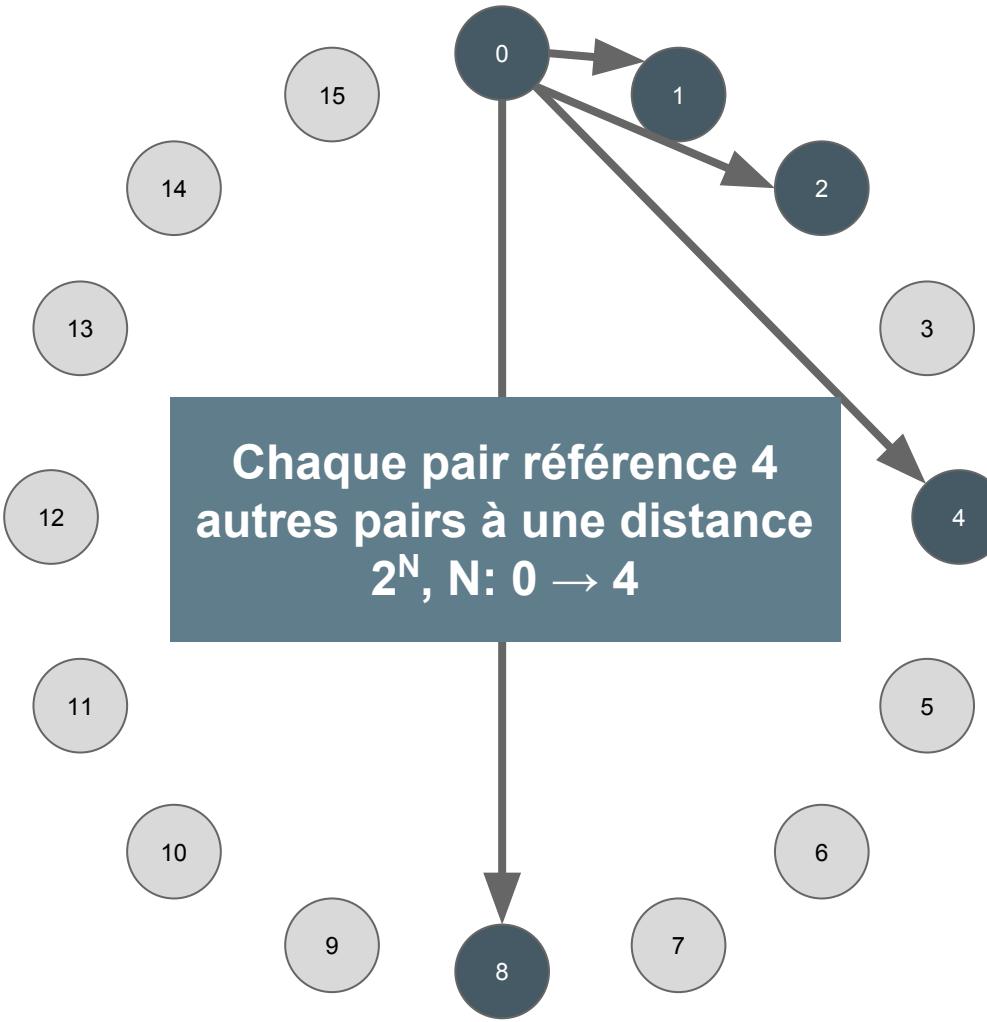
Distributed Hash Table

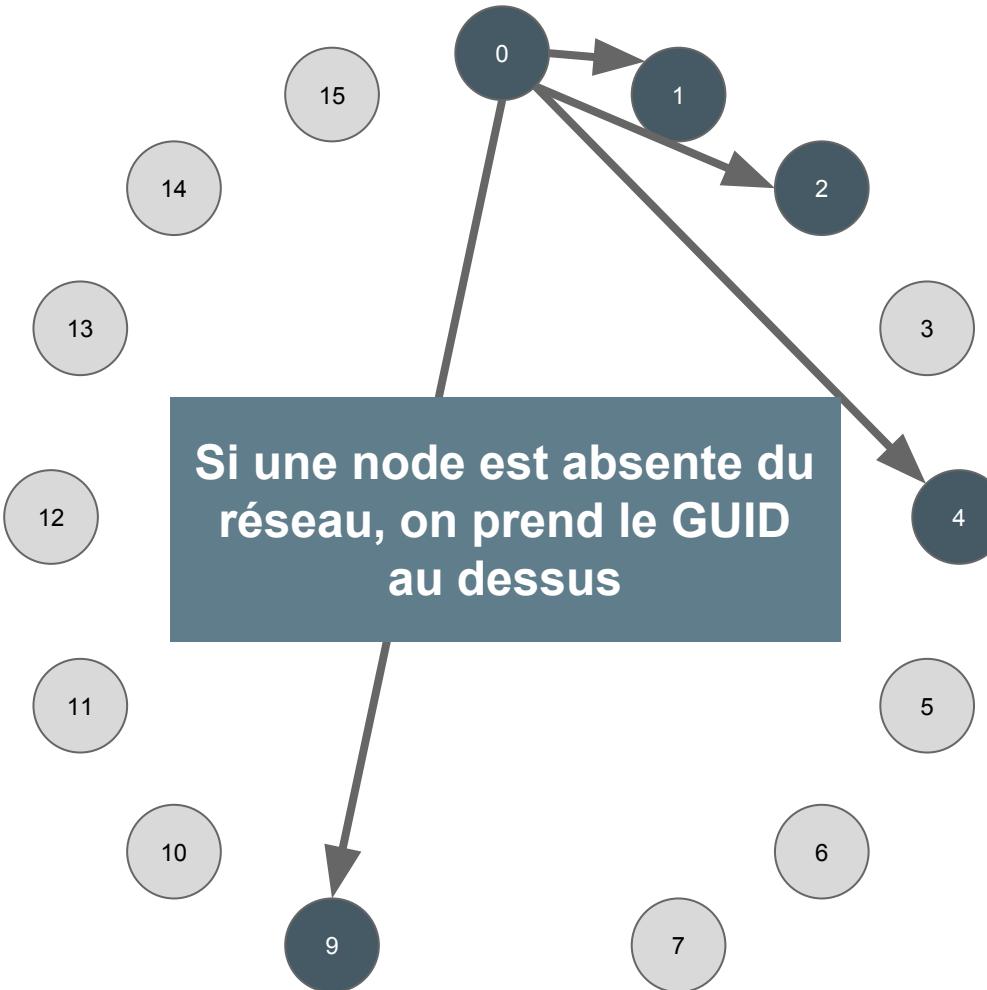
DHT ?

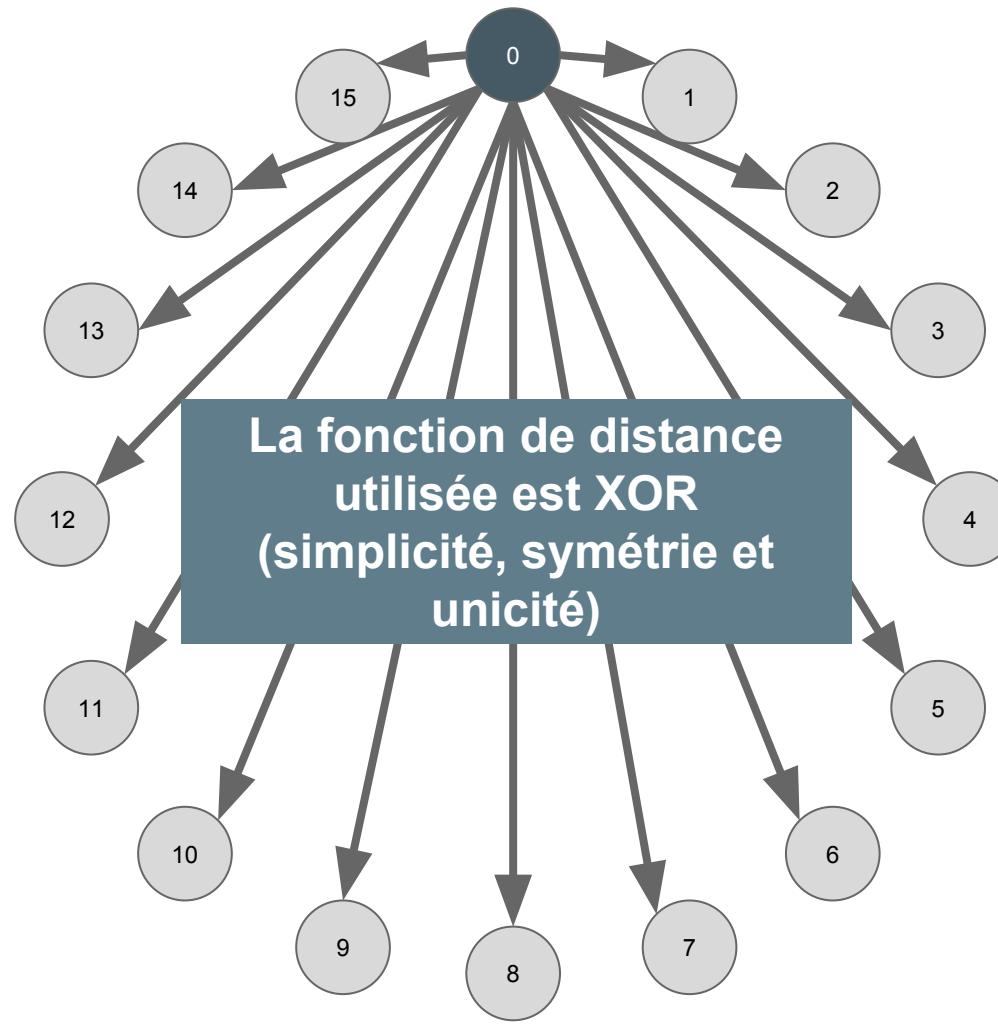
Kademlia



GUID sur 4 bits
0 → 15
15 pairs max.







0

qui possède
foo.txt ?

15

14

1

2

13

3

12

4

11

5

10

6

9

7

8

infohash(foo.txt) = 15

0

15

14

qui possède
foo.txt ?

1

2

13

3

12

4

11

5

10

6

9

7

8

il sait !

$\text{infohash}(\text{foo.txt}) = 15$

15

0

1

14

2

13

3

12

4

11

5

10

6

9

7

8

qui possède
foo.txt ?

