

*Journée du Conseil
scientifique Afric 2016*

LiveTweet du 11 juillet 2016

#JCSA16

afric

PARTICIPANTS



[@AFNIC](#)



[@Mo7sen](#)



[@remasse](#)



[@bortzmeyer](#)



[@mathieuweill](#)



[@benoit_ampeau](#)



[@RamanouB](#)



[@TelecomPTech](#)



[@ltn22](#)



[@OpenPony](#)



[@samiamtimet](#)



[@CryptoPartyRNS](#)



[@asimonstweets](#)



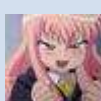
[@koubaak](#)



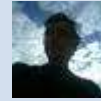
[@pbatreau](#)



[@mcabdel](#)



[@adofou](#)



[@pbeyssac](#)



[@Twest_io](#)



[@OpenPrunus](#)



[@vidal007](#)



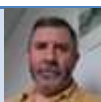
[@DoubleNumerique](#)



[@joel_mau](#)



[@guedou](#)



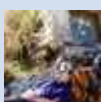
[@btreguier](#)



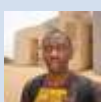
[@lanodan](#)



[@vincenttux](#)



[@mart_e](#)



[@ongolaboy](#)



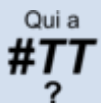
[@jcunniet](#)



[@rsuinux](#)



[@Le_Gai_Murmure](#)



[@quiaTT](#)



[@X_Cli_Public](#)



[@Tutur_Arhz](#)



[@Sebdraven](#)



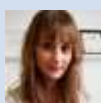
[@YRousse](#)



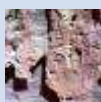
[@libricoleur](#)



[@lauMarot](#)



[@PommierCha](#)



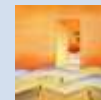
[@privacy_data](#)



[@rpr8395](#)



[@natchiche](#)



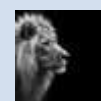
[@THD_IT](#)



[@LucienCastex](#)



[@fzs600N](#)



[@lpenou](#)



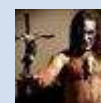
[@michelguillou](#)



[@5t4n7oG](#)



[@fcouchet](#)



[@Nekrofage666](#)



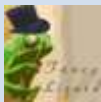
[@ParathorO](#)



[@TBreports](#)



[@ThePortlandBlog](#)



[@Lezard Imperial](#)



[@agumonkey](#)



[@JulienPorschen](#)



[@renaudsn](#)



[@HasniSEO](#)



[@Fondapol](#)



[@victorhery](#)



[@real_panda3](#)

TWEETS



[Stéphane Bortzmeyer @bortzmeyer](#)

Alors que je voulais beaucoup regarder le foute, à la place, je vérifie que tout est complet et correct pour [#JCSA16](#) demain. [#sacrifice](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Pour en savoir plus sur l'état actuel et réel de la crypto, venez demain à [#JCSA16](#) ou suivez-le en strimingue. [twitter.com/newshtwit/stat...](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Demain, toute la France suivra [#JCSA16](#), depuis la Fan Zone rue Barrault, ou bien en streaming. [afnic.fr/fr/l-afnic-en-...](#)



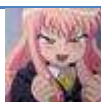
[BIAOU Ramanou @RamanouB](#)

Hello [#JCSA16](#) @AFNIC



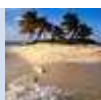
[lauMarot @lauMarot](#)

[#JCSA16](#) Ca stream où ?



[Johann @adofou](#)

En route pour la Journée du Conseil Scientifique de l'Afnic.
Des twittos présent? [#JCSA16](#) [pic.twitter.com/HkcL864NBJ](#)



[Mohsen Souissi @Mo7sen](#)

En route (métro) vers [#JCSA16](#). Une journée chargée et riche en perspective. [#Afnic](#)



[Régis MASSÉ @remasse](#)

Bienvenue à la journée du Conseil Scientifique ! [#JCSA16](#)
[#Afnic](#)



[Benoit Ampeau @benoit_ampeau](#)

C'est parti pour le [#JCSA16](#) [#cryptographie](#). Ce matin tutoriel [#blockchain](#) / contrats [#ethereum](#) par [@bortzmeyer](#) [#Afnic](#)
[@Mines_Telecom](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

L'angoisse de l'orateur avant un tutoriel de trois heures...
[#café](#) [#JCSA16](#)



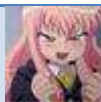
[AFNIC @AFNIC](#)

Suivez [#JCSA16](#) ce matin avec le tuto [#blockchain](#) par [@bortzmeyer](#) à suivre en direct sur [afnic.fr/fr/l-afnic-en-...](#) [pic.twitter.com/leXUfr3osF](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

"blocks": 389364 Mon tutoriel blockchain [#JCSA16](#) va commencer et mon nœud [#Bitcoin](#) n'a pas récupéré son retard d'un long arrêt.

[Johann @adofou](#)

Ca commence mal pour la [#JCSA16](#). Trafic très perturbé sur la [@Ligne6_RATP](#). [#OnVaEtreEnRetard](#)

[Pascal Vella @pascalvella](#)

[#JCSA16](#) dans 10 minutes ! (@ Télécom ParisTech - ENST - [@TelecomPTech](#) in Paris, France)
[swarmapp.com/c/7cWxFsUu6cc](#)

[Mathieu Weill @mathieuweill](#)

Retour sur bancs de l'école. Un peu de blockchain à titre de formation continue [#jcsa16](#)

[Régis MASSÉ @remasse](#)

[@adofou](#) [@Ligne6_RATP](#) L'année prochaine, n'hésite pas à utiliser le blabla car Afnic [#covoiturage](#) [#Afnic](#) [#JCSA16](#)

[Vidal Chriqui @vidal007](#)

"Que faire de rigolo avec la [#blockchain](#) ?"
Une matinée avec [@bortzmeyer](#) [@AFNIC](#) qui promet d'être "amusante" [#JCSA16](#) [pic.twitter.com/9AzwiL3pec](#)

[OpenPony @OpenPony](#)

C'est parti pour une journée au [#JCSA16](#) !! On commence par "Que faire de rigolo avec la blockchain" par [@bortzmeyer](#)

[Philippe Batreau @pbatreau](#)

Que faire de rigolo avec la [#blockchain](#) ? thème de l'intervention de [@bortzmeyer](#) à la [#JCSA16](#) de l'[@AFNIC](#)
[twitter.com/bortzmeyer/sta...](#)

[Prunus @OpenPrunus](#)

Bien arrivé et prêt pour [#JCSA16](#)



[Régis MASSÉ @remasse](#)

C'est parti pour une matinée [#blockchain](#) [@bortzmeyer](#)
[#Afnic](#) [#JCSA16](#)



[Johann @adofou](#)

Début de la [#JCSA16](#) avec [@bortzmeyer](#) sur la Blockchain!
pic.twitter.com/xM4YrkuEn1



[Pierre Beyssac @pbeysac](#)

A [#jcsa16](#) en train d'écouter religieusement [@bortzmeyer](#) sur la [#blockchain](#) "hype complet le truc à la mode dont tout le monde parle".



[Pierre Beyssac @pbeysac](#)

"Avant quand je travaillais sur Internet, on me demandait "c'est quoi", jusqu'en 1994. Maintenant pareil avec [#blockchain](#)" [#jcsa16](#)



[Renaud S @renaudsn](#)

[@bortzmeyer](#) Hello, la caméra et le son sont au top, par contre les slides sont super pixelisés (mais lisibles) ! :([#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

[#JCSA16](#) comme le veut la tradition, les chaussettes du Président du CS s'adaptent à l'évènement :-)
twitter.com/ltn22/status/7...



[BIAOU Ramanou @RamanouB](#)

@[bortzmeyer](#) commence sa présentation sur la [#BLOCKCHAIN](#) [#JCSA16](#) [#AFNIC](#)



[Pascal Vella @pascalvella](#)

[#JCSA16](#) débute ! @[bortzmeyer](#) aborde les aspects sérieux de la [#blockchain](#) en direct sur [afnic.fr/fr/l-afnic-en-...pic.twitter.com/riWQVoJ3zn](#)



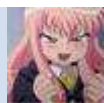
[BIAOU Ramanou @RamanouB](#)

La programmation s'invitera à la deuxième partie du tutoriel [#JCSA16](#) avec @[bortzmeyer](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) à @[TelecomPTech](#) @[bortzmeyer](#) [#blockchain](#)
[pic.twitter.com/juKmyT3mXB](#)



[Johann @adofou](#)

Explication principe du [#blockchain](#) par @[bortzmeyer](#) : des transactions passant d'un état à une autre regroupé dans des bloc chaîné [#JCSA16](#)



Les principes du [#blockchain](#) les blocs sont chaînés [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



[#jcsa16](#) [@bortzmeyer](#) revient sur les idées de base de la [#blockchain](#)

[Pierre Beyssac @pbeysac](#)



Avec le [#blockchain](#) vous n'avez pas besoin de faire confiance aux papes de l'Internet [#JCSA16](#) [@bortzmeyer](#)

[BIAOU Ramanou @RamanouB](#)



[#jcsa16](#) "pair à pair, mais tous les pairs ne sont pas gentils" "problème des gougnafiers" pair indigne ?

[Pierre Beyssac @pbeysac](#)



La blockchain fonctionne en pair-à-pair, sans autorité central. Des pairs gentil, comme méchant [#JCSA16](#)

[Johann @adofou](#)



Les slides de [@bortzmeyer](#) à [#JCSA16](#) sur la [#blockchain](#) sont disponibles sur [afnic.fr/fr/l-afnic-en-... #Afnic](#) [pic.twitter.com/hQCNS9iRrk](#)

[AFNIC @AFNIC](#)



Comment éviter l'explosion des blockchains par des gens malveillants? Deux solutions : Preuve de travail ou preuve de participation [#JCSA16](#)

[Johann @adofou](#)



[@AFNIC](#) [@bortzmeyer](#) Tout ce que vous avez toujours voulu savoir sur la [#blockchain](#) sans jamais oser le demander [#JCSA16](#) [@Mines_Telecom](#)

[Nathalie Chiche @natchiche](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "on évite les gournafiers" avec la preuve de travail. (proof of work) et la preuve de participation (proof of stake)

[Mohsen Souissi @Mo7sen](#)

. @[THD_IT](#) Merci de toute l'aide que tu nous as apportée, comme d'hab. :-) Dommage que tu ne puisses pas être des nôtres aujourd'hui [#JCSA16](#)

[noueP lue.rnel @lpenou](#)

[#JCSA16](#) @[adofou](#) @[pbeysac](#)
lire l'article de @[Torlus](#) :) torlus.github.io/2016/03/04/why...

