Le web décentralisé

Technozaure Novembre 2017

Il était une fois en 2017...

Censure

Turkey Blocks
@TurkeyBlocks

Suivre

Confirmed: All editions of the #Wikipedia online encyclopedia blocked in #Turkey as of 8:00AM local timeturkeyblocks.org/2017/04/29/wik…

07:22 - 29 avr. 2017

86 2 875 1 015

Vikipedi üzerinde ara

Vikipedi'ye hoş geldiniz

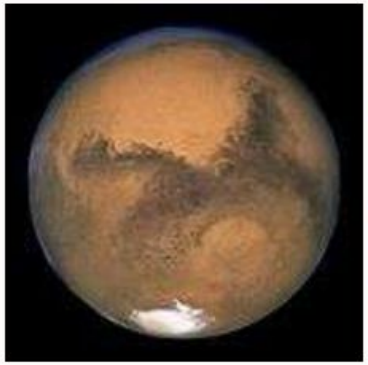
Herkesin katkıda bulunabildiği *Özgür Ansiklopedi*

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 tanrısı Mars'a ithafen adlandırılmıştır. Yüzeyindeki yaygın demir oksitten dolayı kızılımsı bir görünüme 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'nınkine çok benzer. İ… 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

Generalitat de Catalunya
gencat.cat

Català Castellano Aranés English

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

Meses 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

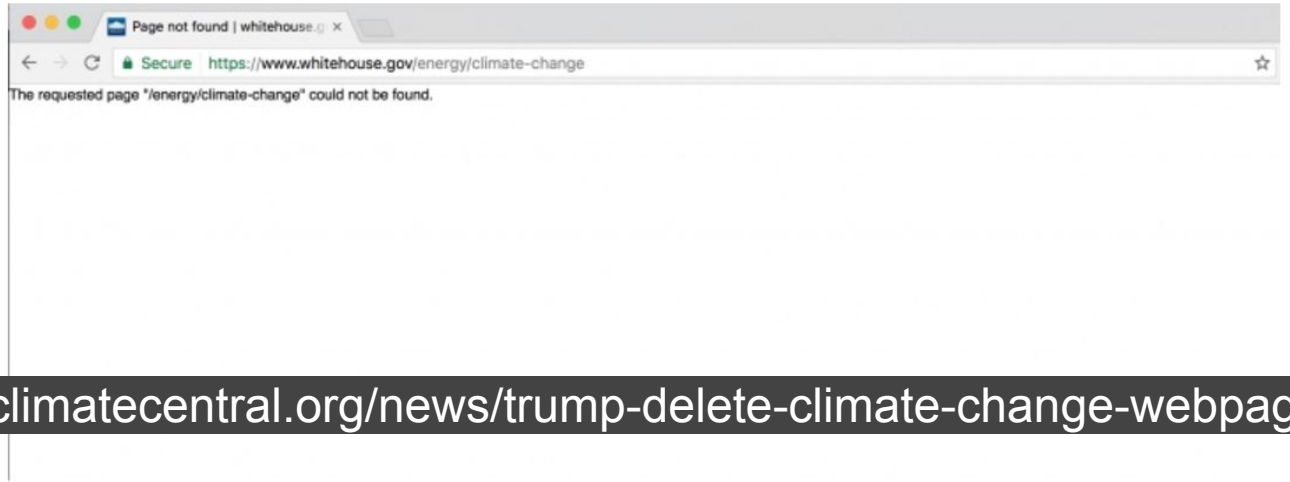
By Brian Kahn

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.

DataRefuge

Datasets Organizations Groups About

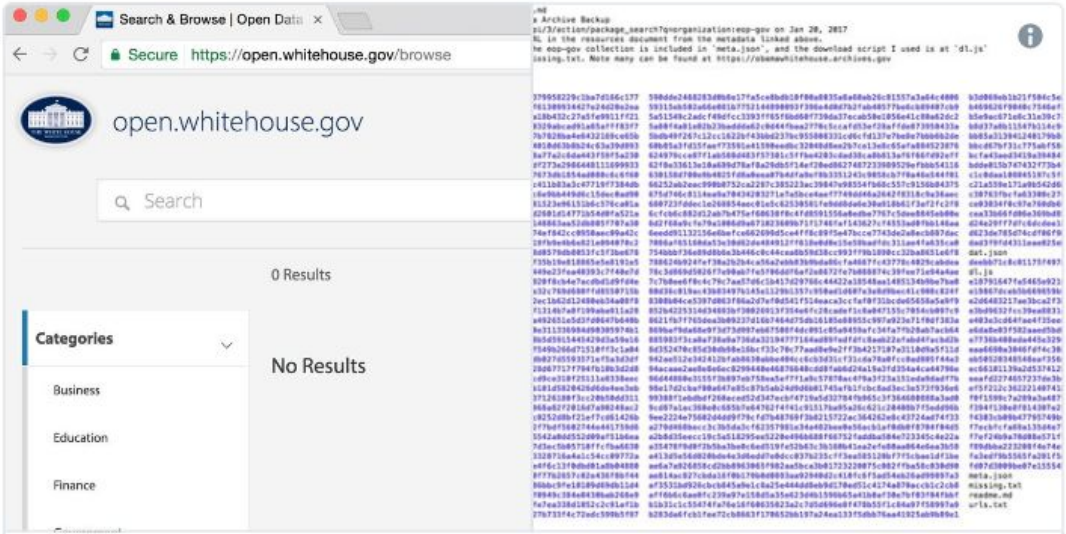
Search

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.

https://datproject.org/explore

Centralisation des services

Recherche

Maps

YouTube

Play

Actualités

Gmail

Drive

Agenda

Google+

Traduction

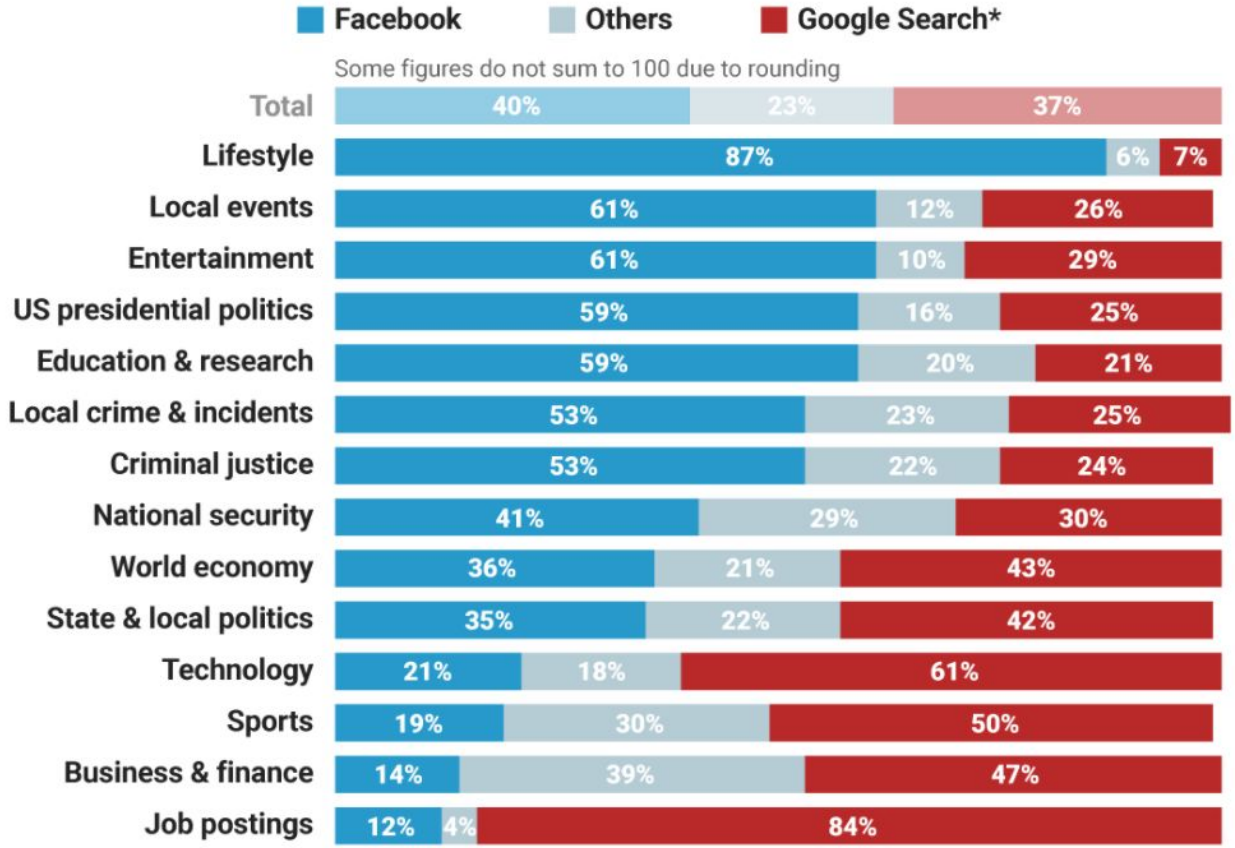
Photos

Inbox

ANDROID

Centralisation du trafic

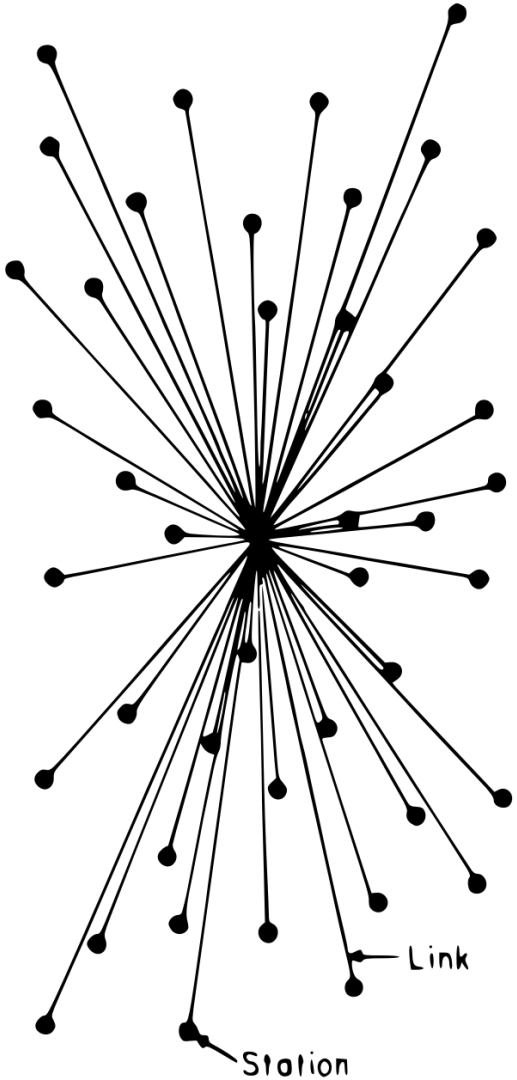
DISTRIBUTION OF REFERRAL TRAFFIC SOURCES BY TOPIC



SOURCE: Parse.ly *Not including Google AMP

statista | BUSINESS INSIDER

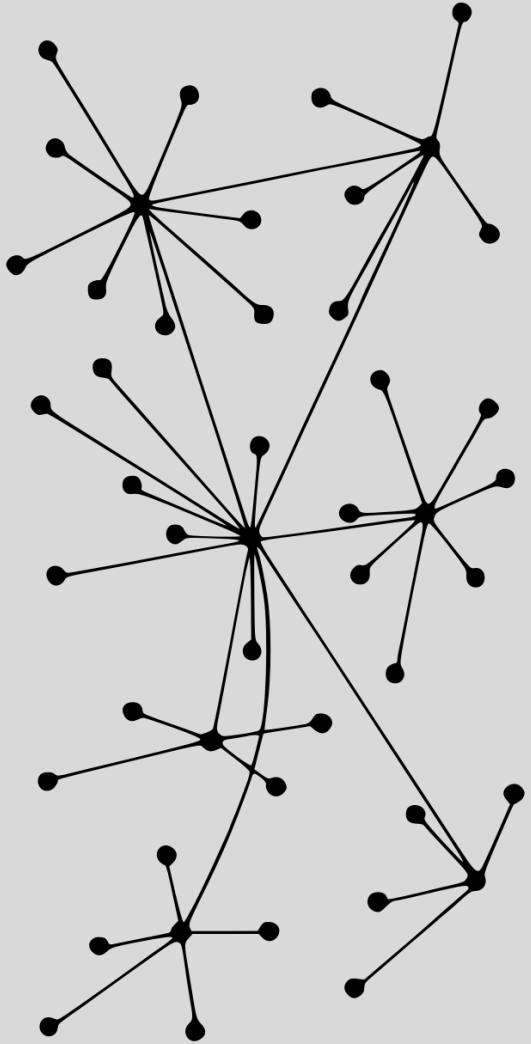
Un point commun ?


Link
Station

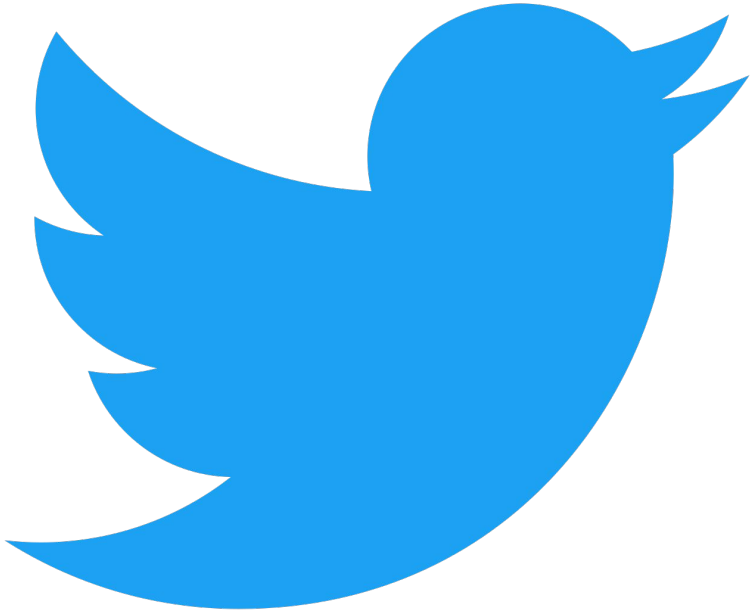
Single point of failure

Single point of control

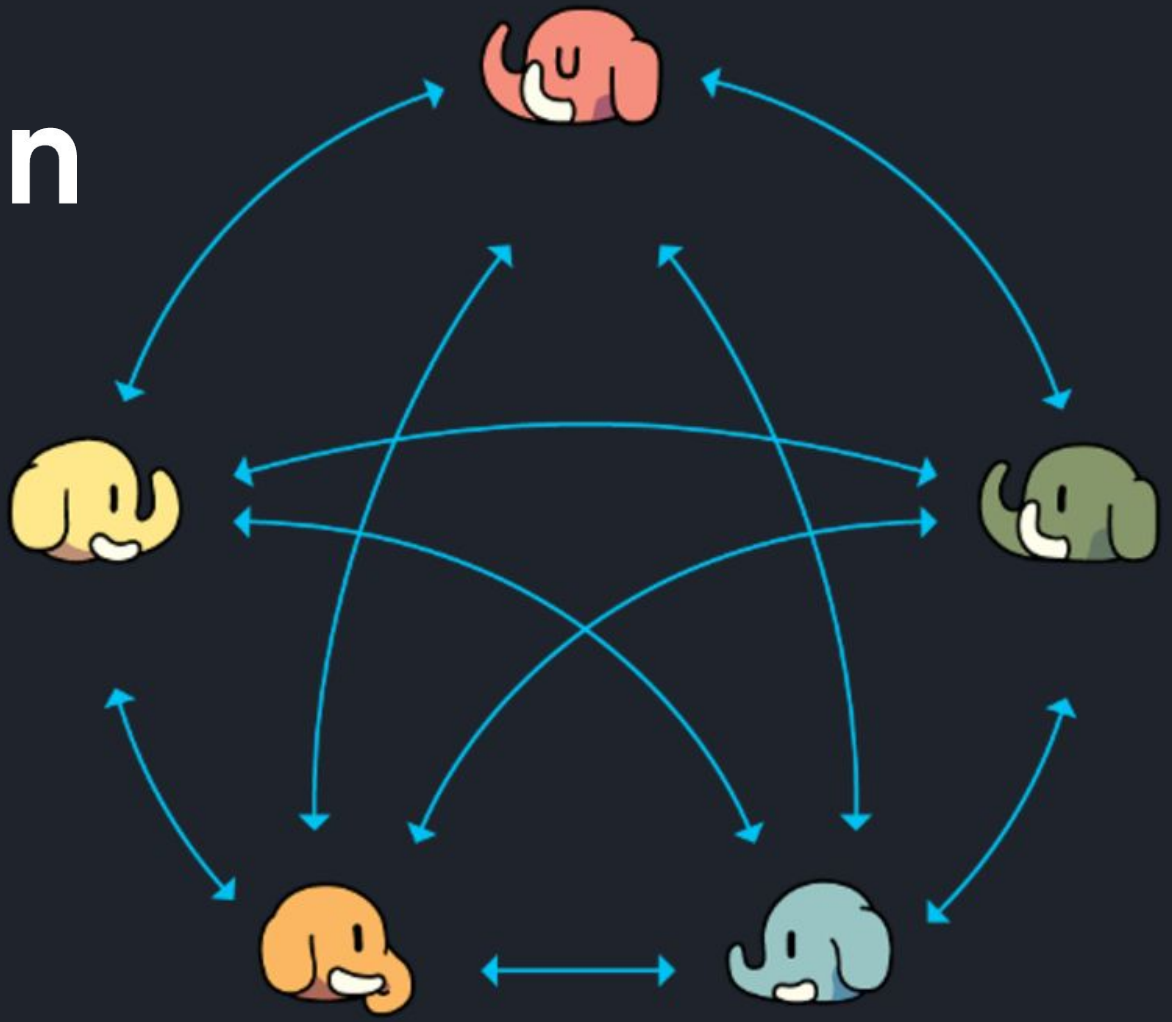
Une solution ?



Décentralisé

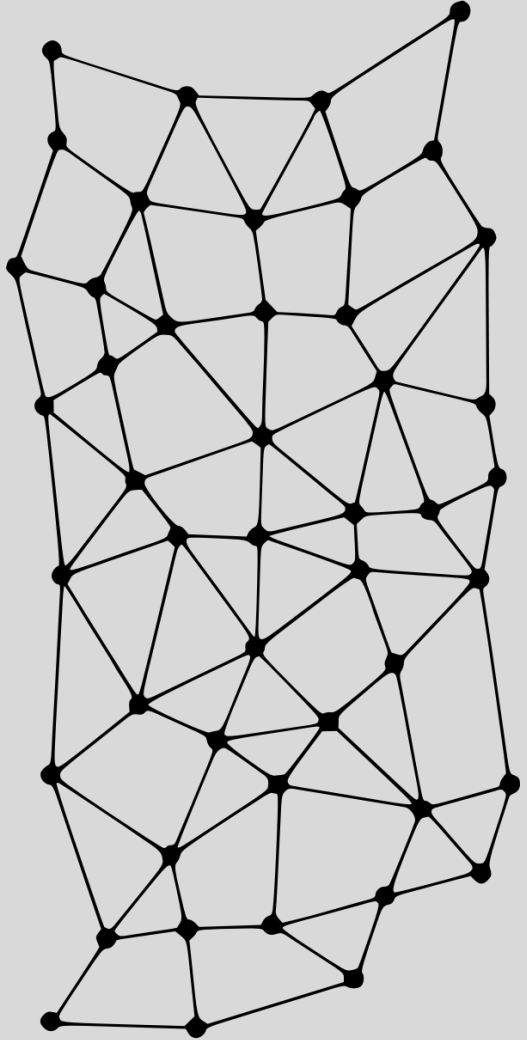


mastodon

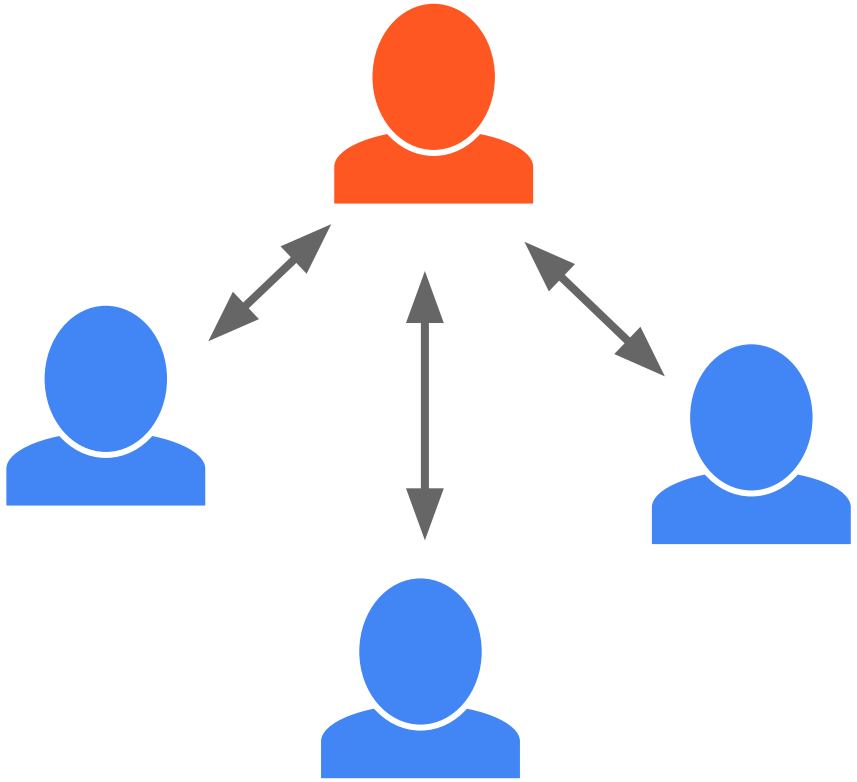


https://joinmastodon.org/

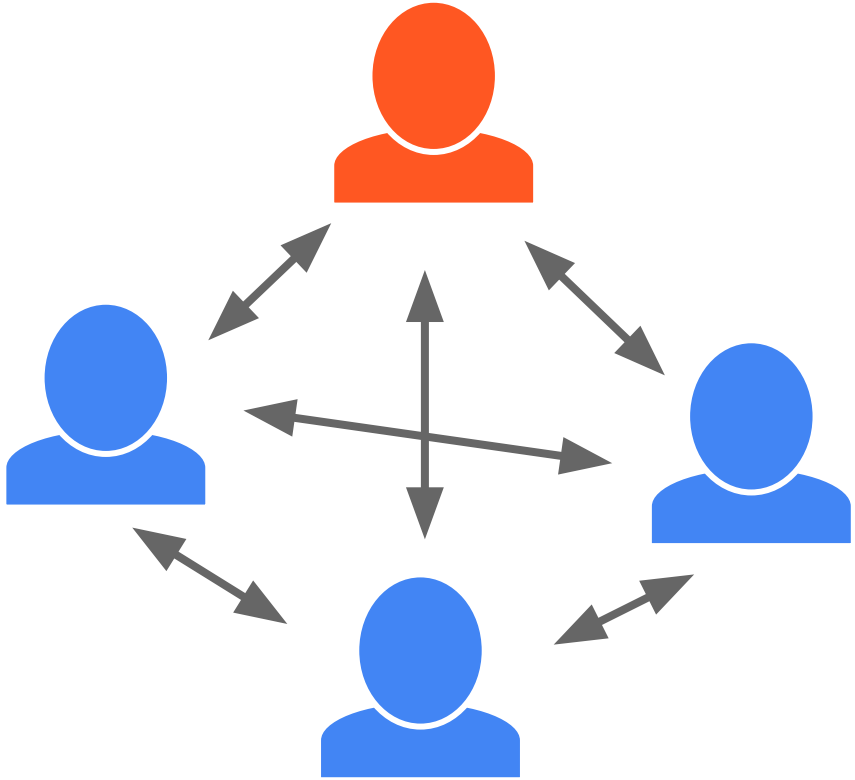
Distribué



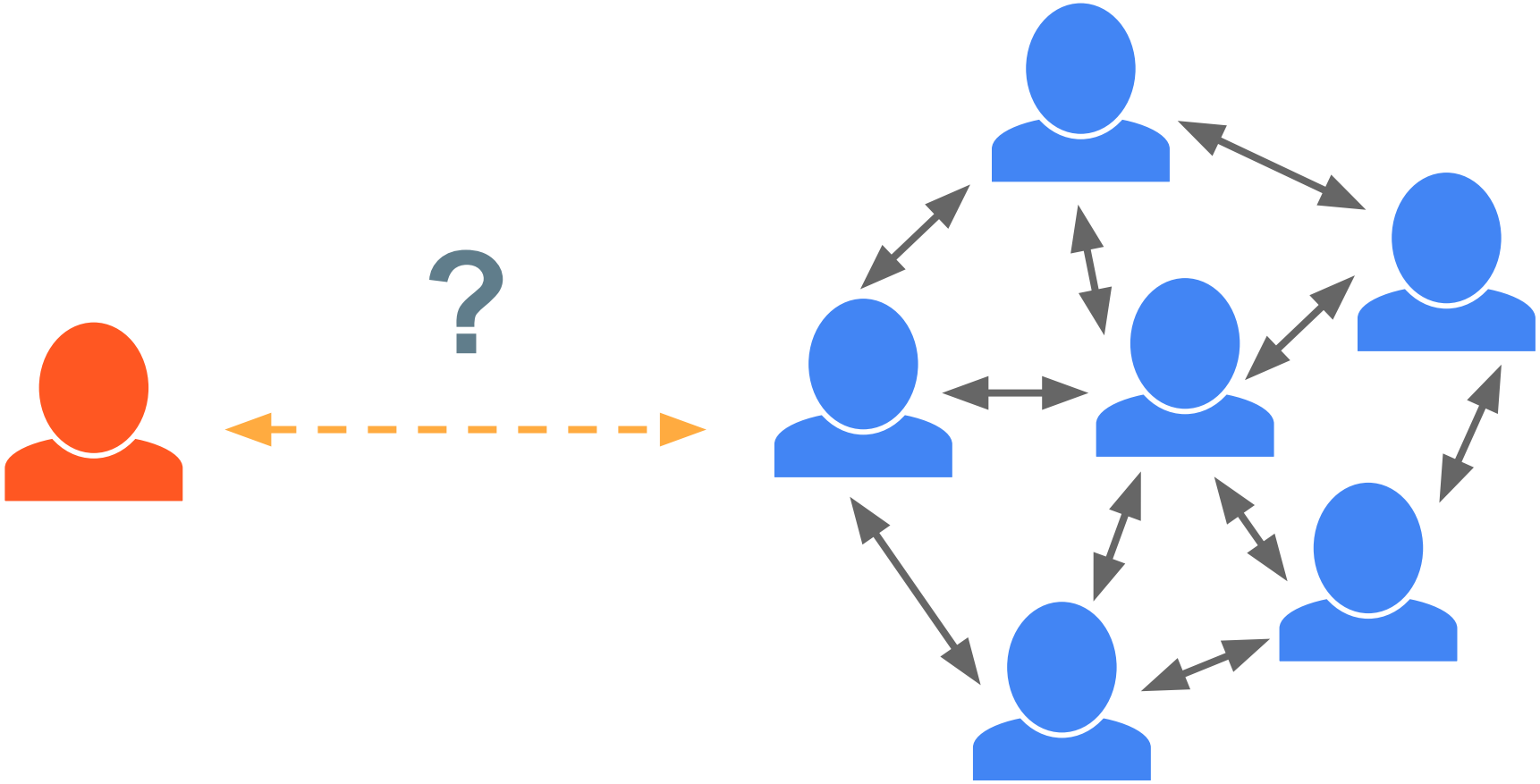

SUBVERSION




git

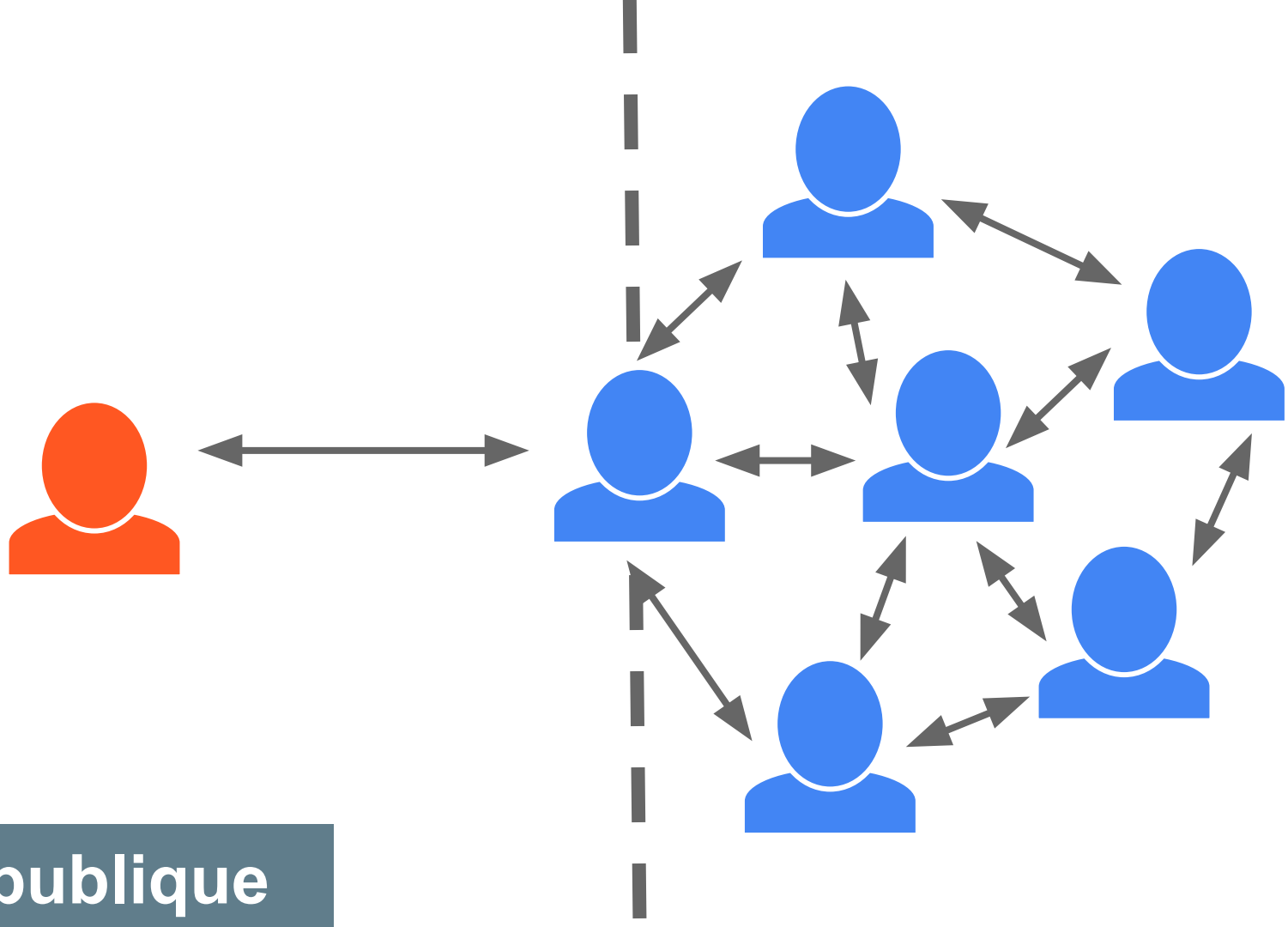


Comment ca marche ?