On prend le plus près

8

9

7

6

5

10

11

12

13

14

15

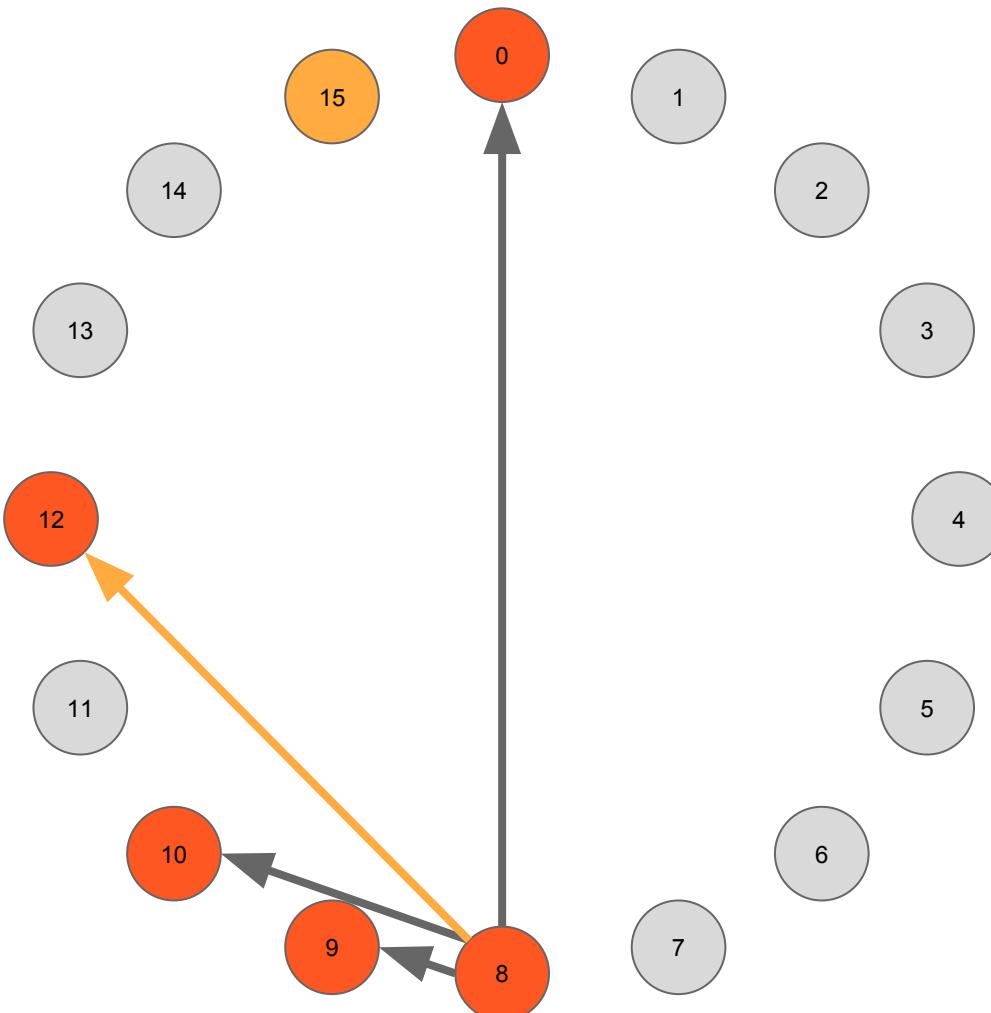
0

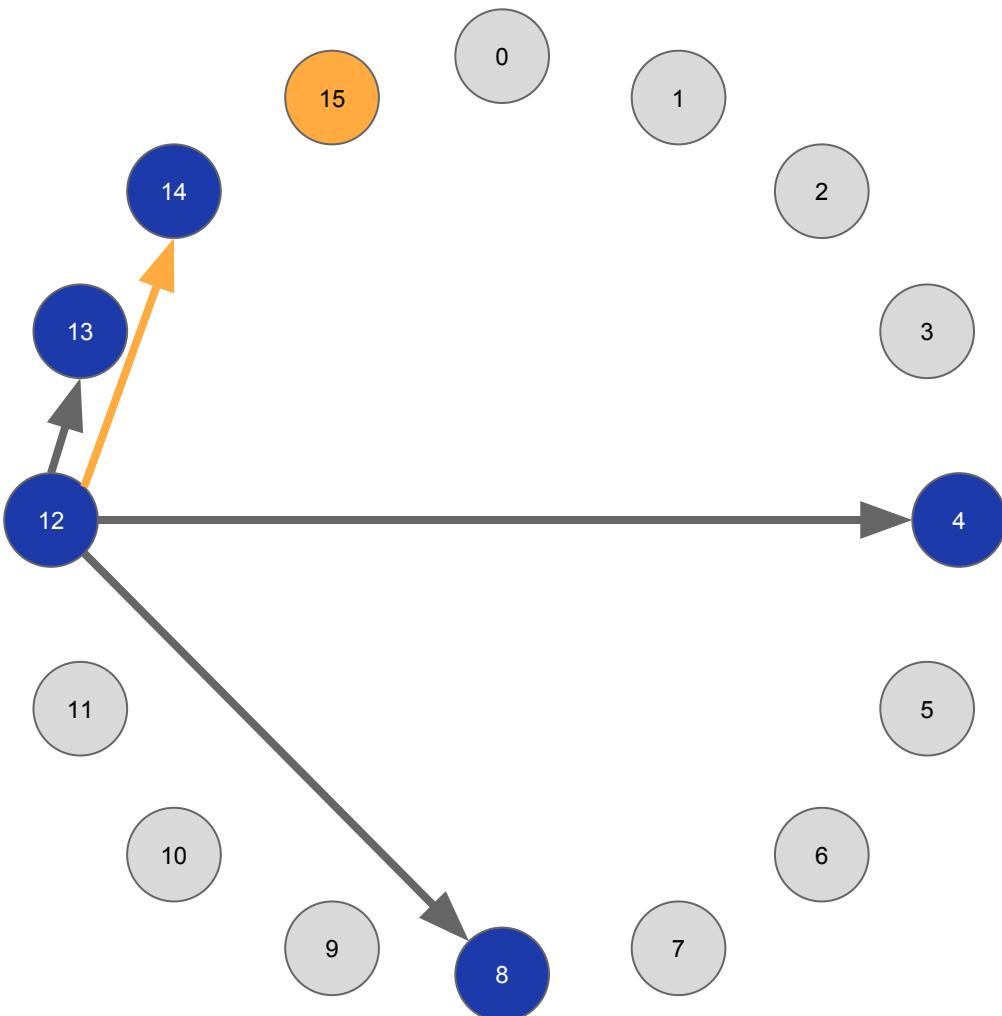
1

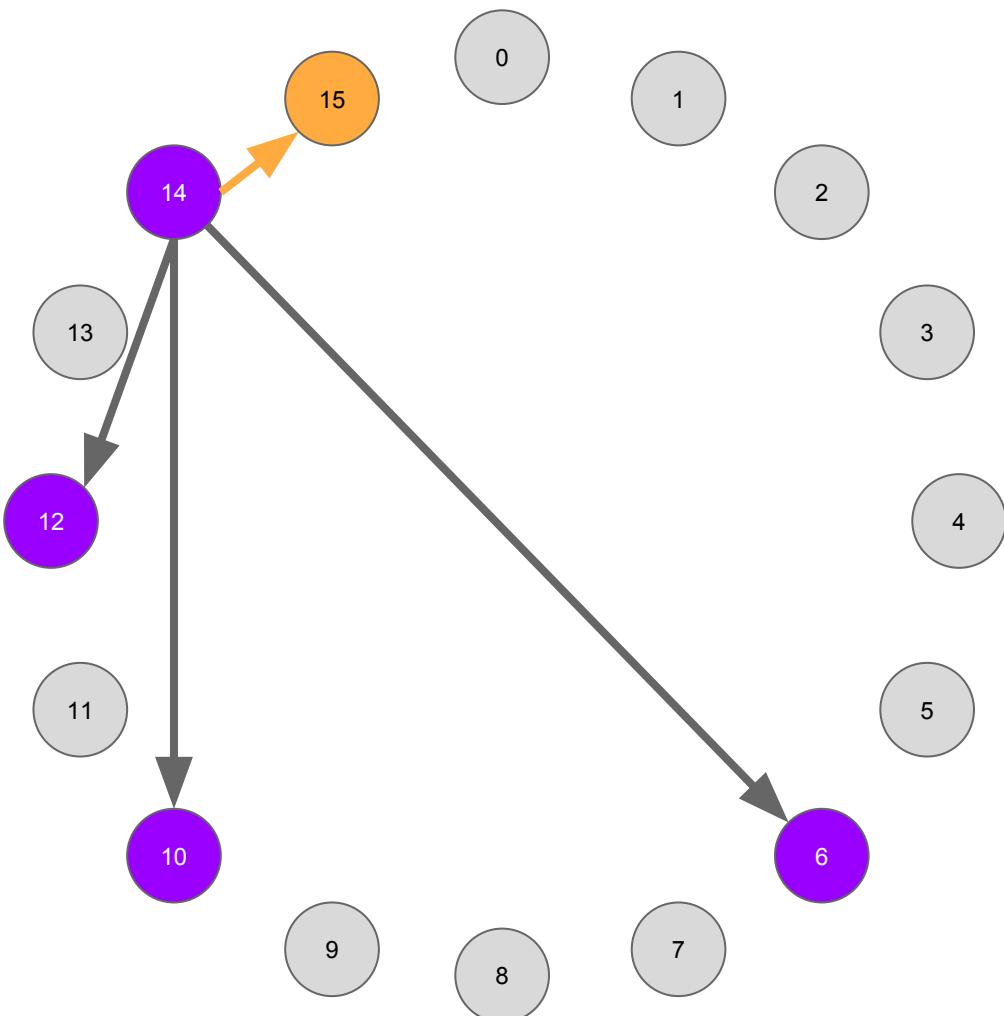
2

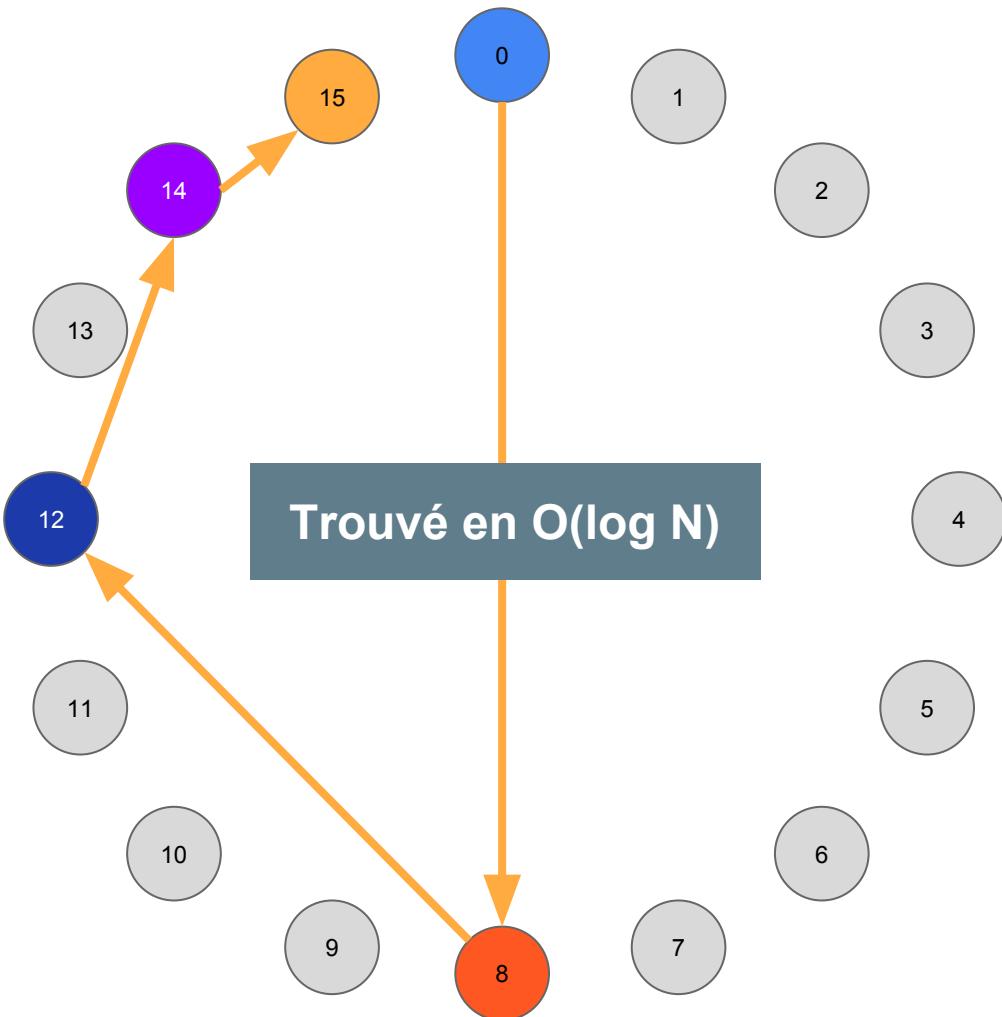
4

3









Démo

Magnet link sur bittorrent

Hadopi

**Haute Autorité pour la diffusion des œuvres
et la protection des droits sur internet**

TELEMA ET LE STUDIO CANAL+ PRESENTENT UN FILM
PRODUIT PAR CHARLES GASSOT

LE FILM DE LES NULS[®]



LA CITE DE LA PEUR

Une comédie familiale.

RÉALISÉ PAR ALAIN BERBERIAN

TELEMA ET LE STUDIO CANAL+ PRESENTENT UN FILM PRODUIT PAR CHARLES GASSOT LE FILM DE LES NULS LA CITE DE LA PEUR EST UNE COMÉDIE FAMILIALE
CHANTAL LAUBY • ALAIN CHABAT • DOMINIQUE FARRUGIA • GÉRARD BARRONI • SAM KAHAN
SCÉNARIO ORIGINAL CHANTAL LAUBY ALAIN CHABAT DOMINIQUE FARRUGIA • DIRECTEUR DE LA PHOTOGRAPHIE LAURENT DAILLAND
MUSIQUE PHILIPPE CHANY • MONTAGE VÉRONIQUE PARNET
PRODUCTEUR DÉLEGUÉ CHARLES GASSOT • PRODUCTEUR EXÉCUTIF DOMINIQUE BRUNNER
UNE PRODUCTION TELEMA LE STUDIO CANAL+ FRANCE 3 CINEMA M6 FILMS

[Pirate Search](#)

Audio Video Applications Games Porn Other [All](#) ▾

Details for this torrent

La citÃ© de la Peur by LADB

Type:	Video > Movies	Uploaded:	2008-05-02 19:15:37
Files:	2	GMT	
Size:	691.28 MiB (724855831 Bytes)	By:	wazany
Spoken language(s):	French		
Texted language(s):	French		
Seeders:	13	Leechers:	0
Comments	1		

Info Hash:

96BFF9E1F47398C3807071B55AD658ED50F2042F

[GET THIS TORRENT](#) [PLAY/STREAM TORRENT](#)

(Problems with magnets links are fixed by upgrading your torrent client!)

Synopsis :

Odile Deray, attachÃ©e de presse, vient au Festival de Cannes pour prÃ©senter le film "Red is Dead".

Malheureusement, celui-ci est d'une telle faiblesse que personne ne souhaite en faire l'Ã©cho.

Mais lorsque les projectionnistes du long-mÃ¢trage en question meurent chacun leur tour dans d'Ã©tranges circonstances, "Red is dead" bÃ©nÃ©ficie d'une incroyable publicitÃ©. Serge Karamazov est alors chargÃ© de protÃ©ger le nouveau projectionniste du film...

```
var _ = require('lodash')
var DHT = require('bittorrent-dht')
var geoip = require('geoip-lite-country')
```

```
var _ = require('lodash')
var DHT = require('bittorrent-dht')
var geoip = require('geoip-lite-country')
```

```
var peers = []
var dht = new DHT()
```

```
var _ = require('lodash')
var DHT = require('bittorrent-dht')
var geoip = require('geoip-lite-country')

var peers = []
var dht = new DHT()
```

```
dht.on('peer', function (peer, infoHash, from) {
  var geo = geoip.lookup(peer.host)
  peers.push(
    peer.host + ':' +
    peer.port + ':' +
    geo.country
  )
})
```

```
var _ = require('lodash')
var DHT = require('bittorrent-dht')
var geoip = require('geoip-lite-country')

var peers = []
var dht = new DHT()

dht.on('peer', function (peer, infoHash, from) {
  var geo = geoip.lookup(peer.host)
  peers.push(
    peer.host + ':' +
    peer.port + ':' +
    geo.country
  )
})
})
```

```
setTimeout(function () {
  dht.destroy()
  console.log(_.uniq(peers))
}, 10 * 1000)
```

```
var _ = require('lodash')
var DHT = require('bittorrent-dht')
var geoip = require('geoip-lite-country')

var peers = []
var dht = new DHT()

dht.on('peer', function (peer, infoHash, from) {
  var geo = geoip.lookup(peer.host)
  peers.push(
    peer.host + ':' +
    peer.port + ':' +
    geo.country
  )
})

setTimeout(function () {
  dht.destroy()
  console.log(_.uniq(peers))
}, 10 * 1000)
```

dht.lookup(infoHash)

```
var _ = require('lodash')
var DHT = require('bitTorrent-dht')
var geoip = require('geoip-lite-country')

var peers = []
var dht = new DHT()

dht.on('peer', function (peer, infoHash, from) {
  var geo = geoip.lookup(peer.host)
  peers.push(
    peer.host + ';' +
    peer.port + ';' +
    geo.country
  )
})

setTimeout(function () {
  dht.destroy()
  console.log(_.uniq(peers))
}, 10 * 1000)

dht.lookup(infoHash)
```

Done crawling

Found 12 peers

```
[ '91.138.225. [REDACTED]:62762:GR',
  '178.194.206. [REDACTED]:17132:CH',
  '5.51.42. [REDACTED]:33457:FR',
  '51.15.3. [REDACTED]:54728:NL',
  '5.51.42. [REDACTED]:45442:FR',
  '88.191.54. [REDACTED]:62348:FR',
  '51.15.3. [REDACTED]:51413:NL',
  '178.194.206. [REDACTED]:60482:CH',
  '82.253.38. [REDACTED]:61818:FR',
  '82.249.8. [REDACTED]:33876:FR',
  '178.194.206. [REDACTED]:45429:CH',
  '178.194.206. [REDACTED]:37603:CH' ]
```

Crawl ended

Done in 10.57s.



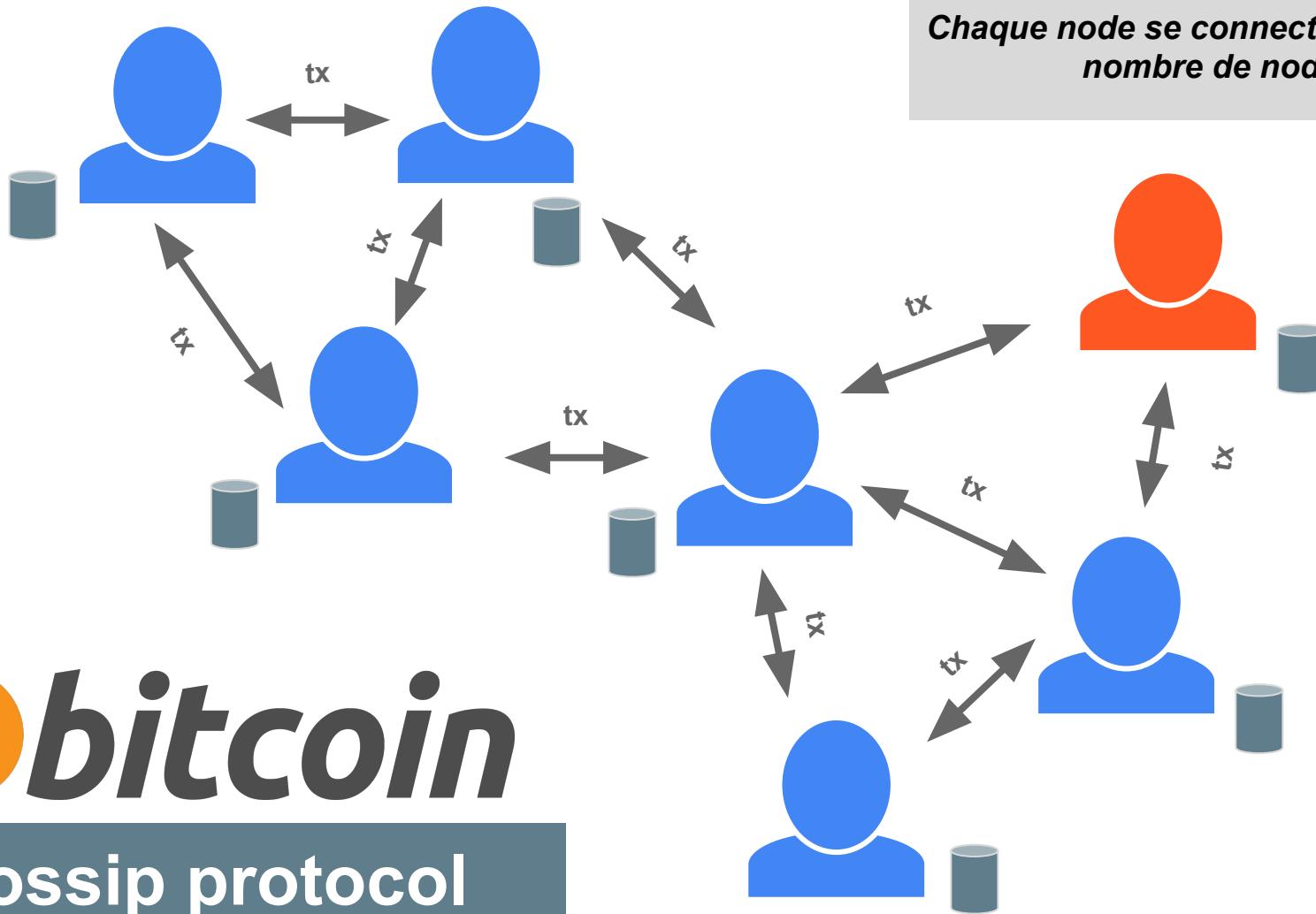


Et la blockchain dans tout ca ?