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) @[bortzmeyer](#) revient sur un père des USA. "une fois qu'on a éjecté le roi, comment on fait" "donner le pays aux riches" [#blockchain](#)

[stanlog @5t4n7oG](#)

.@[AFNIC](#) y a-t'il une captation vidéo de [#JCSA16](#) ? Si oui sera-t-elle dispo en ligne ?

[Johann @adofou](#)

Preuve de travail : Résoudre un puzzle informatique par exemple. Contesté car consommation de CPU/Energie pour "rien". [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)

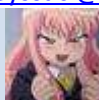
Deux grandes classes de sol. pour éviter les "gournafiers" :-)
- Preuve de travail ;
- Preuve de participation

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "si vous avez une meilleure idée, je suis preneur" (proof of work + proof of stake)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "attaque des 51% ou la dictature de la majorité" "pas si grave que ça, puisque visible, pas de trucs en traître"

[Johann @adofou](#)

Preuve de participation : Vote proportionnel à l'implication. Les 2 classes ont un problème commun : l'attaque des 51% [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "c'est comme dans le logiciel libre" "si les dévs font des choses qui déplaisent, ça se voit et on peut partir"

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "pas vraiment de signe précurseur de [#bitcoin](#), à part quelques articles avec le recul, comme Bitgold de Szabo".
2009 : publi bitcoin

[OpenPony @OpenPony](#)

Un peu d'histoire : 2008-2009 publication de [#bitcoin](#), c'est le vrai début de la [#blockchain](#) [#JCSA16](#)

[Johann @adofou](#)

Histoire blockchain: Peu d'article avant 2008. Publication d'un article fondateur par Satoshi Nakamoto en 2008. C'est un pseudonyme [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "Satoshi Nakamoto est un pseudonyme, on ignore qui il est, Nick Szabo reste un des suspects" :)

[Frédéric Couchet @fcouchet](#)

Commencer la semaine par un tuto [#blockchain](#) par [@bortzmeyer](#) c'est sympa :) Sa présentation [apr1.org/Lc](#) [#JCSA16](#)



Note de service à mes followers : désolé je vais méchamment flooder ma TL avec du [#jcsa16](#) toute la journée.

[Pierre Beyssac @pbeysac](#)[Johann @adofou](#)

Publication du code source de Bitcoin en 2009. Avec le bloc "genèse". Le premier block de la chaîne. 2011 sortie de Namecoin [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)

Histoire 2009 code source de BitCoin publié [#Genese](#) de création du premier Bloc [#blockchain](#) [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) 2013 sortie de NXT, monnaie sans minage qui n'est pas un fork de Bitcoin, ce qui en fait la 1re dans ce cas.

[Johann @adofou](#)

2013 : Sortie de twister et NXT (monnaie sans minage). Ce dernier n'est pas un fork de bitcoin. Code source réécrit. [#JCSA16](#)



Présentation de [@bortzmeyer](#) sur la [#blockchain](#) [afnic.fr/medias/documen...](#) [#JCSA16](#)

[OpenPony @OpenPony](#)



Enfin 1er article sur Ethereum en 2013 (chaîne stockant des programmes et pas juste des données). 2015 genèse. 2016 début du Hype [#JCSA16](#)

[Johann @adofou](#)



2013 : premier article sur [#ethereum](#) 2015 : genèse de [#ethereum](#) et 2016, ça devient le sujet hype ! [#JCSA16](#)

[OpenPony @OpenPony](#)



[#jcsa16](#) "début 2016 = début du hype" (j'aurais dit mi-2015 même mais c'est parce que [@bortzmeyer](#) lit trop twitter)

[Pierre Beyssac @pbeysac](#)



Aujourd'hui on n'est pas encore sûr de où mènera le [#blockchain](#) [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



Nous sommes en mi 2016 : Plein de dev, plein de chercheurs, plein de start-up. Beaucoup de mouvement autour, pas de "standard" [#JCSA16](#)

[Johann @adofou](#)



[#JCSA16](#) la présentation [#blockchain](#) est super bien menée par [#Bortzmeyer](#)

[mcabdelAbdel @mcabdel](#)



Astuce de [@bortzmeyer](#): Pour avoir une bonne levée de fond, placer le mot clé "Chaîne de bloc" ou "Blockchain" partout dans vos slides [#JCSA16](#)

[Johann @adofou](#)



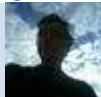
[#jcsa16](#) on va parler de "deux chaînes de blocs intéressantes, [#bitcoin](#) et [#ethereum](#)"

[Pierre Beyssac @pbeysac](#)



Merci [@bortzmeyer](#) d'avoir pensé aux gens qui regardent en streaming ! :) [#JCSA16](#)

[Bruno Tréguier @btreguier](#)



[#jcsa16](#) q du public "je ne comprends pas comment on définit une cohérence de blocs en évolution partout dans le monde au même instant"

[Pierre Beyssac @pbeysac](#)

[Récamier @samiamtimet](#)

[#JCSA16](#) c'est parti. Avec une demi-heure de retard pour moi :{

[Philippe Batreau @pbatreau](#)

Le pdf des slides de [@bortzmeyer](#) sur la [#blockchain](#) [#JCSA16](#) [afnic.fr/medias/document...](#) Que faire de rigolo avec la [#blockchain](#) ?

[Johann @adofou](#)

Question d'un ancien de PSA: "Je ne comprends pas comment on définit une cohérence d'un block en évolue partout dans le monde" [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) rép "en fait ce qui est ordonné ce sont les transactions, il s'agit d'une chaîne de transactions. Regroupement blocs = implém tech"

[Johann @adofou](#)

Réponse : Ce sont les transactions qui sont ordonnées, le regroupement en bloc sont juste là pour aider au bon fonctionnement [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)

Ca [#blockchainise](#) bien déjà entre participant et [@bortzmeyer](#) [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "si vous n'arrivez pas à comprendre du 1er coup, c'est normal, le pb a longtemps semblé impossible à résoudre" "Mérite prix Turing"

[Johann @adofou](#)

[.@bortzmeyer](#) se demande si on peut donner le prix Turing à quelqu'un dont on ne connaît pas l'identité :- [#JCSA16](#)

[OpenPony @OpenPony](#)

Question de [@bortzmeyer](#) : Peut-on remettre le prix Turing à quelqu'un dont on ne connaît pas l'identité ? En parlant de Nakamoto [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "peut-on donner le prix Turing à un auteur anonyme (Nakamoto)" ma suggestion : offrir le prix en argent liquide à venir chercher.



[Récamier @samiamtimet](#)

[#JCSA16 @bortzmeyer](#) : tutoriel [#Blockchain](#)
pic.twitter.com/Eml0vzbMrG



[BIAOU Ramanou @RamanouB](#)

Maintenant [@bortzmeyer](#) parlera de 2 [#blockchain](#) le premier [#bitcoin](#) dont le but est de faire de la cybermonnaie [#JCSA16](#)



Bitcoin est la première chaîne de bloc opérationnelle [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



[Johann @adofou](#)

[#Bitcoin](#) : Première chaîne de blocs opérationnelle. On lui prédit régulièrement sa mort, mais toujours vivant. [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16 #bitcoin](#), "première chaîne de blocs opérationnelle". Sa mort a été annoncée 108 fois à ce jour. Bitcoin en tête en valorisation €.



[Alexandre SIMON @asimonstweets](#)

[#JCSA16](#) by [@AFNIC](#) à [@TelecomPTech](#) J'ARRIVE !!!
pic.twitter.com/vN093jbuvk

	n°	Heure	
	68166	09h50	Here
	837529	09h50	
	2535	10h11	PARIS-EST
	835017	10h16	STRASBOURG
	837531	10h20	METZ
	835763	10h22	EPINAL
	834113	10h27	ST-DIE DES VOSGES
	835079	10h31	LUNEVILLE

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) valo théorique environ 10Mds€, "ce qui comme tout ce qui est financier est du pipeau total, si tt le monde vendait ça s'écroulerait"

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "il y a plein de chaînes de blocs, en choisissant bien le critère de classement chacun peut avoir la sienne en 1er"

[Régis MASSÉ @remasse](#)

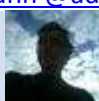
Valorisation actuelle de [#bitcoin](#) évaluée à 10 milliards d'euros [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)

En valorisation, [#bitcoin](#) est en tête, en nb de noeuds, c'est [#ethereum](#) qui est en tête => y a tjrs un critère pr s'autoproclamer #1 [#jcsa16](#)

[Johann @adofou](#)

[#Bitcoin](#) : Valorisation à 10 Milliard d'euros. 80Go de data dans la chaîne. [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

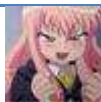
[#jcsa16](#) [#bitcoin](#) chaîne de 80 Go actuellement, ce qui n'est rien pour du [#bittorrent](#) par exemple. Mais trop pour du smartphone ou Rpi.

[Nathalie Chiche @natchiche](#)

@[bortzmeyer](#) Formidable pédagogue pour comprendre simplement (!) la [#blockchain](#) ce matin par @[AFNIC](#) [#JCSA16](#) pic.twitter.com/dR3KonHVgR

[BIAOU Ramanou @RamanouB](#)

[Blockchain.info](#) pour suivre la chaine bitcoin en temps réel [#JCSA16](#)



Question : Pourquoi et comment est définie la taille d'un bloc? [#JCSA16](#) [#blockchain](#)

[Johann @adofou](#)



N'ayant pas créé ma chaîne de blocs, j'essaie de compenser en floodant twitter de blocs de 140c. [#jcsa16](#)
twitter.com/Mo7sen/status/...