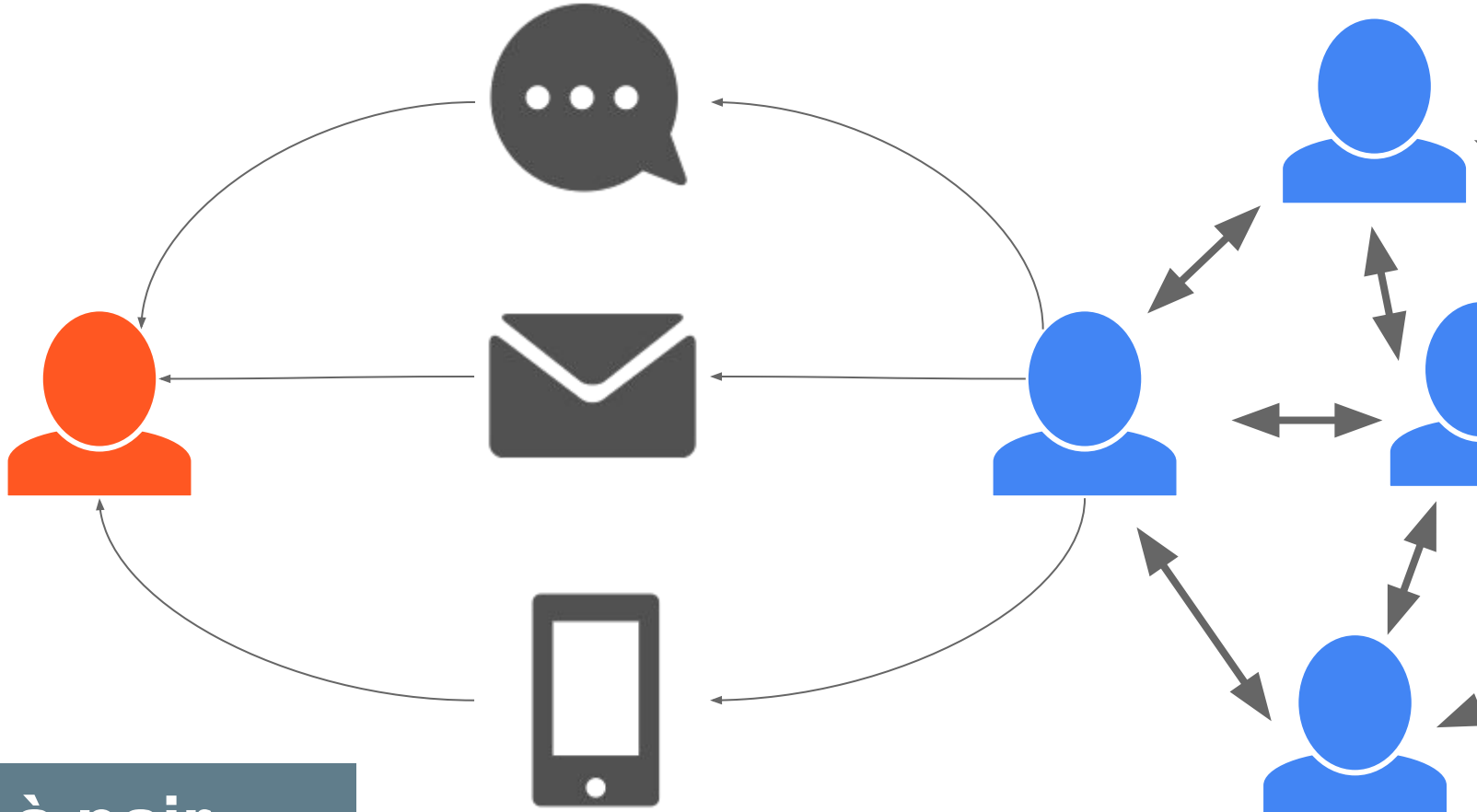


Comment on rentre ?

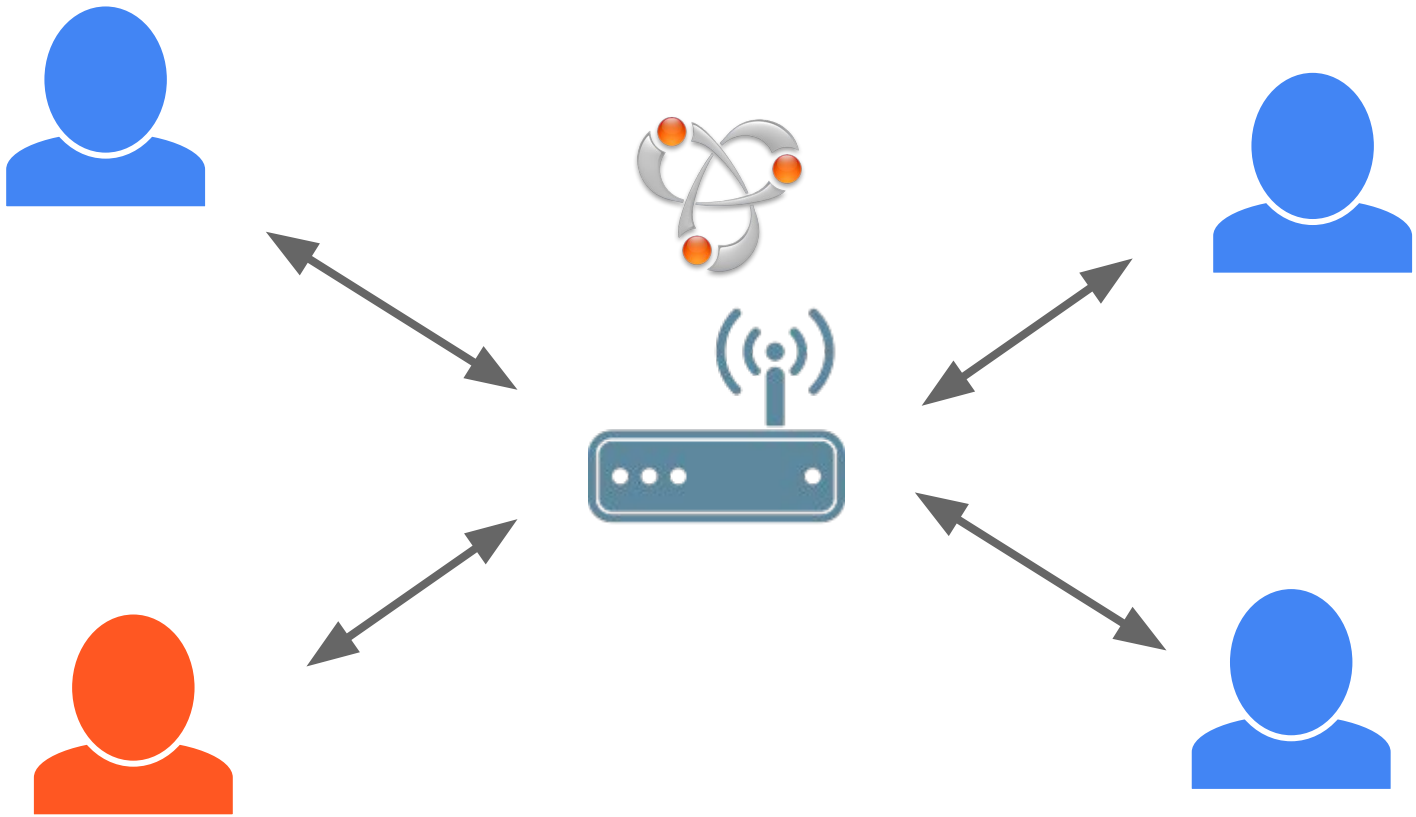
Bootstraping



Node publique



Pair à pair



Multicast DNS (ZeroConf, Apple Bonjour)