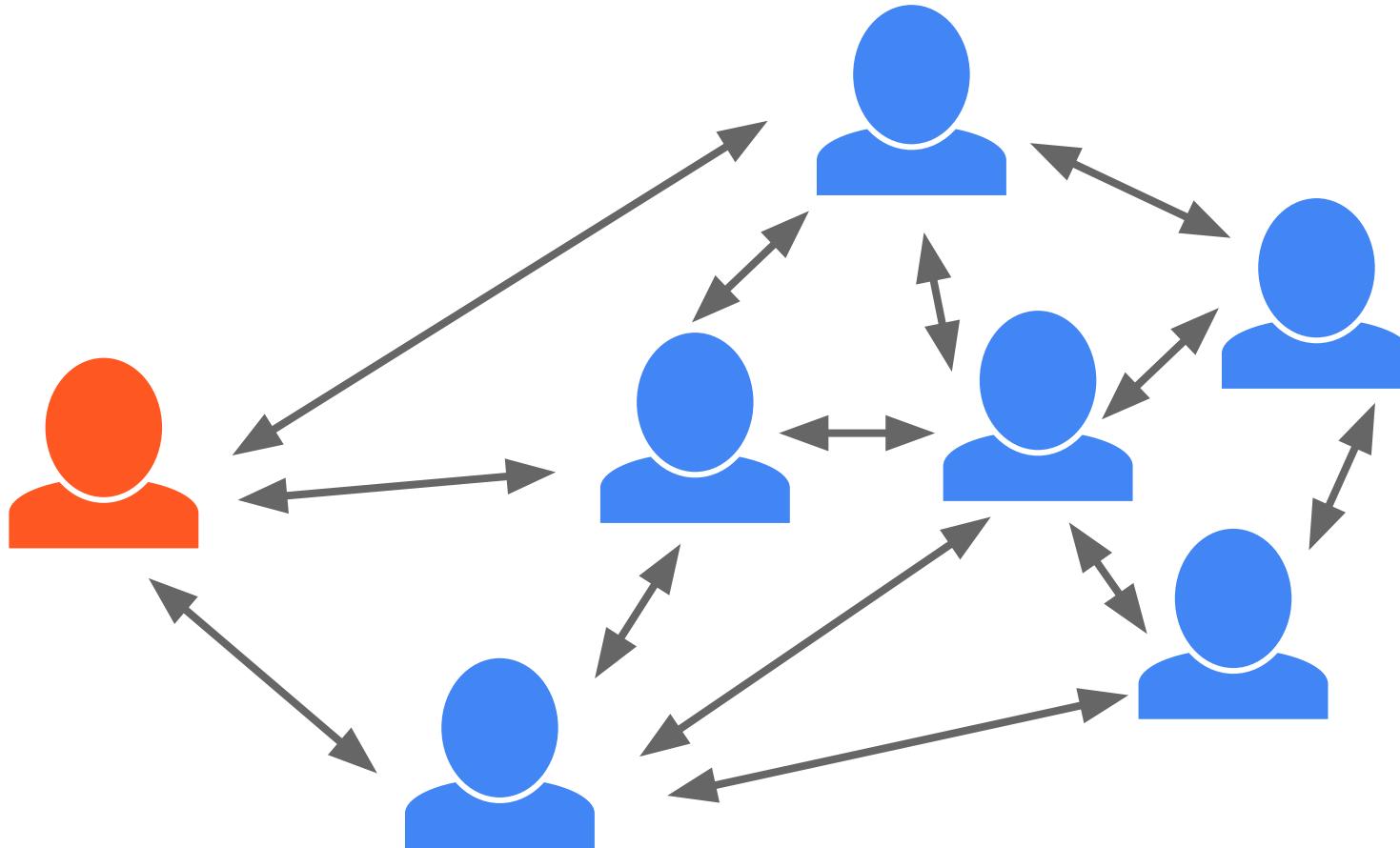


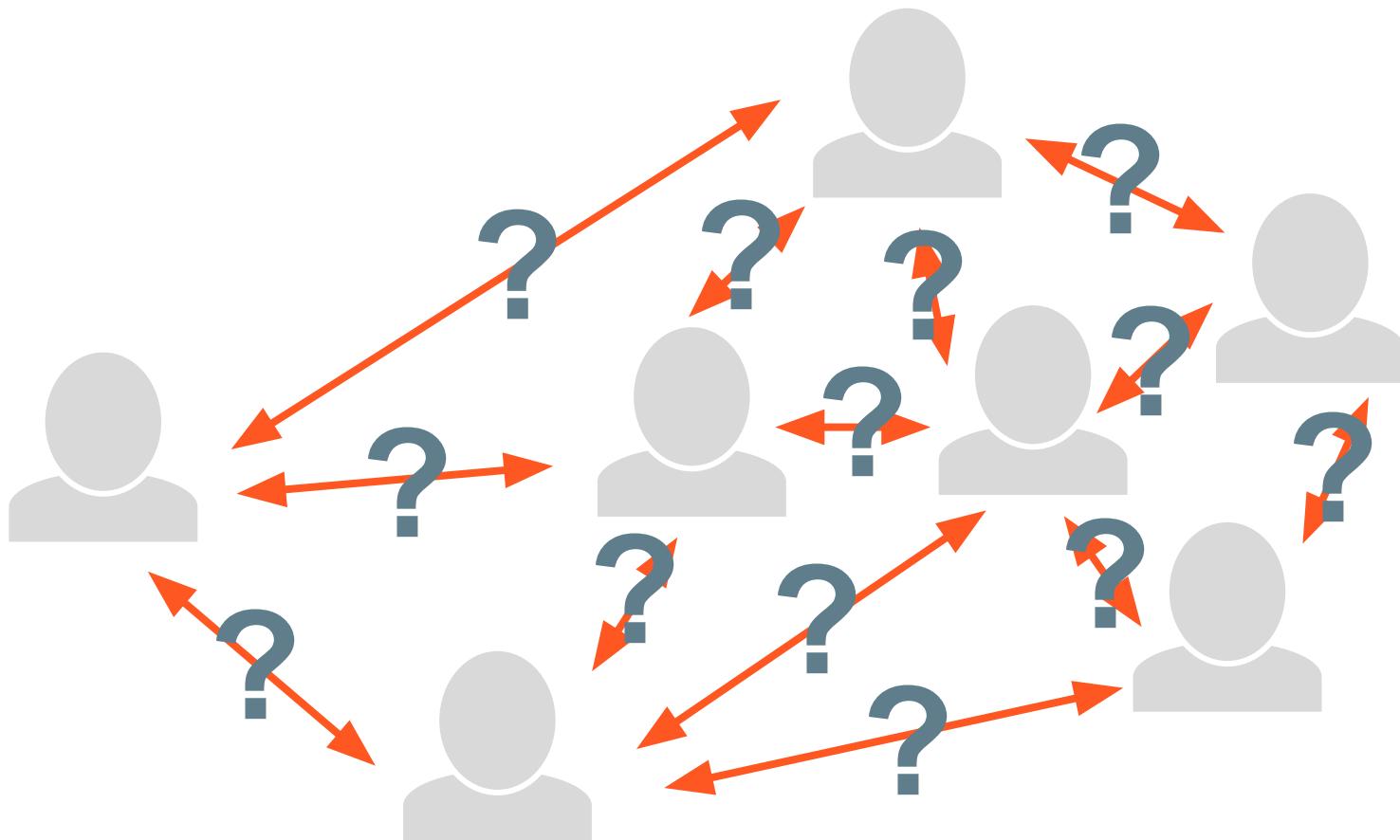
bitcoin

Gossip protocol



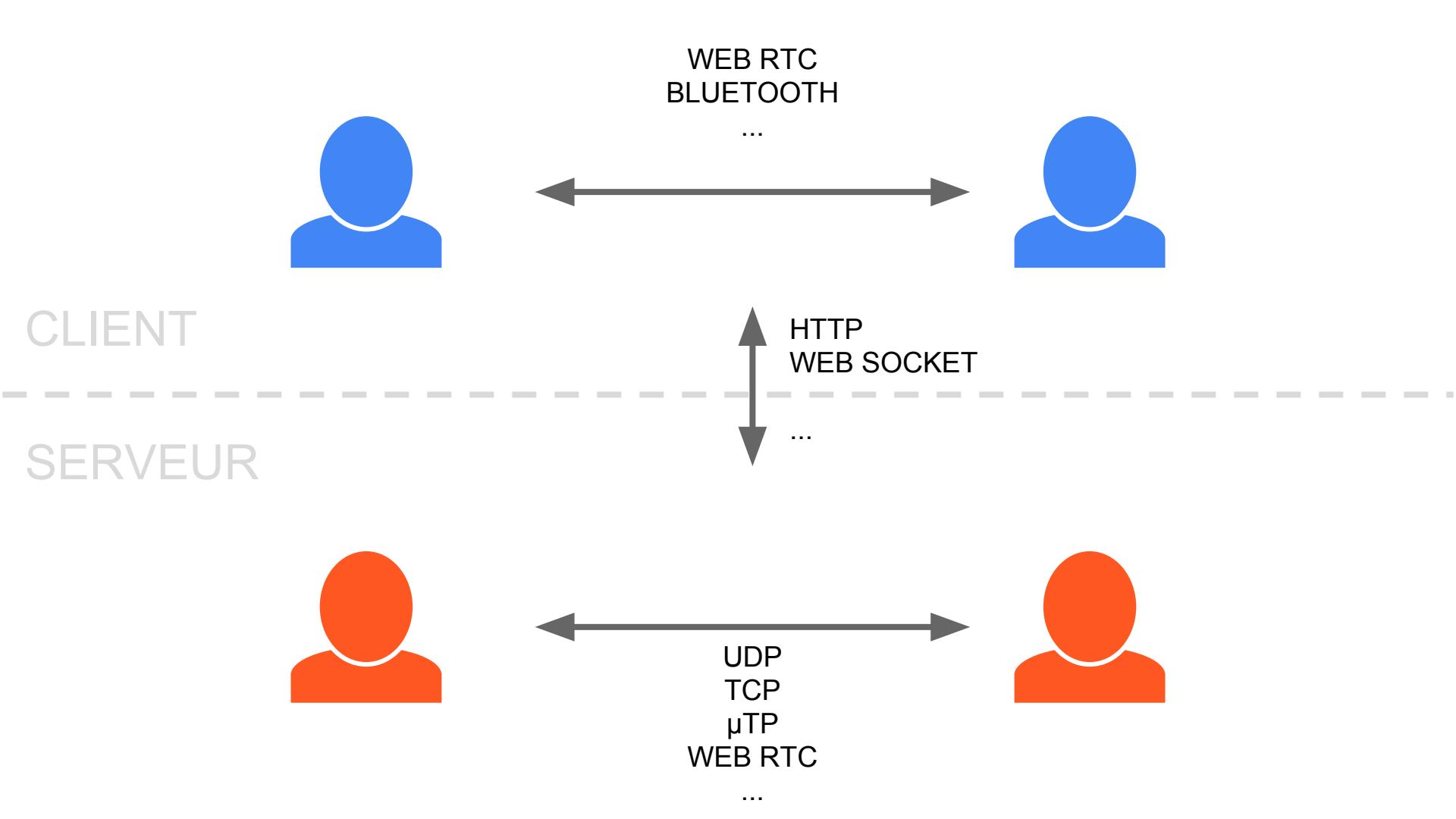
Chaque node se connecte à un grand nombre de nodes

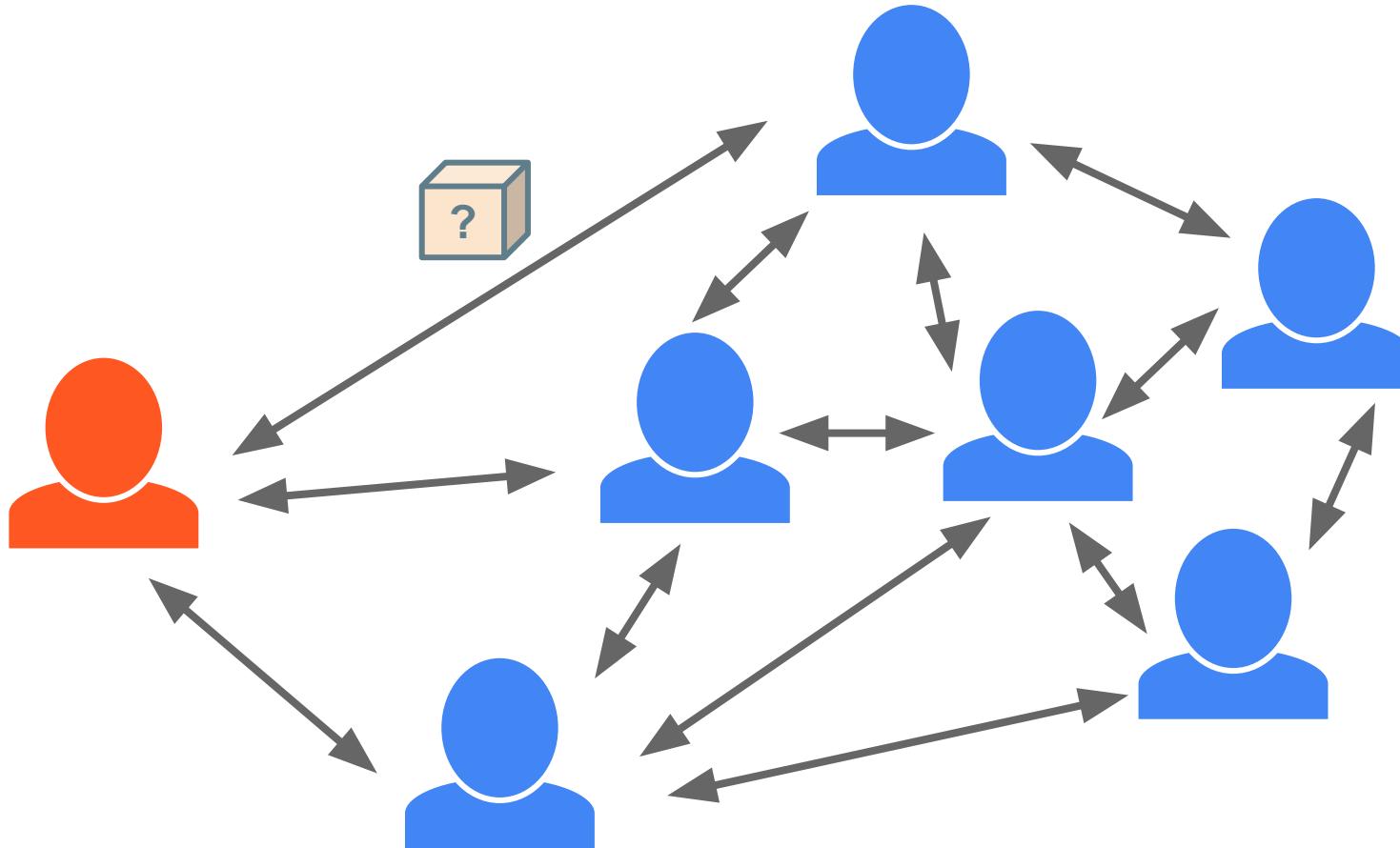




email ? Téléphone ? Courrier ? Pigeon ?

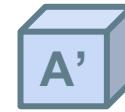
Transport







diff ?



C'est la bonne donnée ?

Content addressed data

Merkle “Tree”

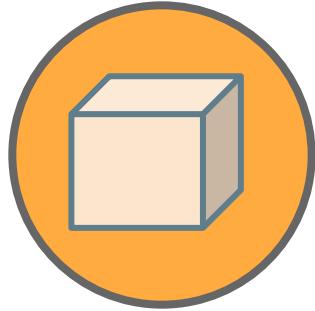
Merkle Directed Acyclic

Graph

Merkle “Tree”

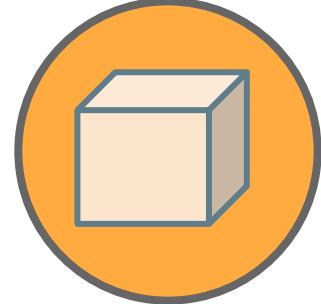
Merkle Directed Acyclic Graph



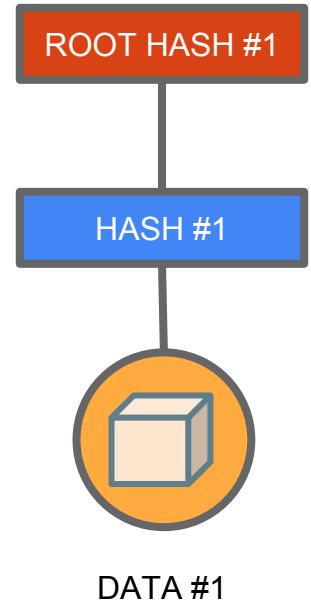


DATA #1

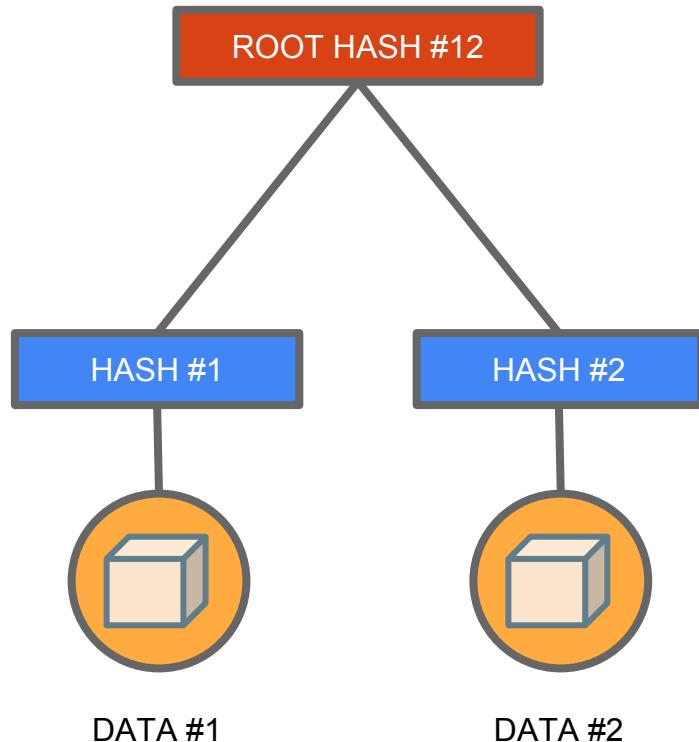
HASH #1

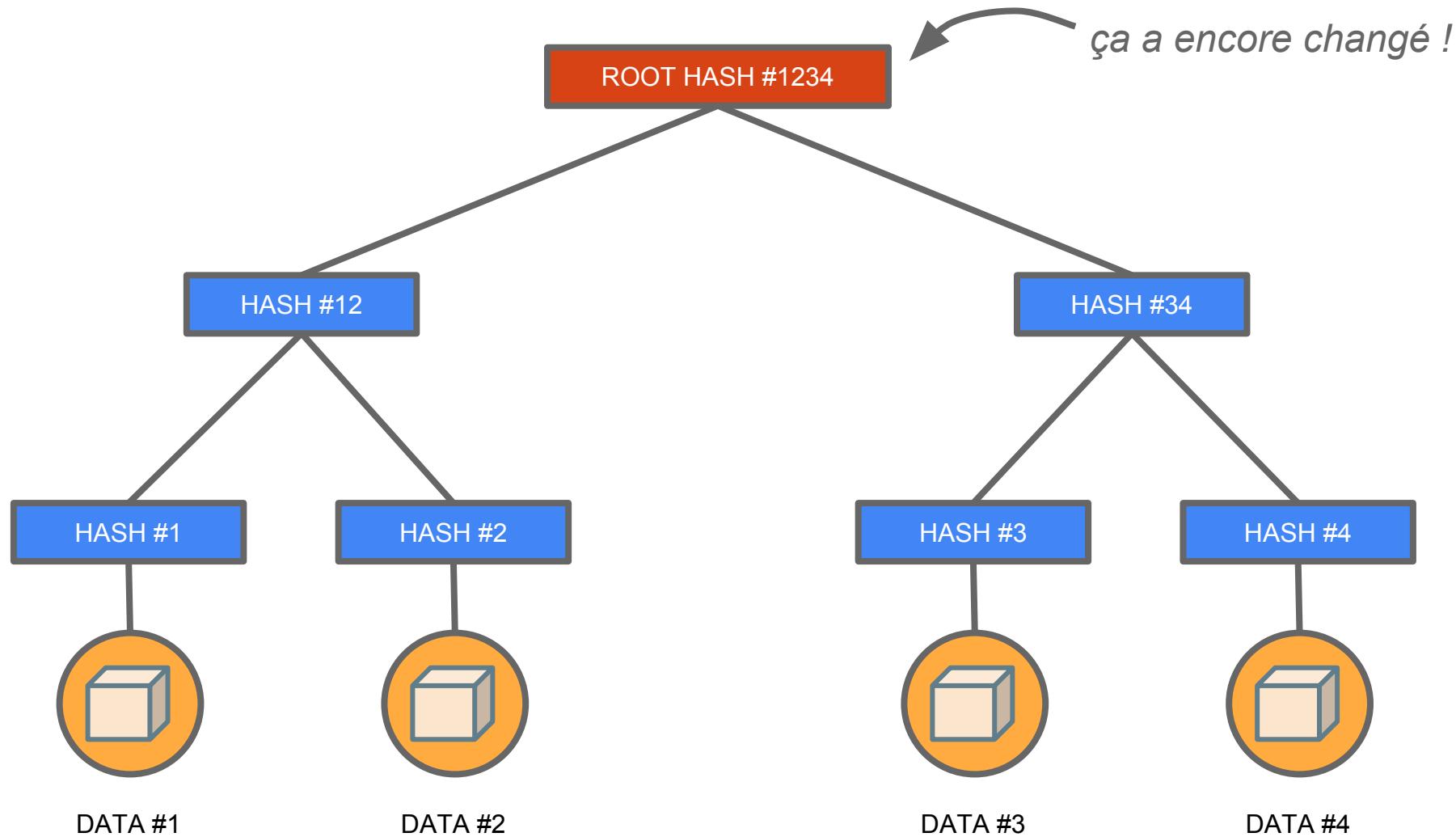


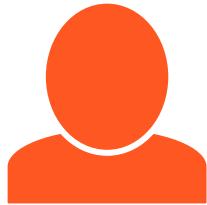
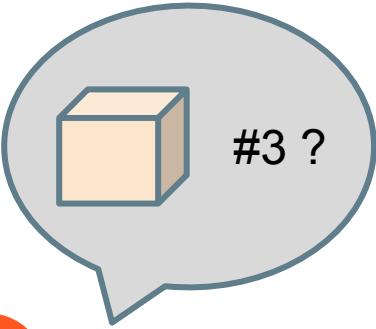
DATA #1



ça a changé !