[Pierre Beyssac @pbeysac](#)



[#jcsa16](#) "l'heure au sens heure légale n'est pas authentifiée. Ce qui l'est, c'est la suite de transactions, donc horloge abstraite"

[Pierre Beyssac @pbeysac](#)



@[bortzmeyer](#) oublie la [#blockchain](#) LA plus intéressante ... celle de [#duniter](#) !!!

[#monnaie libre](#) [#revenue de base](#) [#JCSA16](#) moul.re/blog/

[vincenttux @vincenttux](#)



@[AFNIC](#) Bonjour, qualité vidéo nickel, mais les slides ne sont pas toujours lisibles, comme ici... [#JCSA16](#)
pic.twitter.com/gXHMXYWHMd

[Bruno Tréguier @btreguier](#)



[#jcsa16](#) "prouver qu'1 transaction a eu lieu à 9h30 précises, ce n'est pas possible. On peut prouver que telle transac précède telle autre"

[Pierre Beyssac @pbeysac](#)



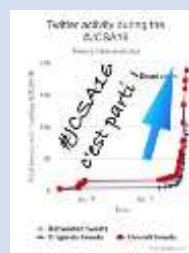
Dans [#bitcoin](#), l'horloge est abstraite : On ne peut pas authentifier l'heure des transactions. Mais juste l'ordre des block et trans [#JCSA16](#)

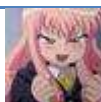
[Johann @adofou](#)



Vu d'ici, on dirait bien que la [#JCSA16](#) by @[AFNIC](#) a commencé... pic.twitter.com/aPI9WlmPUV

[Twest io @Twest_io](#)



[Johann @adofou](#)

Beaucoup de 0 au début du condensat d'une transaction : c'est voulu par la preuve de travail : Beaucoup de calcul pour ce résultat [#JCSA16](#)

[Pascal Vella @pascalvella](#)

Gougnafier a remplacé Mme Michu ? [#JCSA16](#) @[bortzmeyer](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "la chaîne de blocs est vivante" J'espère que @[bortzmeyer](#) n'en a maltraité aucune pour préparer son exposé. [#sociétédeprotection](#)

[Johann @adofou](#)

Les données ne sont pas dans les transactions de [#Bitcoin](#). Elles sont dans un arbre de Merkle à côté. [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) Un bloc [#bitcoin](#) déshabillé par @[bortzmeyer](#) pic.twitter.com/2nFdYegXiv

[Mohsen Souissi @Mo7sen](#)

. @[pbeysac](#) Ta "preuve du travail" se traduit par le nombre de zéros que tu produis, j'ai appris ça de [#bitcoin](#) :-) [#JCSA16](#)

[Régis MASSÉ @remasse](#)

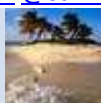
@[asimonstweets](#) A tout à l'heure, on te garde une place assise. [#JCSA16](#) [#Afnic](#)

[Pascal Vella @pascalvella](#)

[#JCSA16](#) en 4ème position on peut faire mieux ? [#Afnic](#) twitter.com/trendinaliaFR/...

[Récamier @samiamtimet](#)

[#jcsa16](#) pour faire du minage sur [#bitcoin](#) faut faire chauffer son cpu. On est récompensé en bitcoin.

[Mohsen Souissi @Mo7sen](#)

Votre mission si vous la voulez bien : passer en tête [#JCSA16](#) !
[@asimonstweets](#) [@AFNIC](#) [twitter.com/trendinaliaFR/...](#)

[Johann @adofou](#)

Événement du week-end sur [#Bitcoin](#) : Division par deux de la récompense pour le minage [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "aujourd'hui vous n'avez quasiment plus aucune chance avec un CPU normal, ni avec un GPU, de trouver un hash [#bitcoin](#)"

[BIAOU Ramanou @RamanouB](#)

Les mineurs récompensés en bitcoins, mais il faut savoir calculer beaucoup de condensa par seconde [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)

Gros raccourci du matin sur [#bitcoin](#) : "la preuve de de travail" (proof-of-work) se mesure par le nb de zéros produits :-)
[#okjesors](#) [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "machine de minage typique : ouverte, baignant dans l'huile (refroidissement), consommant bcp d'électricité".

[OpenPony @OpenPony](#)

Si vous voulez miner du [#bitcoin](#) n'essayez même pas avec un CPU standard (ou même GPU) mais avec des ASIC uniquement [#JCSA16](#)

[Benoit Ampeau @benoitampeau](#)

Désolé les gamers, le GPU ne suffit pas, il faut un ASIC pour miner du bitcoin. [#JCSA16](#)

[Récamier @samiamtimet](#)

[#jcsa16](#) sur une machine ordinaire aucune chance pour miner du bitcoin. Nécessite des ASIC et un prix de l'électricité bas.

[Mathieu Weill @mathieuweill](#)

Division régulière du salaire par deux, face à des tâches toujours plus complexes, le modèle de minage du bitcoin est 100% libéral. [#jcsa16](#)



Tutoriel "La blockchain, des principes de base aux contrats Ethereum" par Stéphane Bortzmeyer [#JCSA16](#)
pic.twitter.com/LJ9bSKleok

[Khaled Koubaa @koubaak](#)[Alexandre Sicard @libricoleur](#)

[#jcsa16](#) "le halving du bitcoin c'était l'événement du week-end, bien plus que la japan expo"

[Bruno Tréguier @btreguier](#)

Des mineurs en Islande ? Je croyais qu'ils étaient tous footballeurs ! :) [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) (j'ai initialement tapé [#bitcoin16](#), oups) "un noeud peut être mineur (insère des blocs) ou pas (se contente de vérifier la chaîne)"

[Régis MASSÉ @remasse](#)

Le minage [#bitcoin](#) est-il bon pour le bilan carbone ? Pas sûr ... [#JCSA16](#) [#Afnic](#)

[Philippe Batreau @pbatreau](#)

la hashocratie du [#bitcoin](#) : une oligarchie de mineurs
[#JCSA16](#) [#blockchain](#)

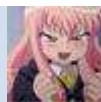
[Mohsen Souissi @Mo7sen](#)

Les "mineurs" [#bitcoin](#) utilisent des CPU très rapides. Ils sont récompensés en BTC. Aucune chance pour un PC ordinaire.
[#JCSA16](#)



[AFNIC @AFNIC](#)

Pour suivre en direct le tuto @bortzmeyer sur la #blockchain à #JCSA16 c'est par ici afnic.fr/fr/l-afnic-en-... #Afnic pic.twitter.com/DleDj8bUe8



[Johann @adofou](#)

Il est rare mais possible que la chaîne se sépare en deux. En cas d'ajout d'un block par deux noeuds au même moment. #JCSA16



[Récamier @samiamtimet](#)

#jcsa16 un nœud #bitcoin peut être mineur (insert des blocs) ou pas (vérifie uniquement)



[Pierre Beyssac @pbeysac](#)

#jcsa16 "commerçant, si vous livrez votre client trop vite, vous risquez que le bloc soit annulé. Attendez un peu qu'il soit confirmé."



[Pierre Beyssac @pbeysac](#)

#jcsa16 "la difficulté de la preuve de travail [nb de 0] est calculée pour qu'il y ait à peu près un bloc toutes les 10 minutes"



[Johann @adofou](#)

Dans ce cas la chaîne sera séparé en deux jusqu'à ce qu'une branche gagne et que l'autre branche soit abandonnée automatiquement #JCSA16



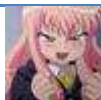
[BIAOU Ramanou @RamanouB](#)

Le minage du Bitcoin permet de trouver le Hash. Mais ne compter pas sur votre CPU de gammer. Il vous faut un ASIC #JCSA16



[Pierre Beyssac @pbeysac](#)

#jcsa16 @bortzmeyer parle de sous-chaînes (pour faire plaisir aux bretons).

[Johann @adofou](#)

Dans un fonctionnement normal, il y aurait les mêmes transactions dans les deux branches temporaire de la chaîne. [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "d'où viennent les 12,5 BTC par bloc" "de nulle part, création monétaire" "pire que la planche à billets ?" "Non pareil"

[Récamier @samiamtimet](#)

[#jcsa16](#) Bitcoin : le système, bitcoin la monnaie. [#Minuscule](#)

[BIAOU Ramanou @RamanouB](#)

Les mineurs de bitcoins gagnent des bitcoins en provenant de nul part, s'ils minent un bloc de chaîne [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)

En +, c concentré sur qq coins de la planète :-)
Faut faire participer les mineurs à la prochaine [#COP21](#) :-)
[#JCSA16](#) [twitter.com/remasse/status...](#)

[Martin T. @mart_e](#)

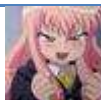
Écouter [@bortzmeyer](#) au [#jcsa16](#) parler de [#bitcoin](#) depuis un petit village Suisse [afnic.fr/fr/l-afnic-en-...](#)
[pic.twitter.com/6380IAKOUe](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "machin a jeté son disque qui contenait 3K BTC"
"abus de langage, les BTC sont dans la chaîne" c'est l'accès à la clé qui est perdu.

[Benoit Ampeau @benoit_ampeau](#)

J'ai l'impression que bcp de participants du [#JCSA16](#) ont des bitcoins dans les yeux après les explications de [@bortzmeyer](#)



[Johann @adofou](#)

Le solde de Bitcoin n'est jamais stocké quelque part, il faut calculer depuis le début de la chaîne. [#JCSA16](#)



[Régis MASSÉ @remasse](#)

Comment gagner des [#bitcoins](#) ? @[bortzmeyer](#) nous dévoile tous les secrets. Mieux que la bourse pour financer mes vacances ! [#JCSA16](#) [#Afnic](#)



[BIAOU Ramanou @RamanouB](#)

Le Bitcoin peut s'échanger contre d'autres monnaies et sur des places de marché. [#JCSA16](#)



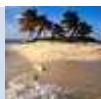
[Récamier @samiamtimet](#)

[#jcsa16](#) Paymium place de marché française pour [#bitcoins](#).