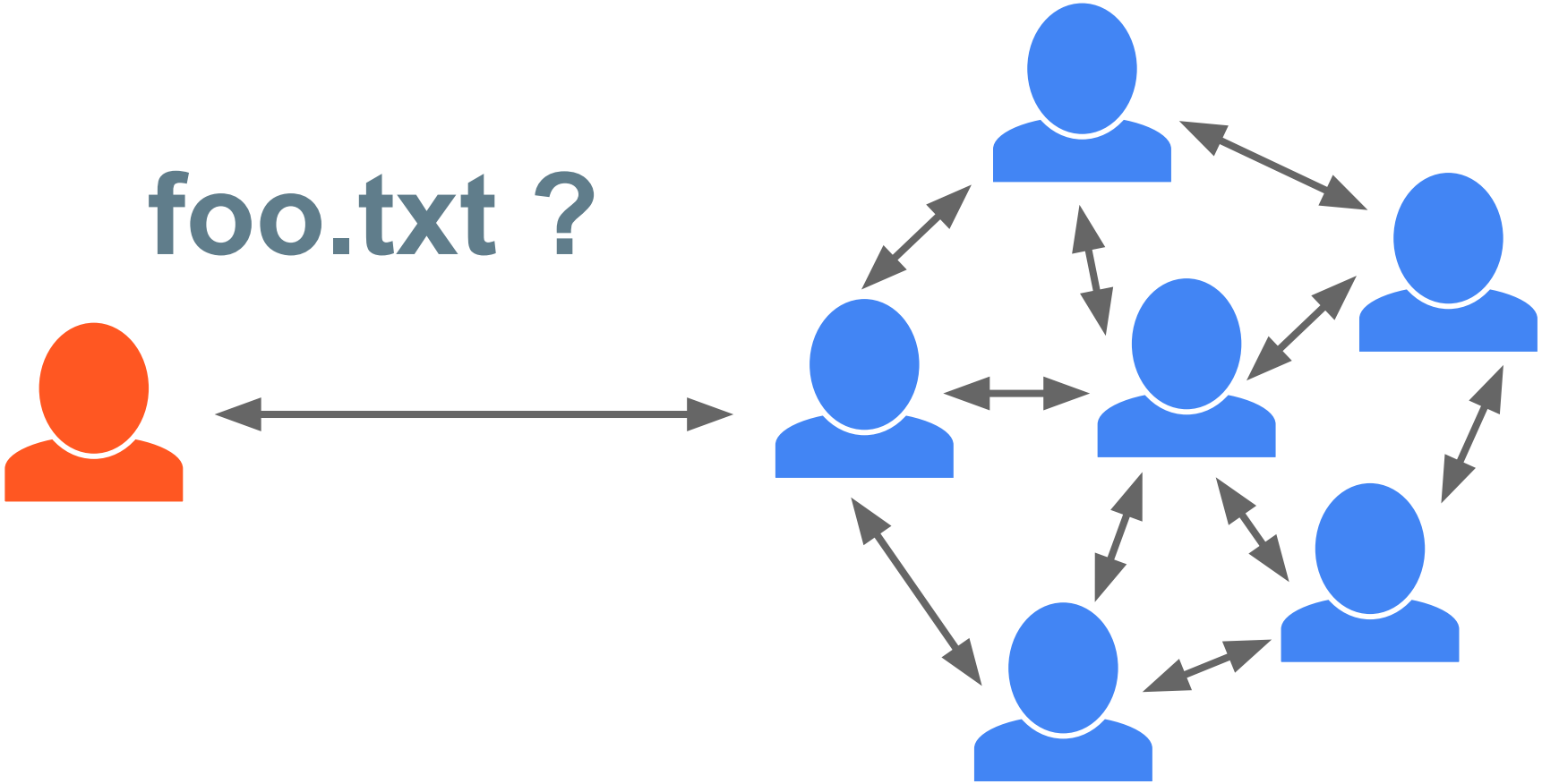
Démo

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
          99.242.230.163
          162.243.194.210
          173.69.49.106
          198.38.93.227
          209.208.110.92
```

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

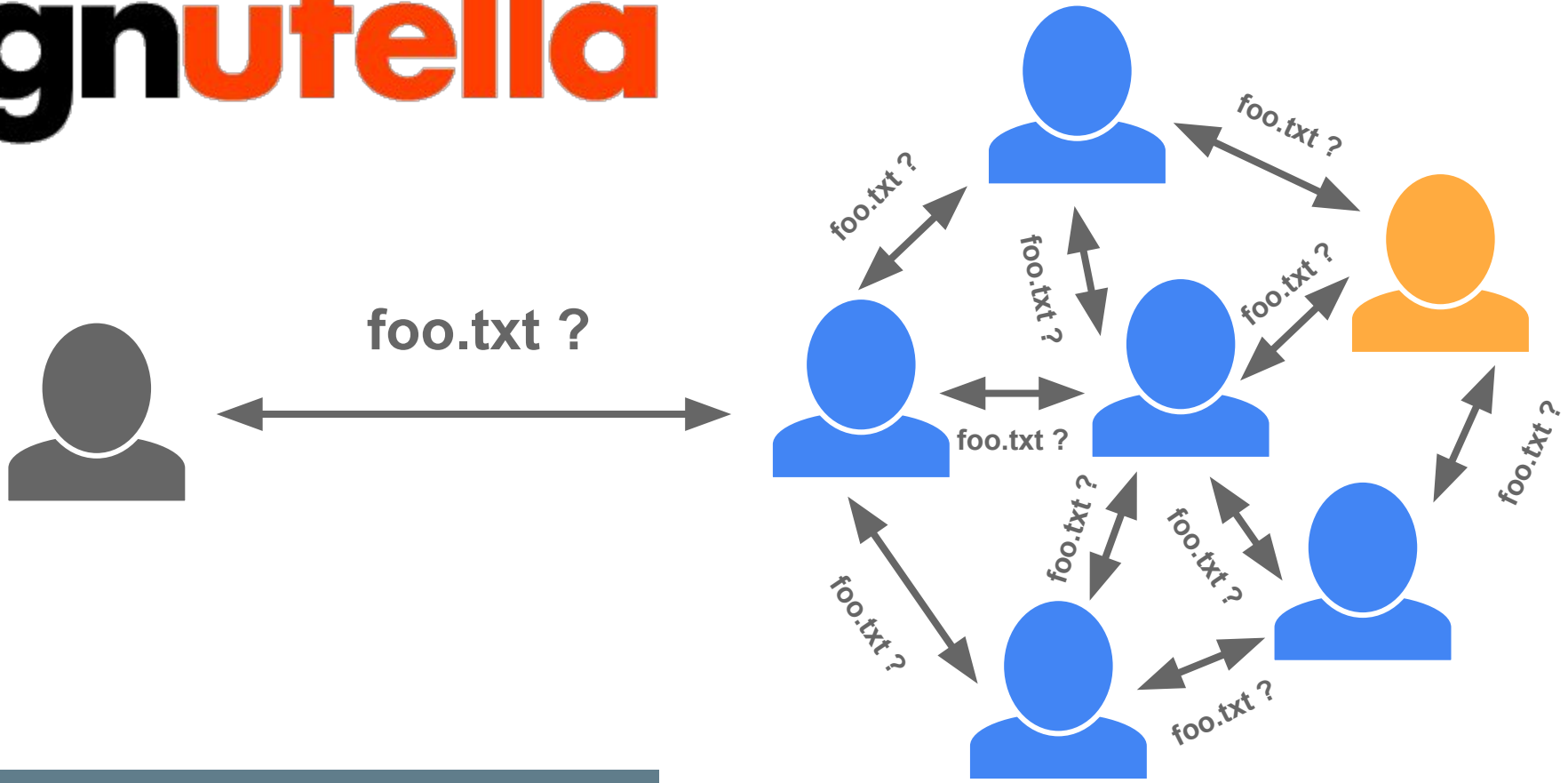

foo.txt ?

Ils sont où mes copains ?

Discovery

Retour dans les années 2000...

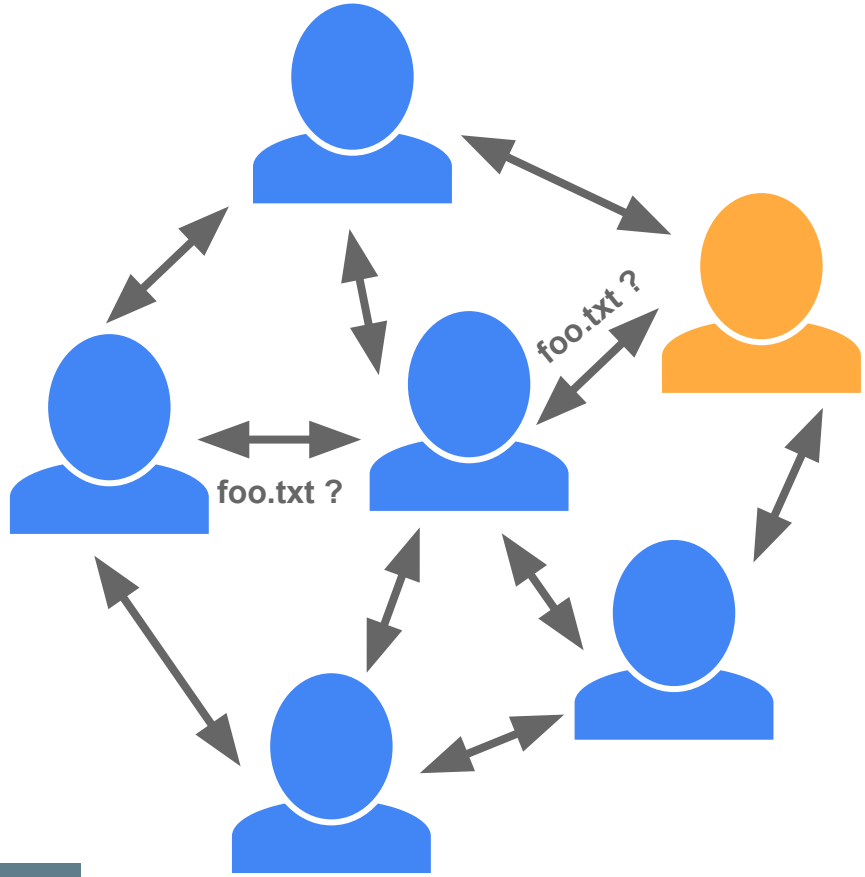
gnutella



Query Flooding

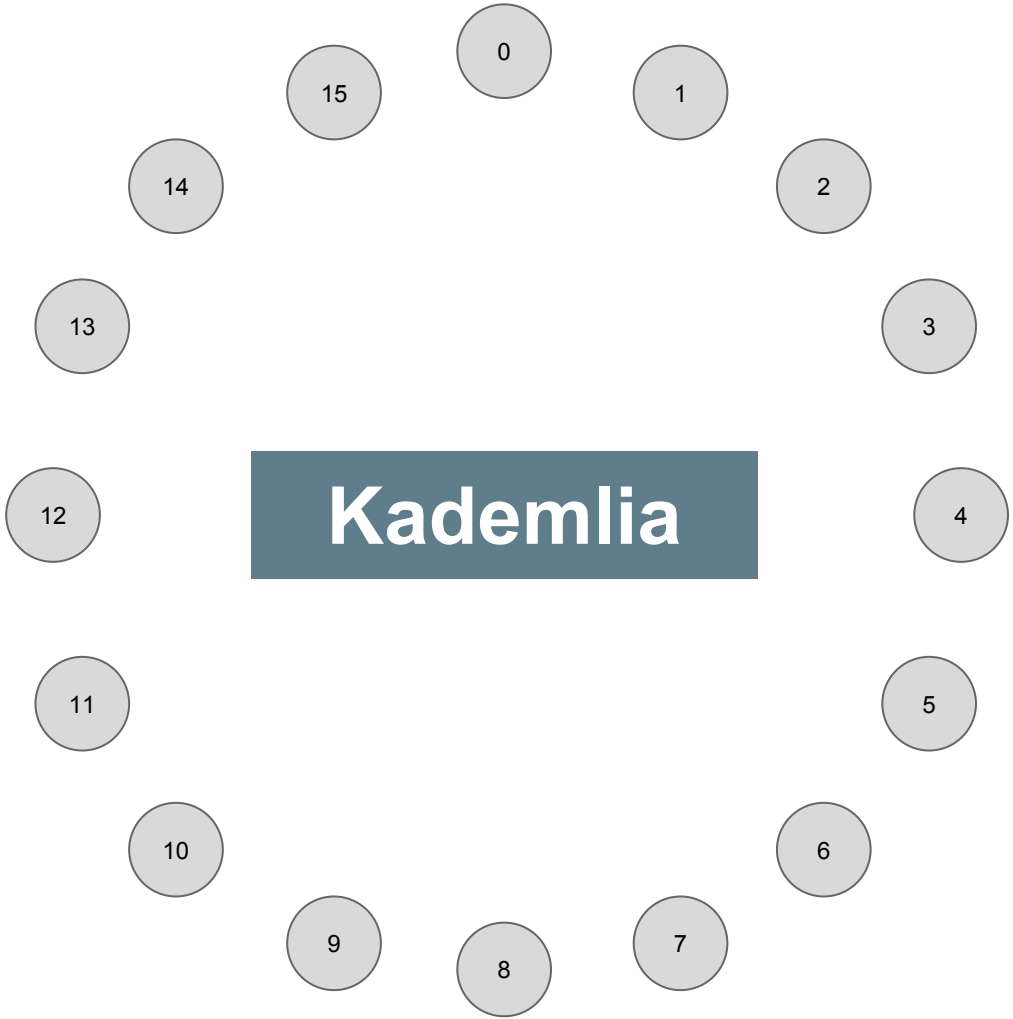
BitTorrent™

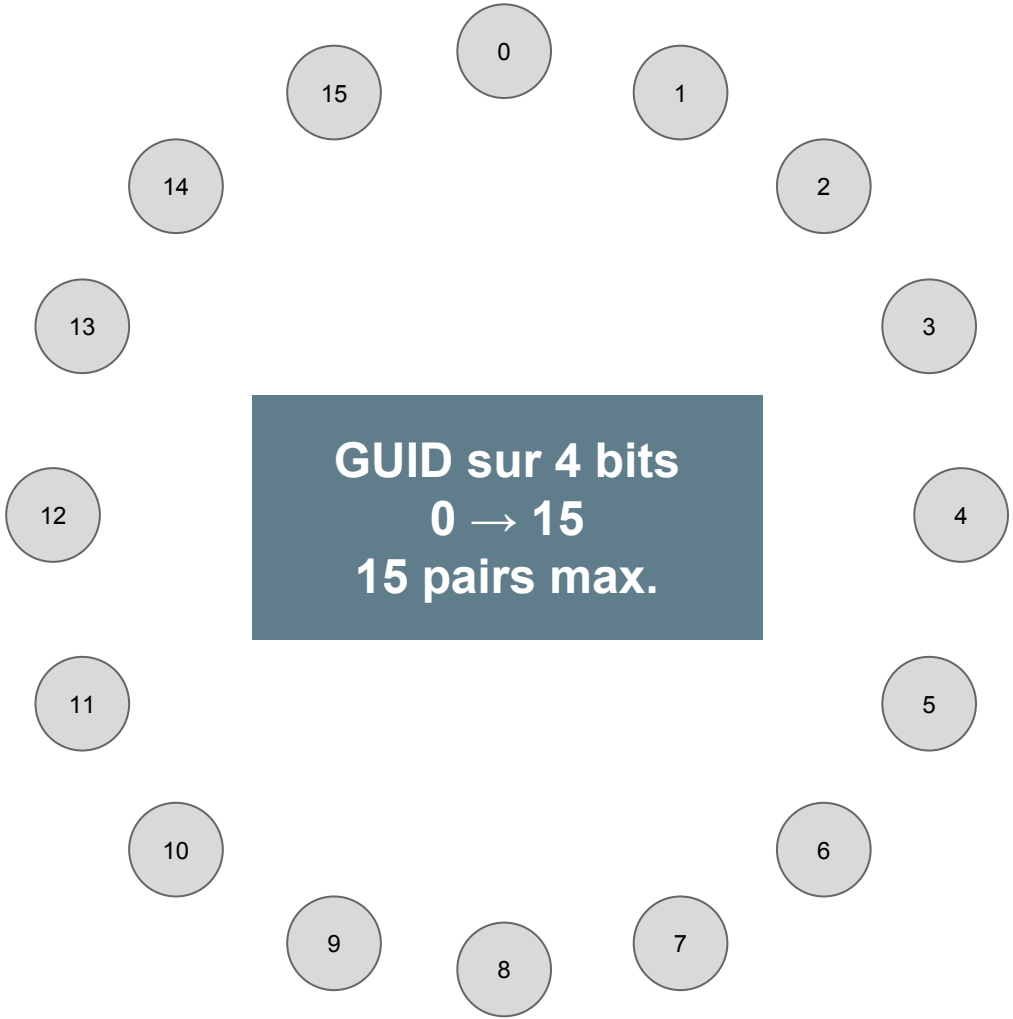
foo.txt ?

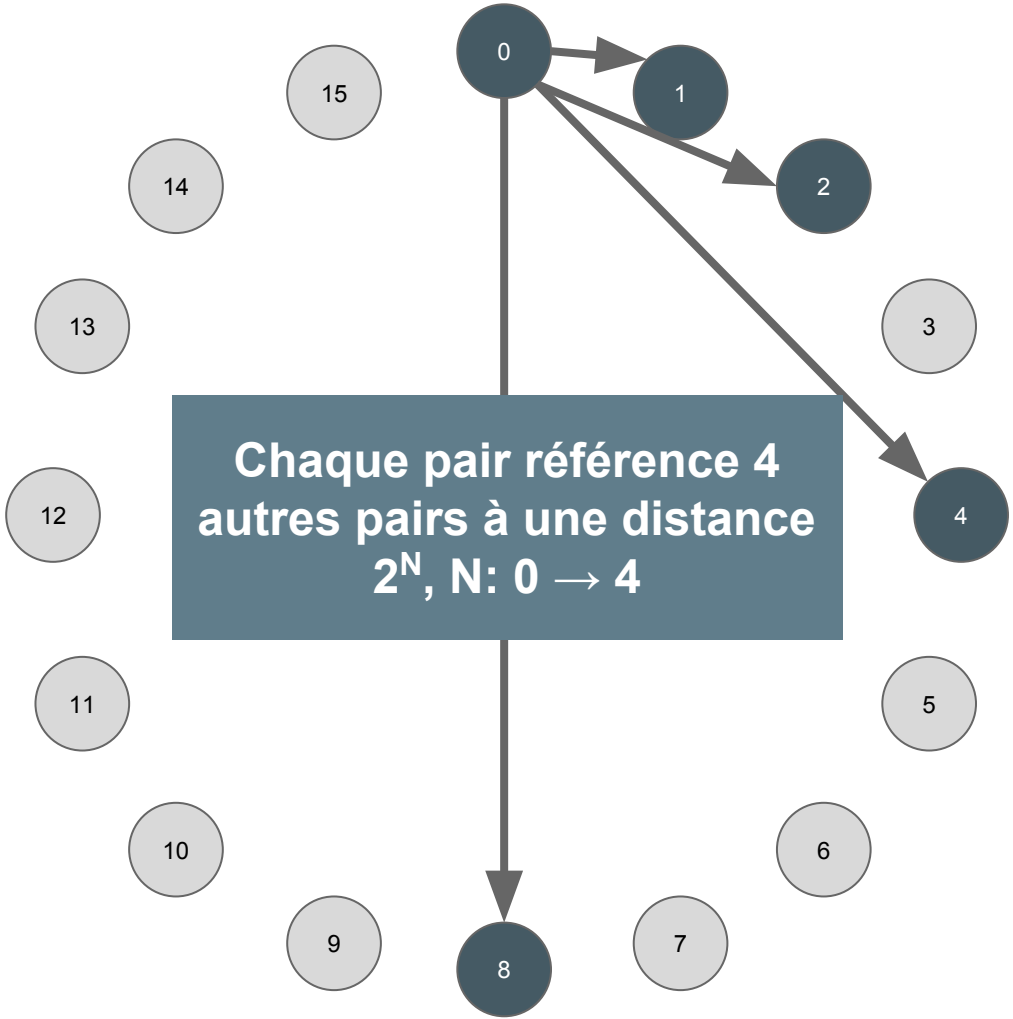


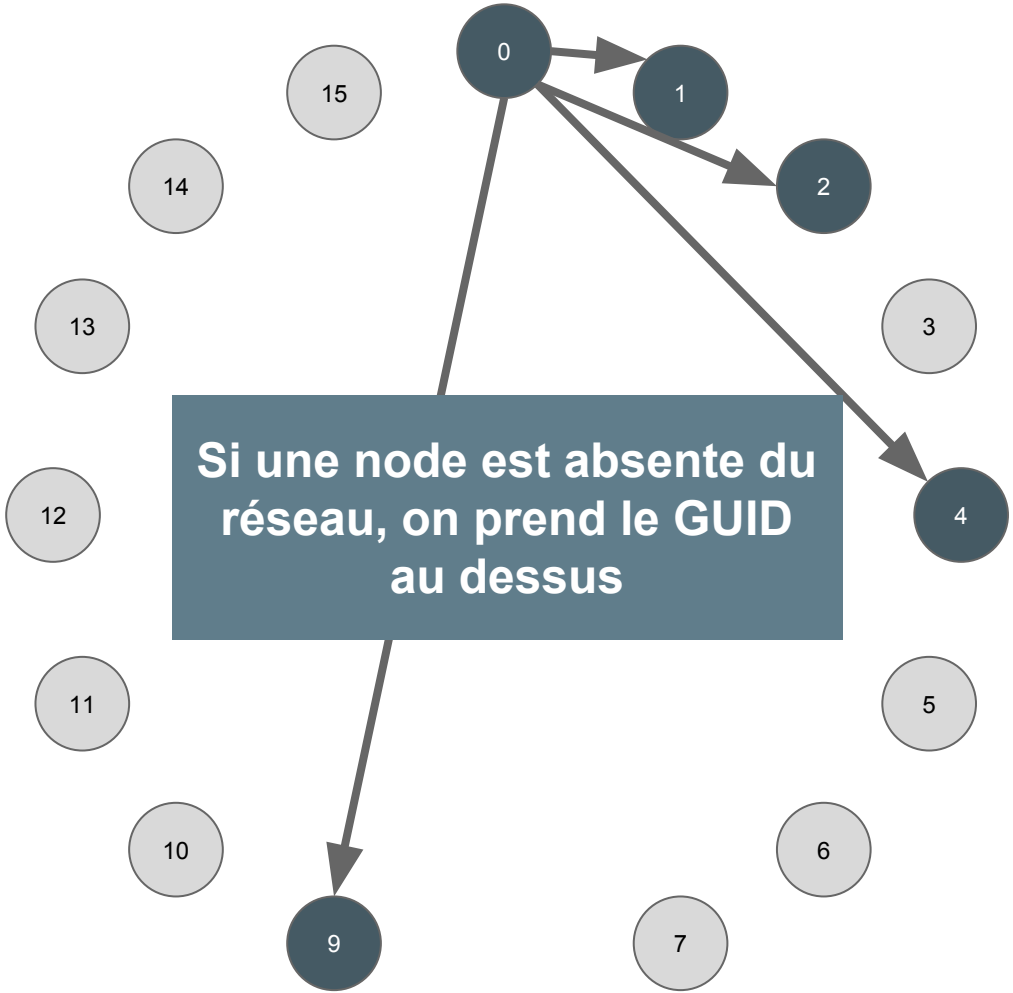
Distributed Hash Table

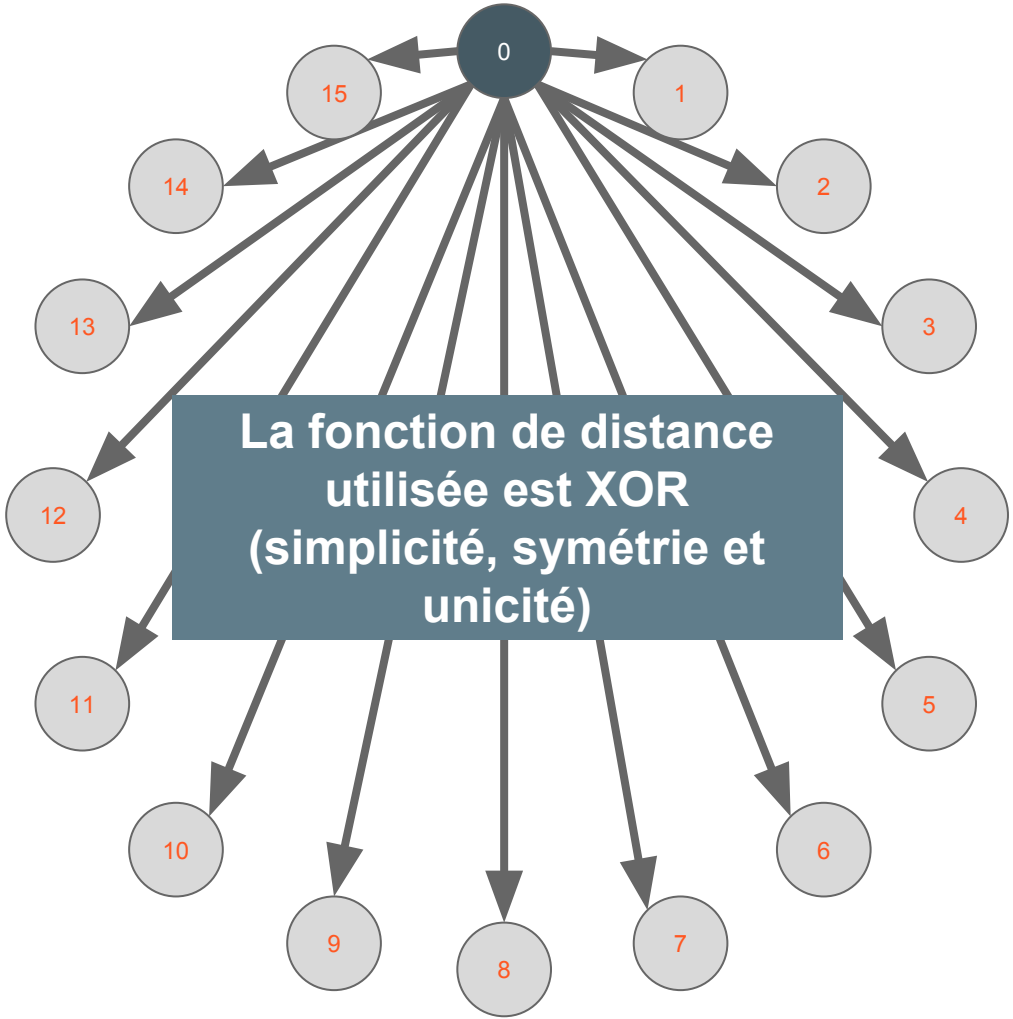
Distributed Hash Table
DHT ?

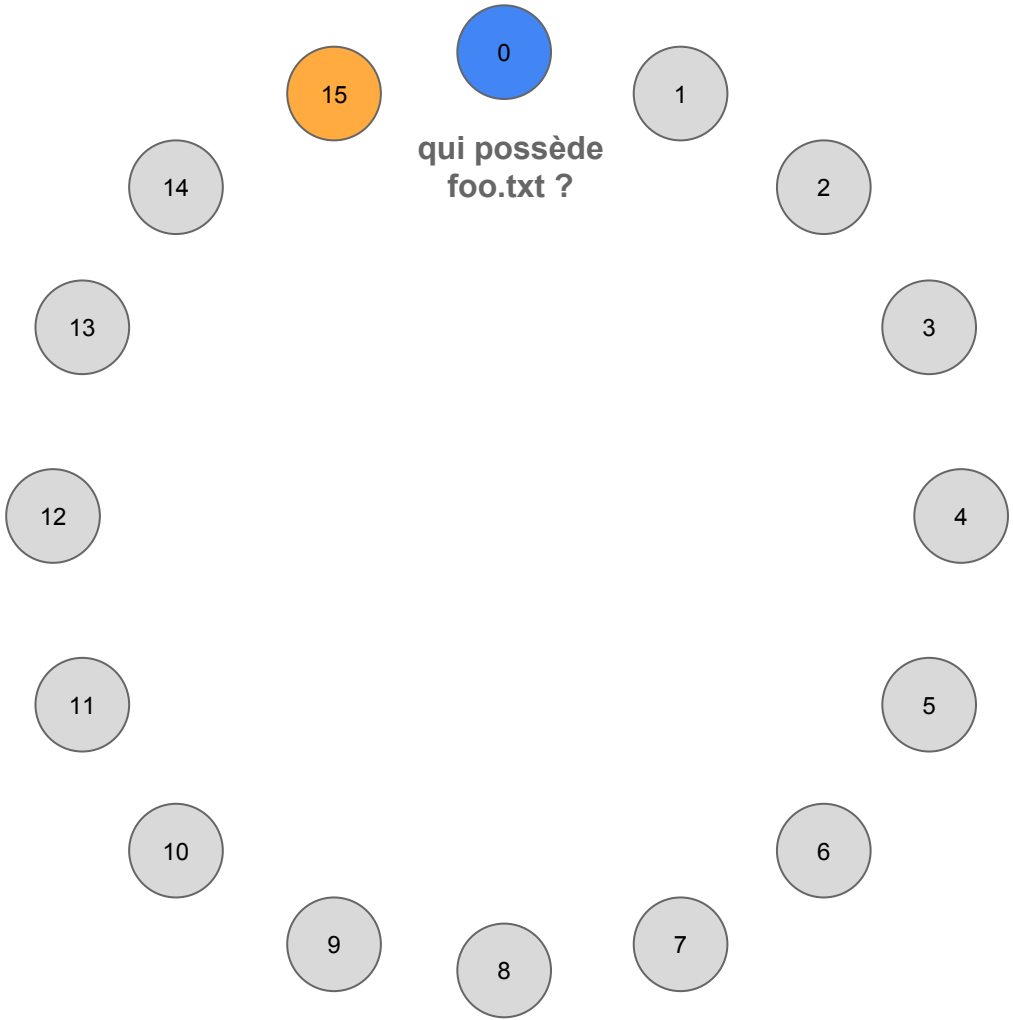

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Kademlia


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
GUID sur 4 bits
0 → 15
15 pairs max.

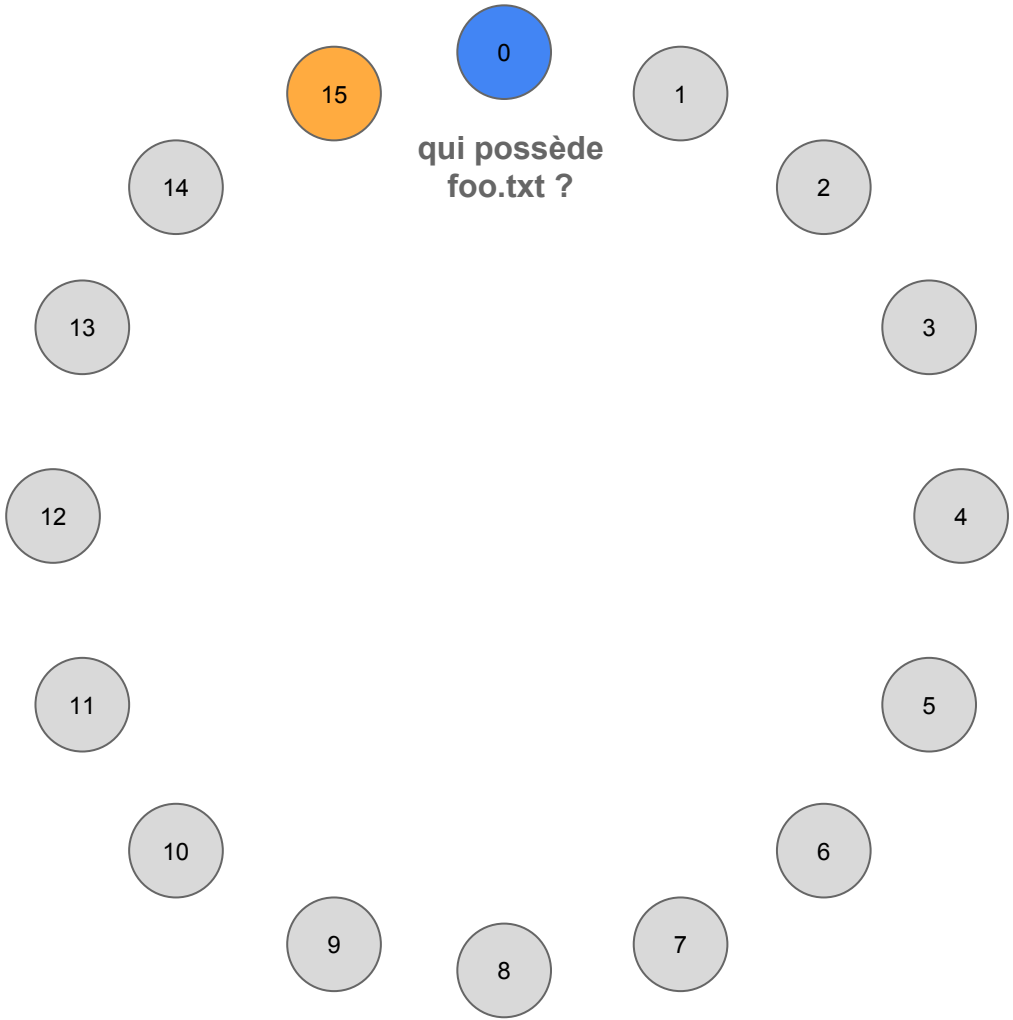

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Chaque pair référence 4 autres pairs à une distance 2^N, N: 0 → 4

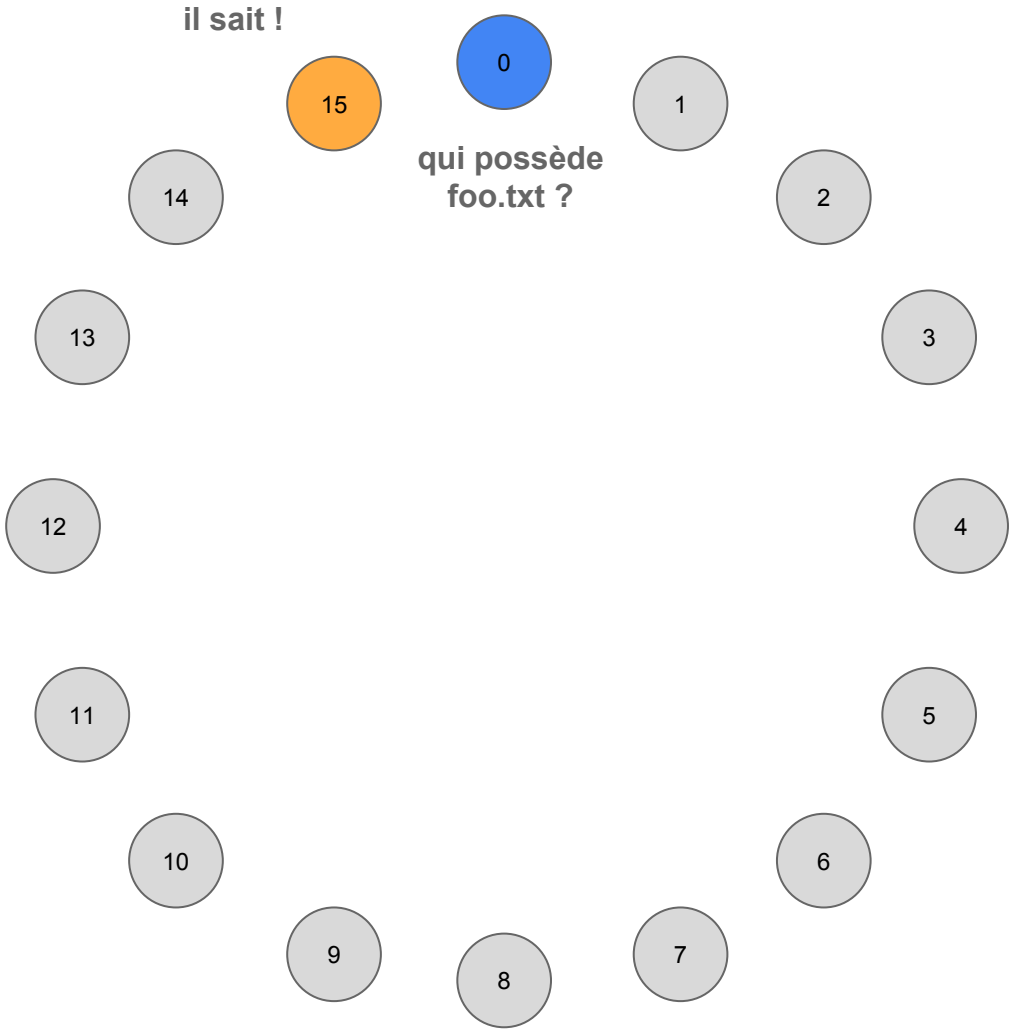

0
1
2
3
4
5
6
7
9
10
11
12
13
14
15
Si une node est absente du réseau, on prend le GUID au dessus


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
La fonction de distance utilisée est XOR (simplicité, symétrie et unicité)

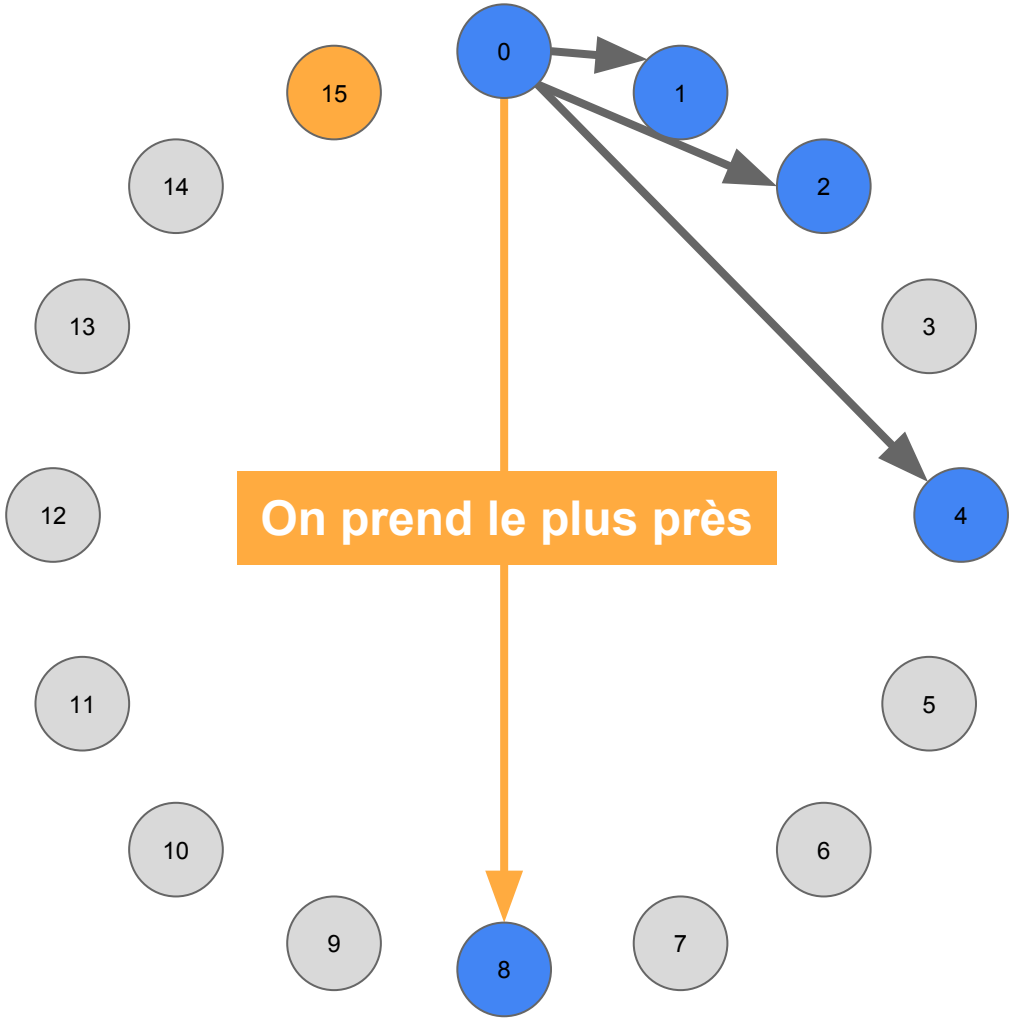

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
qui possède
foo.txt ?

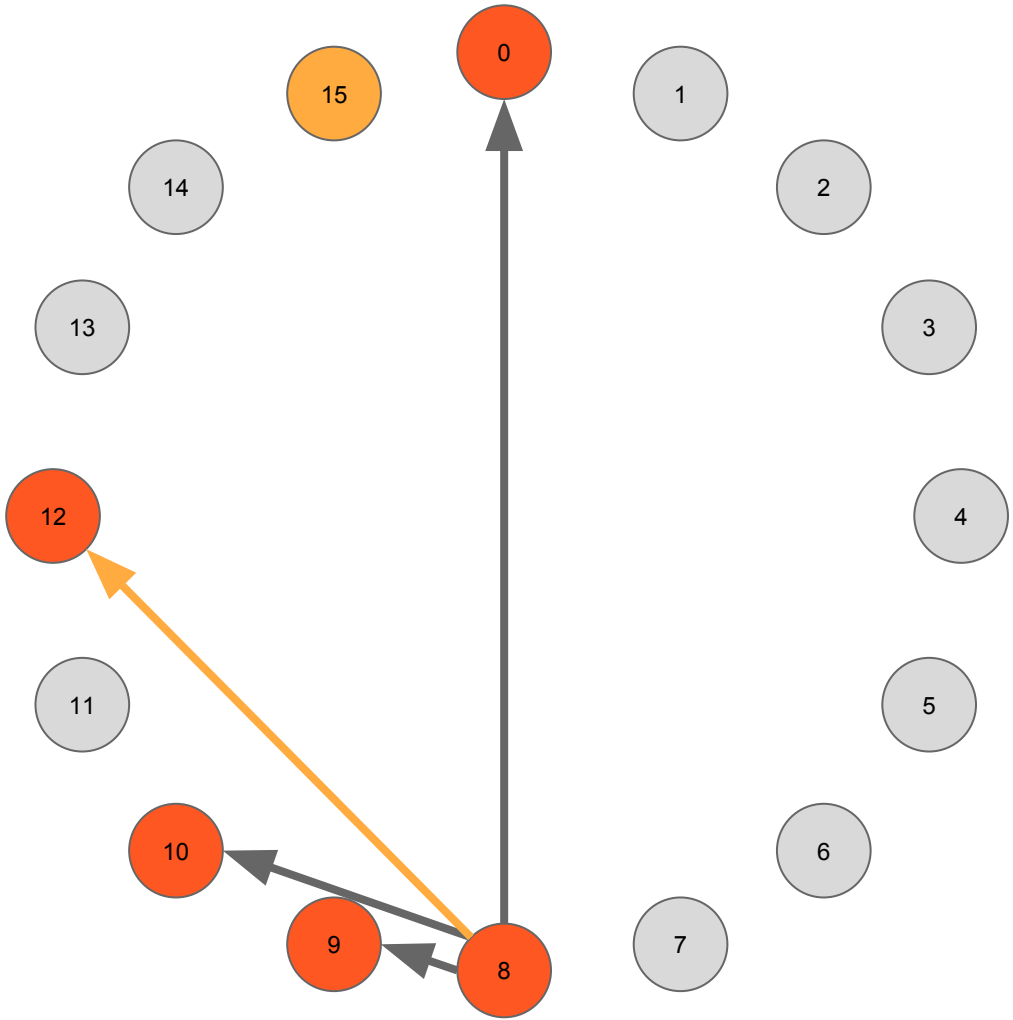
infohash(foo.txt) = 15

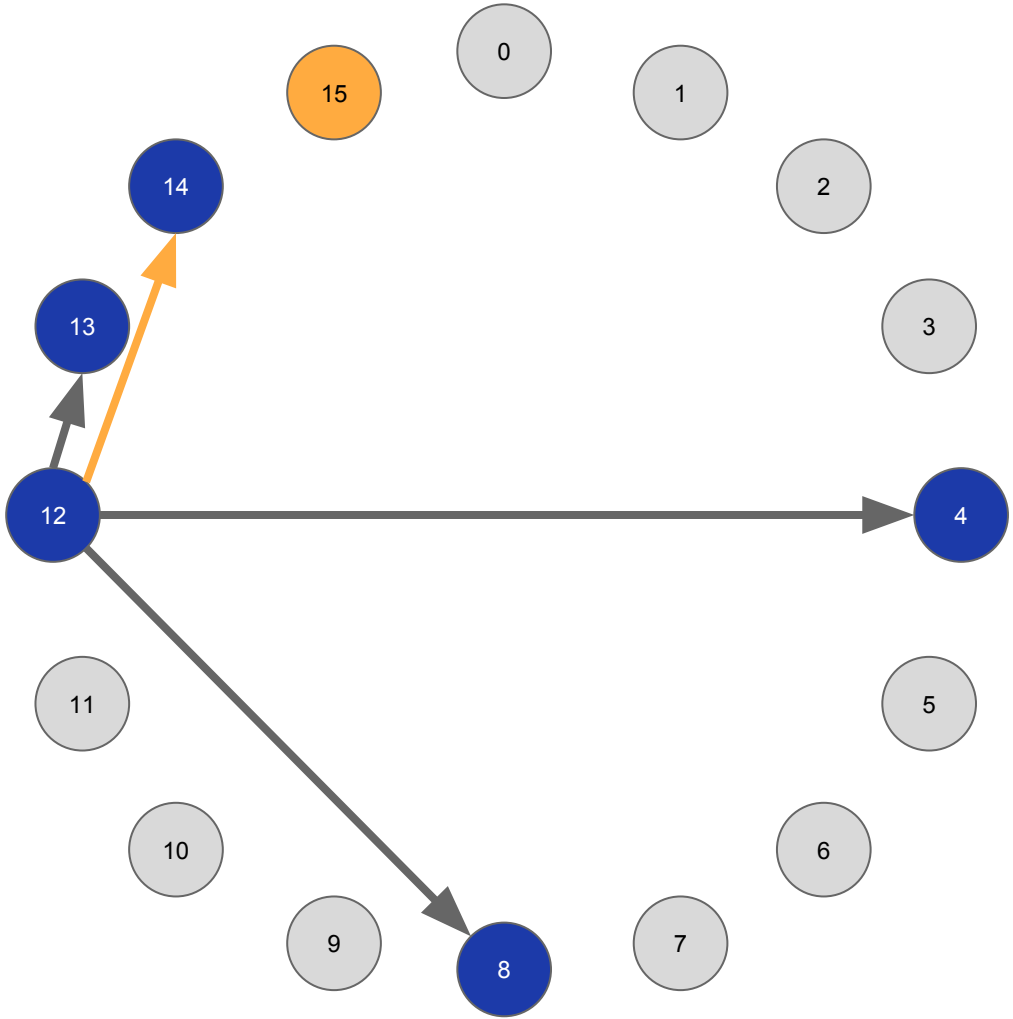


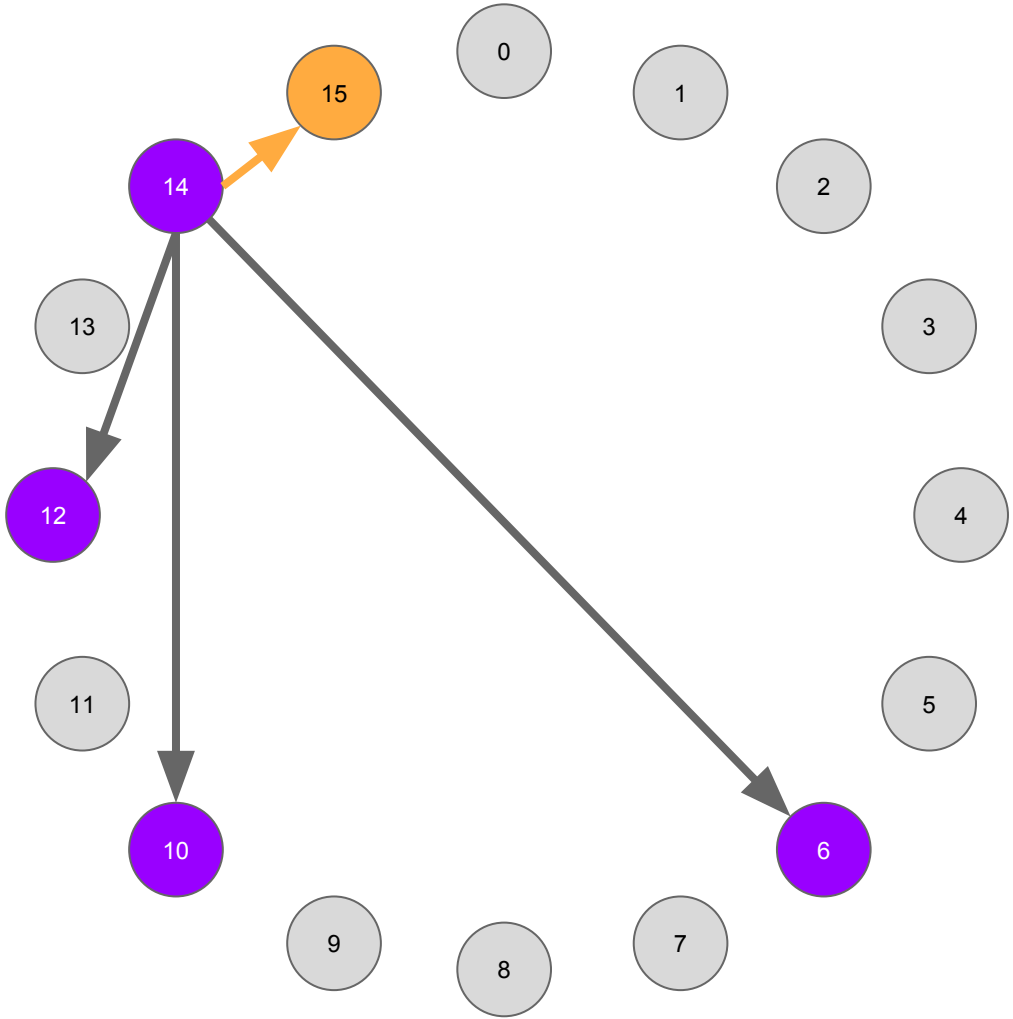


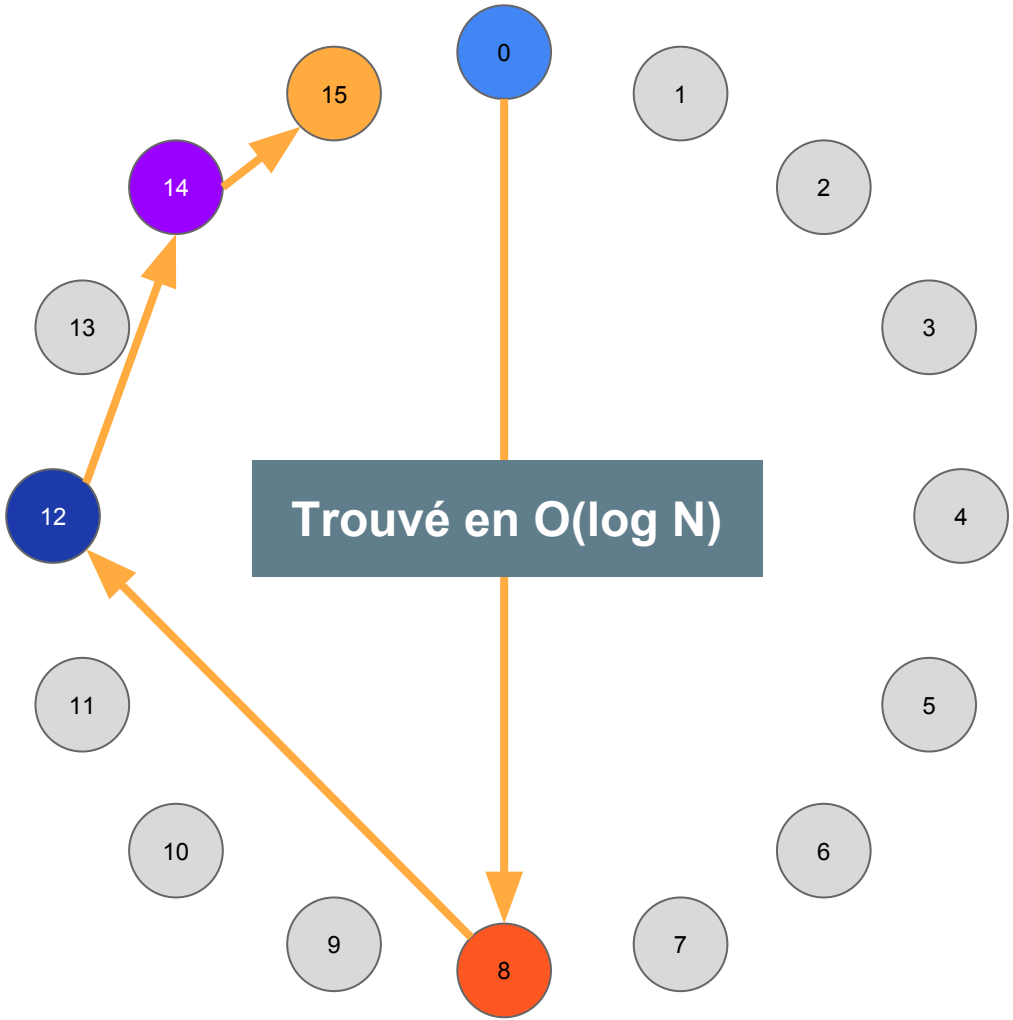
infohash(foo.txt) = 15


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
On prend le plus près


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15


0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Trouvé en O(log N)

Démo

Magnet link sur bittorent

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 CITÉ 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 CITÉ DE LA PEUR UNE COMÉDIE FAMILIALE
CHANTAL LAUBY • ALAIN CHABAT • DOMINIQUE FARRUGIA • GERARD DARMON • CAMI KARMANN
SCÉNARIO ORIGINAL CHANTAL LAUBY ALAIN CHABAT DOMINIQUE FARRUGIA • DIRECTEUR DE LA PHOTOGRAPHIE LAURENT DAILLAND
MUSIQUE PHILIPPE CHANY • MONTAGE VÉRONIQUE PARNET
PRODUCTEUR DÉLÉGUÉ CHARLES GASSOT • PRODUCTEUR EXÉCUTIF DOMINIQUE BRUNNER
UNE PRODUCTION TELEMA LE STUDIO CANAL+ FRANCE 3 CINEMA M6 FILMS

Details for this torrent

La citÃ© de la Peur by LADB

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

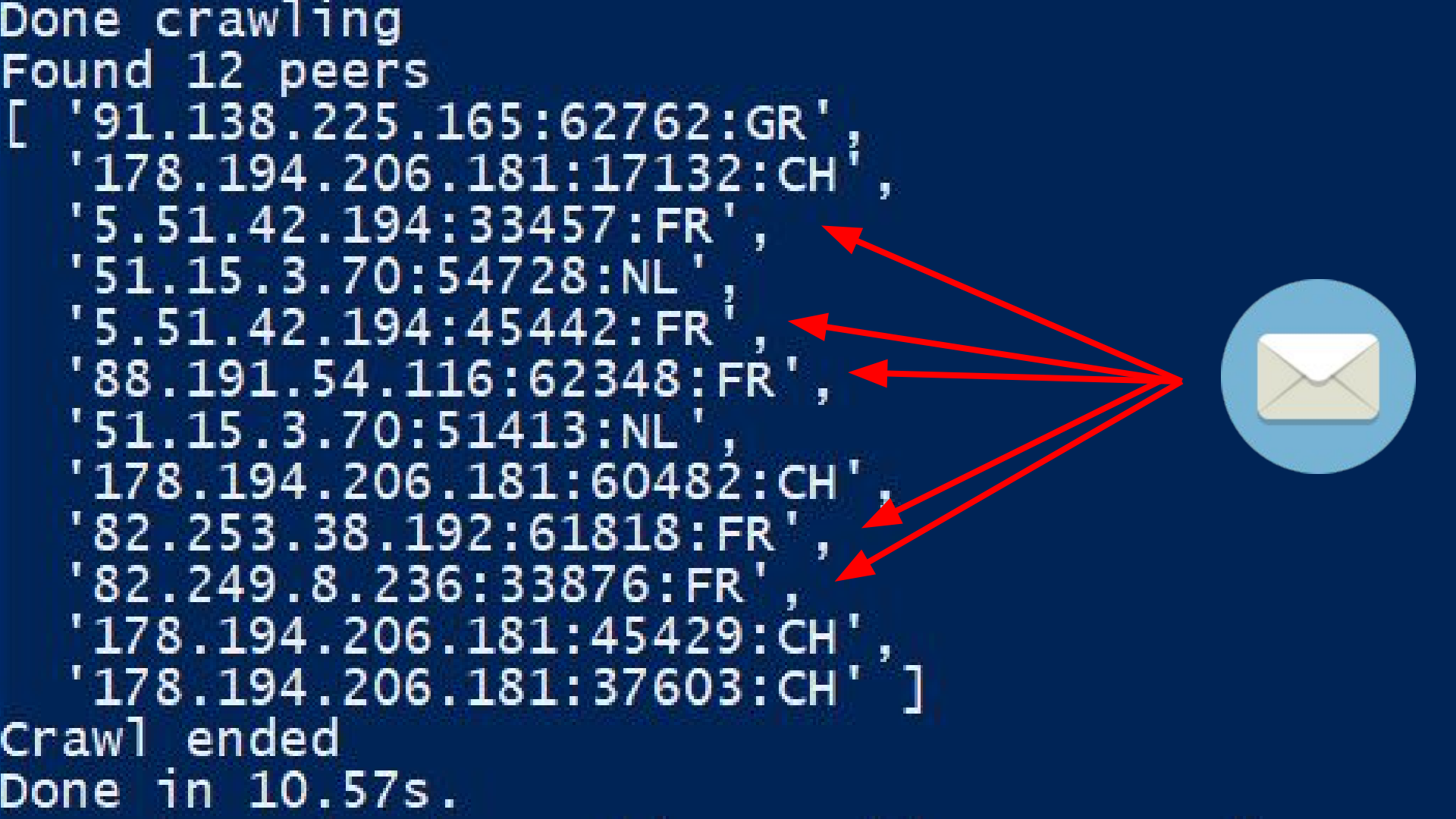
```
var _ = require('lodash')
var DHT = require('bittorrent-dht')
var geoip = require('geoip-lite-country')