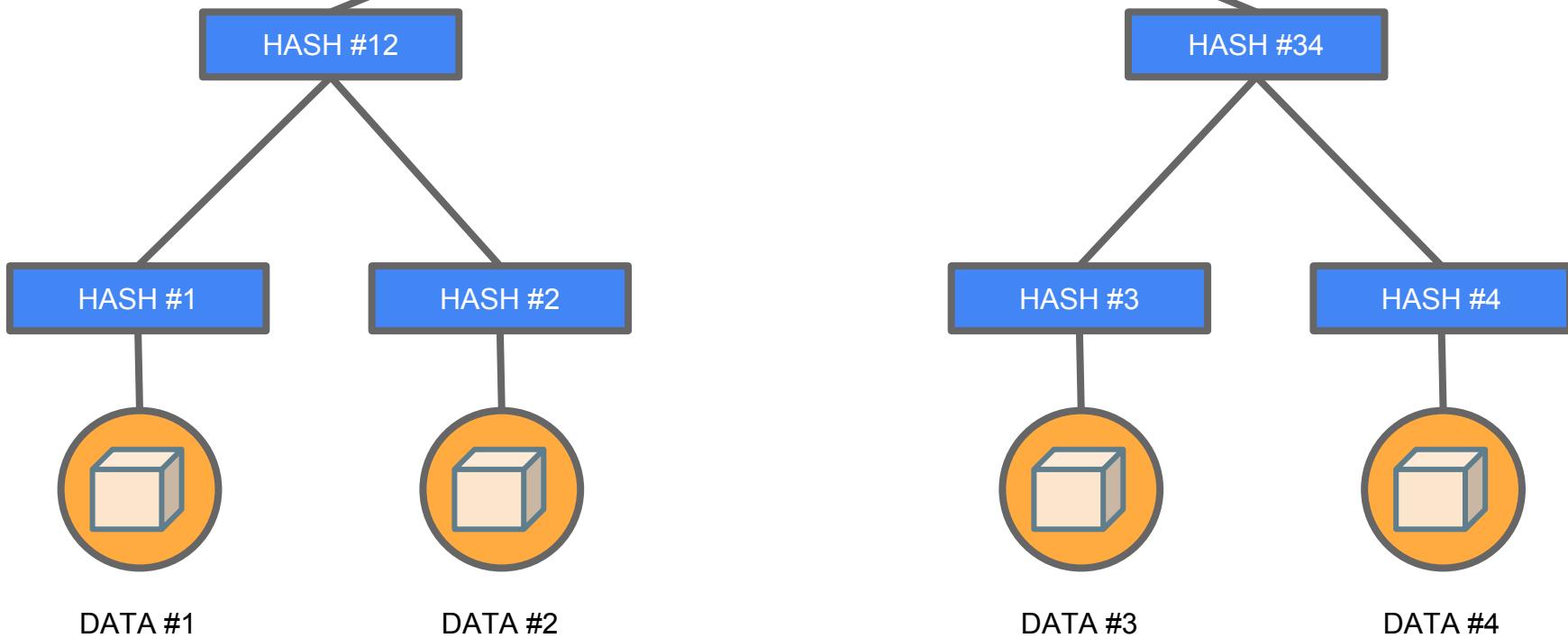


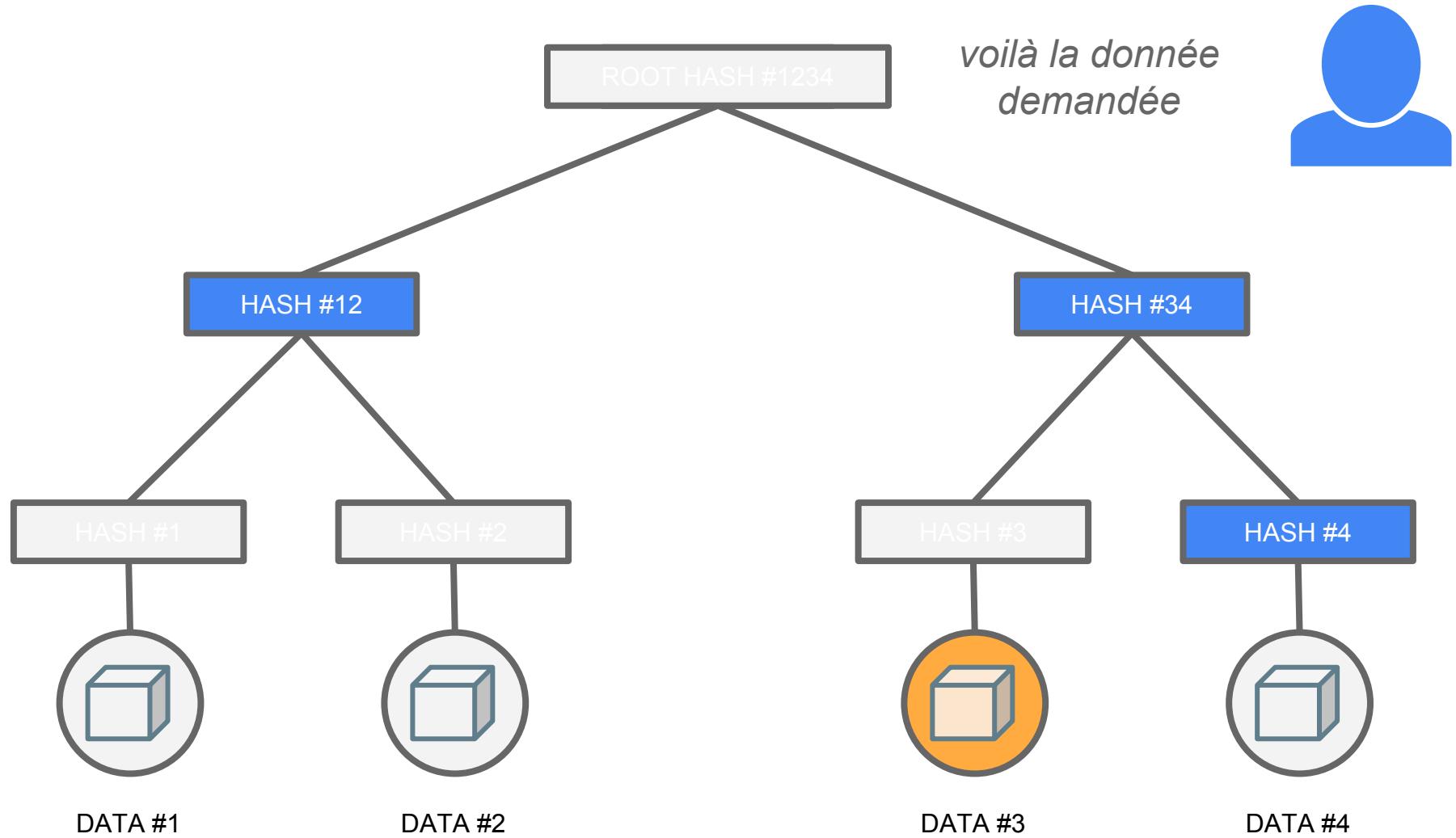


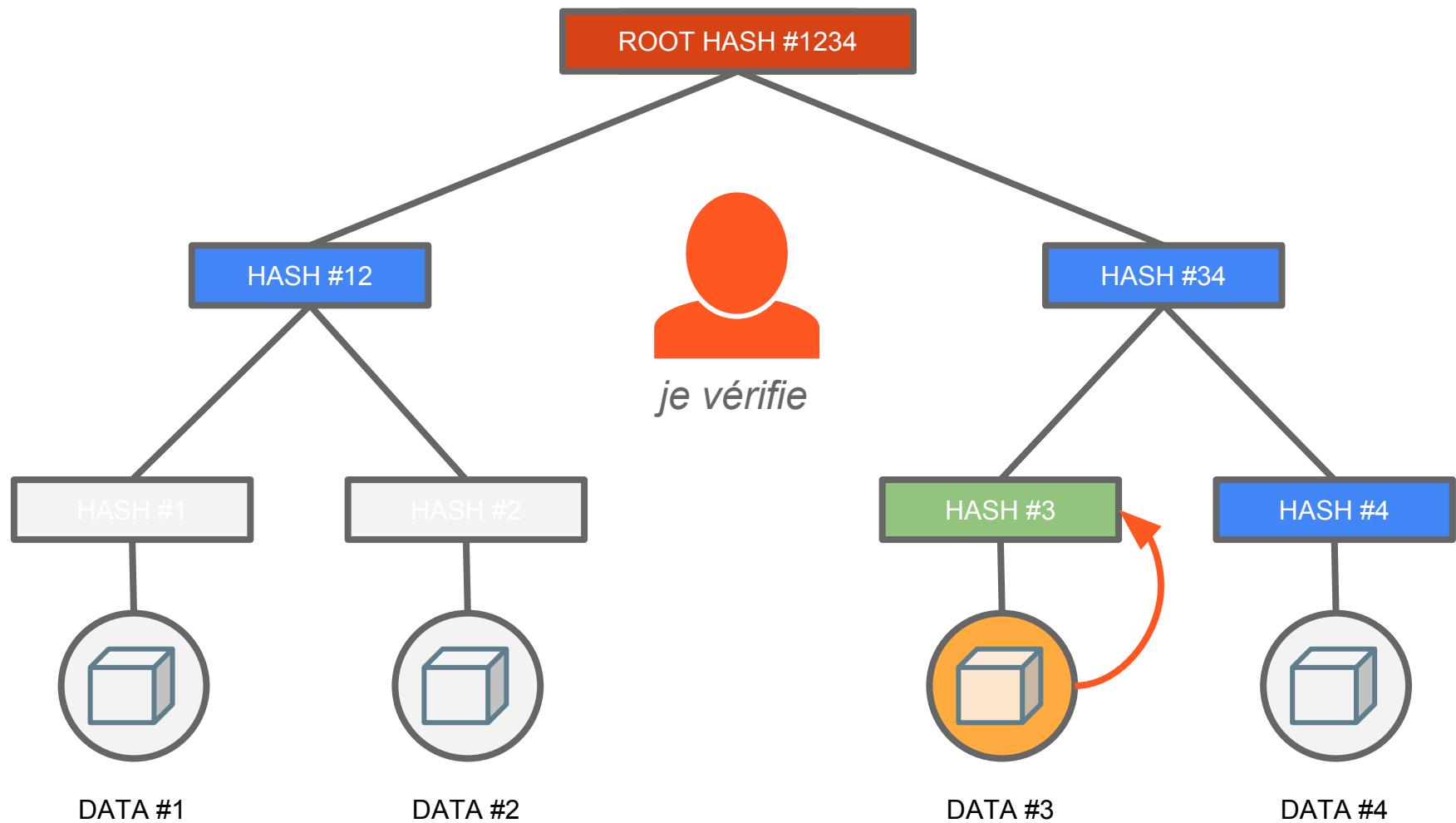


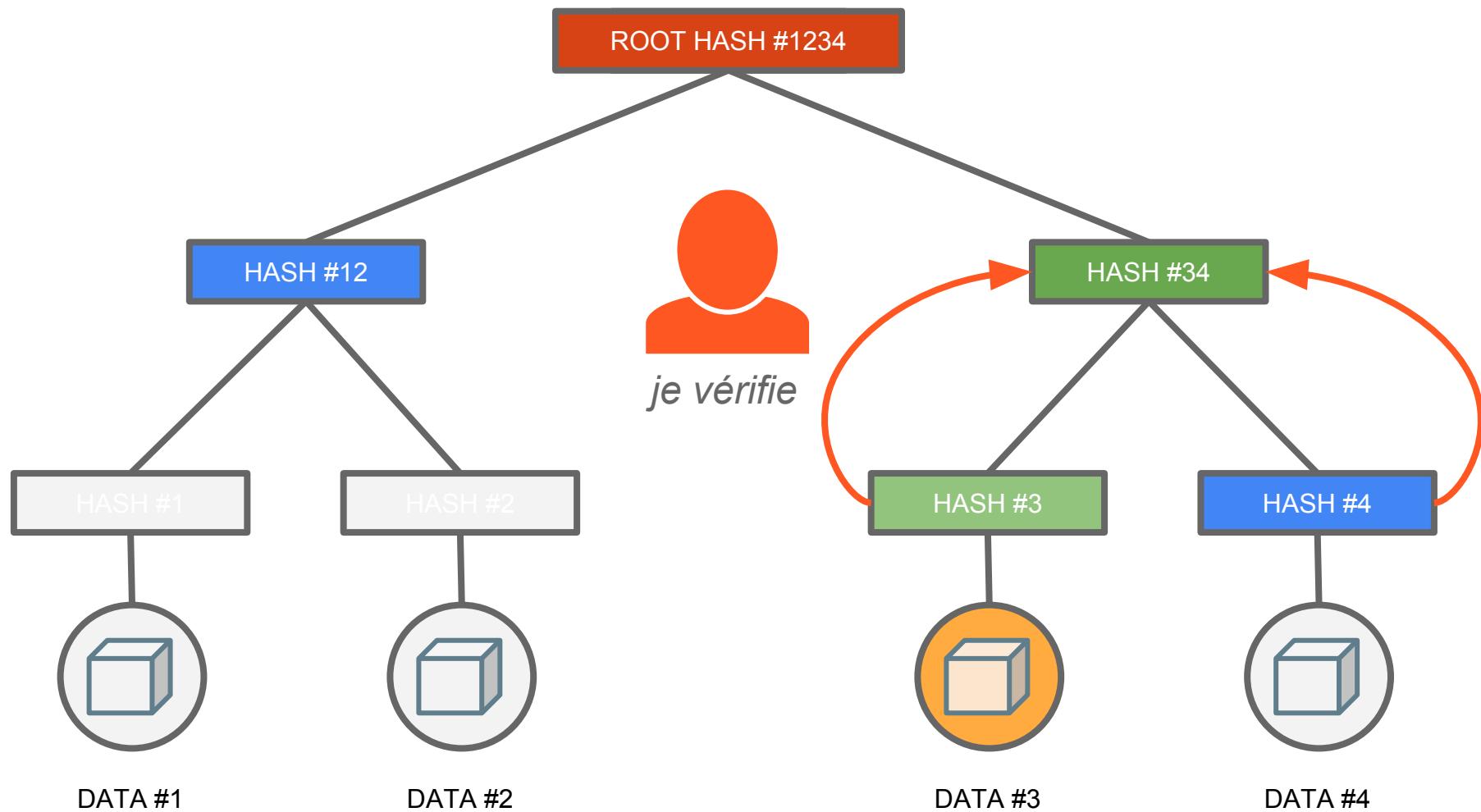
*je connais le
root hash de
source sûre*