[Philippe Batreau @pbatreau](#)

[#JCSA16](#) [#blockchain](#) @[bortzmeyer](#) @[AFNIC](#) Preuve qu'on travaille. pic.twitter.com/ILEyjTner6



[Mohsen Souissi @Mo7sen](#)

Vous voulez gagner 12.5 BTC (qui viennent de nulle part) par unité de travail, devenez mineurs [#bitcoin](#), mais équipez-vous avant :-) [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "récemment un député a fait un discours demandant l'interdiction du Bitcoin, dark illégal etc" "rien de plus faux, tout est légal"



[BIAOU Ramanou @RamanouB](#)

Des distributeurs Automatiques de billets à partir de vos bitcoins. [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "si vous voulez vous lancer dans le crime, je vous préviens, c'est un travail de professionnel".

[mcabdelAbdel @mcabdel](#)

[#JCSA16](#) Pour bien comprendre de quoi on parle : 1 bitcoin = 587 Euros

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "on n'est pas du tout dans un monde far west mais dans un monde très régulé, comme chq fois qu'il y a de l'argent"

[BIAOU Ramanou @RamanouB](#)

[#Vancouver](#) berceaux des DAB de bitcoins [#JCSA16](#)

[Récamier @samiamtimet](#)

[#jcsa16](#) @[bortzmeyer](#) : "le travail de malfrat est un vrai job. Faut maîtriser sa sécurité informatique"

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) bi-clé (public + privé). adresse [#bitcoin](#) = condensat de la clé publique.

[Johann @adofou](#)

Les transactions [#bitcoin](#) sont signées. Chacun doit avoir une bi-clé. Le condensat de la clé publique est l'adresse [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "certains commerçants prennent des paiements Bitcoin, j'ai testé @[gandi_net](#) par exemple"

[Pascal Vella @pascalvella](#)

SelfT [#JCSA16 pic.twitter.com/xaoNkw24LL](#)

[Récamier @samiamtimet](#)

[#jcsa16](#) [#Bitcoin](#) et M. Michu : le gros problème c'est la gestion des clés.



Les bi-clé de blockchain, évitez que les méchants s'emparent et que les gentilles les perdent @bortzmeyer #JCSA16

[BIAOU Ramanou @RamanouB](#)



Ah voilà Mr Michu est arrivé à #JCSA16 cc @bortzmeyer

[Pascal Vella @pascalvella](#)



Gros problème des blockchains : La gestion des clés! (perte, vol etc...). #JCSA16

[Johann @adofou](#)



Pour ceux qui n'ont pas peur (ou pas compris...) vous pouvez vous faire envoyer votre clé privée sur un support métallique... #JCSA16

[Benoit Ampeau @benoit_ampeau](#)



#jcsa16 "j'ai mon portefeuille sur mon smartphone, j'ai 15 millibitcoins dessus (environ 10€)" "vous me volez mon téléphone, vous les avez"

[Pierre Beyssac @pbeysac](#)



Appel au don de #Bitcoin par @bortzmeyer #JCSA16 pic.twitter.com/CMCscGrNNm

[Johann @adofou](#)



#jcsa16 M. Michu n'a pas de nœud complet mais juste un client léger : wallet (sur un smartphone par exemple)

[Récamier @samiamtimet](#)



#JCSA16 si vous voulez remercier @bortzmeyer pour son exposé, qr code pour virement. pic.twitter.com/gZuZ6Da6Wg

[Pierre Beyssac @pbeysac](#)





Envoyons des bitcoins à [@bortzmeyer](#) à cette adresse
"1HtNJ6ZFuc9yu9u2qAwB4tGdGwPQasQGax" [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



N'hésitez pas à soutenir l'activité [#bitcoin](#) de [@bortzmeyer](#) :
le QR code qui remplace le RIB est à l'écran [#afnic](#) [#JCSA16](#)

[Régis MASSÉ @remasse](#)



[#jcsa16](#) "ce n'est pas le 1er à voler une clé privée qui gagne,
c'est le 1er à l'utiliser pour virer l'argent correspondant"

[Pierre Beyssac @pbeysac](#)



[@remasse](#) [@bortzmeyer](#) Ca devrait pas être la clé "adresse"
de [#afnic](#) plutôt ? ;-) [#jeposelaquestion](#) [#jcsa16](#)

[Mathieu Weill @mathieuweill](#)



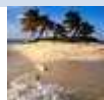
[#jcsa16](#) "le solde d'un compte n'est pas explicitement dans la
chaîne, il faut remonter les transactions de toute la chaîne
pour calculer".

[Pierre Beyssac @pbeysac](#)



[#jcsa16](#) envoyez vos dons en [#bitcoins](#) pour ce super exposé
à [@bortzmeyer](#) en utilisant le QR code affiché.
pic.twitter.com/W9jroWdlqR

[Récamier @samiamtimet](#)



Si vous êtes satisfaits du tutoriel de [@bortzmeyer](#), "envoyez
vos BTC à son adresse", cf. QRcode :-) [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)



[#jcsa16](#) idées idiotes sur BTC "on ne connaît pas Nakamoto"
(vrai mais) je ne connais pas Gutenberg non plus, confiance
ne vient pas de là.

[Pierre Beyssac @pbeysac](#)



[Philippe Batreau @pbatreau](#)

[#JCSA16](#) [#bitcoin](#) [#blockchain](#) Pour envoyer des bitcoin à [@bortzmeyer](#) pic.twitter.com/OYMWoYcFAA



[BIAOU Ramanou @RamanouB](#)

Haha [@bortzmeyer](#) se lâche sur les idées idiotes entendues sur le bitcoin [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "ça ne durera pas" => mort prédite 108 fois "C'est illégal" => "tout ce qui n'est pas explicitement interdit est autorisé"



[Récamier @samiamtimet](#)

[#jcsa16](#) [@bortzmeyer](#) tord qq idées reçues sur [#bitcoin](#) : ça ne durera pas, c'est illégal (zone grise : déclaration des revenus)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "monnaie virtuelle" "c'est le cas depuis Philippe Le Bel" "il avait des arg. très forts pour les gens qui n'étaient pas d'accord".



[OpenPony @OpenPony](#)

La monnaie virtuelle existe depuis Philippe Le Bel : depuis que la monnaie a la valeur que le roi lui donne et non plus l'or contenu [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

C'est de l'humour bien sûr :-). Ni [@AFNIC](#) ni [@bortzmeyer](#) ne sont rémunérés pour les prez [#JCSA16](#) :-)
twitter.com/pbatreau/status...



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "cela ne correspond pas à la production réelle dans le vrai monde" "idem high frequency trading" :)



[mcabdelAbdel @mcabdel](#)

[#JCSA16](#) On vient d'apprendre que les Bitcoins ne sont pas soumis à l'impôt.... hé hé hé



[BIAOU Ramanou @RamanouB](#)

Idées idiotes : [#OnNeConnaitPas](#) [#CaNeDureraPas](#)
[#CestIllégal](#) [#CestVirtuelle](#) [#PasDuVraiTravail](#) [#CestAnonyme](#)
[#JCSA16](#)



[OpenPony @OpenPony](#)

[#bitcoin](#) n'est pas anonyme : tout est public et traçable. Il est fourni du pseudonymat. [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "c'est anonyme" par défaut, tout est traçable. "pas d'anonymat à part dans les articles de Paris Match ou les discours des députés"



[BIAOU Ramanou @RamanouB](#)

Bitcoin n'est pas vraiment anonyme [#JCSA16](#)



[Johann @adofou](#)

Des idées idiotes répandu sur [#bitcoin](#) [#JCSA16](#)
pic.twitter.com/Qg62HncA34



[OpenPony @OpenPony](#)

Si vous voulez devenir criminel, [@bortzmeyer](#) confirme qu'il faut aller à l'école avant ! [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

[@RamanouB](#) Euh, [#JCSA16](#) ne fait pas partie des idées idiotes :-)



[Récamier @samiamtimet](#)

[#jcsa16](#) Bitcoin : pas d'anonymat, mais un pseudonymat.



[Nekrofage666 @Nekrofage666](#)

[#JCSA16](#) Est-ce que l'on pourra revoir/télécharger la vidéo sur la Bitcoin/Blockchain par Mr Bortzmeyer ? merci



[#jcsa16](#) reste 5 mn pour parler d'ethereum (ça va être dense)

[Pierre Beyssac @pbeysac](#)



[#jcsa16](#) "ethereum a un code qui part de zéro" (pas un fork de bitcoin)

[Pierre Beyssac @pbeysac](#)



[#jcsa16](#) Autre chaîne de blocs : [#ethereum](#) .

[Récamier @samiamtimet](#)



[#ethereum](#) en 5 min ? [@bortzmeyer](#) peut le faire !! Mais nous aurons mal à la tête ! [#JCSA16](#)

[OpenPony @OpenPony](#)



[#ethereum](#) : Code fait de zéro, chaîne généraliste. Séparation de la spécification et de la mise en oeuvre. Ethereum à une monnaie [#JCSA16](#)

[Johann @adofou](#)



[#jcsa16](#) "ethereum a une spéc séparée du code, et plusieurs implémentations. Peut servir à autre chose que la monnaie"

[Pierre Beyssac @pbeysac](#)



[@Mo7sen](#) Il me faut mettre un "." avant [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



Et [@bortzmeyer](#) tord le cou à beaucoup d'idées reçues autour du [#bitcoin](#)
[@AFNIC](#) [#JCSA16](#) [#blockchain](#) pic.twitter.com/9mcKLFkqJz

[Vidal Chriqui @vidal007](#)



[#jcsa16](#) Ethereum : chaîne généraliste. Mais possède une monnaie : l'ether.

[Récamier @samiamtimet](#)



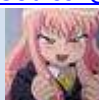
[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "ethereum a du minage, preuve de travail". "2e en capitalisation mais loin derrière Bitcoin"



[Mohsen Souissi @Mo7sen](#)

Principes de [#ethereum](#) :
- code fait de zéro, chaîne généraliste, séparation spec et mise en oeuvre, a une monnaie (l'ether) [#JCSA16](#) (1/2)



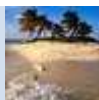
[Johann @adofou](#)

Le code d'[#ethereum](#) est créé spécifiquement pour être dur à implémenter dans un ASIC pour donner une chance au PC standard [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) et maintenant un bloc [#ethereum](#) déshabillé à son tour pic.twitter.com/W2p44WW1Ks



[Mohsen Souissi @Mo7sen](#)

Principes de [#ethereum](#) :
Plusieurs concepts en commun avec [#Bitcoin](#) (2/2) [#JCSA16](#) [#PT](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) Ethereum : stocker du code dans la chaîne. Possède un langage de Turing



[Johann @adofou](#)

Stocker des chose dans la chaîne : déjà un langage limité dans Bitcoin. [#Ethereum](#) à au contraire un langage de Turing. [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

On survit encore de justesse :) [#jcsa16](#)
twitter.com/Turblog/status...