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)
```

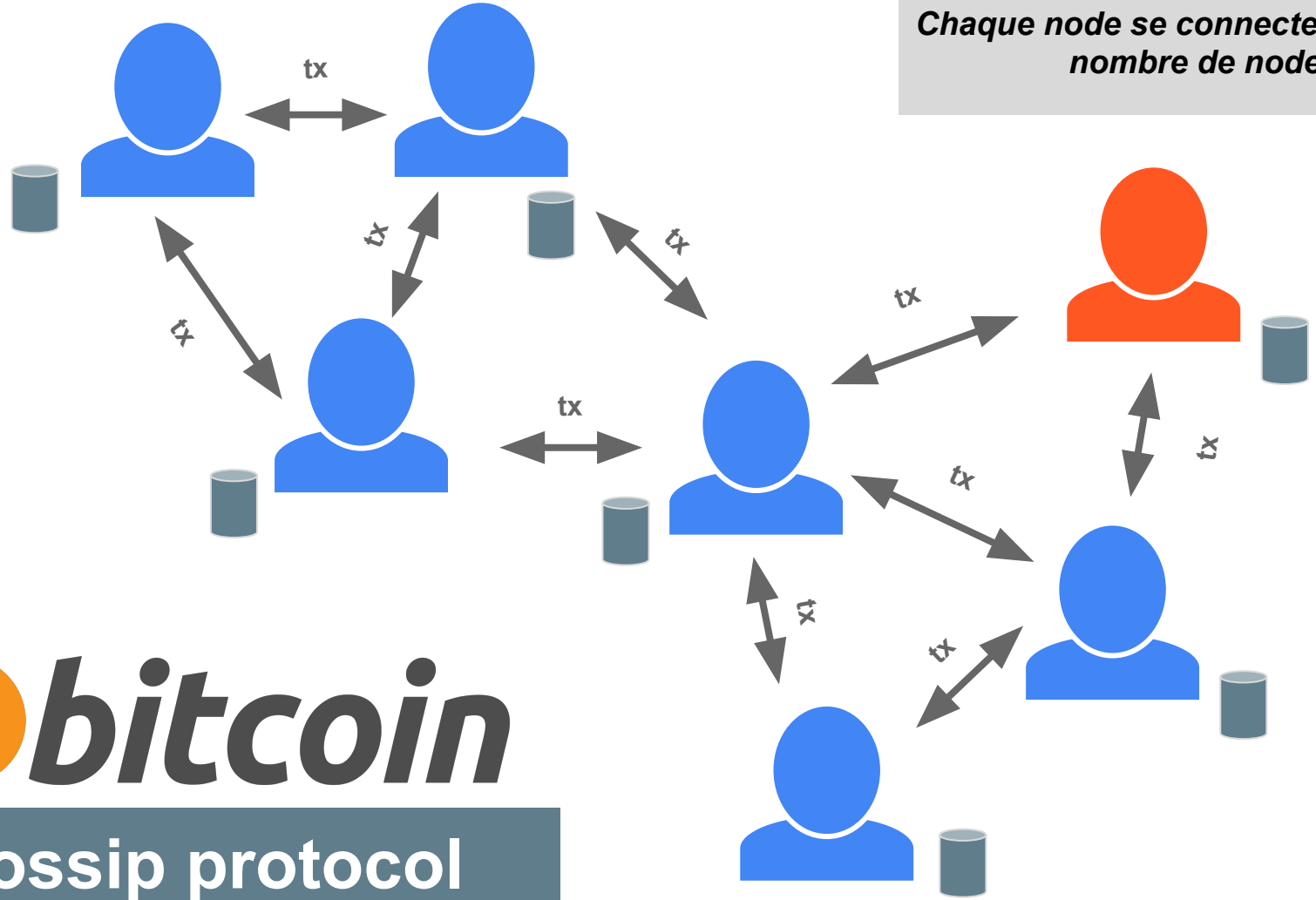
dht.lookup(infoHash)