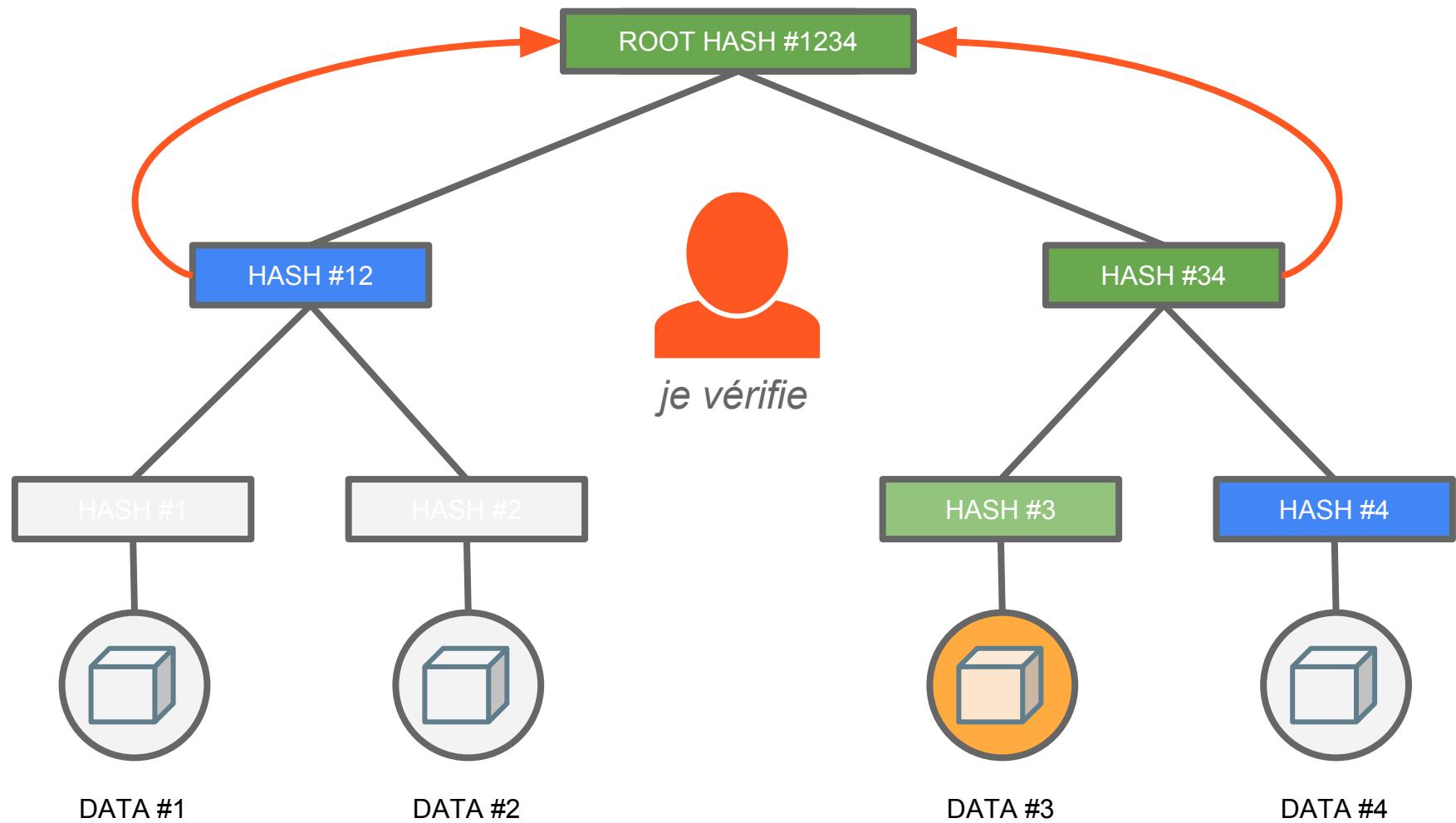
ROOT HASH #1234

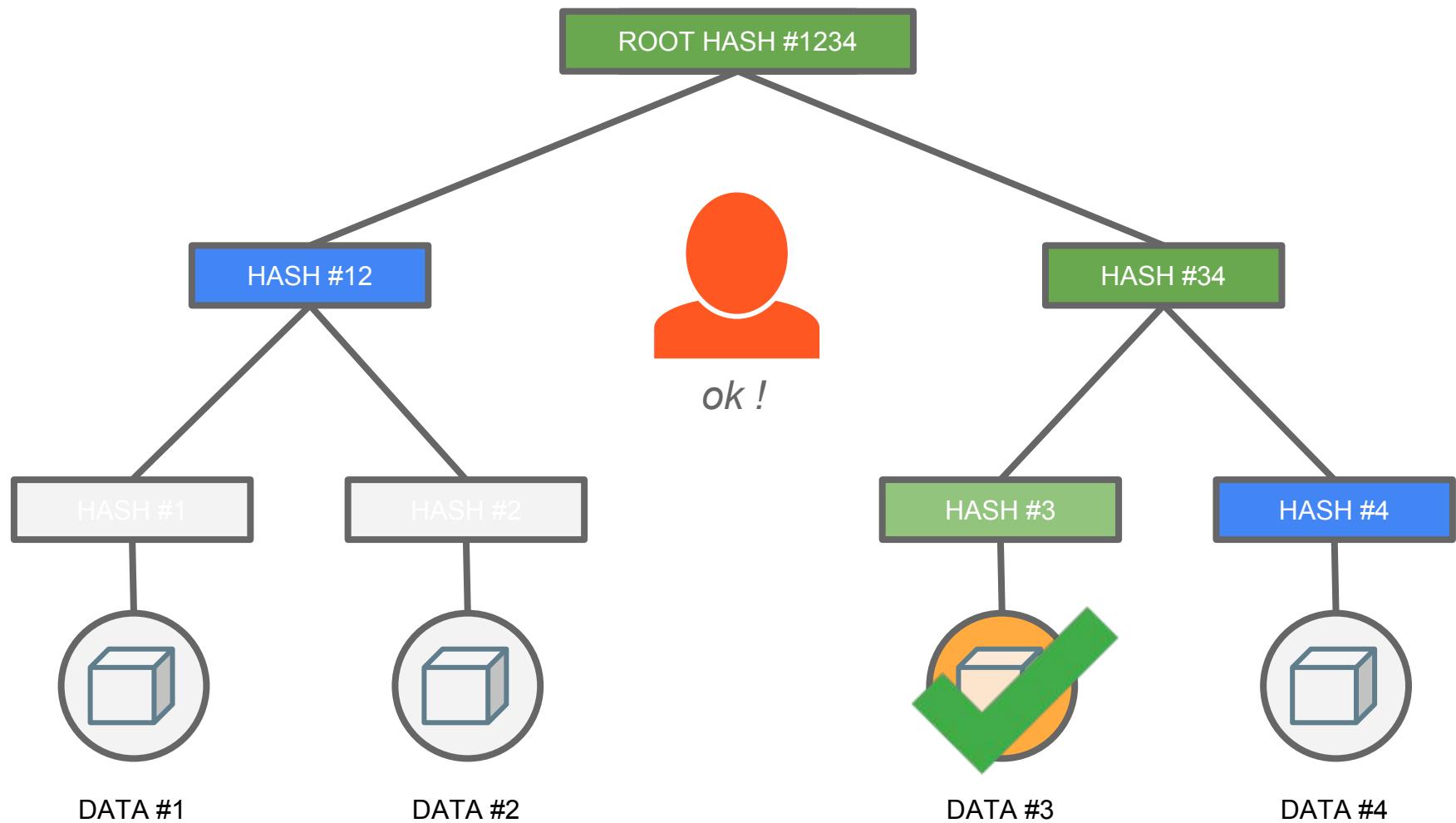




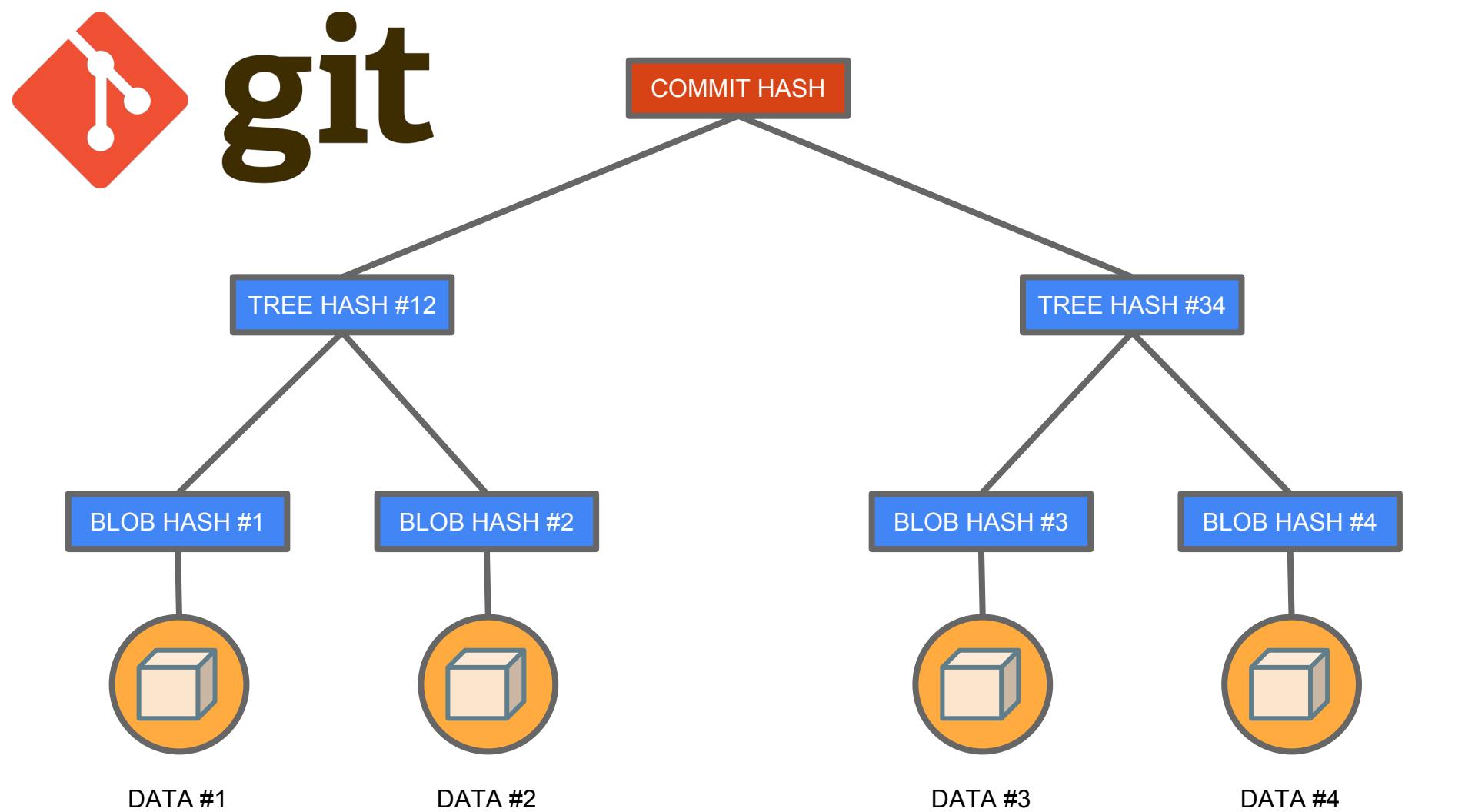


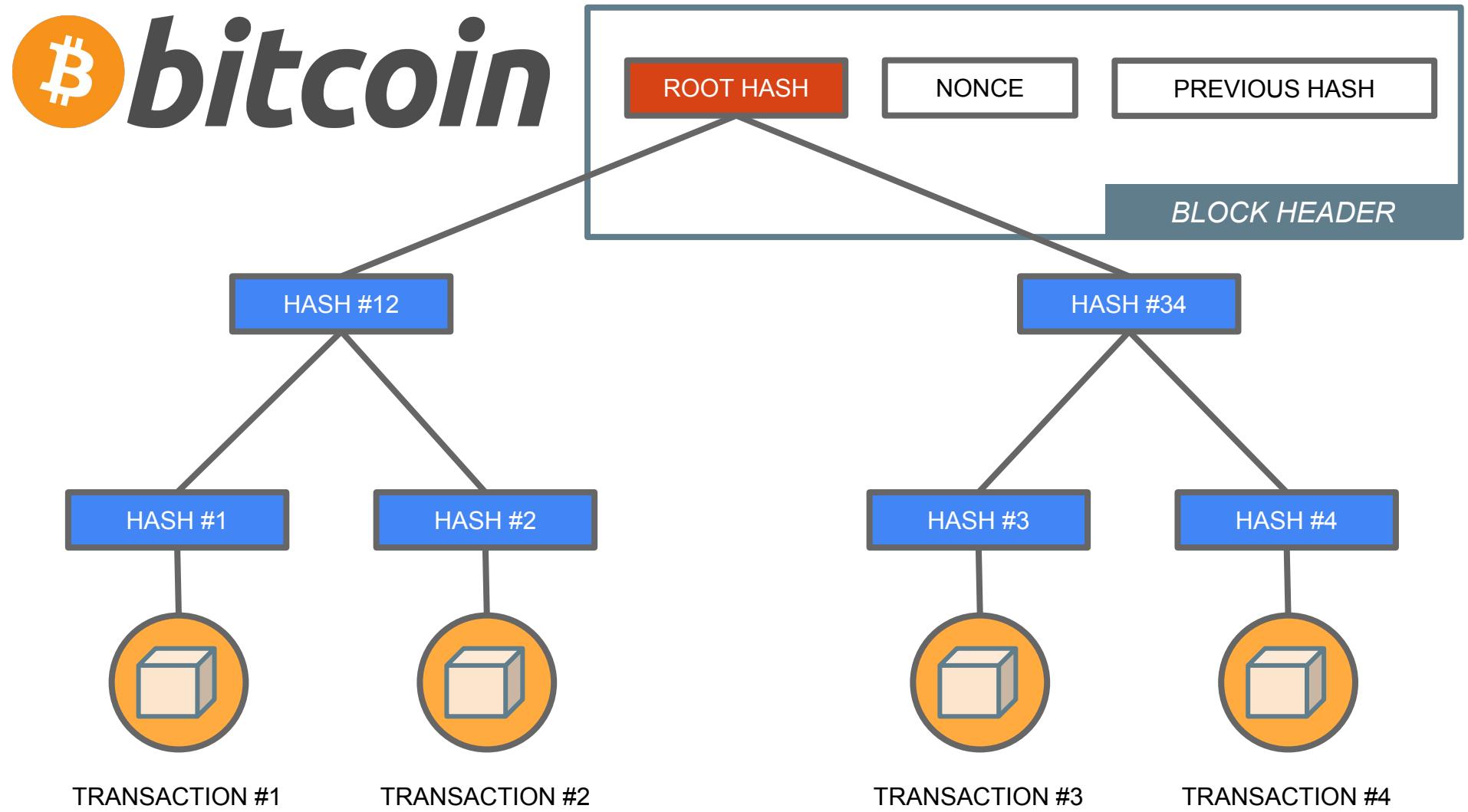






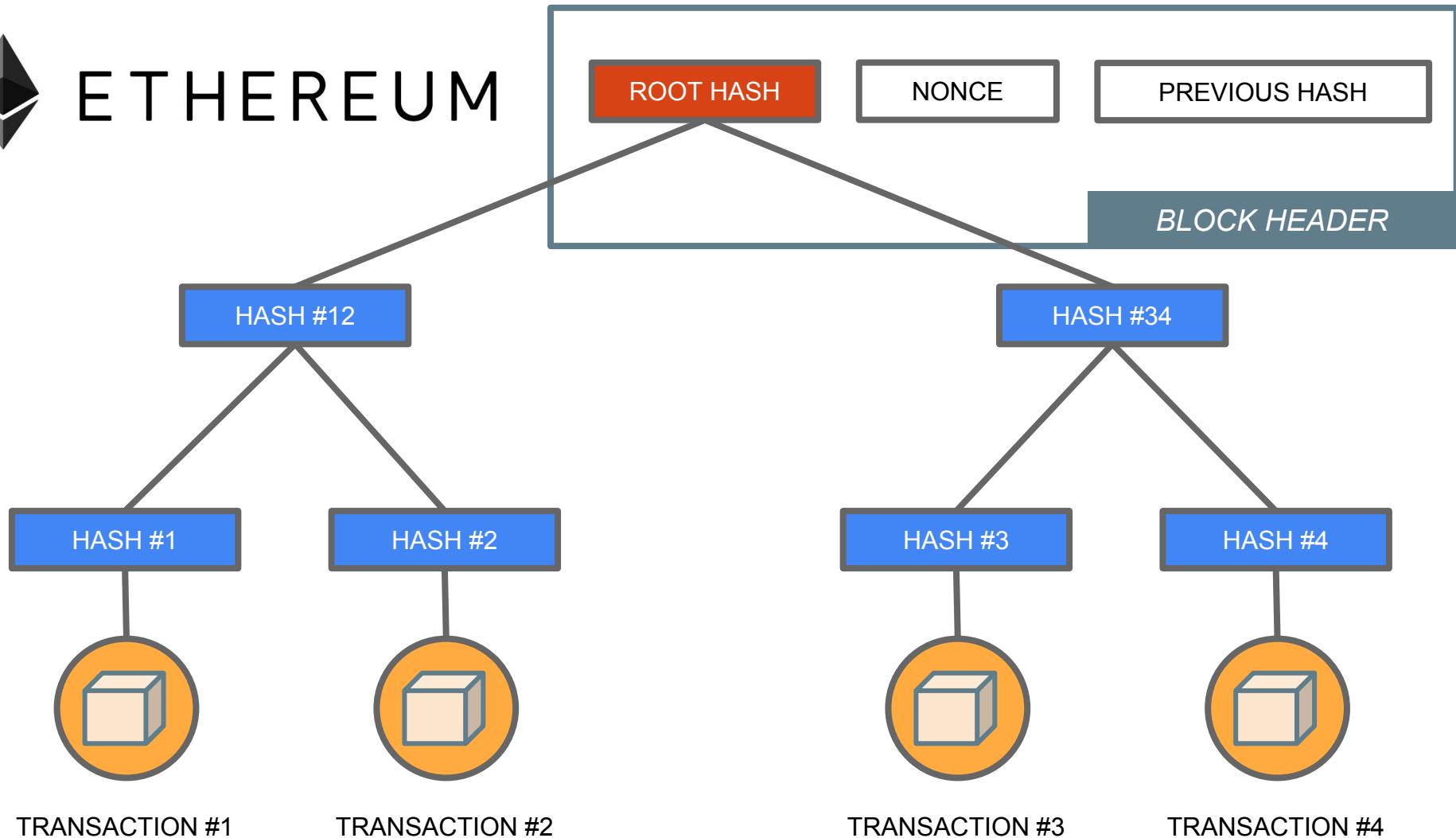
Utilisé ?