[Johann @adofou](#)

Les programmes sont exécutés par tout les noeuds de la chaîne. Tout est possible. Conséquence sur la sécurité et fiabilité [#ethereum](#) [#JCSA16](#)



Au contraire de [#bitcoin](#), [#ethereum](#) est un véritable langage de turing (niveau d'un langage d'assemblage). [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)



Autre solution : les sidechains (rootstock ou blockstack) [#JCSA16](#)

[Johann @adofou](#)



.@[bortzmeyer](#) vient de nous expliquer que finalement la taille compte [#JCSA16](#)

[Sebdraven @Sebdraven](#)



Trop bonne la photo de @[adofou](#)... on dirait que @[bortzmeyer](#) est en impression sur l'affiche @[AFNIC](#) [#JCSA16](#) ! pic.twitter.com/R6zgCcYbTP

[Alexandre SIMON @asimonstweets](#)



Regardez la 2ème partie de la présentation de @[bortzmeyer](#) sur [#blockchain](#) à 11h20 afnic.fr/fr/l-afnic-en-... [#JCSA16](#) pic.twitter.com/mfV2O1sg6Y

[Pascal Vella @pascalvella](#)





Twest io @Twest io

Pas de doute... ça cause [#blockchain](#) et [#bitcoin](#) avec [@bortzmeyer](#) à la [#JCSA16](#)
[#wordscld](#)
twest.io/jcsa16/ pic.twitter.com/bY06Rx0RaQ



Victor hery @victorhery

Flash nécessaire pour suivre le live de [#JCSA16](https://afnic.fr/fr/livestream) : (afnic.fr/fr/livestream) @AFNIC



Pierre Beyssac @pbeysac

#jcsa16 reprise avec @bortzmeyer sur ethereum. Ch blocs "Tout ce qui a besoin de vérif publique, sans autor. centrale" registre, cadastre...



Johann @adofou

Qu'est-ce qui est bien adapté à la chaîne de bloc? Tout ce qui a besoin de vérification publique (sans autorité central).
#JCSA16



Pierre Beyssac @pbeysac

#jcsa16 "si c'est pair à pair, ce n'est plus du DNS"



Willy Manga @ongolaboy

ça peut toujours être intéressant de suivre [#JCSA16](#) voire en streaming comme a dit qqn ici :)



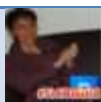
OpenPony @OpenPony

Usages de [#blockchain](#) registres, cadastres, monnaies (notamment micro-paiements) [#JCSA16](#)



Johann @adofou

Bullshit Bingo de la [#JCSA16](#). Mot "Uberisation" à cocher sur votre carton ! :-)



Récamier @samiamtimet

#JCSA16 retour de la pause café pic.twitter.com/n6yfiEU6Aw



Récamier @samiamtimet

#JCSA16 la chaîne de blocs : le plus cher calculateur public
[#BlockChain](#)



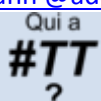
Johann @adofou

Ce qui n'est pas adapté à la chaîne de blocs? Calculateur le plus lent et cher du monde : Pas de long calcul ou de gros stockage [#JCSA16](#)



Johann @adofou

Question : "Il y a t-il un système de "snapshot" pour ne pas devoir calcul depuis le début de la chaîne?" [#JCSA16](#)



qui a TT ? @quiaTT

TT update. Vous savez qui a mis [#JCSA16](#) en TT ? Moi oui. Bien joué @AFNIC. Parole de robot.



Johann @adofou

Réponse : Il y a des optimisations, surtout dans Etheureum, qui permet de faire gagner du temps. Mais c'est propre à l'implémentat° [#JCSA16](#)



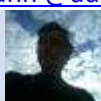
Récamier @samiamtimet

#JCSA16 les enveloppes Soleau (?) de retour sur la scène
[#BlockChain](#)



Johann @adofou

BINGO. Combo Java + SQL + transaction bancaire dans la même phrase. @bortzmeyer [#JCSA16](#)



Pierre Beyssac @pbeysac

[#jcsa16](#) comparaison entre l'"empreinte écologique" de la blockchain et celle des couches-surcouches-sursurcouches de Java & regul banques :-P



[Récamier @samiamtimet](#)

[#JCSA16](#) longs calculs et coût écologique ne sont pas spécifiques à [#Blockchain](#). Les transactions financières classiques st gourmandes aussi



[BIAOU Ramanou @RamanouB](#)

La chaine est le plus lent et le plus cher calculateur du monde inadaptée pour Long Calculs et Gros stockages, slides [@bortzmeyer #JCSA16](#)



[AFNIC @AFNIC](#)

Vous pouvez poser vos questions [#blockchain](#) à [@bortzmeyer](#) via Twitter en utilisant [#JCSA16](#) ! Live toujours sur [afnic.fr/fr/l-afnic-en...](#)



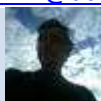
[Johann @adofou](#)

Terminologie : Un smart contract est un programme. Ecrit par un programmeur. Puis compilé dans le langage EVM. [#JCSA16 #ethereum](#) 1/2



[Johann @adofou](#)

2/2 Ensuite ce programme est exécuté par tout les noeuds, et chacun doivent trouver le même résultat. [#JCSA16 #ethereum](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) contrat ethereum : compilé come tout programme, puis exécuté par EVM = ethereum virtual machine.



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) tous les noeuds exécutent le contrat et doivent trouver le même résultat. Le contrat peut manipuler de l'argent (envoyer, recevoir)



[Johann @adofou](#)

Un contrat = Programme. Programme = Bug possible. Donc bug possible dans un contrat. Que ce passe t-il alors? [#JCSA16 #ethereum](#)



[Vidal Chriqui @vidal007](#)

La définition d'un [#smartcontract](#) par [@bortzmeyer #ethereum @AFNIC #JCSA16 #blockchain](#) [pic.twitter.com/cin2TTEGF1](#)





[OpenPony @OpenPony](#)

contrat [#ethereum](#) = programme donc logiciels ont des bogues. Langage fonctionnel ? vérification formelles ?
[#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) les problèmes des "contrats" dans [#Ethereum](#) : les bogues et la sécurité : DDOS



[Johann @adofou](#)

Donc un contrat présente des problèmes de sécurité, puisque exécuté par tout les noeuds. Par exemple DDOS par une boucle infini [#JCSA16](#)



[OpenPony @OpenPony](#)

Si contrat avec boucle sans fin: fait péter [#ethereum](#) --> protection par l'essence qui propulse les contrats et se paie en ether [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

Bien que les "contrats intelligents" (smart contracts) soient des contrats et intelligents, ils pvnt ê bugés !
[#onnousauraitmenti #JCSA16](#)



[Johann @adofou](#)

Protection de [#ethereum](#) : Protection par "l'essence" (qui propulse les contrats. Il faut payer le calcul). Rien n'est gratuit
[#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "quand le réservoir est vide, le contrat s'arrête : plus d'essence"



[Récamier @samiamtimet](#)

[#JCSA16](#) Pour se protéger contre bogues et sécurité : l'essence. Payer pour exécuter son contrat. Plus d'essence : le programme s'arrête.



[Laurent Toutain @ltn22](#)

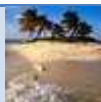
l'ethereum précède l'essence? @[bortzmeyer](#) [#JCSA16](#)



[Johann @adofou](#)

Exemple du principe de l'essence avec [#ethereum](#) [#JCSA16](#)
pic.twitter.com/ewmp2luGQn





[Mohsen Souissi @Mo7sen](#)

Les "smart contracts" de [#ethereum](#) ne st finalement pas si propres que ça : ils utilisent des éner. fossiles, de l'essence !
[#JCSA16](#) [#ecolo](#)



[OpenPony @OpenPony](#)

Avant de lancer un programme, il faut provisionner suffisamment d'essence mais impossible à prévoir à l'avance
[#JCSA16](#)



[Benoit Ampeau @benoit_ampeau](#)

"Mad max style", on doit payer en essence [#JCSA16](#)



[Vidal Chriqui @vidal007](#)

.@[bortzmeyer](#) nous parle de la sécurité des [#smartcontracts](#) [#ethereum](#) et du mécanisme de "gas"
[@AFNIC](#) [#JCSA16](#) pic.twitter.com/czJosokds1



[OpenPony @OpenPony](#)

Un contrat doit être sûr et vérifié par utilisateur : doit donc être simple à analyser [#JCSA16](#)



[Johann @adofou](#)

Pourquoi "smart contract" est un mauvais terme? Parcequ'un contract doit être sur et vérifiable. Impossible! [#JCSA16](#)



[BIAOU Ramanou @RamanouB](#)

Très difficile d'écrire des programmes (Contrats) sans bugs by @[bortzmeyer](#) [#JCSA16](#)



L'EVM exécute du code machine, pas le code source, la vérification du code source ne suffit pas. [#JCSA16](#)

[OpenPony @OpenPony](#)



[#JCSA16](#) un contrat Ethereum doit être sûr et doit être vérifié par les utilisateurs (ils paient l'essence pour l'exécuter)

[Récamier @samiamtimet](#)



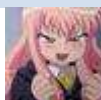
Donc un contrat doit être simple. Dumb contract serait un terme plus adapté. En prime EVM exécute du code machine [#ethereum](#) [#JCSA16](#)

[Johann @adofou](#)



"La complexité est l'ennemi de la sécurité"
[@bortzmeyer](#) sur les [#smartcontracts](#) [#ethereum](#)
[#JCSA16](#) [@AFNIC](#) pic.twitter.com/1Xclia9Egp

[Vidal Chriqui @vidal007](#)



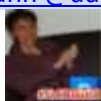
Terminologie : DAO (Decentralized Autonomous Organisation). Une entité stockée sur une chaîne. [#ethereum](#) [#JCSA16](#)

[Johann @adofou](#)



La DAO est une organisation sans RGS, sans intervention humaine, protégée des passions humaines et arbitraire du pouvoir [#JCSA16](#) [#ethereum](#)

[Johann @adofou](#)



[#JCSA16](#) [@bortzmeyer](#) présente la notion de DAO.
Decentralized Autonomous Organisation. Entité stockée sur la chaîne.