```
Done crawling
Found 12 peers
[ '91.138.225.165:62762:GR',
  '178.194.206.181:17132:CH',
  '5.51.42.194:33457:FR',
  '51.15.3.70:54728:NL',
  '5.51.42.194:45442:FR',
  '88.191.54.116:62348:FR',
  '51.15.3.70:51413:NL',
  '178.194.206.181:60482:CH',
  '82.253.38.192:61818:FR',
  '82.249.8.236:33876:FR',
  '178.194.206.181:45429:CH',
  '178.194.206.181:37603:CH' ]
Crawl ended
Done in 10.57s.
```



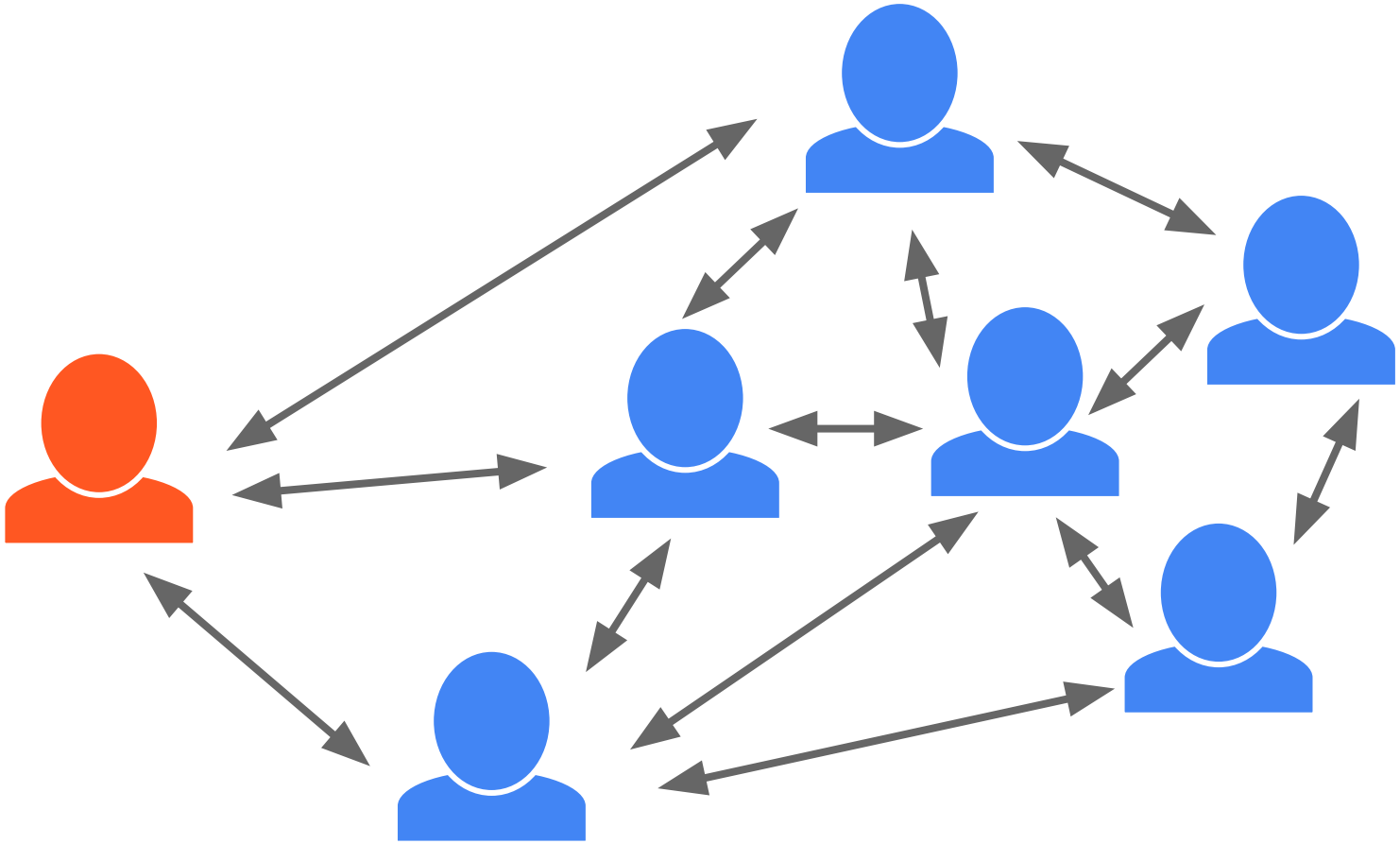
Et la blockchain dans tout ca ?

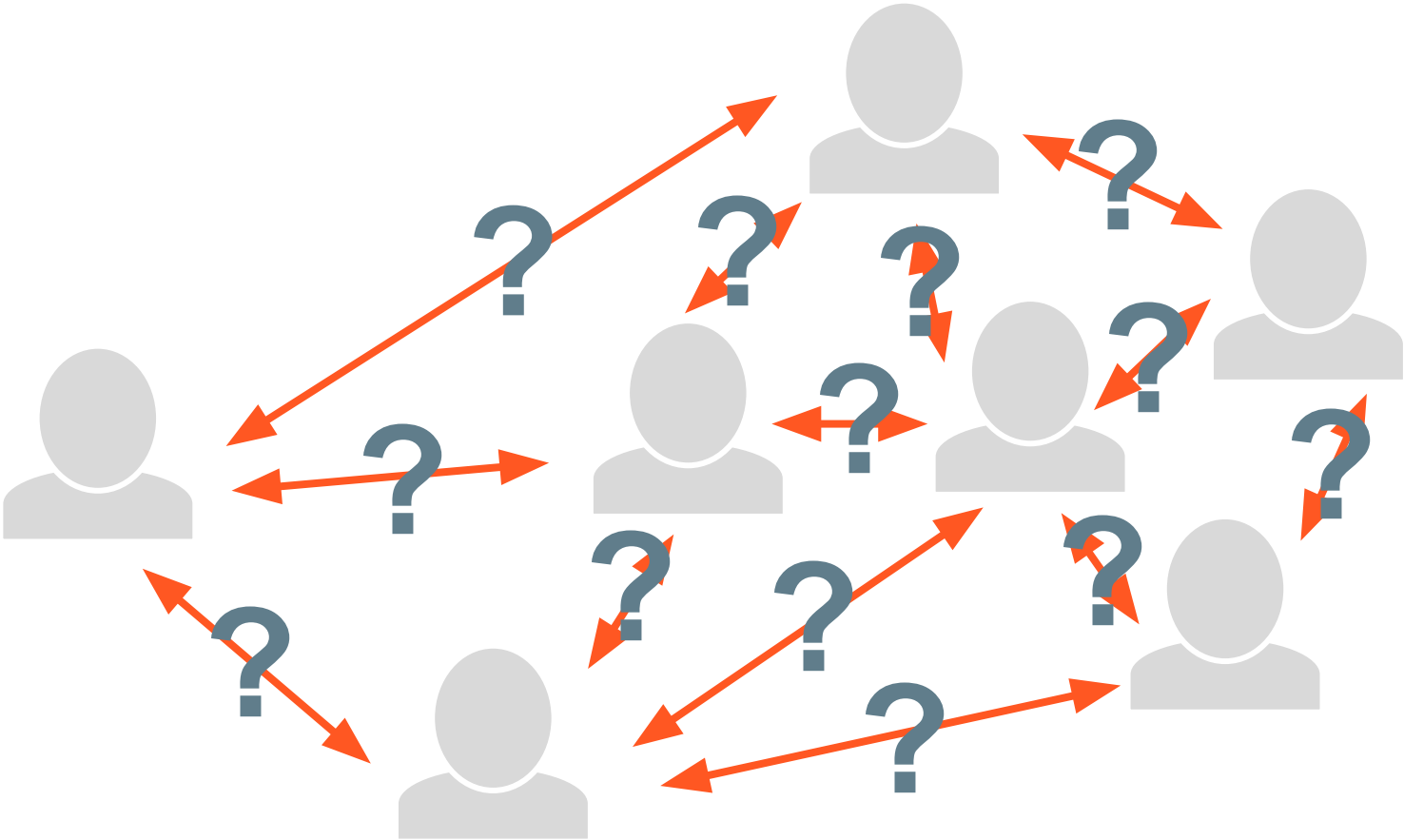
Chaque node se connecte à un grand nombre de nodes



bitcoin

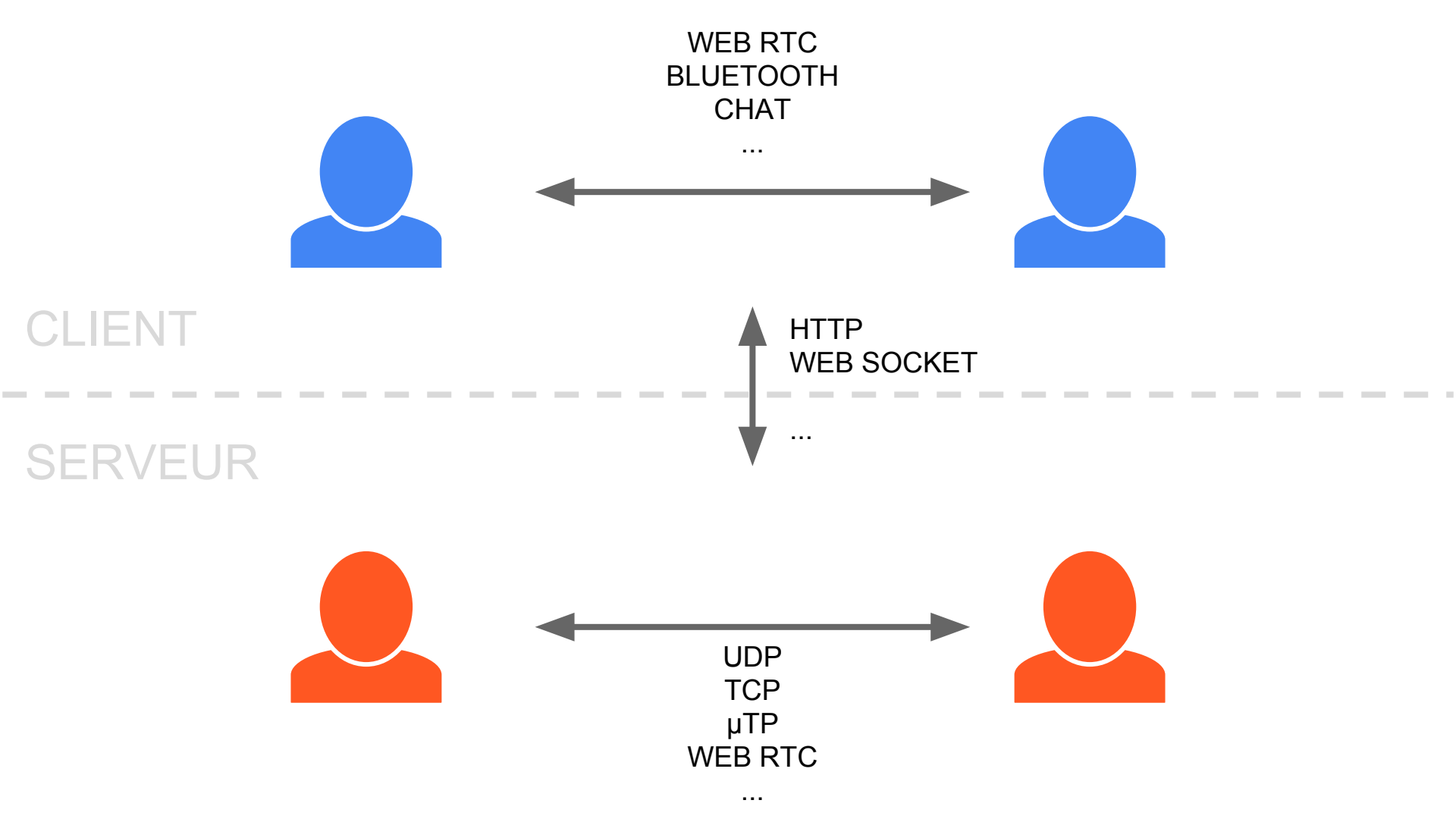
Gossip protocol

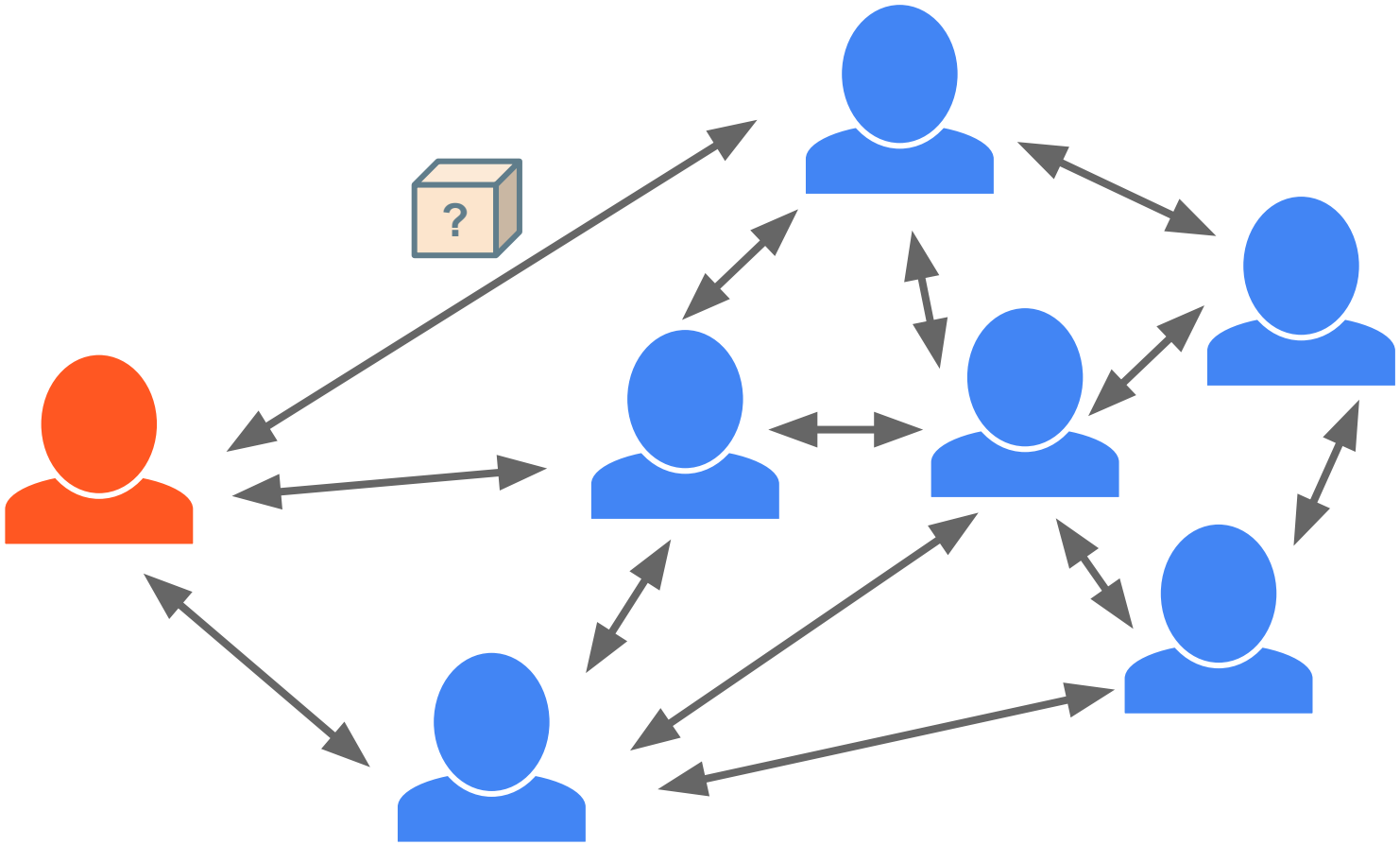


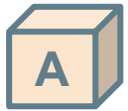


email ? Téléphone ? Courrier ? Pigeon ?

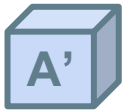
Transport


WEB RTC
BLUETOOTH
CHAT
...
CLIENT
HTTP
WEB SOCKET
...
SERVEUR
UDP
TCP
µTP
WEB RTC
...





diff ?

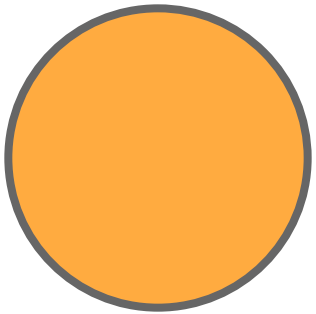


C'est la bonne donnée ?

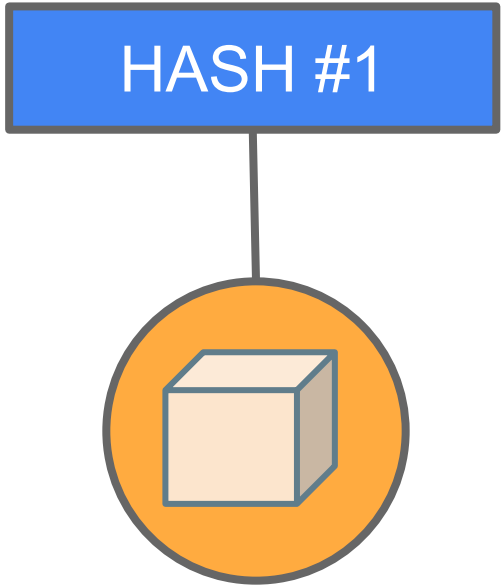
Content addressed data

Merkle “Tree”
Merkle Directed Acyclic Graph

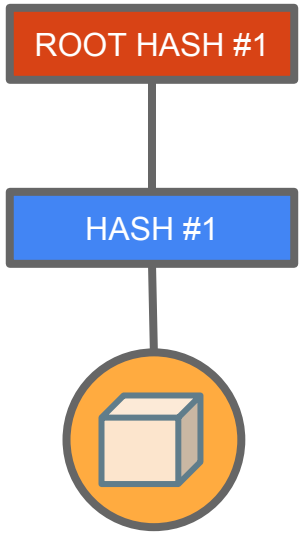
Merkle “Tree”
Merkle Directed Acyclic Graph



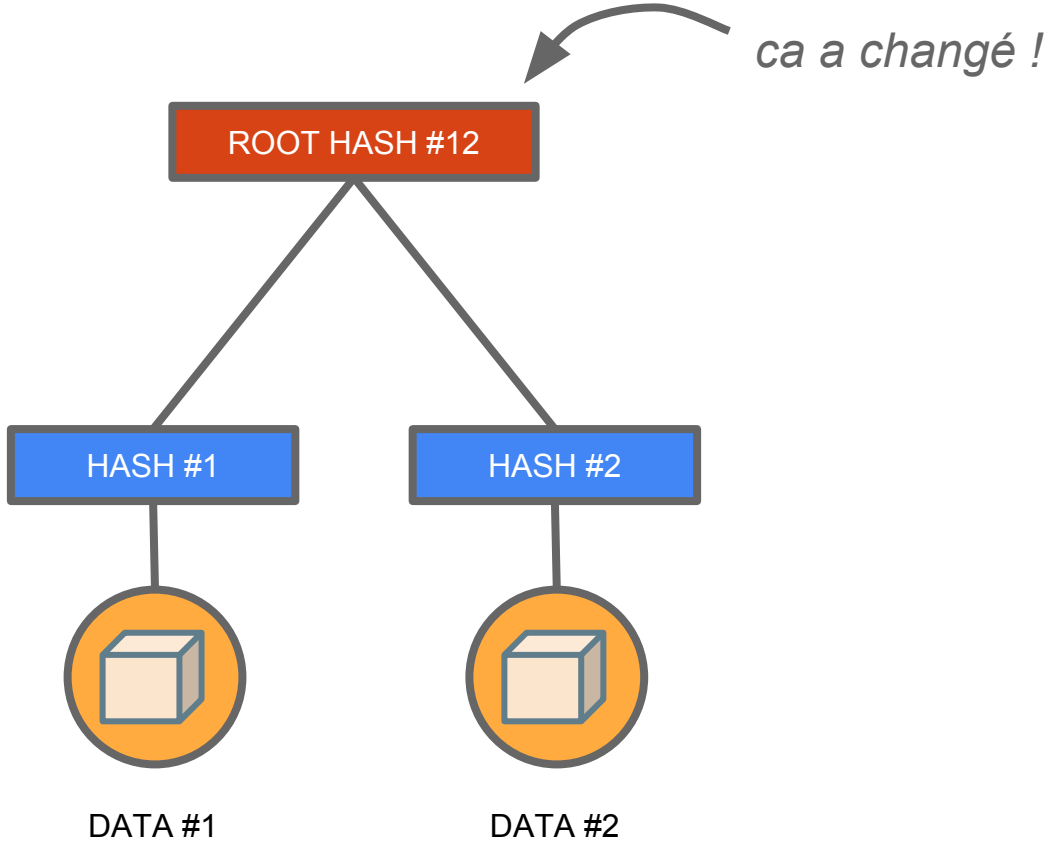
DATA #1

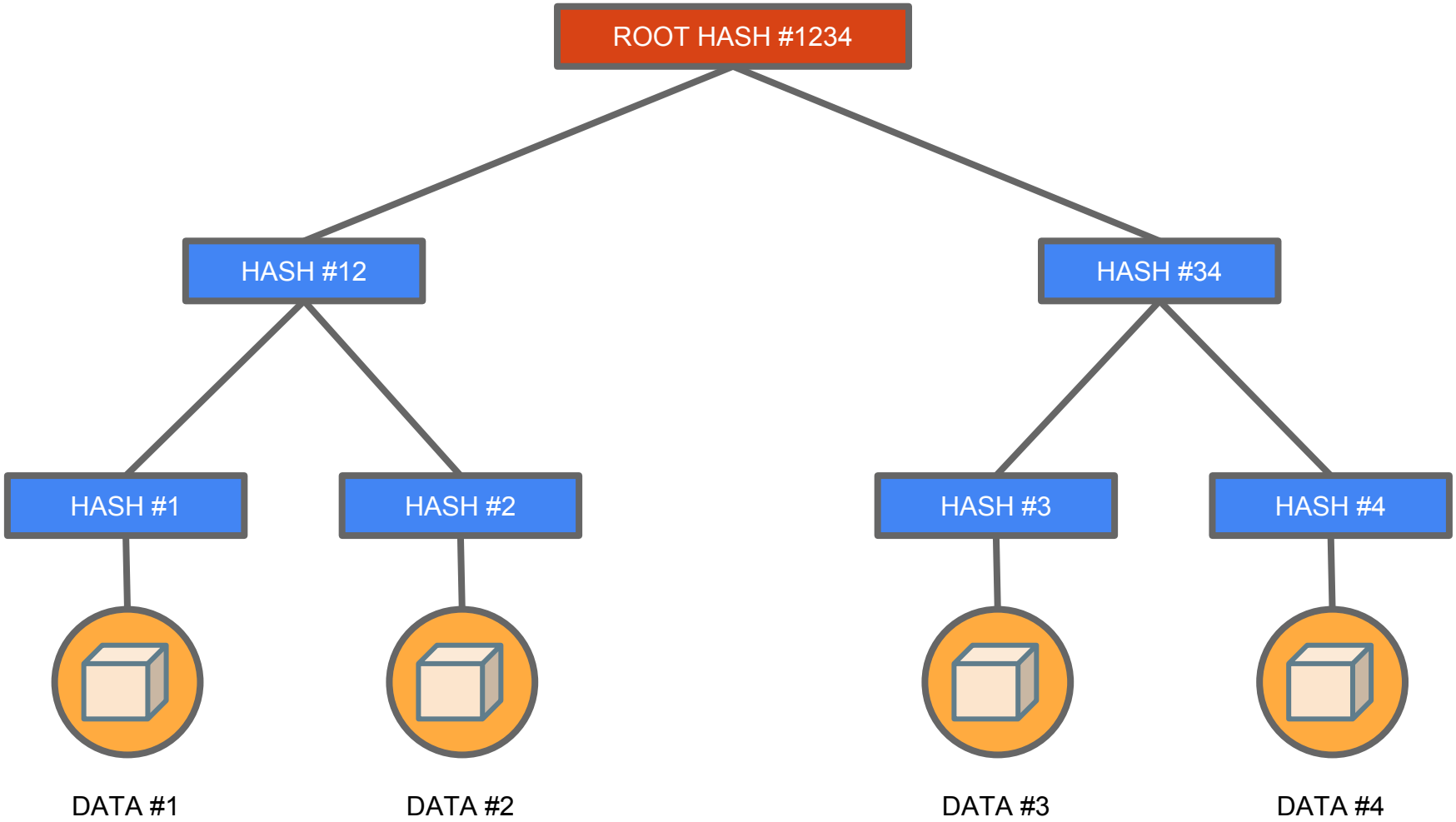


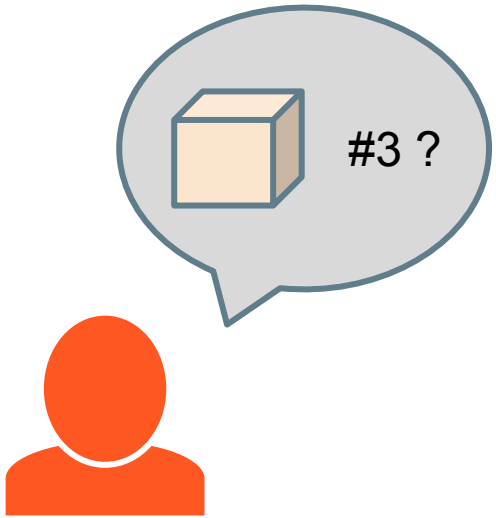
DATA #1



DATA #1


ca a changé !
ROOT HASH #12
HASH #1
HASH #2
DATA #1
DATA #2


ROOT HASH #1234
HASH #12
HASH #34
HASH #1
HASH #2
HASH #3
HASH #4
DATA #1
DATA #2
DATA #3
DATA #4


#3 ?

je connais le root hash de source sûre

ROOT HASH #1234

HASH #12

HASH #34

HASH #1

HASH #2

HASH #3

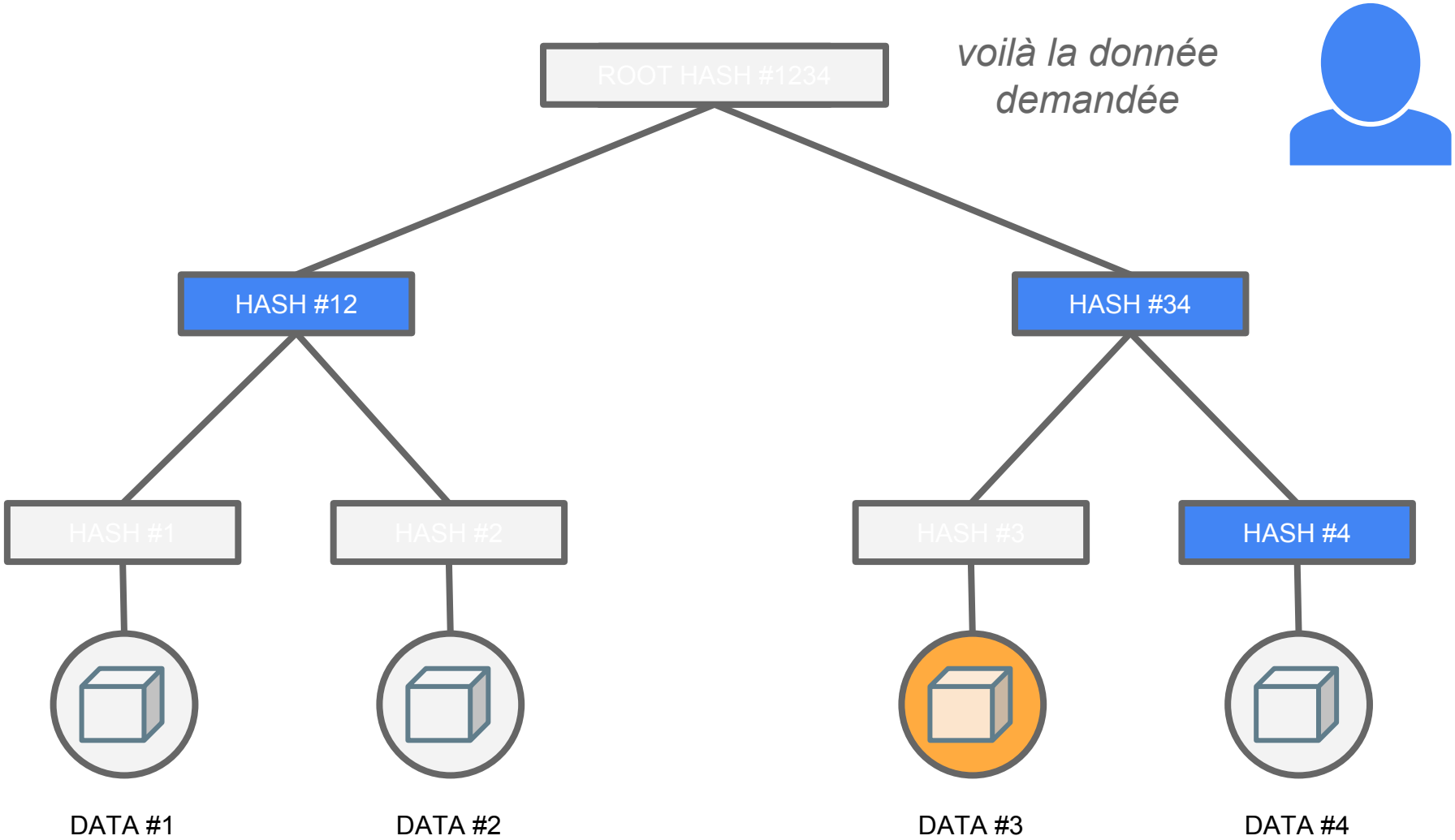
HASH #4

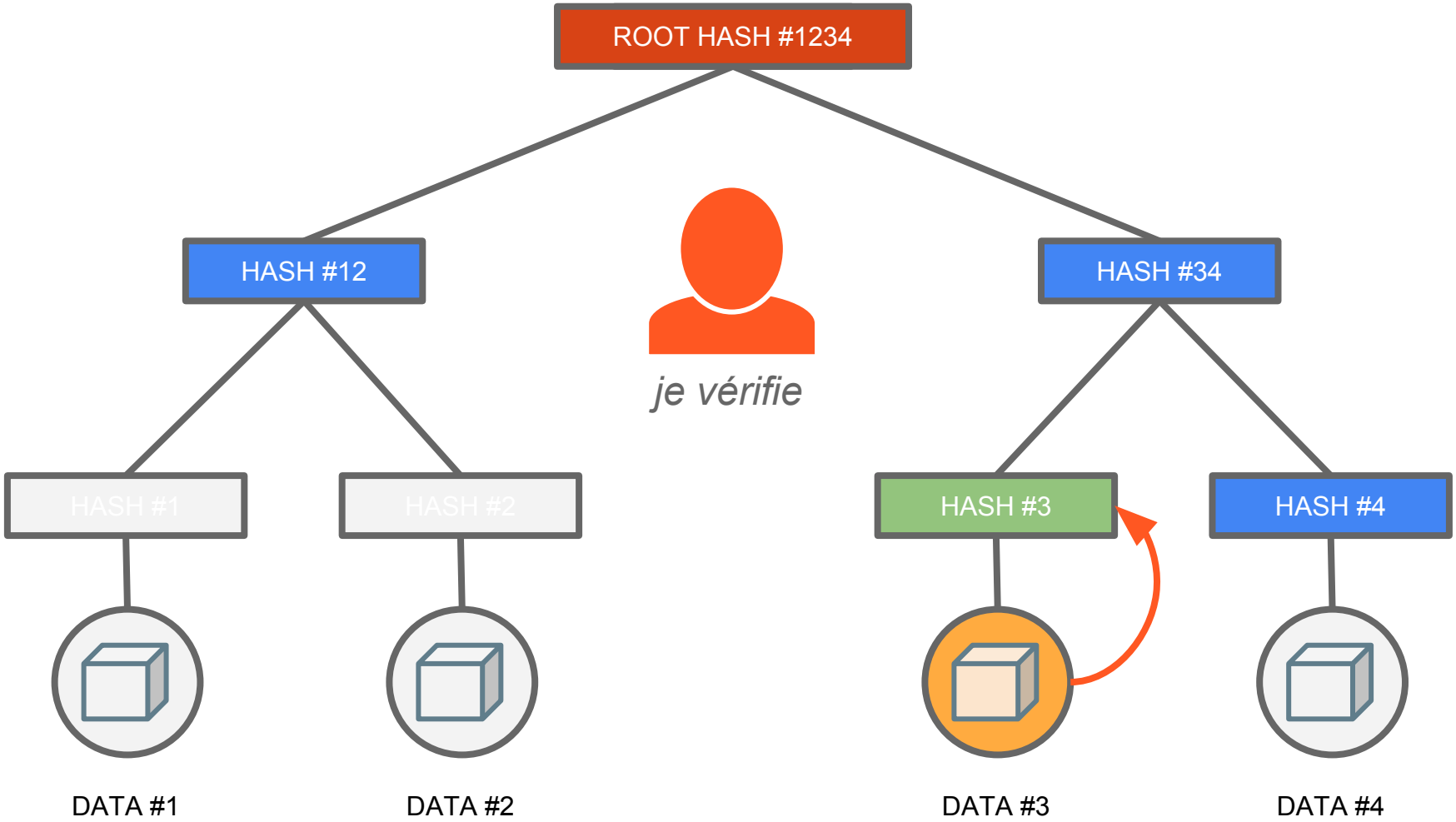
DATA #1

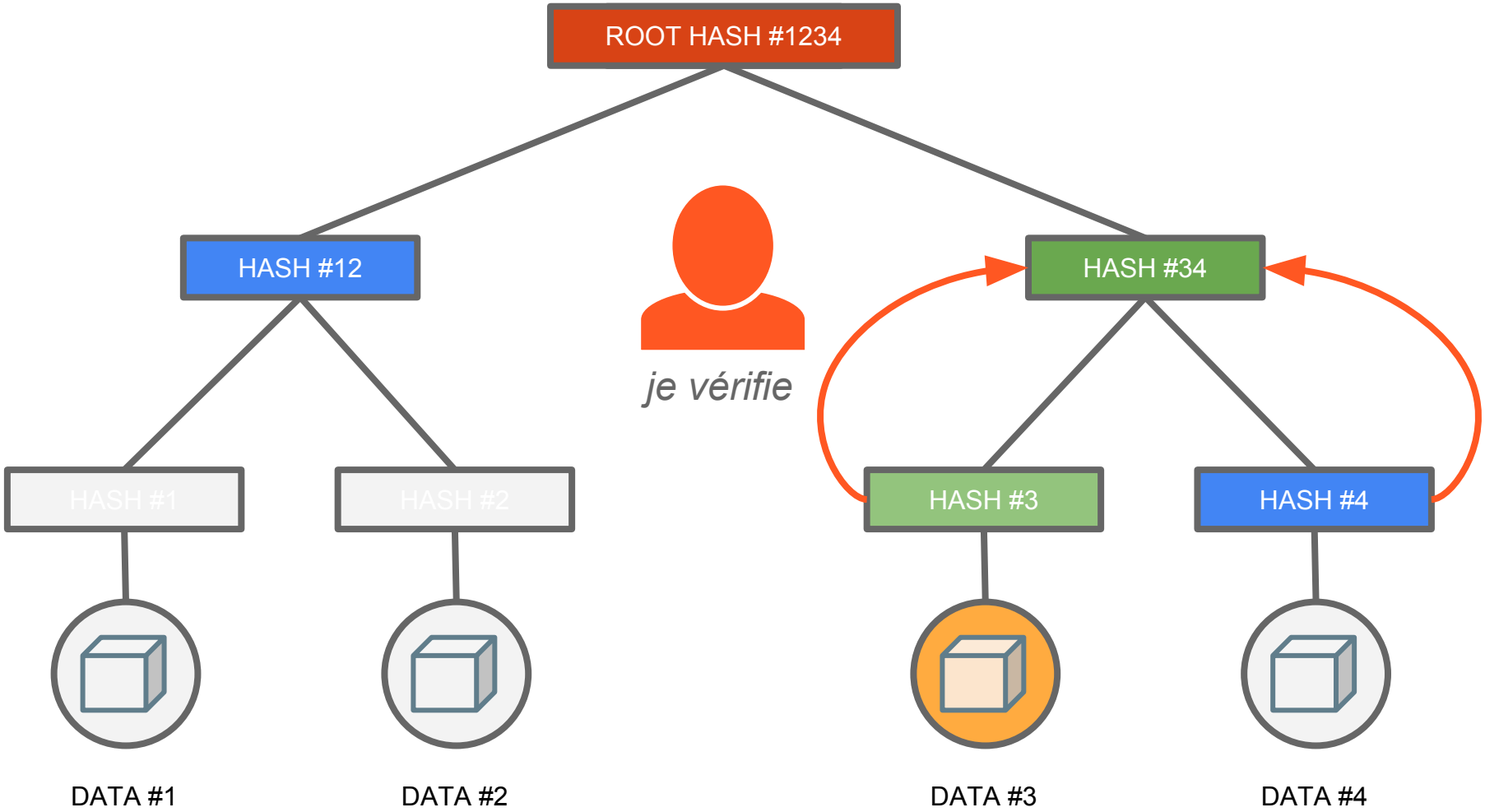
DATA #2

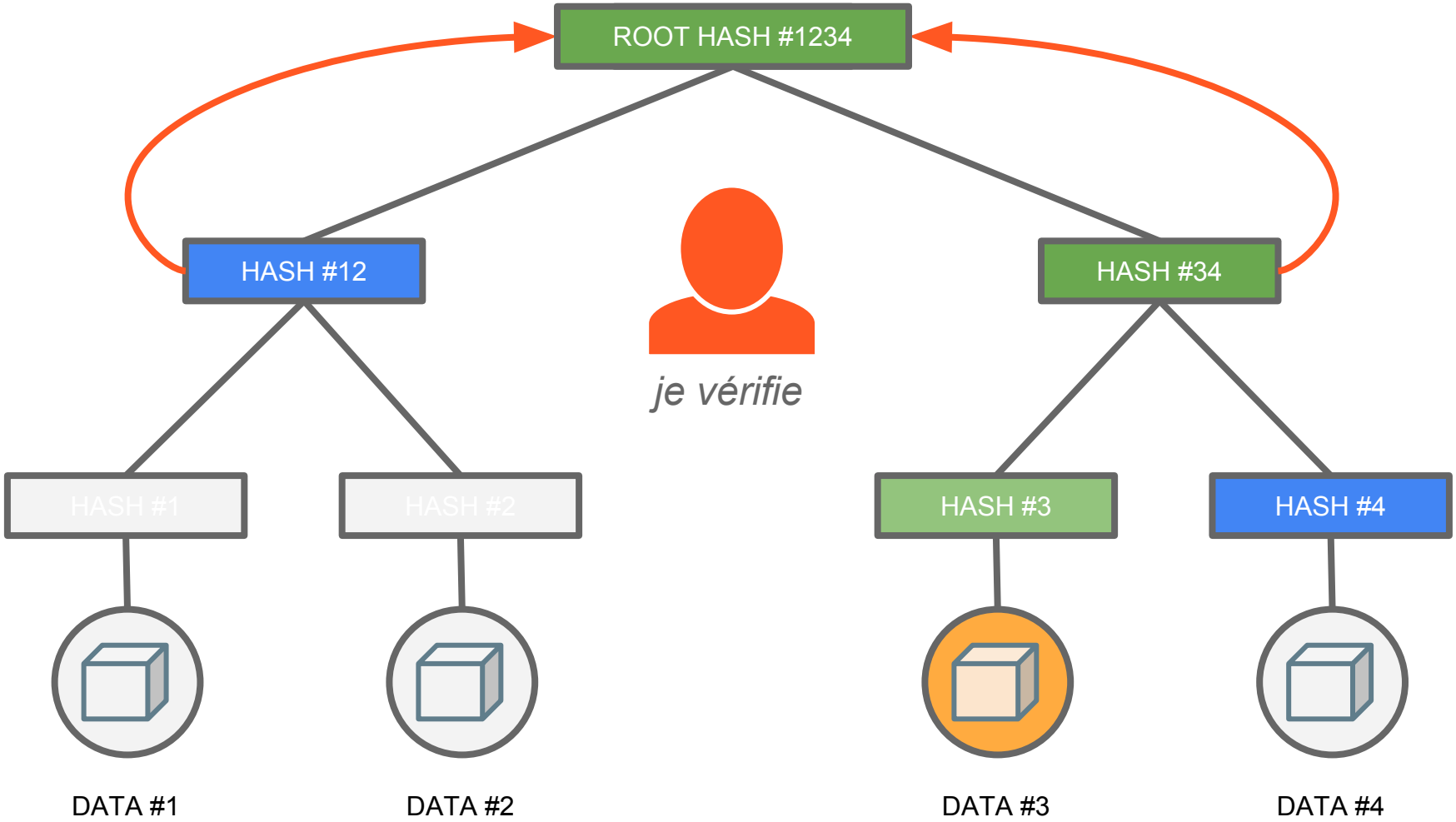
DATA #3

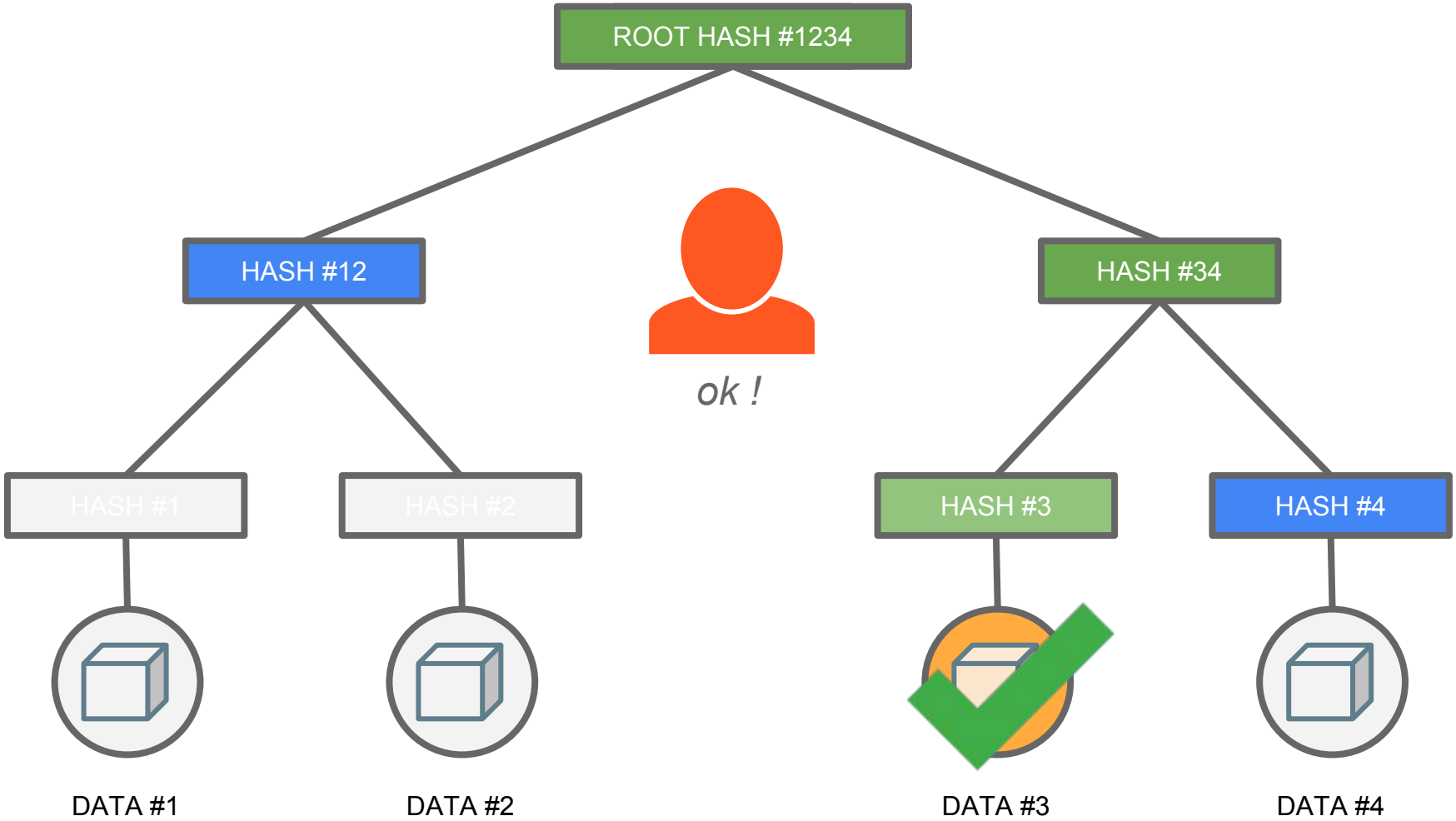
DATA #4


ROOT HASH #1234
voilà la donnée demandée
HASH #12
HASH #34
HASH #1
HASH #2
HASH #3
HASH #4
DATA #1
DATA #2
DATA #3
DATA #4