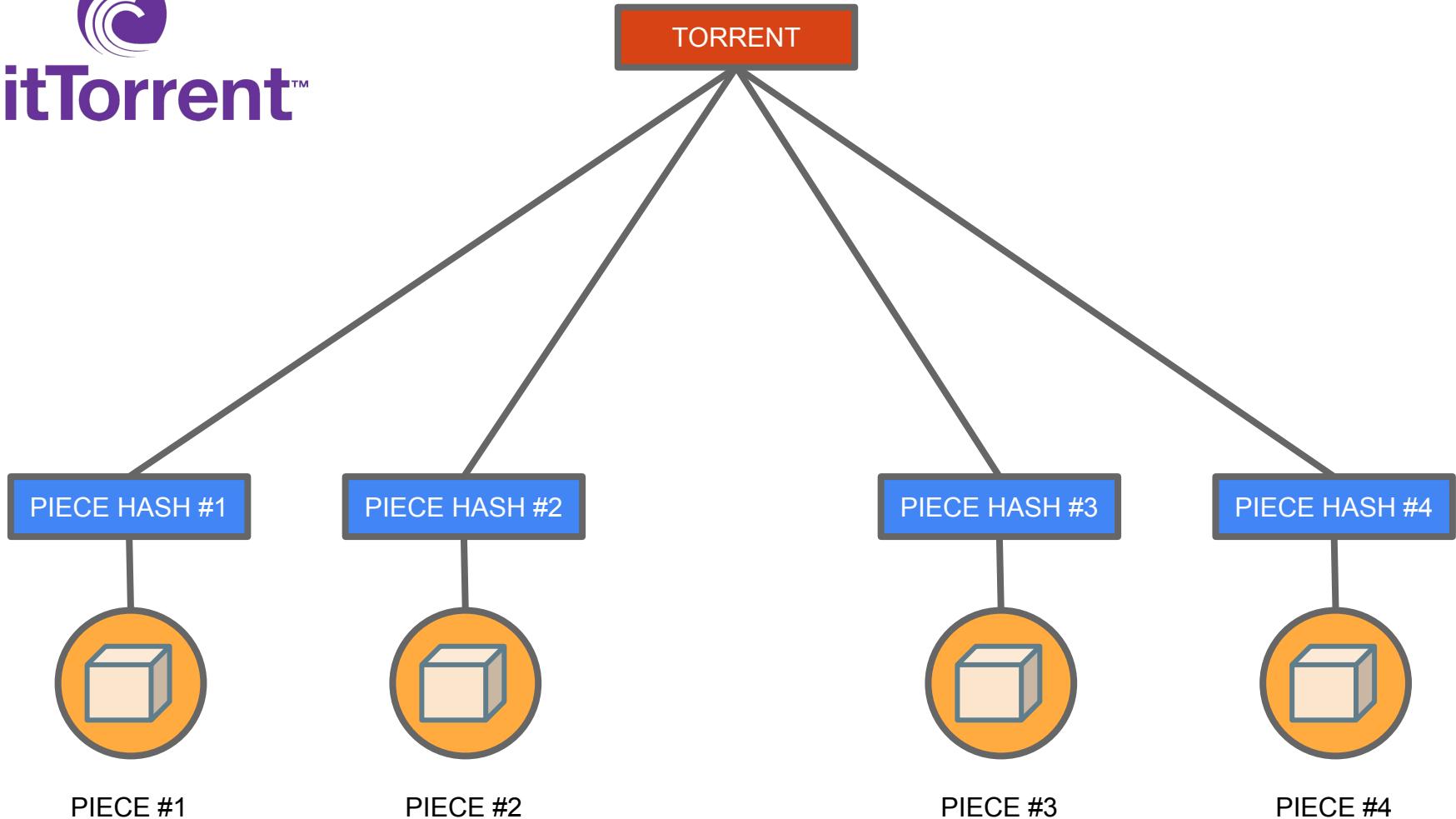
ETHEREUM

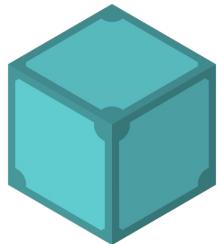




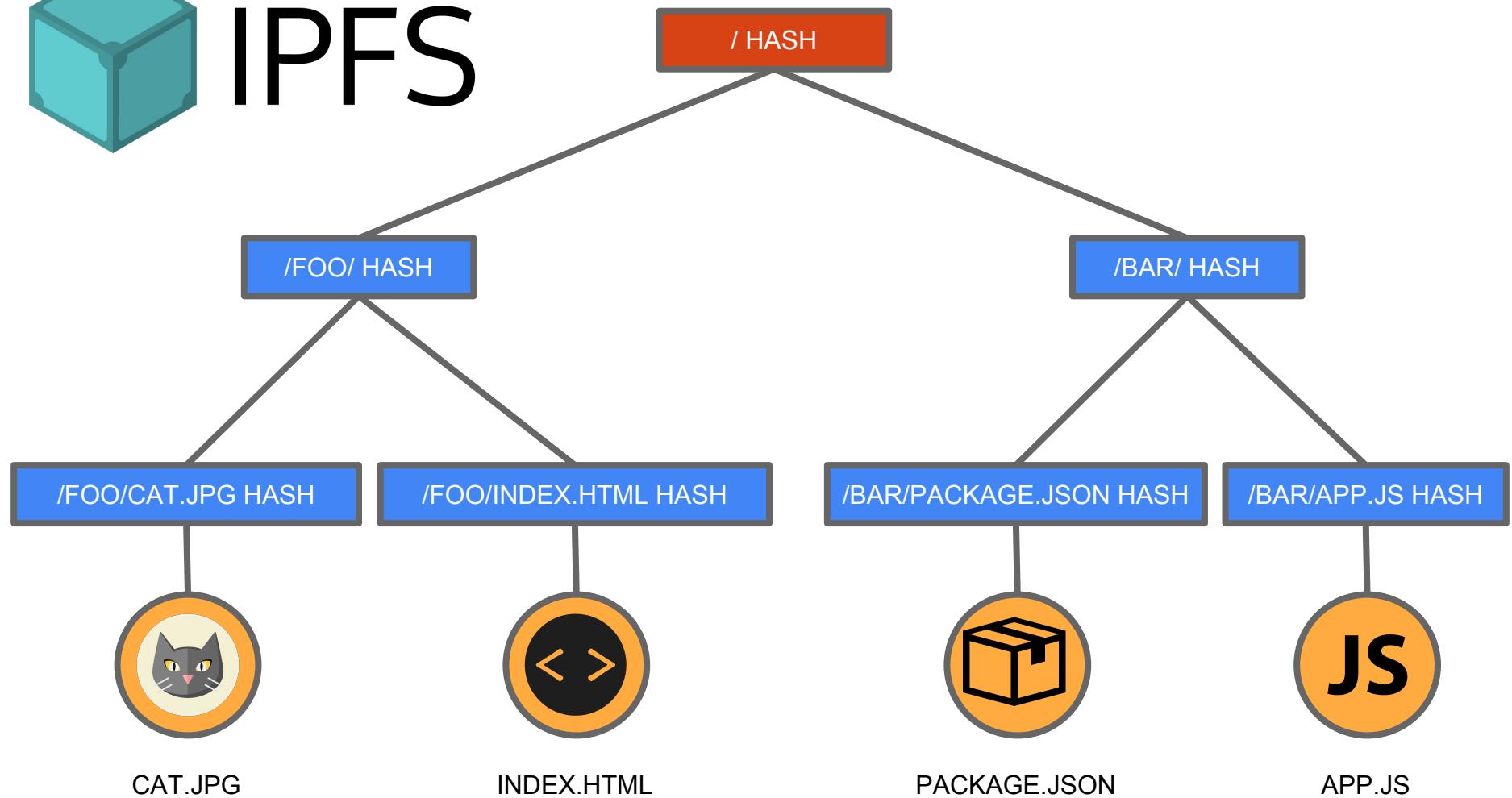
BitTorrent™

TORRENT



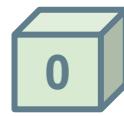


IPFS

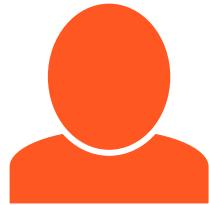




<https://ipld.io>



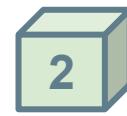
+1





+2





Salt u! ca Comment ca ?va

Conflict resolution

Conflict-free Replicated Data Types CRDT ?



INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Conflict-free Replicated Data Types

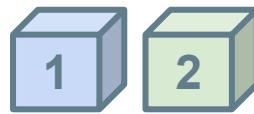
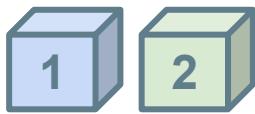
Marc Shapiro, INRIA & LIP6, Paris, France

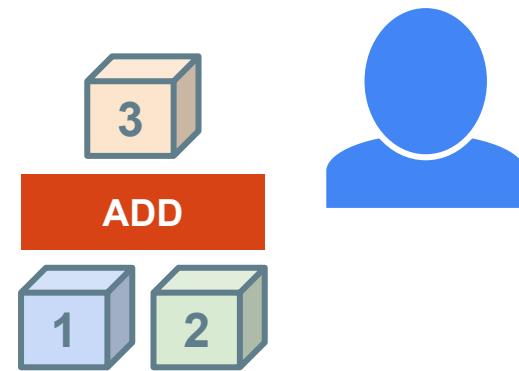
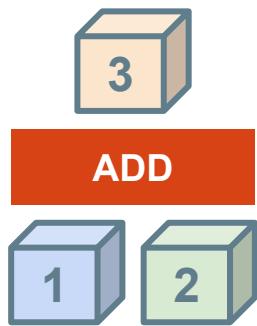
Nuno Preguiça, CITI, Universidade Nova de Lisboa, Portugal

Carlos Baquero, Universidade do Minho, Portugal

Marek Zawirski, INRIA & UPMC, Paris, France







Grow-only Counter



-1



ADD



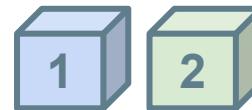
- ADD



-3



ADD



- ADD





2

ADD

1 2

- ADD

1



0

ADD

1 2

- ADD

3





-1

ADD

1 2

- ADD

1 3

-1

ADD

1 2

- ADD

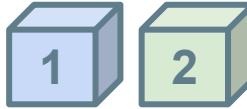
1 3



Positive-Negative Counter



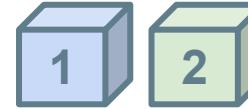
ADD



- ADD



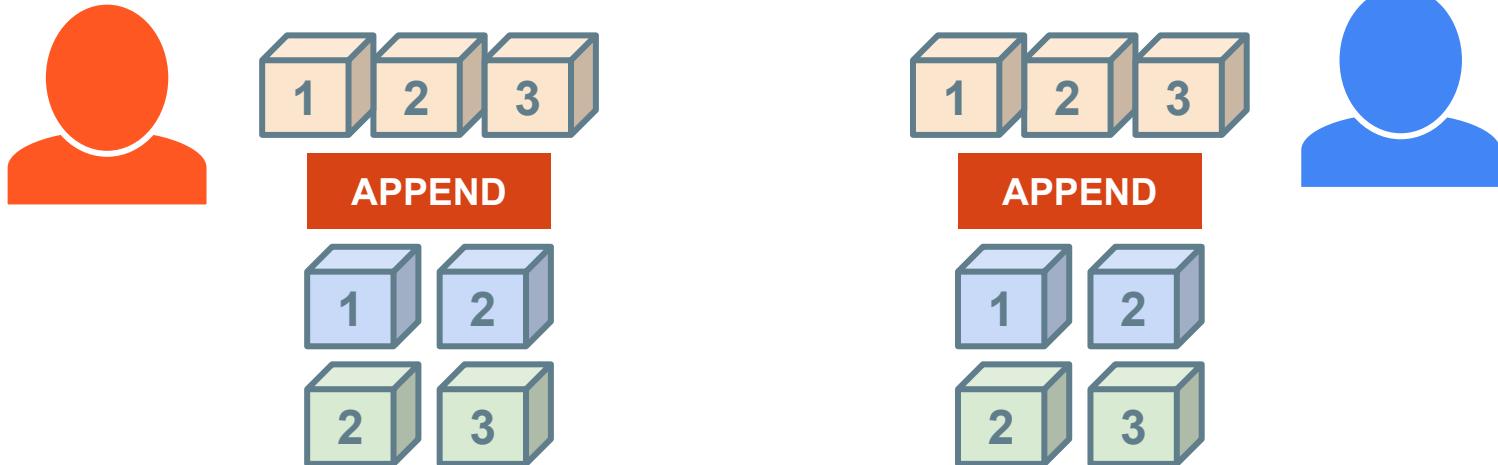
ADD



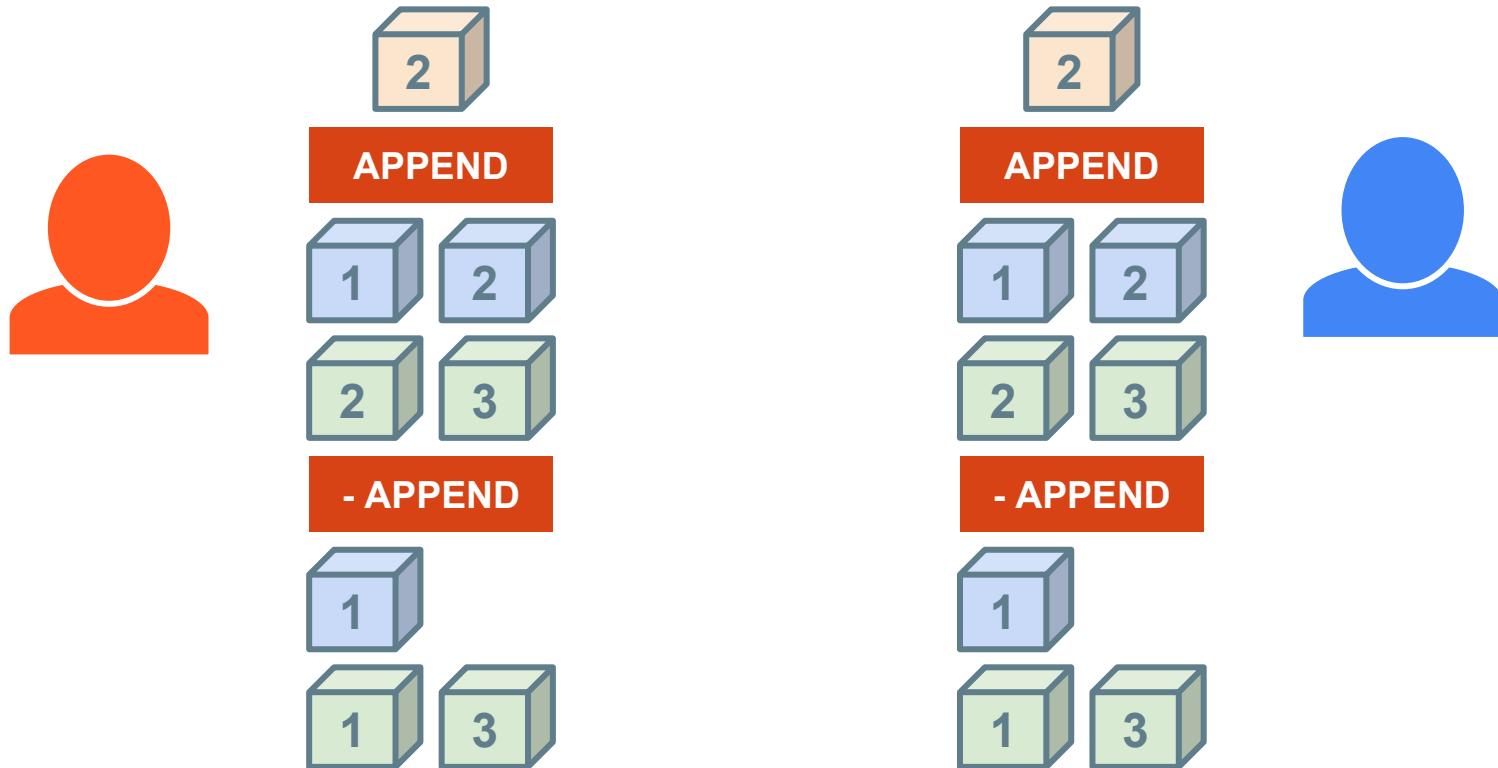
- ADD



Grow-only Set



2-Phase Set



2-Phase Set

+



Timestamp



=

Last-Write-Wins-Element-Set

OR-Set

MC-Sets

U-Set

LWW-Register

MV-Register

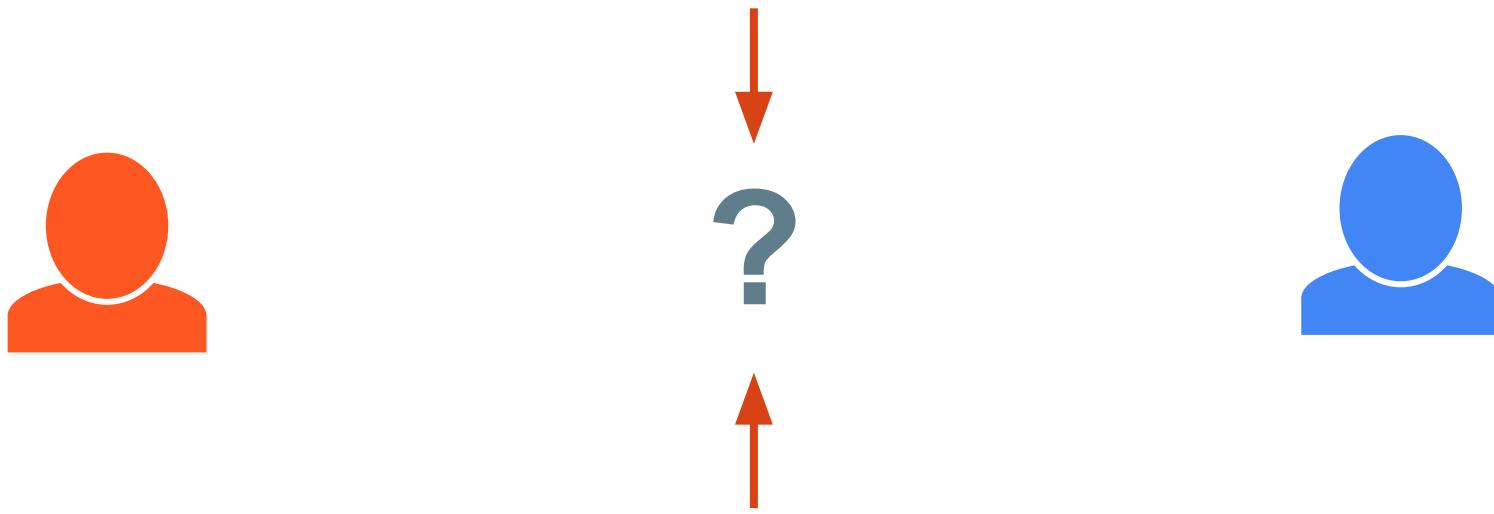


Add-only monotonic DAG

Add-Remove Partial Order

...