[Récamier @samiamtimet](#)



En théorie, le but d'une DAO est de donner une sécurité des utilisateurs pour le protéger des arbitraires [#JCSA16](#)

[OpenPony @OpenPony](#)



[#jcsa16](#) DAO = decentralized autonomous organisation.
"exemple registre de noms de domaine, but DAO : éviter des saisies type scihub.io etc"

[Pierre Beyssac @pbeysac](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) bug contrat ethereum, on fait quoi ? On ne peut pas faire un procès à un programme.



[OpenPony @OpenPony](#)

Quel recours en cas de bogue dans la DAO ? [#JCSA16](#)



[Johann @adofou](#)

Oui mais si une DAO cafouille, quels recours? Débat sur sujet en cours. Très intéressant à suivre d'après [@bortzmeyer](#) [#JCSA16](#) [#ethereum](#)



[Johann @adofou](#)

Une DAO... nommé DAO. C'est un fond d'investissement: on y met des ethers, des gens proposent des projects, les investisseurs votent [#JCSA16](#)



[OpenPony @OpenPony](#)

The DAO est une DAO particulière de fond d'investissement qui a récolté 100 millions d'euros mais avec plusieurs bugs [#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) The DAO est 1 DAO particulière. C'est un fonds d'investissement qui a récolté 100 M€ en ethers.



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) The DAO a récupéré l'équivalent de 100 M€, le plus gros crowdfunding de l'histoire. Bogue : un voleur a emporté 1/3 des fonds.



[Johann @adofou](#)

Gros succès : DAO à récolté un total de 100M€ d'investissements! Mais il y avait plusieurs bug dans le contrat... [#JCSA16](#) [#ethereum](#)



[OpenPony @OpenPony](#)

Un bug a permis le vol d'un tiers du contrat de The DAO malgré les relectures [#JCSA16](#)



[Johann @adofou](#)

Résultat : Un voleur a utilisé plusieurs bug et à pu emporter 1/3 des 100M€. Malgré relecture et audits du code [#JCSA16](#) [#ethereum](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) Une [#bogue](#) dans le contrat de The DAO a permis à 1 voleur de se tirer avec le 1/3 des fonds !!



[#ethereum](#) vol possible grâce aux bogues. [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



@[bortzmeyer](#) et les médias, c'est une belle histoire ;) [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



[#jcsa16](#) un langage qui ne permettrait d'écrire que des programmes sans bug est impossible (au sens Turing).

[Pierre Beyssac @pbeysac](#)



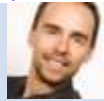
Des questions de haut vol, posées à @[bortzmeyer](#) dans la salle et sur le chat [#JCSA16](#) [#blockchain](#)

[Mohsen Souissi @Mo7sen](#)



[#jcsa16](#) le bug n'était pas dans ethereum mais dans un contrat ethereum particulier.

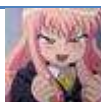
[Pierre Beyssac @pbeysac](#)



Inauguration du [#Snapchat](#) [#Afnic](#) au [#JCSA16](#) avec un snap de @[bortzmeyer](#) [#blockchain](#) cherchez le compte [afnic.fr](#) [pic.twitter.com/GRH30gcMmK](#)

[Pascal Vella @pascalvella](#)



[Johann @adofou](#)

Suite à ce vol, un débat a été lancé sur [#ethereum](#) : Doit-on modifier le code source pour empêcher le voleur de retirer ses fonds? [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) réflexions sur la "gouvernance" ethereum. (attention pas comme souvent au sens "les gouvernements voudraient mettre la main dessus")

[Johann @adofou](#)

Débat de fond : La "Gouvernance" de la chaîne de bloc. Gouvernance dans le sens "prise de décision". [#JCSA16](#) [#ethereum](#)

[Khaled Koubaa @koubaak](#)

Un débat intéressant autour de la "gouvernance" de la chaîne [#blockchain](#) [#JCSA16](#) pic.twitter.com/mOkvX60ELg



[@aeris22](#) C'est tout de même un bug :) [#JCSA16](#)

[OpenPony @OpenPony](#)[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "que faire après le vol de The DAO ?" fork de chaîne. soft fork (le code continue à marcher) ou hard fork (tout mettre à jour) ?

[Récamier @samiamtimet](#)

[#JCSA16](#) Que faire après un tel vol ? Fork de la chaîne.

[Mathieu Weill @mathieuweill](#)

Gros potentiel de cross community working group là... et je m'y connais... [#jcsa16](#) twitter.com/adofou/status/...

[OpenPony @OpenPony](#)

fork: coupure de chaîne, soft fork: transac ex-valides refusées, vieux code fonctionne, hard fork: tout mettre à jour [#JCSA16](#)



[#HardFork](#) je ne connaissais pas Euh ;) [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



Il est proposé dans la salle d'utiliser médiation plutôt que gouvernance [#JCSA16](#)

[OpenPony @OpenPony](#)



Une spectatrice propose "Consensus" plutôt que "Gouvernance". [#JCSA16](#) [#ethereum](#)

[Johann @adofou](#)



[#JCSA16](#) Grand débat autour de la "gouvernance" de la chaîne après un accident tel que le vol de 1/3 des fonds

[Récamier @samiamtimet](#)



[#jcsa16](#) [@bortzmeyer](#) compare hardiment la situation de fork possible ethereum et le [#brexit](#) (50% contents, 50% mécontents)

[Pierre Beyssac @pbeysac](#)



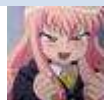
[#jcsa16](#) "empêcher les minoritaires furieux de se barrer" :-D [#démocratie](#)

[Pierre Beyssac @pbeysac](#)



[#JCSA16](#) [@bortzmeyer](#) hard fork et soft fork au service de la gouvernance de la chaîne [#blockchain](#) [@AFNIC](#)
pic.twitter.com/ufz2FVOvb4

[Philippe Batreau @pbatreau](#)



Langage le plus utilisé pour écrire des contrats dans [#ethereum](#) : Solidity [#JCSA16](#)

[Johann @adofou](#)



@adofou je crois que @natchiche proposait le terme "médiation" #JCSA16

[Pascal Vella @pascalvella](#)



#Solidity : principal langage des contrats. impératif de haut niveau, compilé en EVM avec quelques primitives #JCSA16

[OpenPony @OpenPony](#)



#JCSA16 #Ethereum the gory details : le langage #Solidity

[Récamier @samiamtimet](#)



#jcsa16 "le code source" Langage "Solidity", compilé en EVM. Ques fonctions prédéfinies (comme send pour envoyer argent)

[Pierre Beyssac @pbeysac](#)



#Solidity langage impératif pour l'écriture des contrats #Blockchain #JCSA16

[BIAOU Ramanou @RamanouB](#)



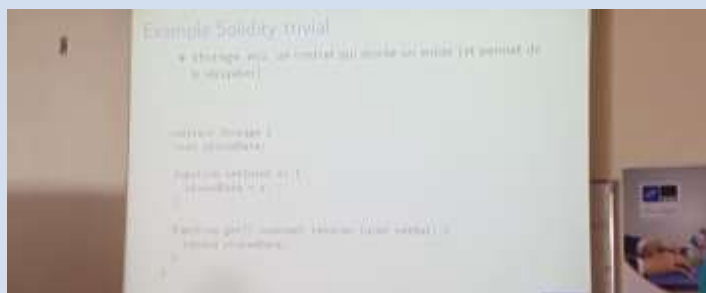
Débat philosophique et constitutionnaliste sur la qualification de la majorité nécessaire pour consensus ds les "contrats ethereum" #JCSA16

[Mohsen Souissi @Mo7sen](#)



Exemple très simple de code #Solidity #Ethereum #JCSA16 pic.twitter.com/Dxfd2tU2Jj

[Johann @adofou](#)



#hardfork concept by @bortzmeyer #JCSA16 pic.twitter.com/b4MOqfGXij

[Pascal Vella @pascalvella](#)





Storage stocke un entier et permet de le récupérer. Get récupère l'entier et Send le renvoie [#JCSA16](#)

[OpenPony @OpenPony](#)



[#jcsa16](#) Beaucoup de regrets de n'être pas parmi vous aujourd'hui, trop loin de Paris... Salut à tous...

[Michel Guillou @michelguillou](#)



[#JCSA16](#) geth implémentation de [#Ethereum](#) la plus répandue

[Récamier @samiamtimet](#)



[#Solidity](#) is one of programming languages for the [#blockchain](#) presented at the [#JCSA16](#)
pic.twitter.com/NEIMPKEGV2

[Khaled Koubaa @koubaak](#)



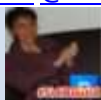
[#jcsa16](#) plusieurs mises en oeuvre d'ethereum, la plus répandue est en Javascript : geth.

[Pierre Beyssac @pbeysac](#)



J'ai trouvé des bitcoins dans mes poches sans même le savoir, merci [#JCSA16](#)

[Lézard Impérial @Lezard Imperial](#)



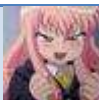
[#JCSA16](#) le way : 10 puissance -18 d'un ether.