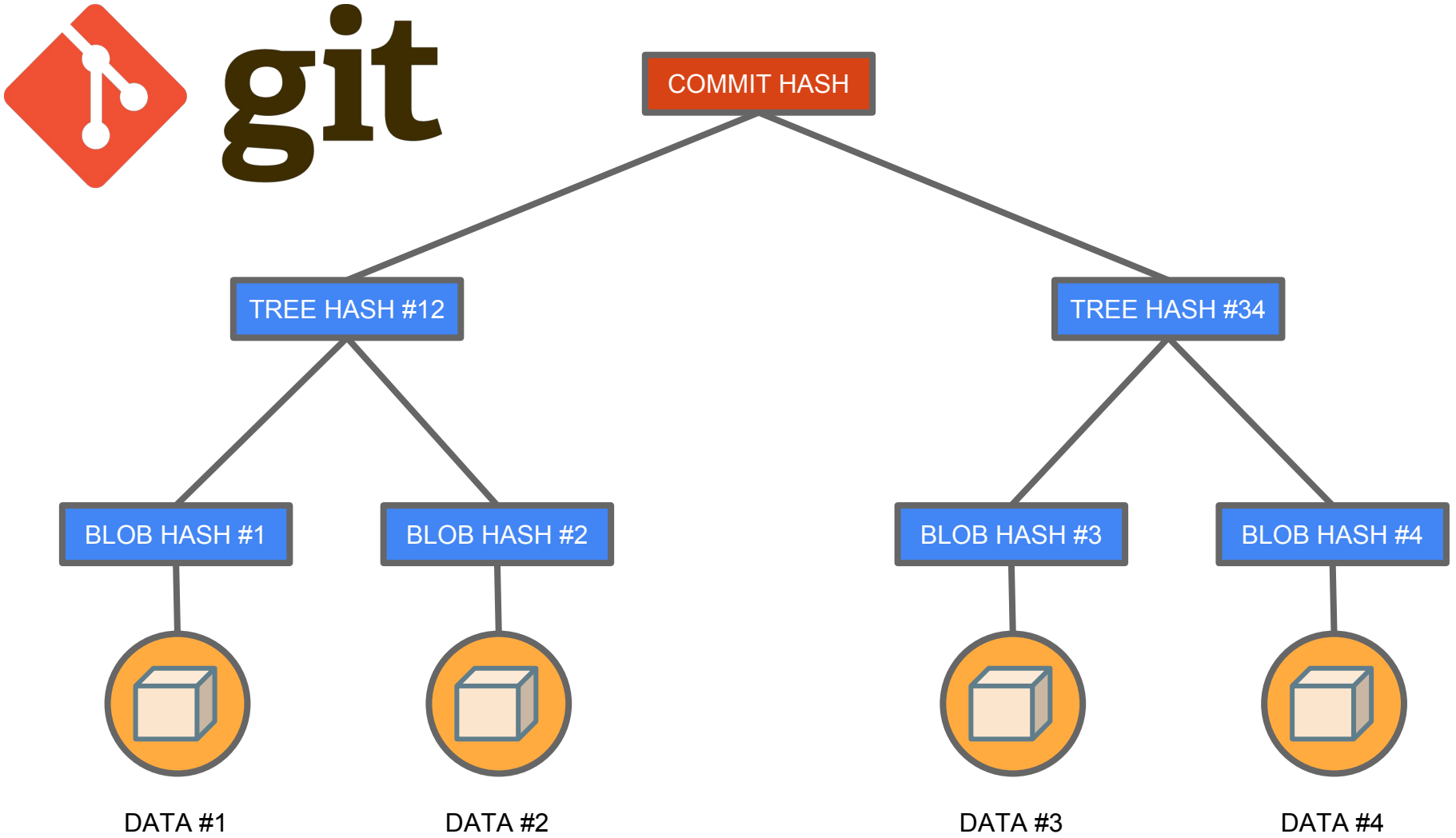

ROOT HASH #1234
HASH #12
HASH #34
je vérifie
HASH #1
HASH #2
HASH #3
HASH #4
DATA #1
DATA #2
DATA #3
DATA #4

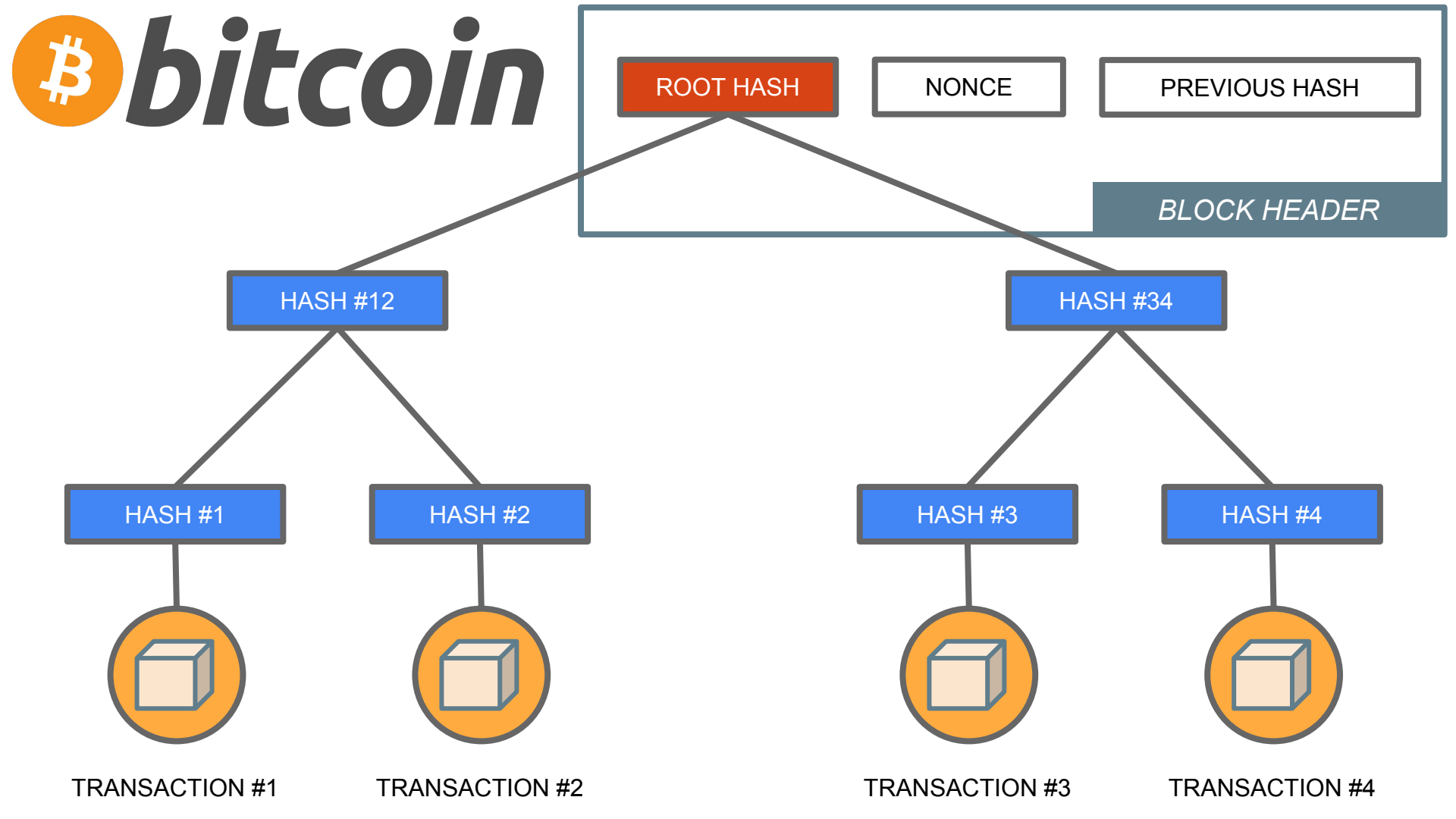

ROOT HASH #1234
HASH #12
HASH #34
je vérifie
HASH #1
HASH #2
HASH #3
HASH #4
DATA #1
DATA #2
DATA #3
DATA #4

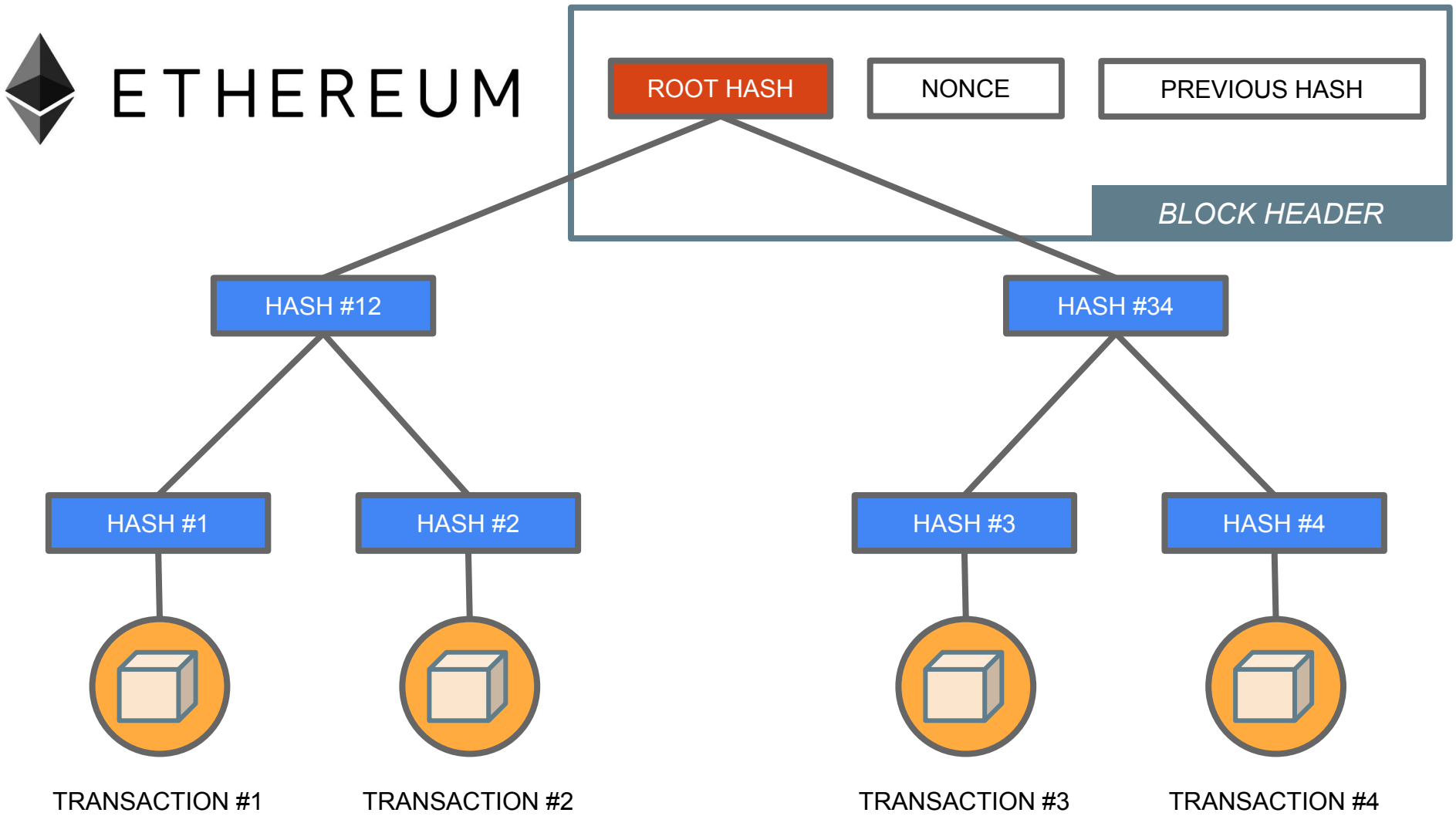

ROOT HASH #1234
HASH #12
HASH #34
je vérifie
HASH #1
HASH #2
HASH #3
HASH #4
DATA #1
DATA #2
DATA #3
DATA #4

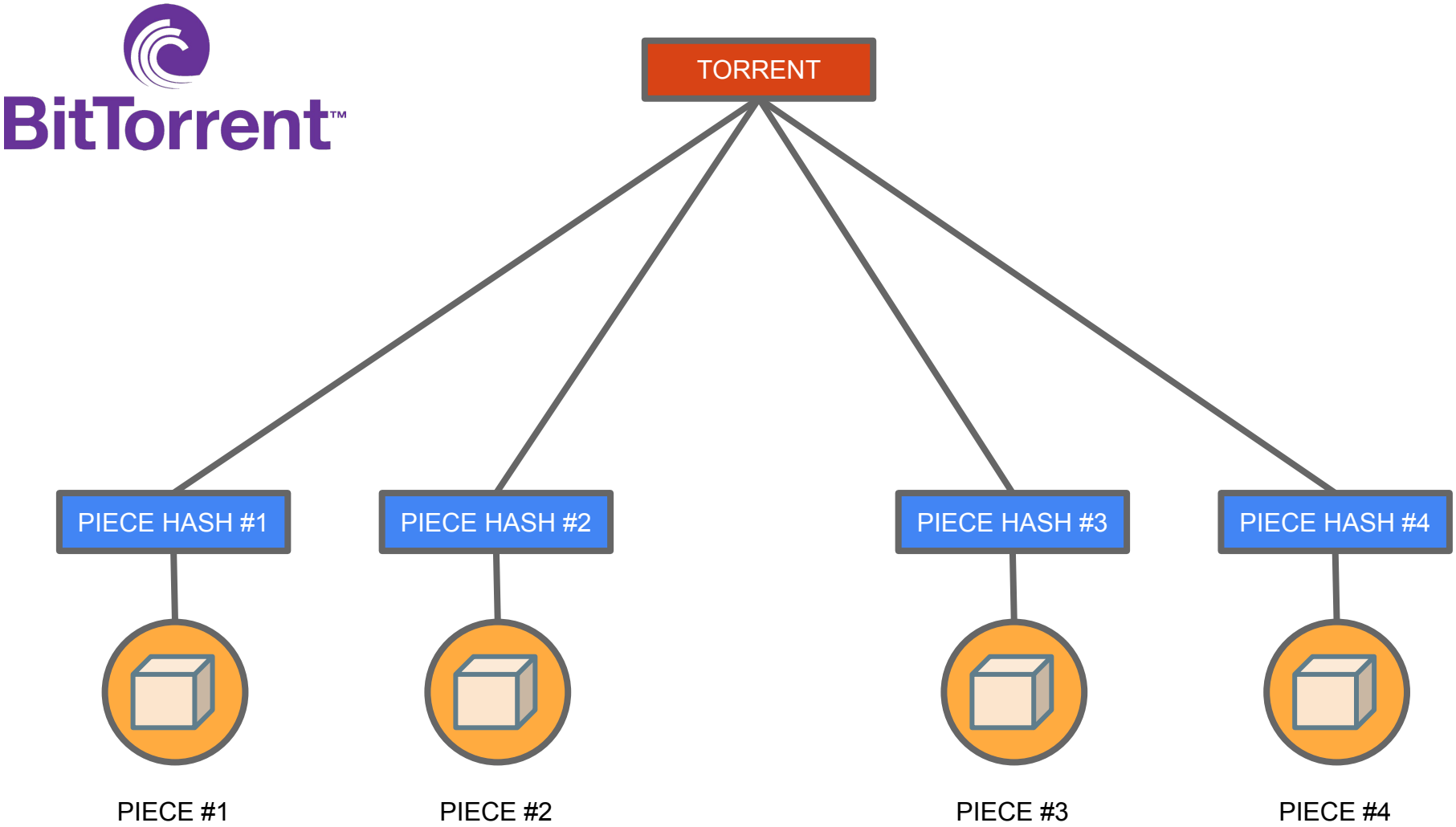

ROOT HASH #1234
HASH #12
HASH #34
ok !
HASH #1
HASH #2
HASH #3
HASH #4
DATA #1
DATA #2
DATA #3
DATA #4

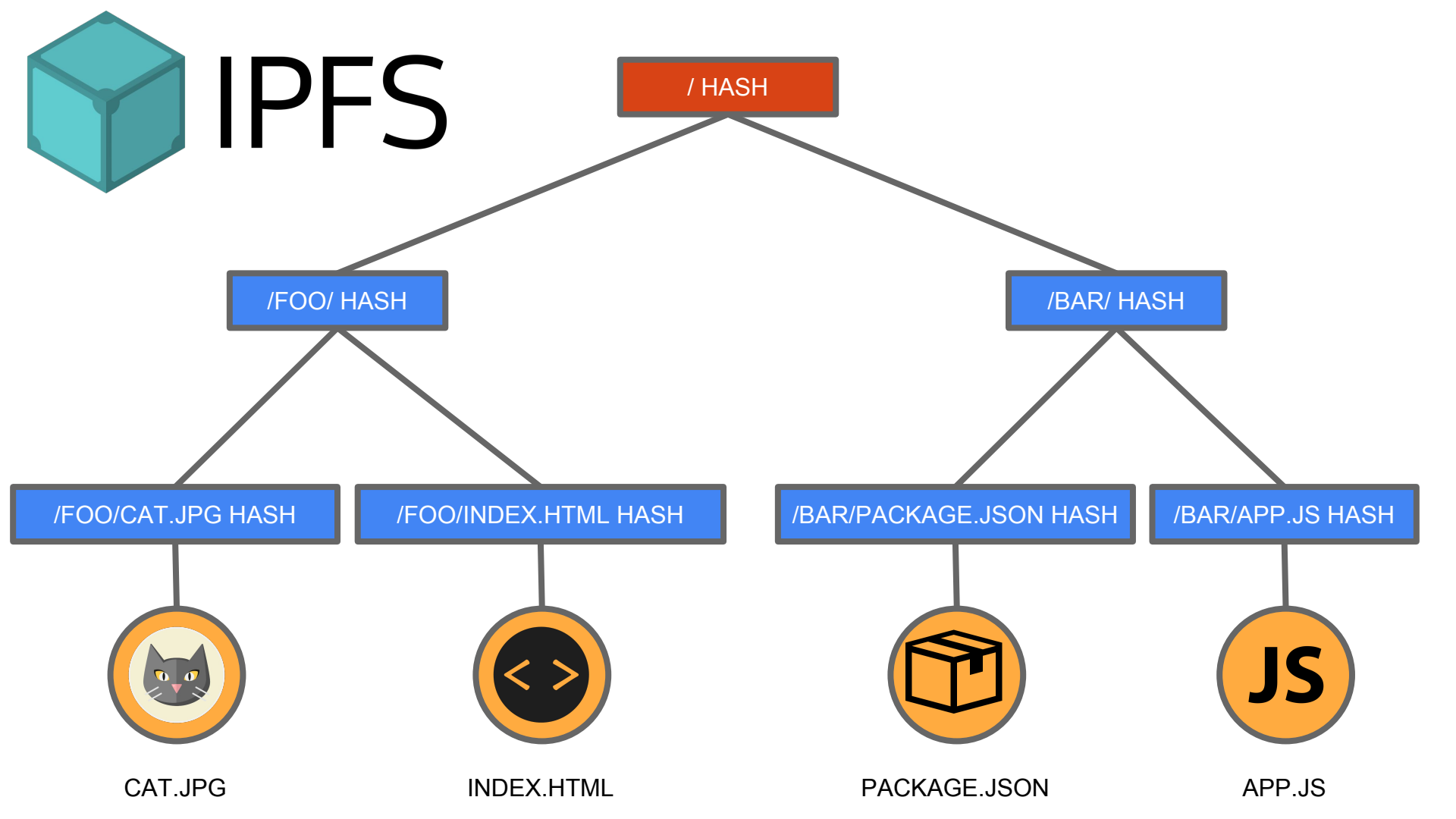
Utilisé ?


git
COMMIT HASH
TREE HASH #12
TREE HASH #34
BLOB HASH #1
BLOB HASH #2
BLOB HASH #3
BLOB HASH #4
DATA #1
DATA #2
DATA #3
DATA #4

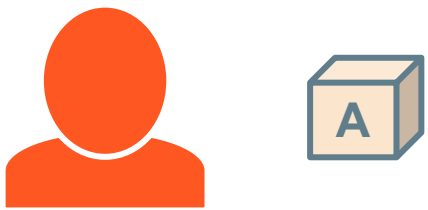
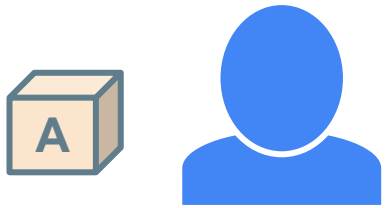

bitcoin
ROOT HASH
NONCE
PREVIOUS HASH
BLOCK HEADER
HASH #12
HASH #34
HASH #1
HASH #2
HASH #3
HASH #4
TRANSACTION #1
TRANSACTION #2
TRANSACTION #3
TRANSACTION #4

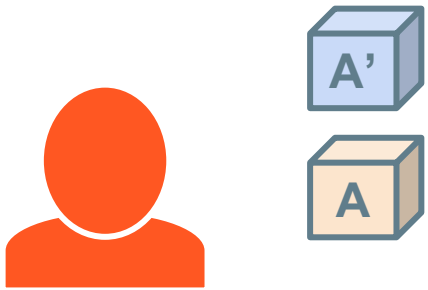

ETHEREUM
ROOT HASH
NONCE
PREVIOUS HASH
BLOCK HEADER
HASH #12
HASH #34
HASH #1
HASH #2
HASH #3
HASH #4
TRANSACTION #1
TRANSACTION #2
TRANSACTION #3
TRANSACTION #4

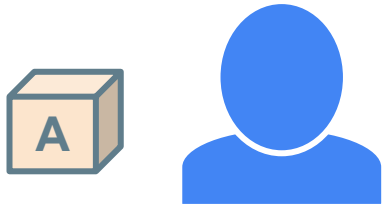

BitTorrent™
TORRENT
PIECE HASH #1
PIECE HASH #2
PIECE HASH #3
PIECE HASH #4
PIECE #1
PIECE #2
PIECE #3
PIECE #4

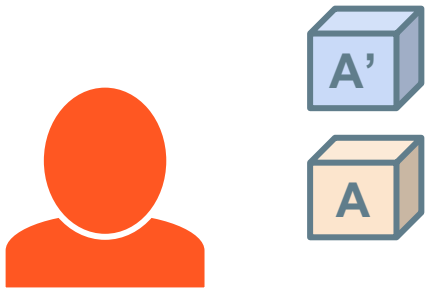

IPFS
/ HASH
/FOO/ HASH
/BAR/ HASH
/FOO/CAT.JPG HASH
/FOO/INDEX.HTML HASH
/BAR/PACKAGE.JSON HASH
/BAR/APP.JS HASH
JS
CAT.JPG
INDEX.HTML
PACKAGE.JSON
APP.JS

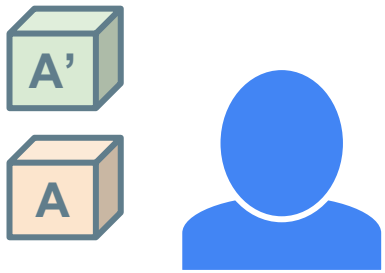
https://ipld.io


A

A


A’
A


A


A’
A


A’
A


A’
A
?
A’
A

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

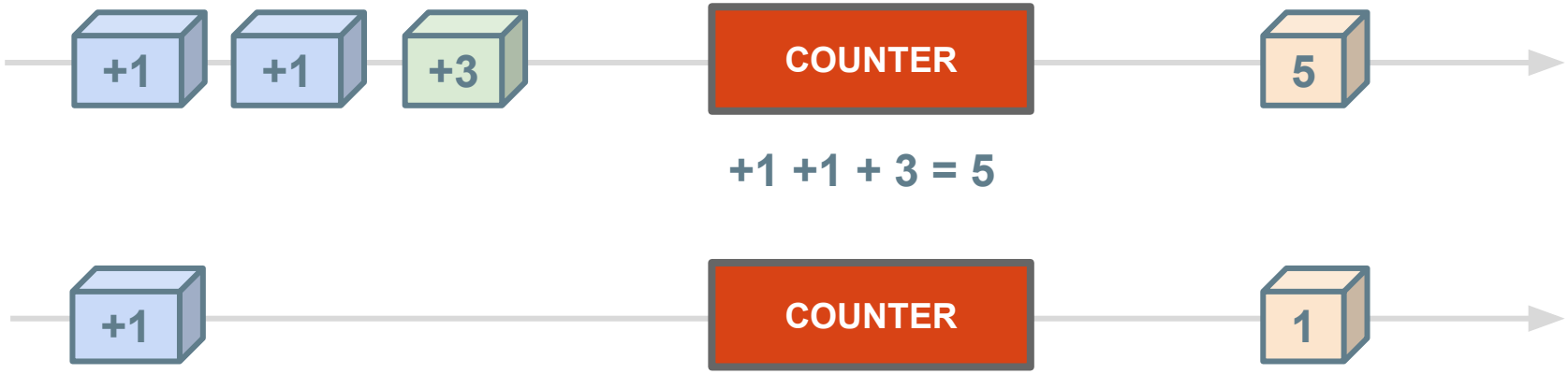
Marek Zawirski, INRIA & UPMC, Paris, France

Operation based (CmRDT)

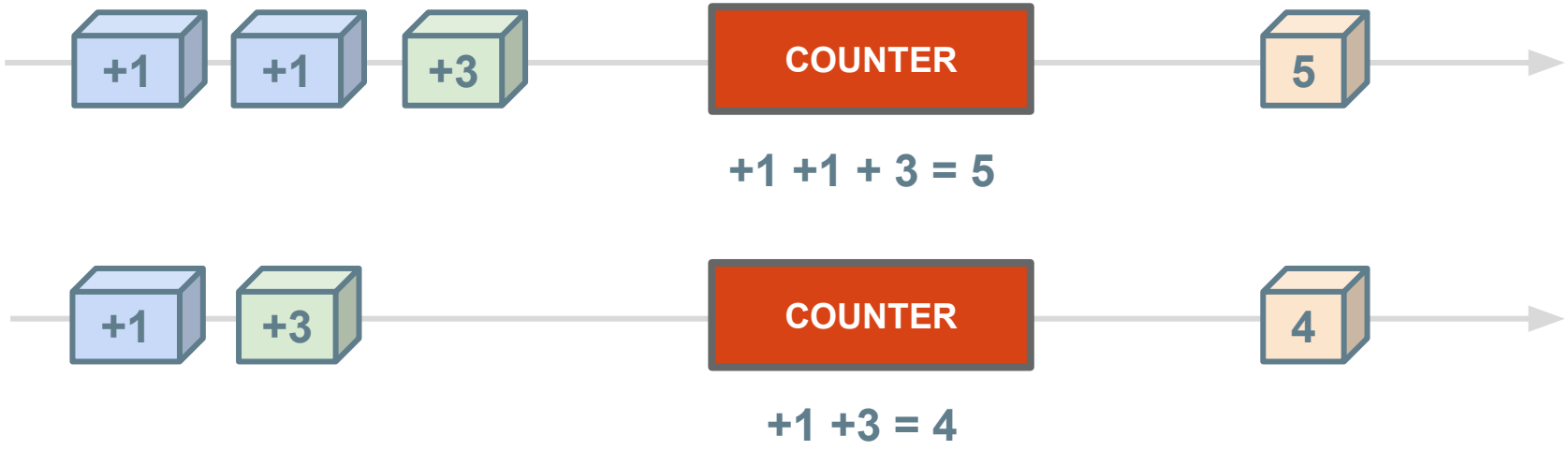
Operation based (CmRDT)

+1 +1 + 3 = 5

Operation based (CmRDT)



Operation based (CmRDT)