Compromis sur les fonctionnalités (Ajout, Suppression, Modification...)



Compromis sur la performance (bande passante, perte de paquet, mémoire...)

Utilisé ?



Bases de données distribuées



Distributed Data



SOUNDCLOUD

News feed

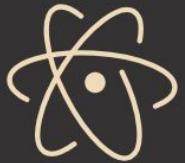


Chat (70M utilisateurs)



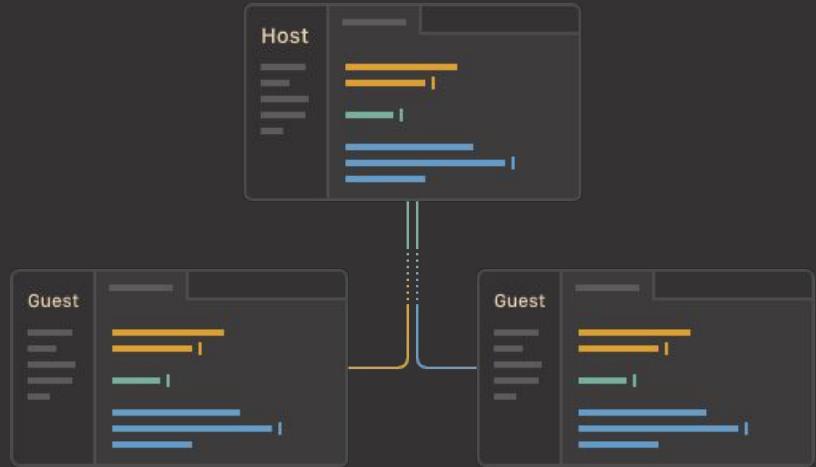
Sync. des localisations
favorites

Mais aussi...



Collaborate in real time in Atom

Teletype^(beta) for Atom lets developers share their workspace with team members and collaborate on code in real time.



Mais aussi...

Démo

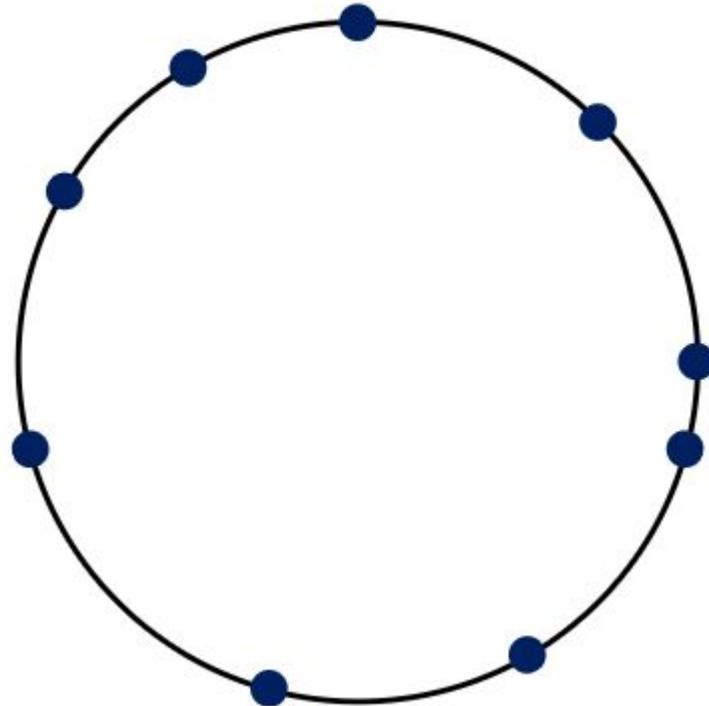
à la fin de la présentation

<https://acailly.github.io/roti/>

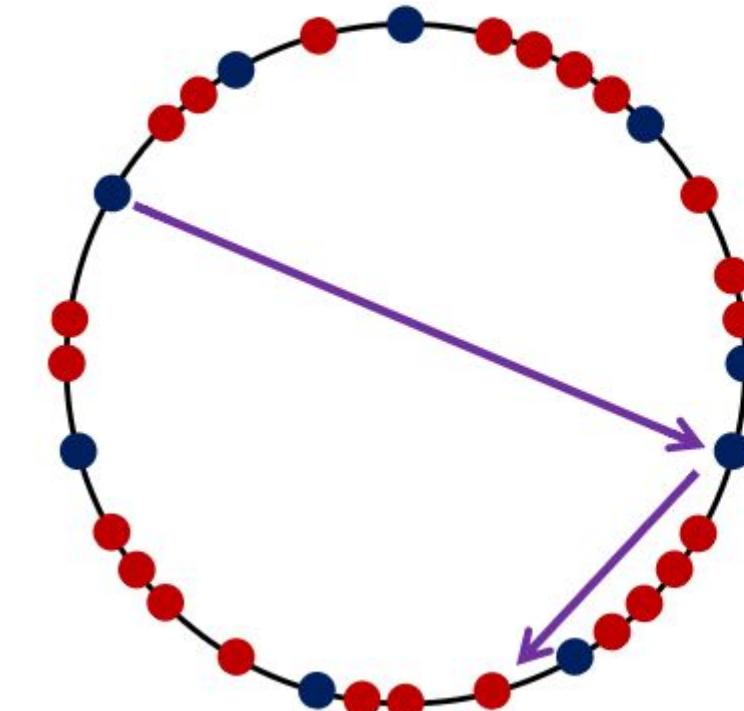


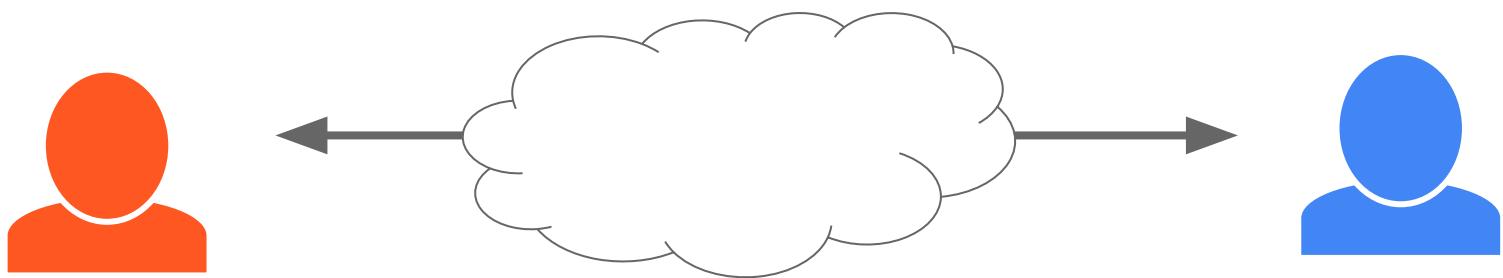
Et si on quittait le monde des bisounours ?

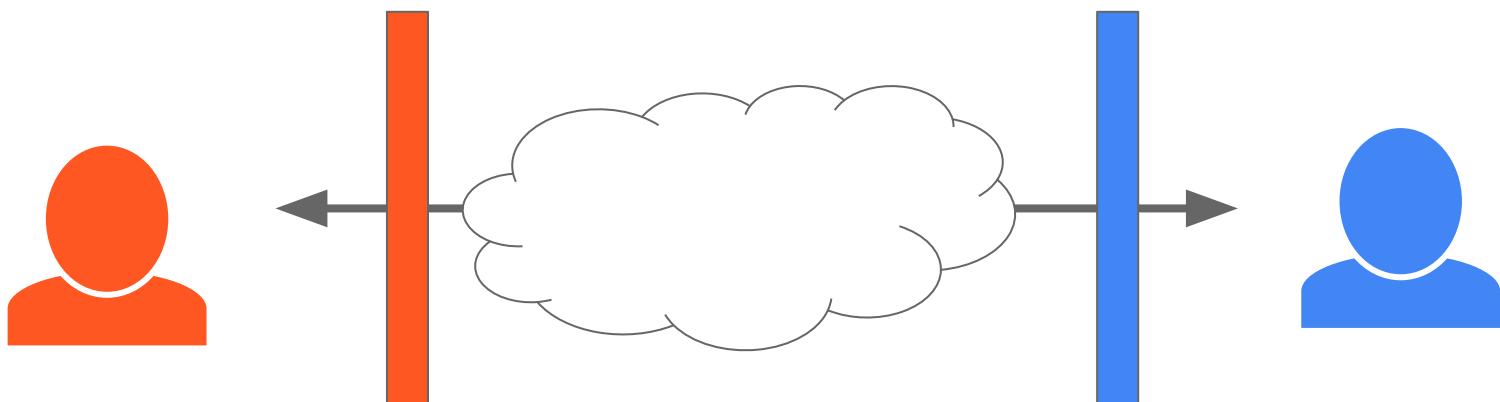
Sybil attack



Brute-force attack







Réseau privé

Réseau public

Réseau privé

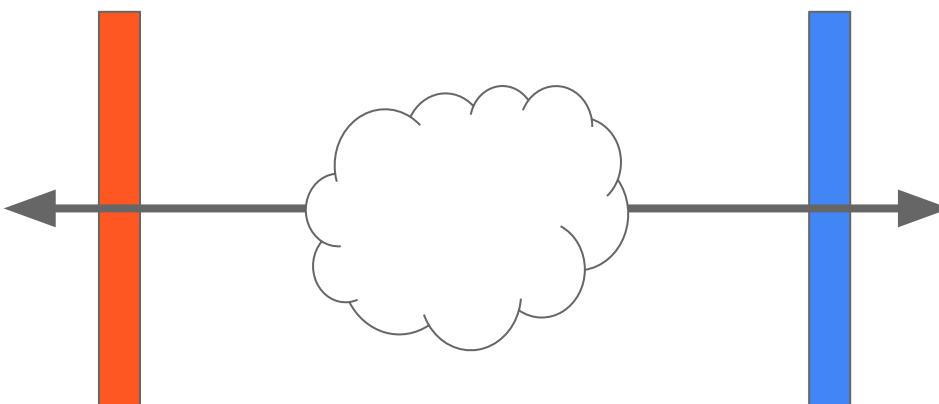
p^{☆\$# de proxy !}

NAT Traversal (Network Address Translation)

Session Traversal Utilities for NAT (STUN)

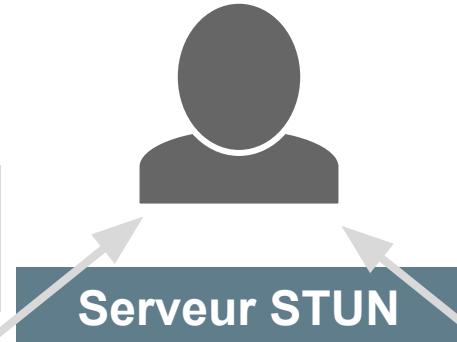


Adresse IP
privée



Adresse IP
privée

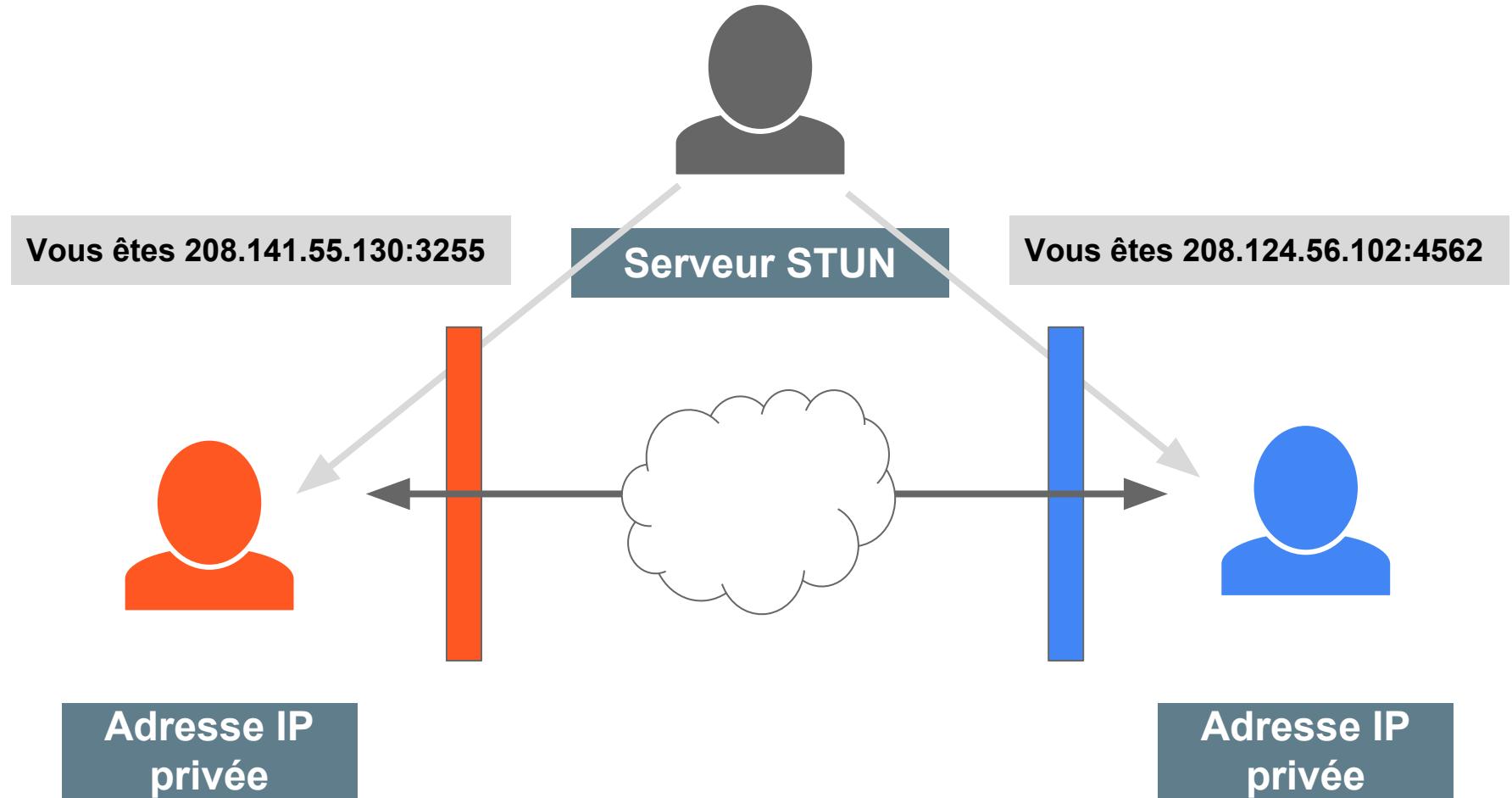
Quelle est mon adresse IP publique ?
Suis-je accessible de l'extérieur ?