[Récamier @samiamtimet](#)



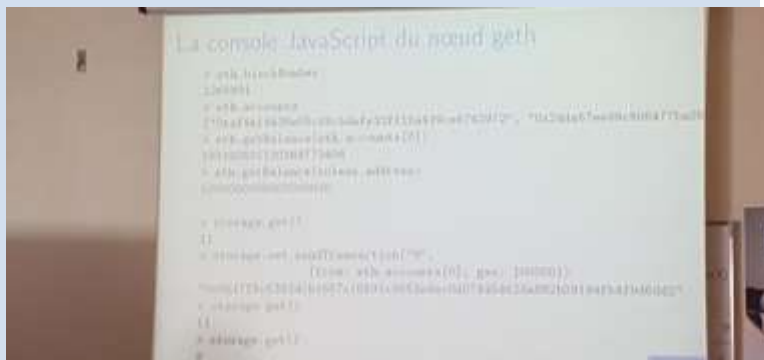
[#jcsa16](#) taille maximum d'un entier [#ethereum](#) : 256 bits.

[Pierre Beyssac @pbeysac](#)



Johann @adofou

Console Javascript du noeud geth [#ethereum](#) [#JCSA16](#)
pic.twitter.com/1h498j3iCE



Pierre Beyssac @pbeysac

La console geth. [@bortzmeyer](#) [#JCSA16](#)
pic.twitter.com/3oieZI3Tw0



Récamier @samiamtimet

[#JCSA16](#) changer l'état de la chaîne de blocs nécessite de payer de l'essence.



Philippe Batreau @pbatreau

Si vous voulez coder en javascript un noeud geth de la chaîne
[#JCSA16](#) [@bortzmeyer](#) [@AFNIC](#) [#blockchain](#)
pic.twitter.com/hfzbOEIfta





Vidal Chriqui @vidal007

.@bortzmeyer nous dissèque un [#Smartcontract](#) [#ethereum](#) écrit en [#Solidity](#)
[#JCSA16](#) @AFNIC [#blockchain](#) [pic.twitter.com/CdtcT2fdFO](#)



BIAOU Ramanou @RamanouB

@bortzmeyer donne du sourire aux geeks avec [#Solidity](#) au [#JCSA16](#)



Pierre Beyssac @pbeysac

[#jcsa16](#) "si je suis radin et spécifie un prix ridicule pour l'essence, aucun mineur ne voudra exécuter ma transaction"



Récamier @samiamtimet

[#JCSA16](#) pour un contrat simple, le compilateur est capable de calculer le "volume" d'essence nécessaire.



Mathieu Weill @mathieuweill

Qui dit prix de l'essence sur Ethereum dit potentiel de taxe non ? [#jcsa16](#) [#grospotentiel](#)



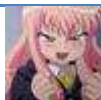
Récamier @samiamtimet

[#JCSA16](#) le prix de l'essence en ether dépend de l'offre et de la demande



Mohsen Souissi @Mo7sen

Jargon [#ethereum](#) : [#ether](#), [#essence](#), [#électricité](#), [#stockage](#), [#mineurs](#)... C bcp de logistique et transport & énergie tt ça...
[#JCSA16](#)



Question troll sur le chat : Est-ce que Solidity porte bien son nom? [#JCSA16](#) [#ethereum](#)

[Johann @adofou](#)



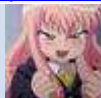
[#JCSA16](#) "La chaîne n'oublie rien". [#Blockchain](#)

[Récamier @samiamtimet](#)



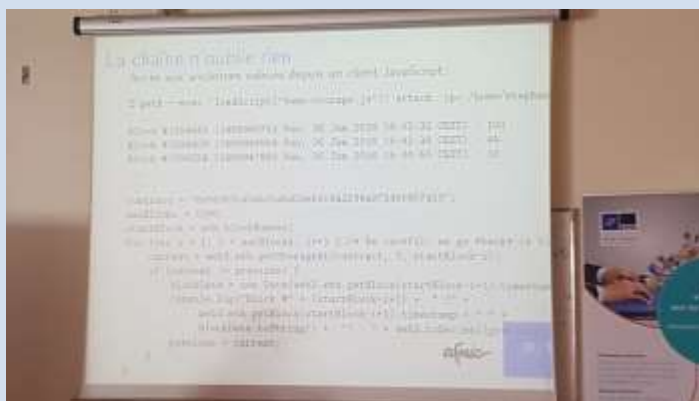
[#jcsa16](#) "le langage Solidity porte-t-il bien son nom ?" :-D question de ou relayée par [@Mo7sen](#)

[Pierre Beyssac @pbeysac](#)



La blockchain n'oublie rien ! [#JCSA16](#) [#ethereum](#)
pic.twitter.com/L6m6YFrS5h

[Johann @adofou](#)



Pas de droit à l'oubli... [#JCSA16](#) twitter.com/adofou/status/...

[Mathieu Weill @mathieuweill](#)



Les fonctions comme send peuvent échouer : tester le code n'est pas obligatoire... [#JCSA16](#)

[OpenPony @OpenPony](#)



Sécurité de [#Solidity](#) : Langage impératif : difficile de raisonner dessus. les fonctions peuvent échouer. [#JCSA16](#) [#ethereum](#)

[Johann @adofou](#)



[#JCSA16](#) Solidity langage impératif. Difficile de raisonner dessus.

[Récamier @samiamtimet](#)



[#jcsa16](#) "il faut tenir compte des codes retour" cas typique de "send". Maintenant Solidity fait un warning si on ignore, avant : rien.

[Pierre Beyssac @pbeysac](#)

[Situnas @ParathorO](#)

[#JCSA16](#) comme il y a deux milles, les Oliviers, les gencives latives

[Johann @adofou](#)

Sécurité de [#Solidity](#): Tester le code de retour n'est pas obligatoire. Un contrat peut en appeler un autre... ! [#JCSA16](#) [#ethereum](#)

[Mohsen Souissi @Mo7sen](#)

Il faudrait instaurer "Le droit au silence de l'Ether" :-)
[#JCSA16](#) [twitter.com/mathieuweill/s...](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) un contrat peut en appeler un autre mais c'est dans une autre transaction. send exécute un contrat s'il y en a un à la destination.

[Vidal Chriqui @vidal007](#)

"Le langage [#Solidity](#) porte-t-il bien son nom ?"
Jolie question posée à [@bortzmeyer](#) et relayée par [@Mo7sen](#)
[#JCSA16](#) [#blockchain](#) [@AFNIC](#)

[Johann @adofou](#)

...Qui va généré une autre transaction. Même si la première échoue, la seconde transaction restera [#JCSA16](#) [#ethereum](#)

[Johann @adofou](#)

Sécurité de [#Solidity](#) : Pas de distinction compte/contrat. Si fonction pas réentrante, l'état peut changer pendant!
[#JCSA16](#) [#ethereum](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "c'est pas vraiment des surprises, c'était dans la doc" (slogan Perl assez classique) mais on se fait avoir facilement.

[OpenPony @OpenPony](#)

Modification de registre de nom de domaine par [@bortzmeyer](#) en 3 slides à venir ! [#JCSA16](#)

[Récamier @samiamtimet](#)

[#JCSA16](#) un registre de noms de domaines en 3 slides
[#Ethereum](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) [@bortzmeyer](#) cite qq'un "on pourrait remplacer ICANN par un contrat ethereum de 3 lignes" "pas tout à fait qd même" [#ouf](#)

[BIAOU Ramanou @RamanouB](#)

Maintenant @[bortzmeyer](#) se lance dans : "Comment remplacer un Registre de nom de domaine en 3 Slides"
[#JCSA16](#)

[Philippe Batreau @pbatreau](#)

[#JCSA16](#) [twitter.com/RamanouB/statu...](#)

[Vidal Chriqui @vidal007](#)

Les problèmes de sécurité des [#smartcontracts](#) [#ethereum](#) écrits en [#solidity](#)

Par @[bortzmeyer](#)

[#JCSA16](#) @AFNIC [pic.twitter.com/Exy8J8T97F](#)

[Récamier @samiamtimet](#)

[#JCSA16](#) l'Icann peut être écrit en 3 lignes de code [#Ethereum](#)
[#Joke](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) @[bortzmeyer](#) présente un contrat pour gérer un registre de nom. Réservation, whois, transfert, destruction, gérant sans privilège.

[Khaled Koubaa @koubaak](#)

1 Szabo = 10 puissance -6 de Ether [#ethereum](#) [#blockchain](#)
[#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)

Un registre de noms en [#Solidity](#), c'est un exemple d'application [#Ethereum](#)

Est-ce suffisamment solide tout ça ?

[#JCSA16](#)

[Laurent Toutain @ltn22](#)

[#JCSA16](#) après l'uberisation des notaires, l'uberisation de l'AFNIC? @[bortzmeyer](#)

[OpenPony @OpenPony](#)

L'historique d'un nom de domaine devient accessible à tous
[#JCSA16](#)



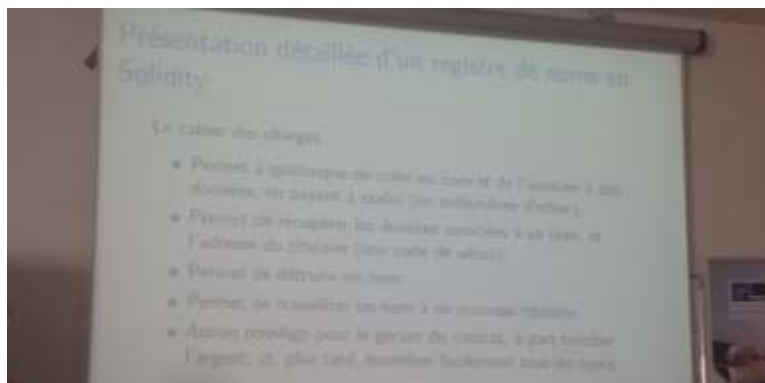
[Récamier @samiamtimet](#)

[#JCSA16](#) écrire une concaténation de chaînes de caractères en [#Solidity](#) c'est galère



[Khaled Koubaa @koubaak](#)

Cahier des charges pour écrire un registre des nom en [#Solidity](#) [#JCSA16](#) [#blockchain](#) pic.twitter.com/DRxDSMDfOi



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) les mappings de Solidity renvoient toujours une valeur, vide le cas échéant. Déroutant pour les Pythonistes/Rubyistes.