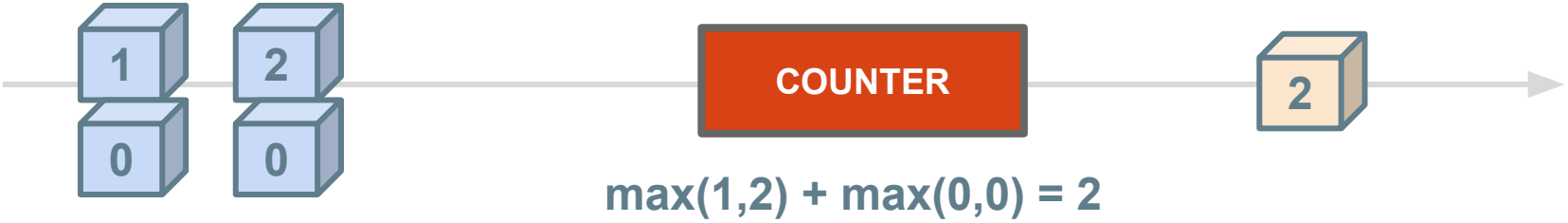
Operation based (CmRDT)

Operation based (CmRDT)

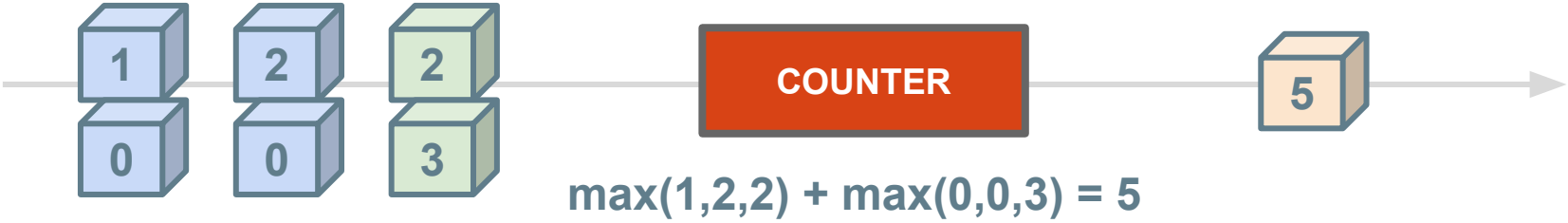
- **Nécessite peu de bande passante**
- **Faible tolérance au réseau (exactly once delivery)**

Operation based (CmRDT)

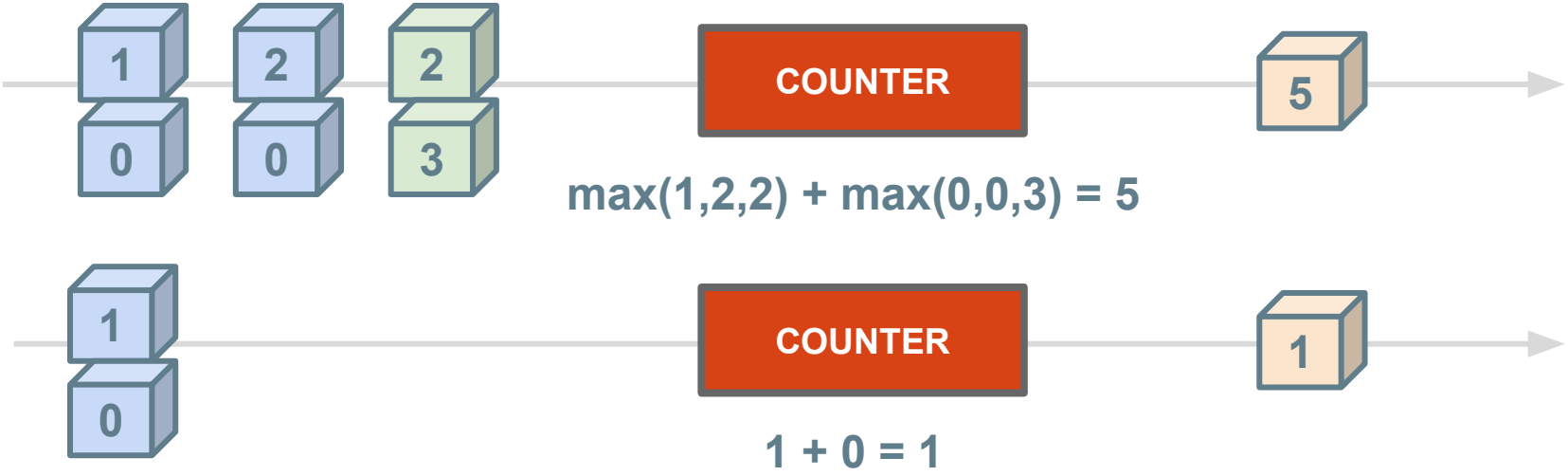
State based (CvRDT)



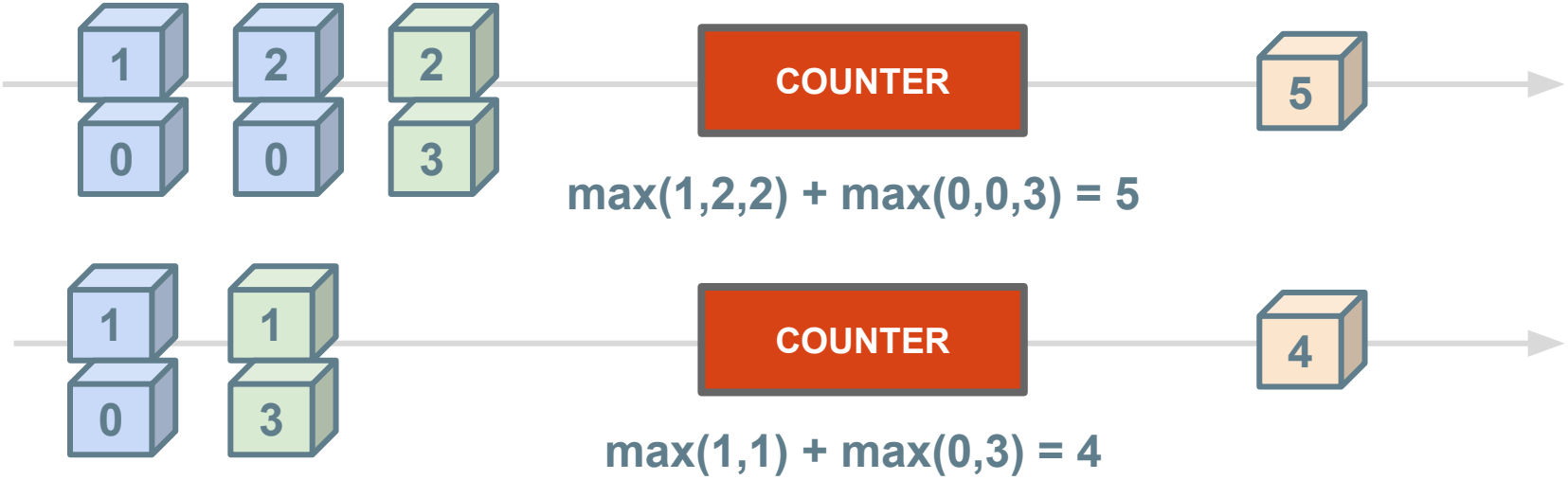
State based (CvRDT)



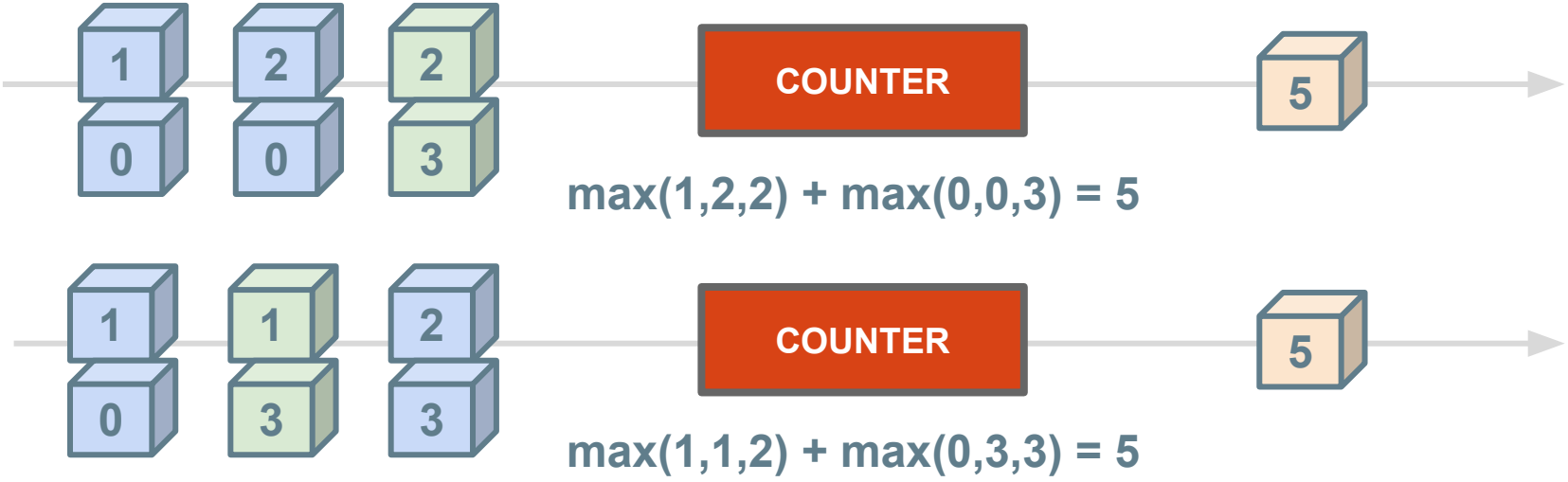
State based (CvRDT)



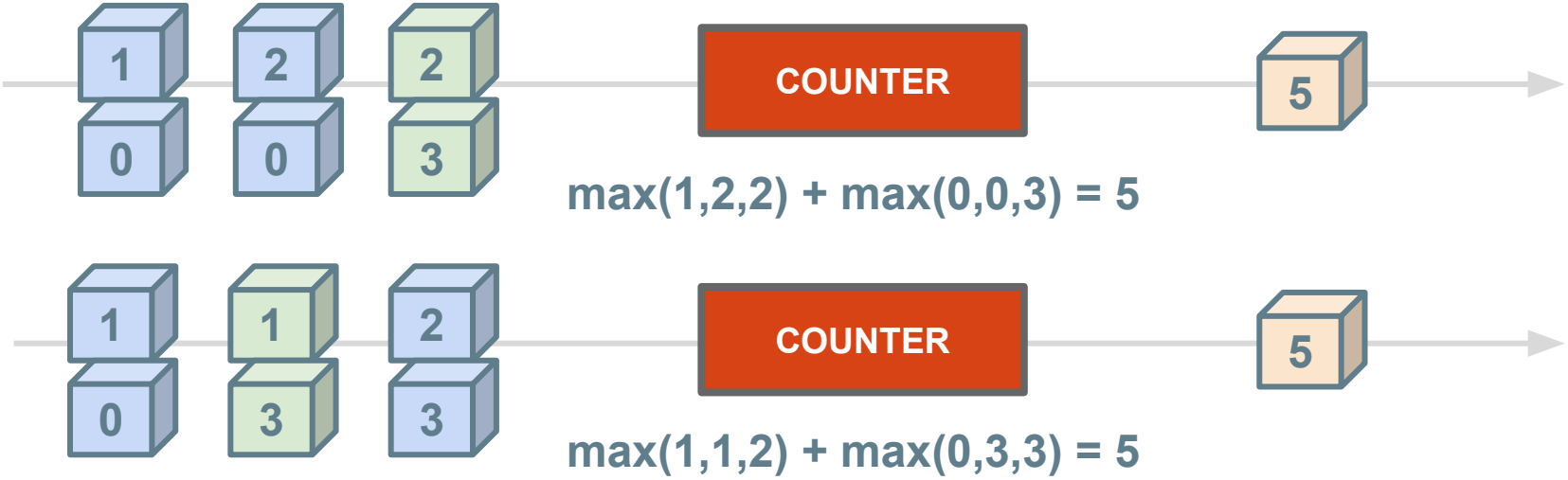
State based (CvRDT)



State based (CvRDT)



State based (CvRDT)



- **Nécessite de la bande passante**
- **Tolérance au réseau (packet loss)**

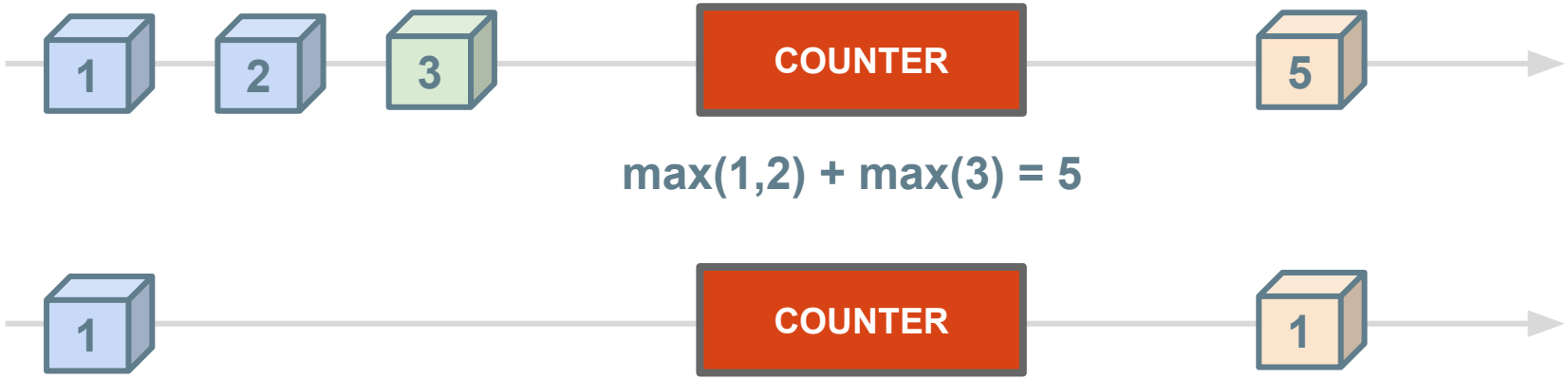
State based (CvRDT)

Delta state based (δ-CRDT)

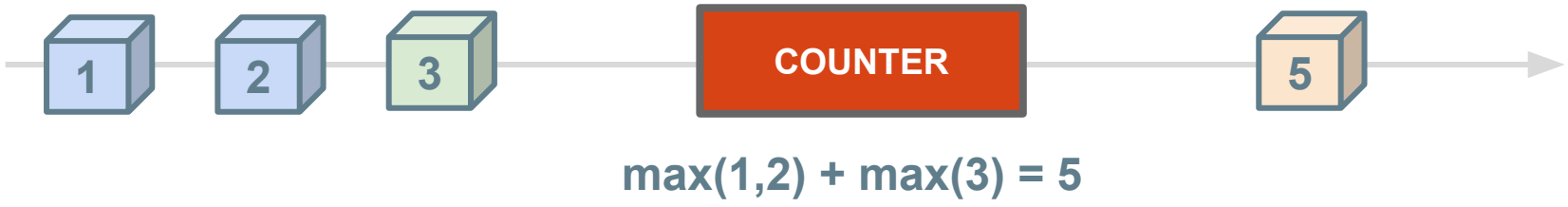
Delta state based (δ-CRDT)

max(1,2) + max(3) = 5

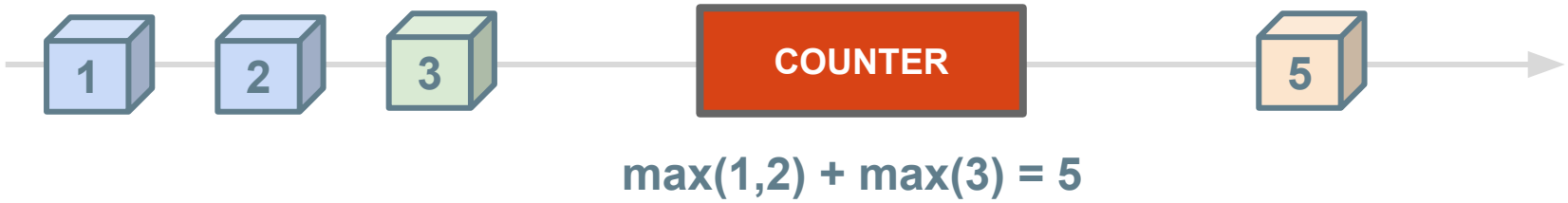
Delta state based (δ-CRDT)



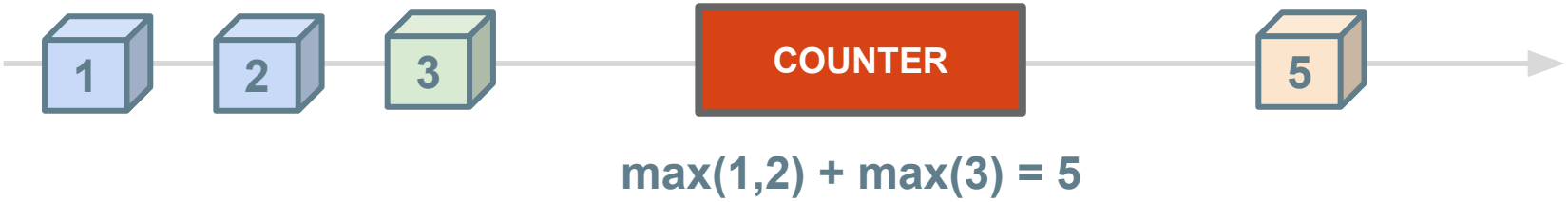
Delta state based (δ-CRDT)



Delta state based (δ-CRDT)



Delta state based (δ-CRDT)



- **Nécessite peu de bande passante**
- **Tolérance moyenne au réseau (at least once delivery)**

Delta state based (δ-CRDT)

Utilisé ?

Bases de données distribuées

Distributed Data

Chat (70M utilisateurs)

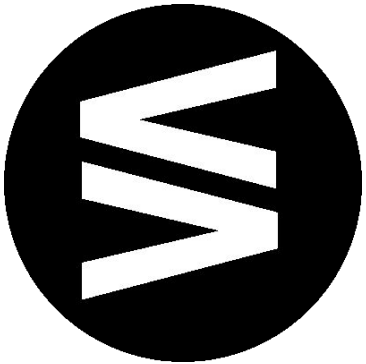
News feed

Sync. des localisations favorites

Mais aussi...

Y.js

Swarm.js



Libs JavaScript

orbit-db

P2P Chat

KVStore
Eventlog
Feed
Documents
Counters

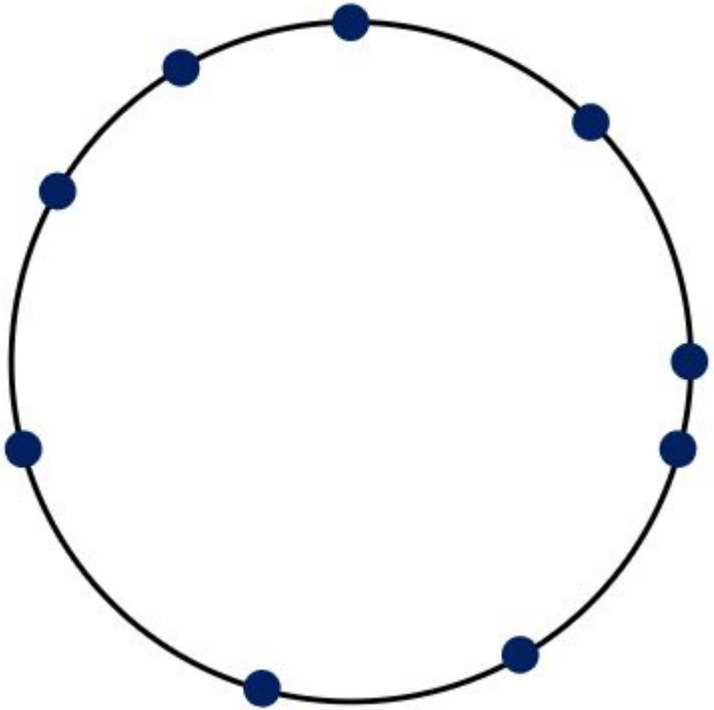
… et pour notre sujet ?

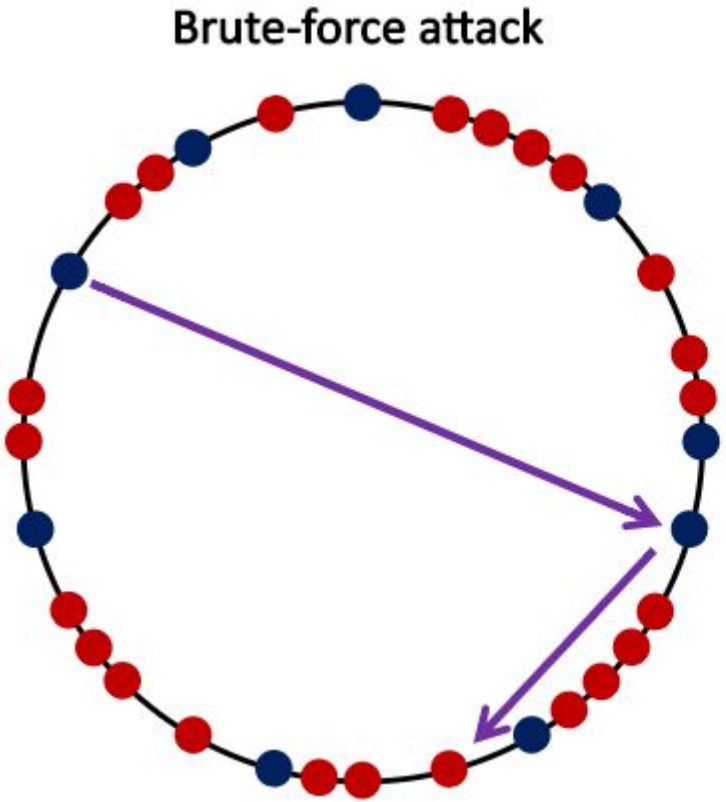
Démo

à la fin de la présentation

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

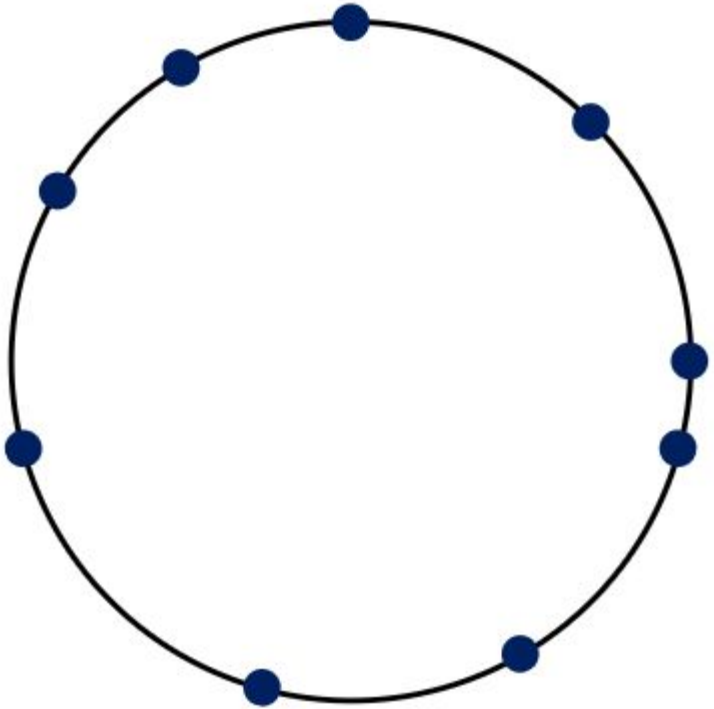
Et si on quittait le monde des bisounours ?

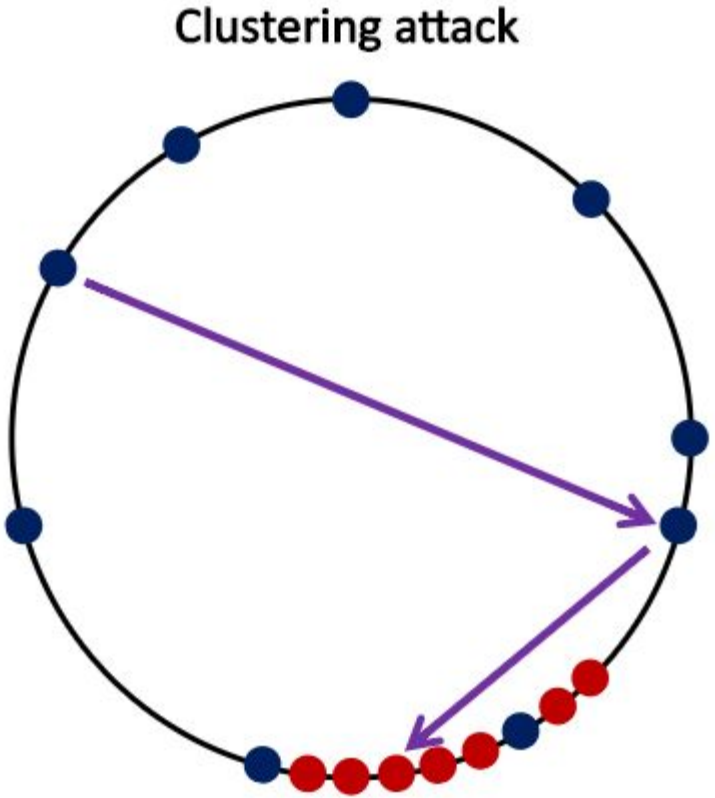




Sybil attack

http://slideplayer.com/slide/9719156/

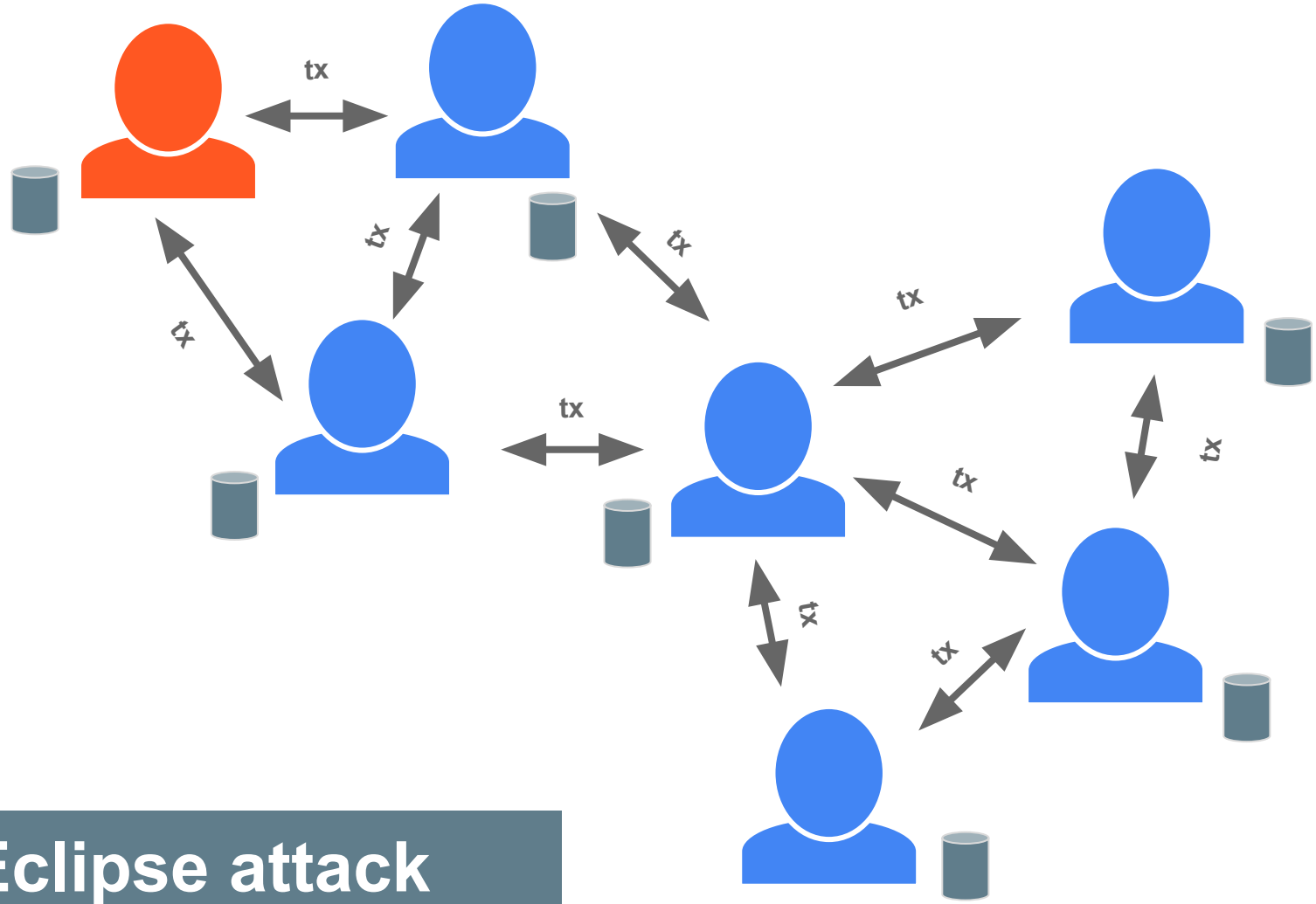




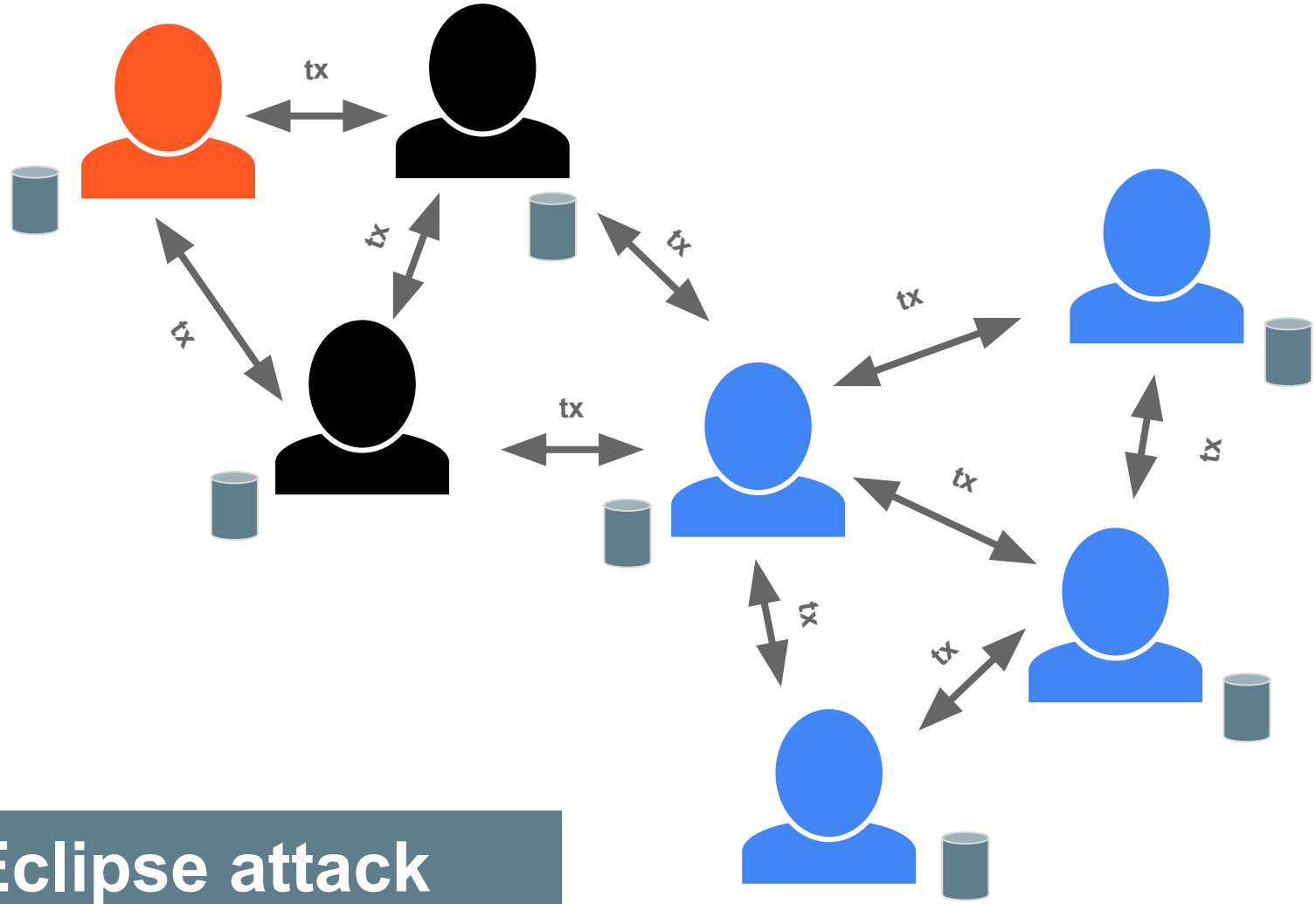
Sybil attack

http://slideplayer.com/slide/9719156/

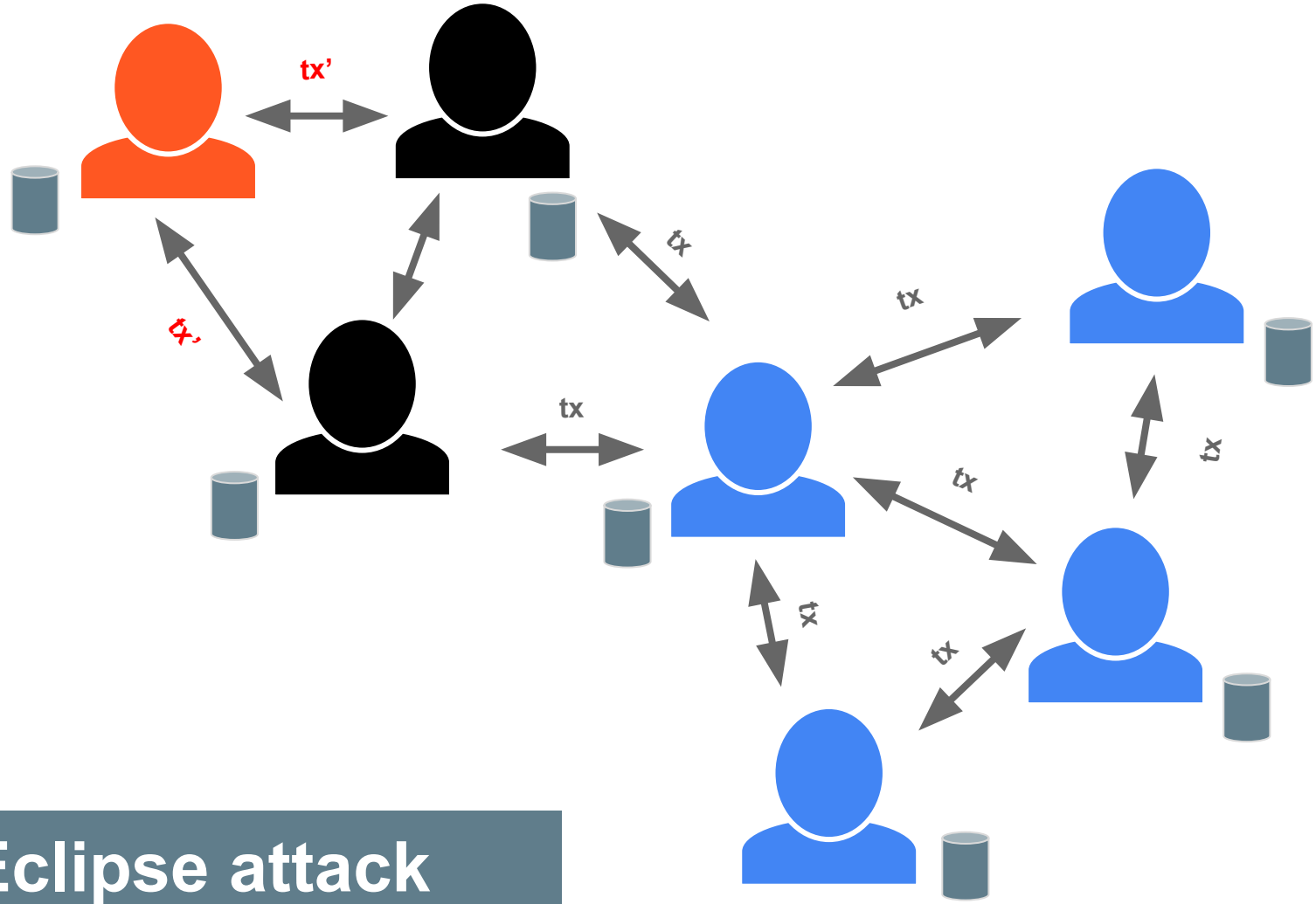