Adresse IP
privée



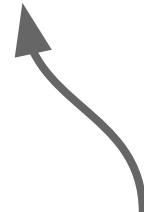
Adresse IP
privée



Adresse publique du routeur

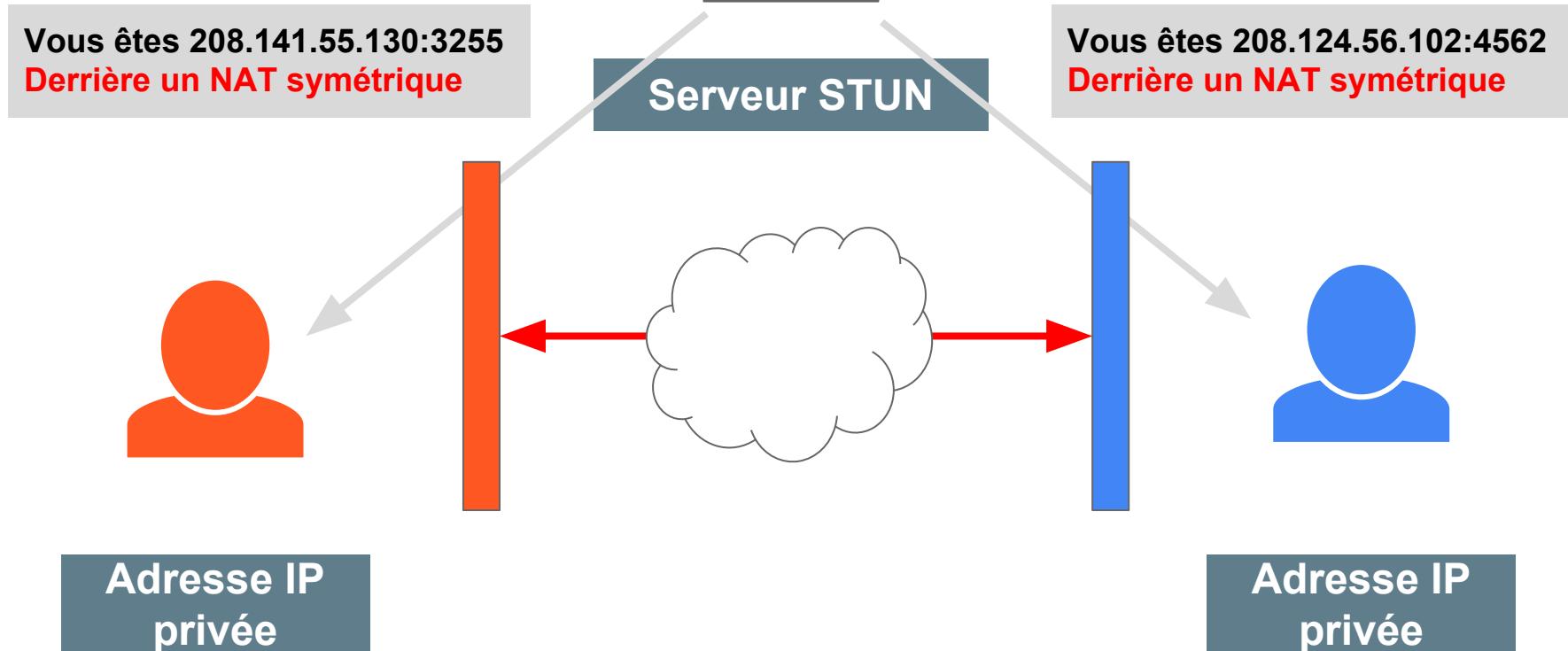


208.141.55.130:3255

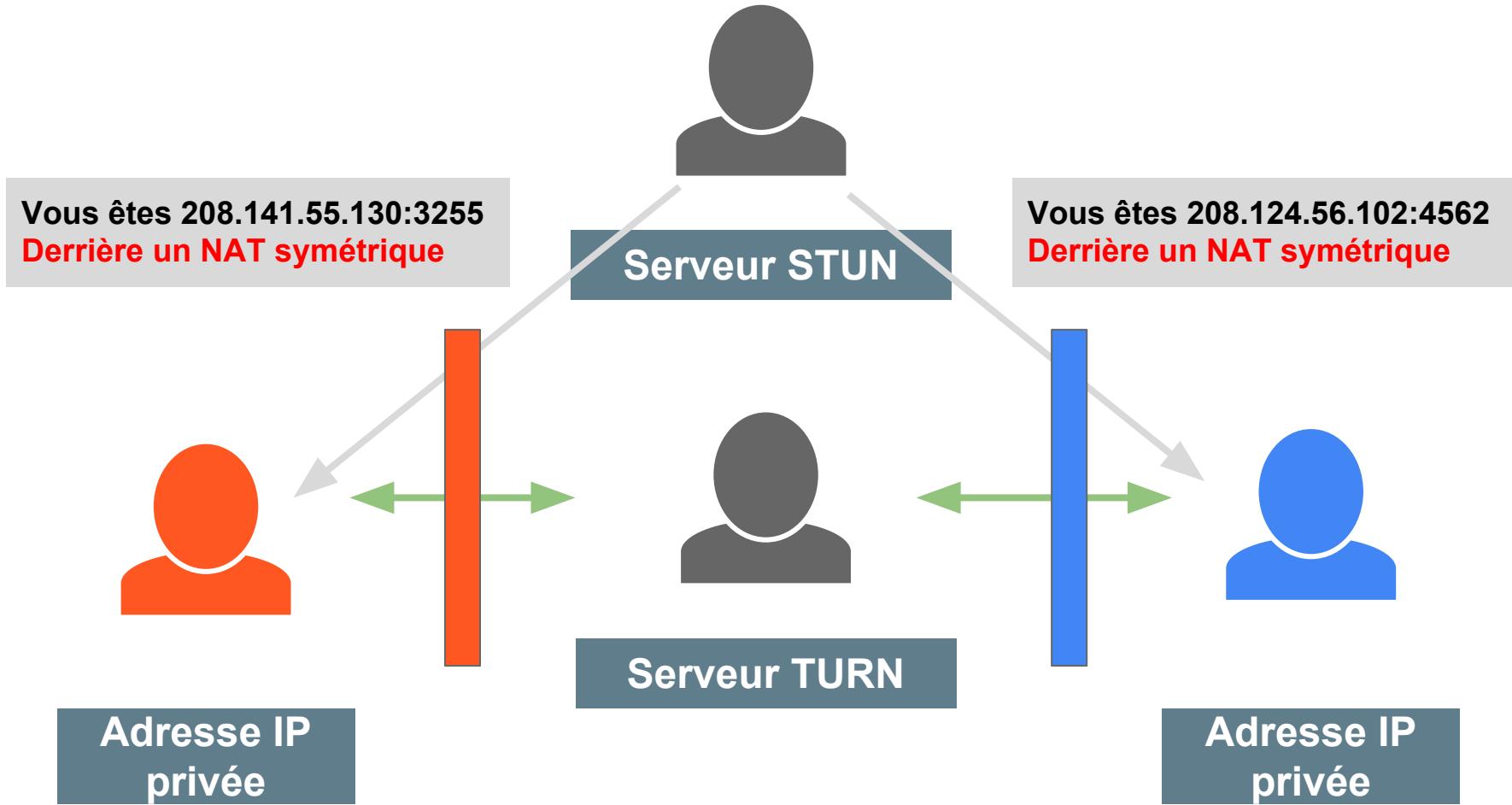


Port unique pour chaque device
derrière le routeur

Qui n'accepte que les connexions entrante s'il y a une connexion sortante sur ce pair



Traversal Using Relays around NAT (TURN)





Que nous réserve le futur ?





Scalabilité ?

Impact écologique ?

Arnaques ?

Centralisation ?

IPFS is the Distributed Web

A peer-to-peer hypermedia protocol
to make the web faster, safer, and more open.

Try it

Watch demo

The IPFS Stack

applications

Using the Data

IPNS

naming

IPLD

merkldag

Defining the Data

libp2p

exchange

routing

network

Moving the Data

<https://www.coindesk.com/257-million-filecoin-breaks-time-record-ico-funding/>

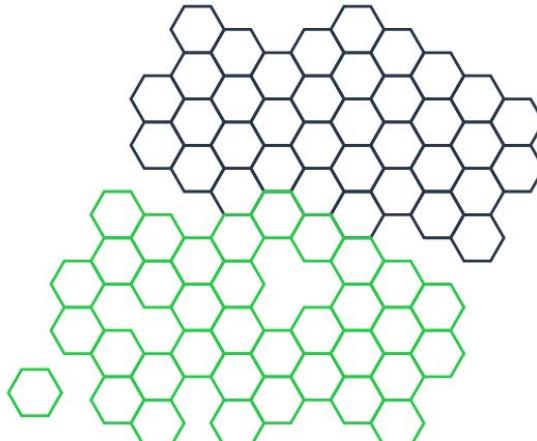


\$257 Million: Filecoin Breaks All-Time Record for ICO Funding

Sep 7, 2017 at 20:45 UTC by Stan Higgins

A distributed **data** community

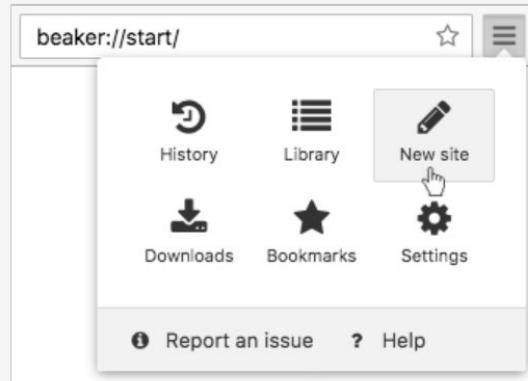
Dat is a nonprofit-backed community & open protocol for building apps of the future.



Rethink the Web browser

Beaker is a peer-to-peer browser with tools to create and host websites. Don't just browse the Web, build it.

<https://beakerbrowser.com/>



Can your browser do this?



None of us are as smart as all of us.

Fork



@leokewitz
December 13th, 2017
3 min read

New release 0.2.0

I'm really happy to announce that I finally learned how to version ^[^1]! Also there are a lot of new features!

Footnotes

As you might noticed one of the new features is being able to add footnotes ^[^2]. Footnotes can be inlined or manually referenced.

```
This is how you manually[^manual] reference something[^1].
```

```
This is how you add inline^[You don't need to specify inlined notes at the end of the file.] notes.
```

```
...
```

```
// In the end of the file...
```

```
[^1]: This is something.
```

```
[^manual]: Manual.
```

kontain 0.0.4

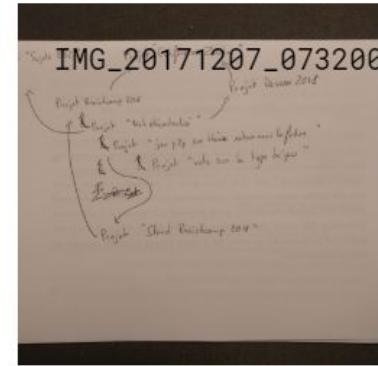
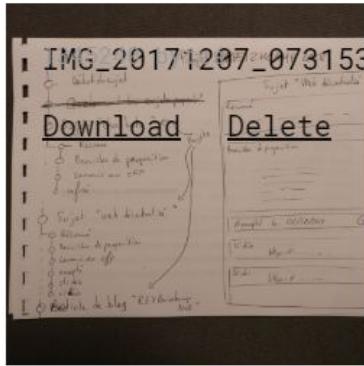
peer-to-peer file sharing

drop files anywhere

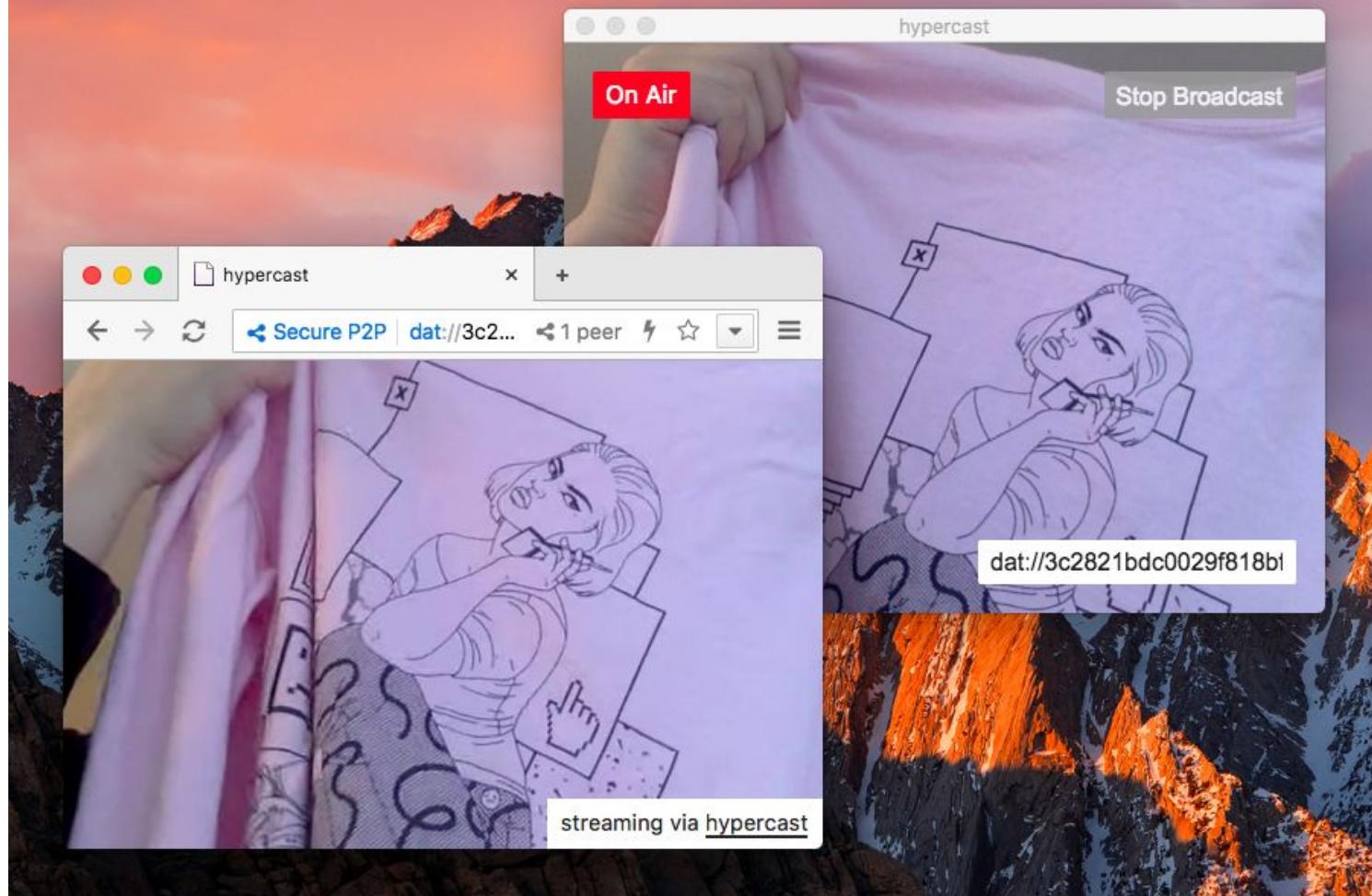
carbon.png

```
require('lodash')
= require('bittorrent-dht'
ip = require('geoip-lite-co
```

guide.txt



<http://hex22.org/projects/ntain/>



<https://github.com/louiscenter/hypercast>



Paul Frazee

Following

Web nerd re-decentralizing the Web. Unblockchain consultant. Founder of the Beaker browser and Hashbase. Previously Secure Scuttlebutt.

Make sure your profile stays online! Share your profile URL with a public peer like Hashbase.

Feeling ambitious? Deploy your own public peer.

Copy your profile URL ↗

Who to follow



Tim Caswell

Follow



Ross Schulman

Follow



Sander Moolin

Follow



PsaeBrai

Follow

Posts

68

Following

39



Paul Frazee · 4d ago

No need to fret that you're missing frets. Fritter now tells you (once again) when there are new frets.



Paul Frazee · 4d ago

Fritter update was published. You shouldn't need to be afraid to click on links anymore.



Paul Frazee · 4d ago

Doing some work on Fritter today, fixing some of the annoying things like the issue clicking on links and the lack of "new posts" notification. Also going to look at Sander's mentions PR (finally!). Also using this to QA our 0.8 fork & edit flows... which needs a little work but it's working ok so far.



Paul Frazee · 4d ago

Replying to this post

Cool idea! I'm certain people will find that interesting and worth talking about.





168 Entries

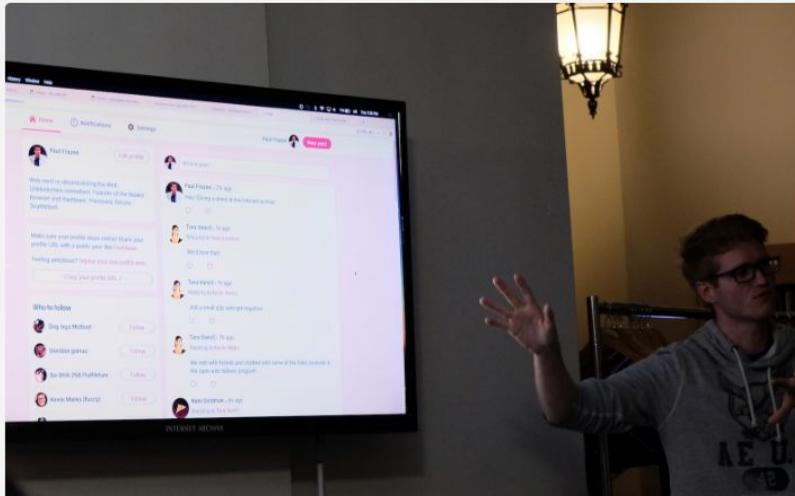
0 Mentions

0 Whispers

2170 Discoveries

~neauoire quoted **~jimpick** 13 days ago

very cool! Where was this? Where even is the internet archive?

**~jimpick** Scene from the Internet Archive...[Expand Entry](#)

Mozilla Add-ons Blog

<https://blog.mozilla.org/addons/2018/01/26/extensions-firefox-59/>



Extensions in Firefox 59

Support for Decentralization Protocols

Mozilla has always been a [proponent of decentralization](#), recognizing that it is a key ingredient of a healthy Internet. Starting with Firefox 59, several protocols that support decentralized architectures are approved for use by extensions. The newly approved protocols are:

- [Dat Project](#) (dat://)
- [IPFS](#) (dweb:// ipfs:// ipns://)
- [Secure Scuttlebutt](#) (ssb://)

Firefox [itself](#) does not implement these protocols, but having them on the approved list means the browser recognizes them as valid protocols and extensions are free to provide implementations.

Mais aussi...



Scuttlebot
a peer-to-peer log store

<http://scuttlebot.io/>



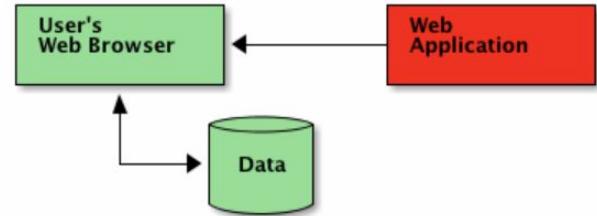
<https://solid.mit.edu/>



<https://matrix.org/>



remoteStorage



<https://remotestorage.io/>

<https://unhosted.org/>



<https://ethereum.org/>

Defending Internet Freedom through Decentralization: Back to the Future?

Chelsea Barabas

Neha Narula

Ethan Zuckerman

**The Center for Civic Media &
The Digital Currency Initiative
MIT Media Lab, August 2017**

<http://dci.mit.edu/decentralizedweb>

Démo

Rotonde



Rotonde is a social feed protocol.

<https://louis.center/p2p-social-networking/>

Démo

ROTI en pair à pair



@AntoineCailly



acailly

<https://acailly.github.io/roti/>