Proof of work



Eclipse attack



Eclipse attack



Eclipse attack

Denial Of Service

Man in the middle

51% attack

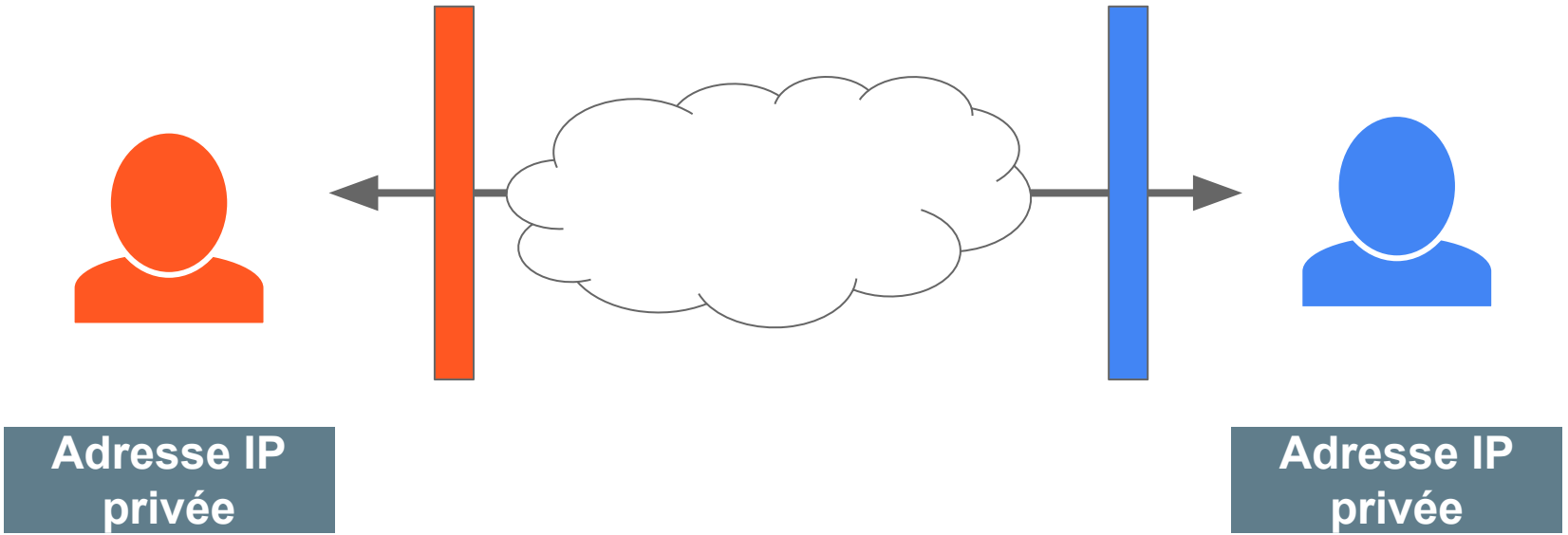
...


Réseau privé
Réseau public
Réseau privé

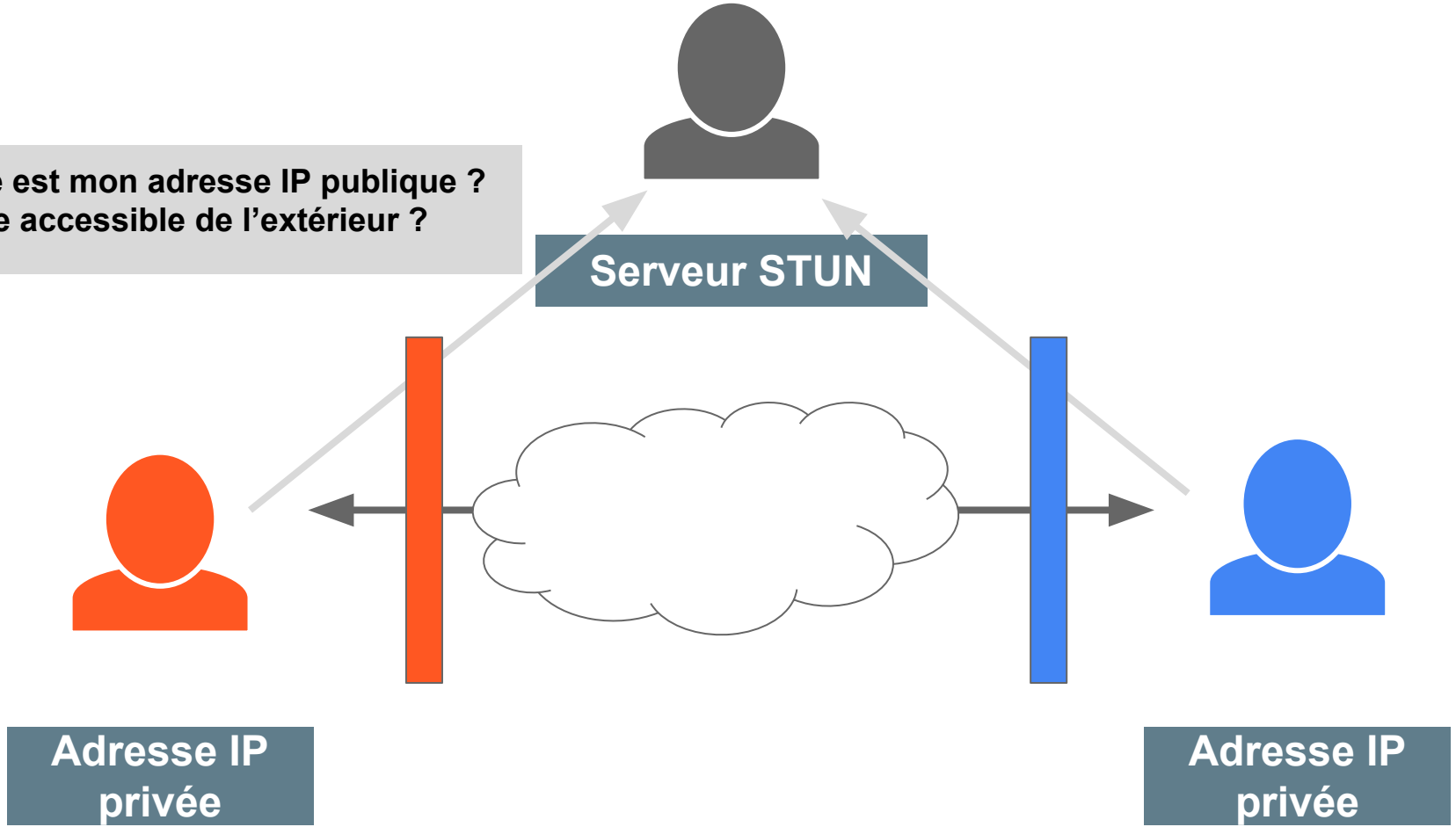
a.k.a La box internet

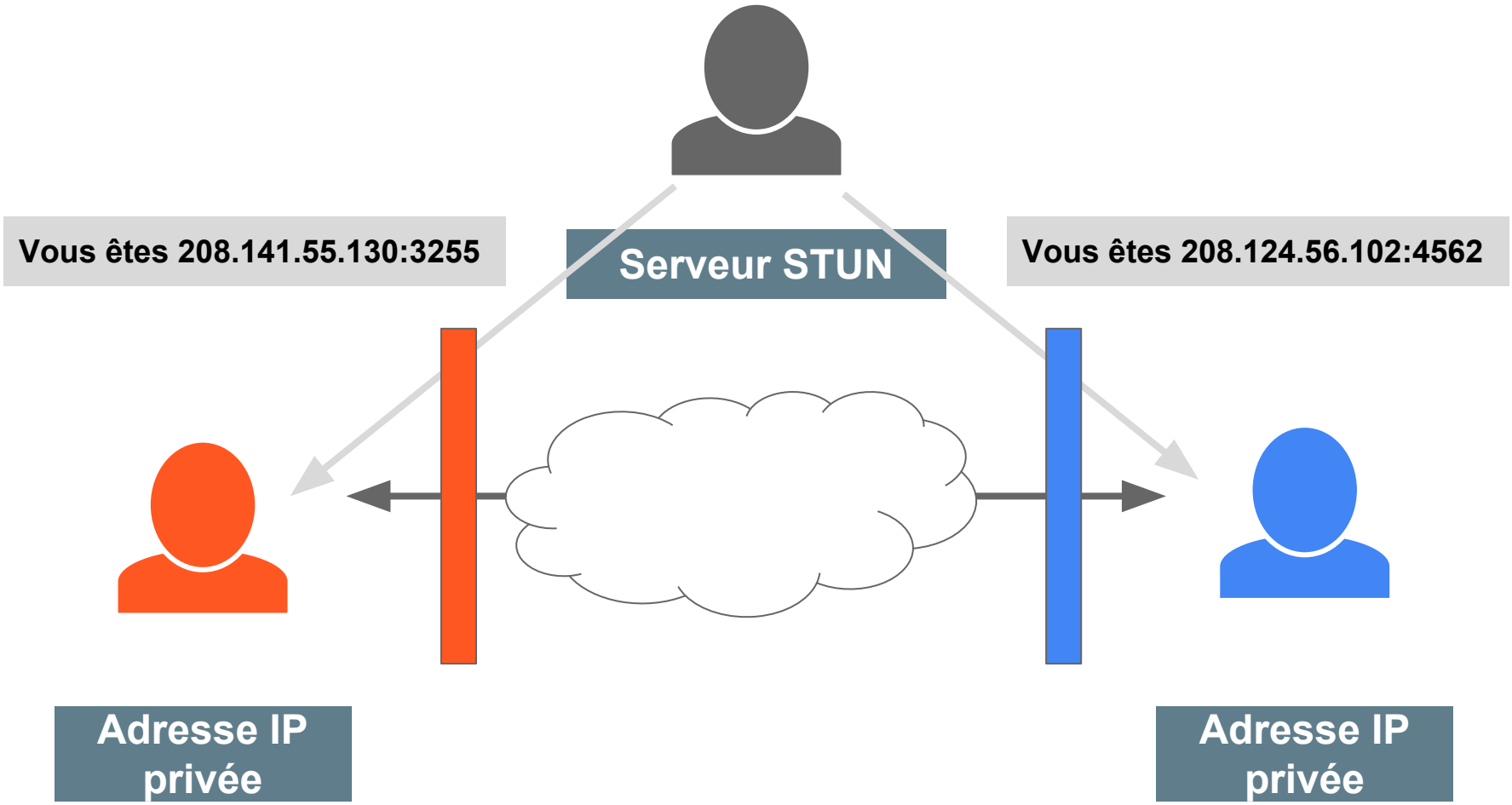
NAT Traversal (Network Address Translation)

Session Traversal Utilities for NAT (STUN)

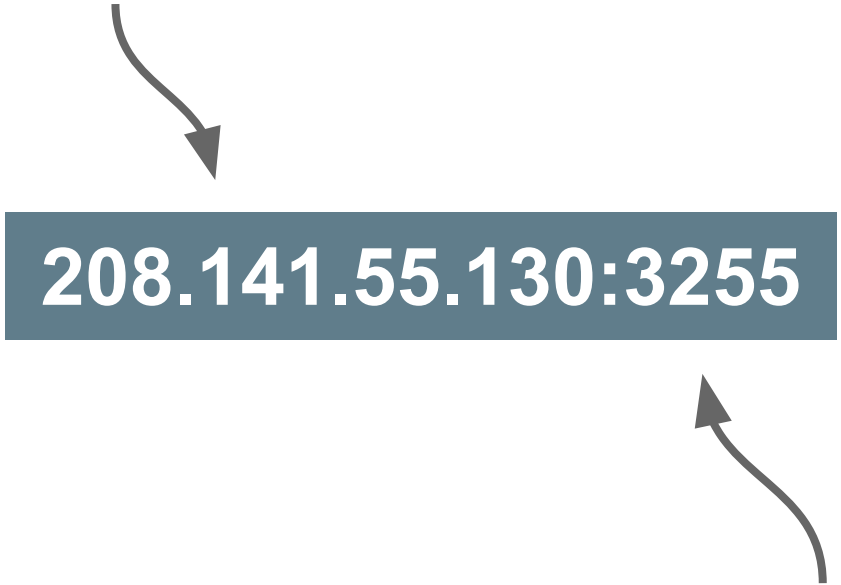

Adresse IP privée
Adresse IP privée

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



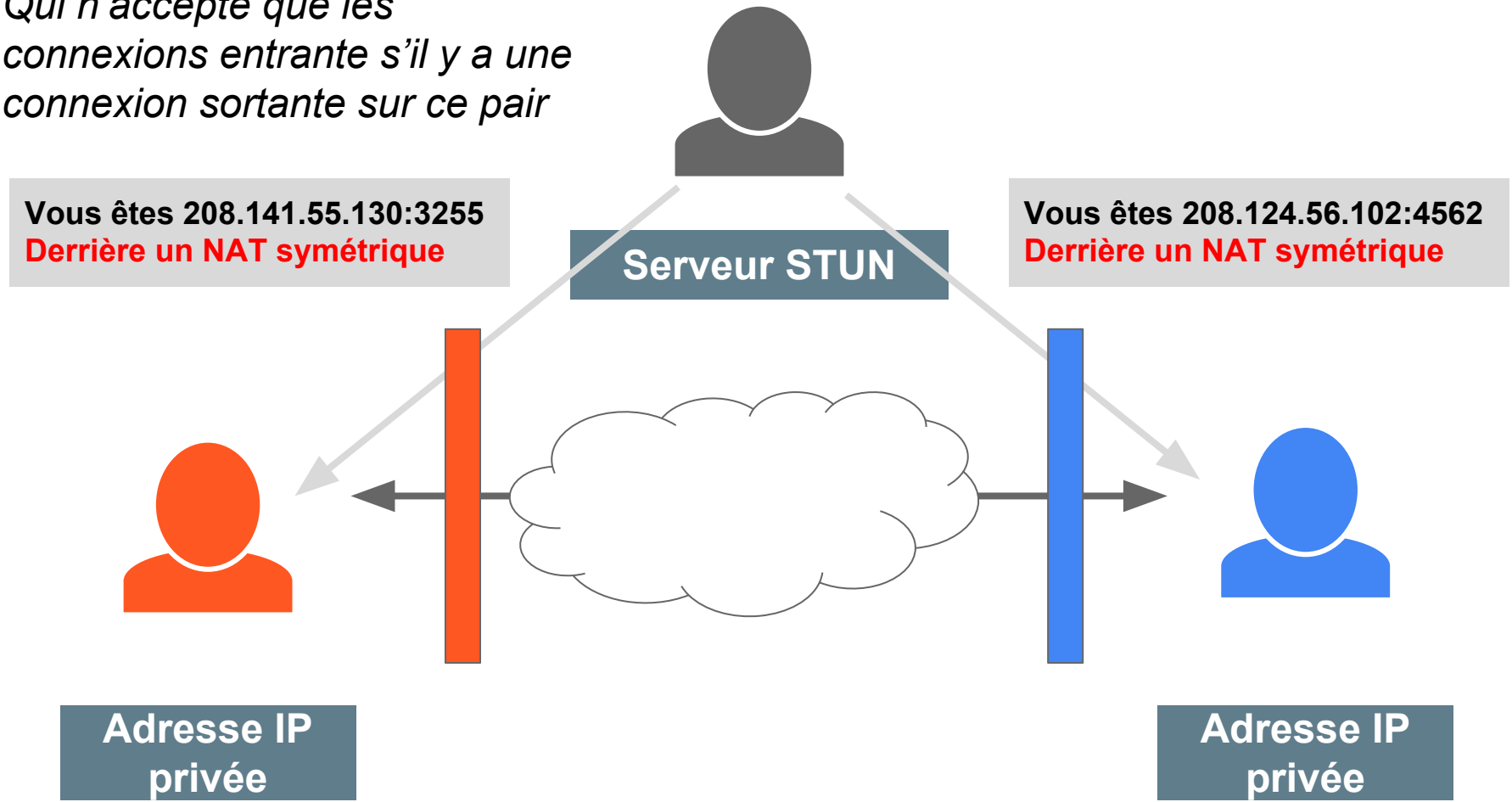

Vous êtes 208.141.55.130:3255
Serveur STUN
Vous êtes 208.124.56.102:4562
Adresse IP privée
Adresse IP privée

Adresse publique du routeur

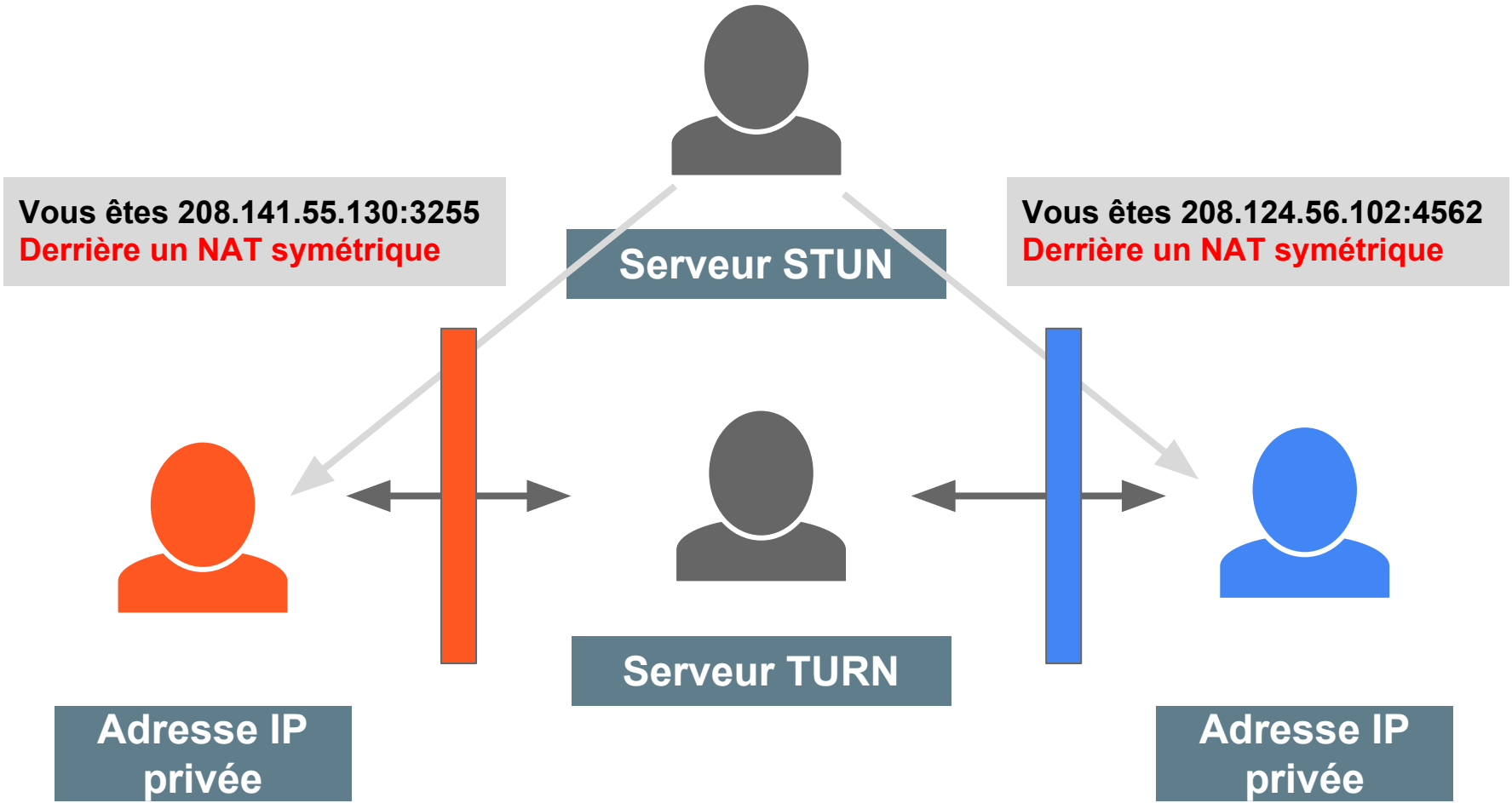


Port unique pour chaque device
derrière le routeur

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

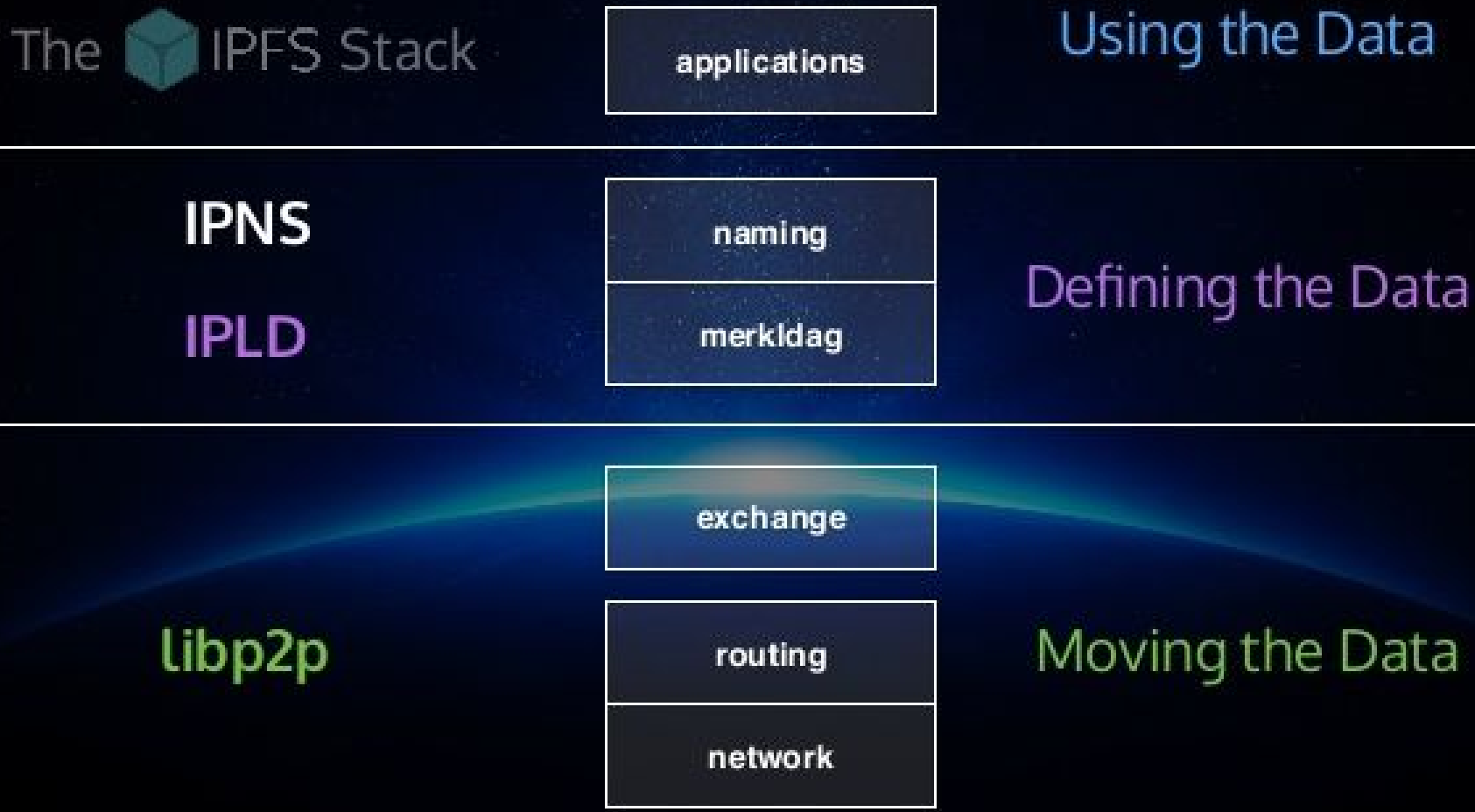


Traversal Using Relays around NAT (TURN)


Vous êtes 208.141.55.130:3255
Derrière un NAT symétrique
Serveur STUN
Vous êtes 208.124.56.102:4562
Derrière un NAT symétrique
Serveur TURN
Adresse IP privée
Adresse IP privée

Que nous réserve le futur ?


Scalabilité ?
Impact écologique ?
Arnaques ?
Centralisation ?


The IPFS Stack
applications
Using the Data
IPNS
IPLD
naming
merkldag
Defining the Data
exchange
libp2p
routing
network
Moving the Data
https://ipfs.io/

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

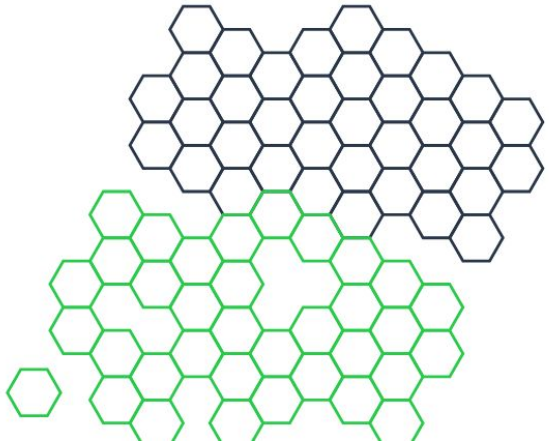
https://datproject.org/

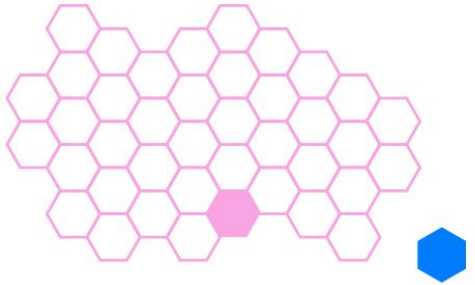
Dat Project

BLOG DOCS ABOUT

A distributed data community

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





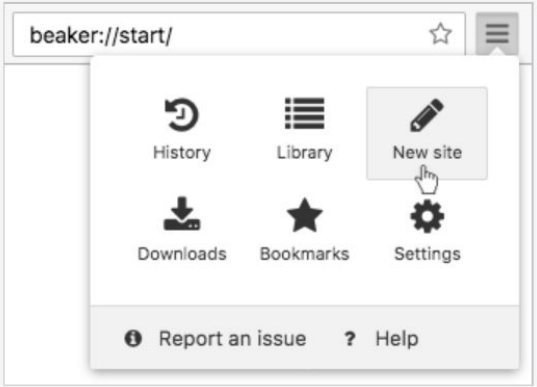
Beaker

Blog Docs Install Beaker

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?

Mais aussi...

Scuttlebot

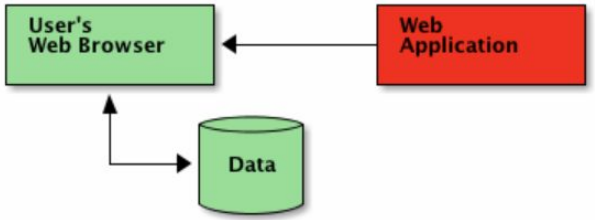
a peer-to-peer log store

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

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