[Mohsen Souissi @Mo7sen](#)

L'unicité du "registre en solidity" [#ethereum](#) est garantie par la règle PAPS. Ça règle le problème de l'homonymie. [#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) [@bortzmeyer](#) s'est amusé à ré-écrire l'[@AFNIC](#) en qq lignes de Solidity [#Ethereum](#)



[Pascal Vella @pascalvella](#)

Il reste 20 minutes pour poser vos questions à [@bortzmeyer](#) [#JCSA16](#) afnic.fr/fr/l-afnic-en-... [#blockchain](#) pic.twitter.com/vfE3DPMMYT





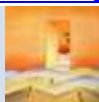
[Pierre Beyssac @pbeysac](#)

[#JCSA16](#) début du code d'[@AFNIC](#) v2 (ou AR41 v3 ?) par [@bortzmeyer](#) pic.twitter.com/ffKsO4SFC9



[Mohsen Souissi @Mo7sen](#)

[@RamanouB](#) non, il évalue les "faiblesses de la concurrence" :- [#JCSA16](#) [@bortzmeyer](#)



[Ivan Diego Mesequer @THD_IT](#)

Je crois que je vais rendre l'écoute des conférences/interventions de [@bortzmeyer](#) obligatoire pour mes fils

[#JCSA16](#)



[Hasni KHABEB @HasniSEO](#)

Avec [@bortzmeyer](#) Présentation détaillée d'un registre de noms en [#Solidity](#) [#JCSA16](#) pic.twitter.com/4ifwvgeiA0



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) Solidity garantit qu'une valeur est initialisée à 0/false/vide etc.



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "le code réel commence par tester que la valeur payée est supérieure au prix, là c'est du code raccourci pour les slides"



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) [@bortzmeyer](#) explique comment avoir des noms de domaine gratuits avec son code simplifié :)



[Mohsen Souissi @Mo7sen](#)

Non [@bortzmeyer](#) ne ré-écrit pas le code d'un TLD en [#Solidity](#). Il explore les limites et faiblesses de la concurrence :- [#PoC](#) [#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) avec un 'throw' on pompe toute l'essence d'un contrat



[OpenPony @OpenPony](#)

Quand on toutit sur [#blockchain](#) et [#ethereum](#) à [#JCSA16](#) : on est add par tous les robots sur tout un tas de listes...



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "il faut être le titulaire pour modifier les données, le NIC lui-même ne l'a pas" "son seul privilège est de toucher l'argent"



[Vidal Chriqui @vidal007](#)

Comment réécrire l'[#afnic](#) et la gestion des noms de domaine dans [#ethereum](#)
[@bortzmeyer](#) [#JCSA16](#) [#blockchain](#)
pic.twitter.com/t6ObfF8hPn



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "seul le titulaire peut transférer, le NIC ne peut pas"



[Johann @adofou](#)

Code [#Solidity](#) pour écrire un service de nom de domaine dans [#ethereum](#) [#JCSA16](#) pic.twitter.com/ZZNHieWI5Y



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) `sendTransaction("icann", "127.0.53.53", ...)`

[Mathieu Weill @mathieuweill](#)

Je note que [@bortzmeyer](#) est surtout en train d'ubériser les registrars, plutôt que [@AFNIC #jcsa16](#) [#ceciestjusteunexercice](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) dans la réalité on n'utilisera pas la console mais on fera du JSON RPC :) (...)

[Récamier @samiamtimet](#)

[#JCSA16](#) [@bortzmeyer](#) démontre qu'un registre de noms de domaine peut être une DAO

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "l'essence n'apparaît jamais explicitement dans la chaîne, son existence suivant volume & prix est dépensée en ethers"

[Bruno Tréguier @btreguier](#)

Remarquables présentations de [@bortzmeyer](#) ce matin à [#JCSA16](#), sur la [#blockain](#), le [#bitcoin](#), [#Ethereum](#), les [#DAO](#), etc.

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "je vais bien séparer chaîne de blocs/bitcoin/ethereum".

[OpenPony @OpenPony](#)

La chaîne de blocs est une invention génial qui ouvre le champ des possibles ! [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)

Conclusion de [@bortzmeyer](#) [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "la chaîne de blocs est une invention géniale" (+1) "résout le triangle de Zooko"

[Récamier @samiamtimet](#)

[#JCSA16](#) [@bortzmeyer](#) à [@Mo7sen](#) : "La sécurité c'est compliqué" [#PrivateJoke](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "bitcoin a sans doute pas mal d'avenir, mais pb de gouvernance à résoudre". "ses pb ne mettent pas en cause la chaîne de blocs"



[OpenPony @OpenPony](#)

Bitcoin a pris beaucoup d'expérience (et d'argent). On connaît les problèmes, on sait ce qu'il faut faire sans impacter [#blockchain](#) [#JCSA16](#)



[BIAOU Ramanou @RamanouB](#)

Bitcoin à d'avenir et également beaucoup de problèmes [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "les cryptomonnaies actuelles ne tiendront peut-être pas, mais il peut y en avoir d'autres"



[OpenPony @OpenPony](#)

[#ethereum](#) et les contrats sont une bonne idée ! On n'a pas arrêté Wordpress malgré les bugs ! [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

L'[#essence](#) s'évapore vite dans l'[#ether](#), c'est pour ça qu'on ne peut pas le taxer :- [#Blockchain](#) [#JCSA16](#)
[twitter.com/pbeysac/statu...](https://twitter.com/pbeysac/status...)



[Bruno Tréguier @btreguier](#)

@AFNIC Les présentations de [#JCSA16](#) seront-elles disponibles par la suite ?



[Johann @adofou](#)

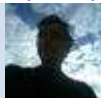
Quelques slides de conclusions [#JCSA16](#)





[OpenPony @OpenPony](#)

Internet et le web ont survécu à PHP, [#ethereum](#) devrait survivre ! [#JCSA16](#)



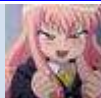
[Pierre Beyssac @pbeysac](#)

[#jcsa16](#) "si le web a survécu à PHP et Javascript, ethereum peut survivre à TheDAO" (on notera la condition prudente et neutre)



[Mohsen Souissi @Mo7sen](#)

On arrive à la conclusion du tutoriel [#blockchain](#) [#JCSA16](#)



[Johann @adofou](#)

Optimisme prudent de [@bortzmeyer](#) [#JCSA16](#)
pic.twitter.com/ttW0MVZqW4



[Khaled Koubaa @koubaak](#)

Conclusion final du tutorial : le crypto-monnaie aura du future même si [#bitcoin](#) se casse la figure [#blockchain](#) [#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) Fin du super exposé de [@bortzmeyer](#) sur la [#BlockChain](#)



[OpenPony @OpenPony](#)

Merci [@bortzmeyer](#) pour cette présentation pleine d'humour et sans ennui sur [#ethereum](#) [#bitcoin](#) et [#blockchain](#) [#JCSA16](#)



[Laurent Toutain @ltn22](#)

[#jcsa16](#) c'est quoi les quatre fonctions promises. J'ai trouvé laser, lampe et stylet. pic.twitter.com/hvU3AfhrM





Vidal Chriqui @vidal007

"Si le web a survécu à [#PHP](#) et [#javascript](#), [#ethereum](#) pourra survivre aux bugs the [#TheDAO](#)"

@[bortzmeyer](#)

@[AFNIC](#) [#JCSA16](#) [#blockchain](#) [#daohack](#)



BIAOU Ramanou @RamanouB

Fin de présentation de @[bortzmeyer](#) sur le Blockchain. Merci [#JCSA16](#)



@[ltn22](#) Admirer le logo @[AFNIC](#) ? [#JCSA16](#)

Mathieu Weill @mathieuweill



Pierre Beyssac @pbeysac

[#jcsa16](#) "peut-on imaginer une arnaque type Ponzi sur ethereum" "le code est visible ce qui, bien que sans garantie, permet l'examen public".



AFNIC @AFNIC

Fin de la matinée [#JCSA16](#) retour du live à 14h ! On parlera [#Cryptographie](#), [#GNU](#) et [#Tor](#) ! Programme, slides et live [afnic.fr/fr/l-afnic-en-...](#)



Pascal Vella @pascalvella

Cocktail [#JCSA16](#) [pic.twitter.com/SqT00zgvsj](#)



Tweet Binder Reports @TBreports

Amazing stats of [#JCSA16](#)
[tweetbinder.com/rsmini/AF6uZN9...](#)
925 tweets and 146 users via @[TweetBinder](#)
[pic.twitter.com/5iM2uHTcpI](#)





@[pbeyssac](#) @[adofou](#) @[samiamtimet](#) @[fzs600N](#)
and @[Mo7sen](#) are the most active users of [#JCSA16](#) via
[@TweetBinder](#) pic.twitter.com/9oITOG2xW1

[Tweet Binder Reports @TBreports](#)



Joël MAU @joel mau

Voir ici de préférence sur mobile afnic.fr/fr/l-afnic-en-... pour les vidéos [#JCSA16](https://twitter.com/Keltounet/stat...) à [@Mines_Telecom](https://twitter.com/Keltounet/stat...)



Récamier @samiamtimet

[#JCSA16](https://pic.twitter.com/XLLJc2YZLN) Programme de l'après-midi



Reprise de [#JCSA16](#) dans quelques minutes ! Suivez le live sur [afnic.fr/fr/l-afnic-en-...](#) #Afnic

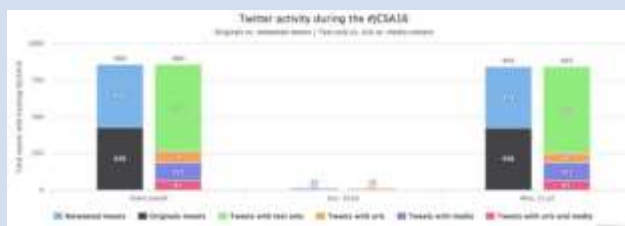
AFNIC @AFNIC



[Twetst io @Twetst io](#)

Petit point [#Twitter](#) de la [#JCSA16](#) avant la reprise de l'apm
860 tweets

top twittos [@pbeysac](#) [@adofou](#) [@samiamtimet](#)
pic.twitter.com/NkvQ6eeScX



[Johann @adofou](#)

Cocktail déjeunatoire à la [#JCSA16](#). Merci ! [@AFNIC](#) !
pic.twitter.com/J8UEnDOKi6



[Twetst io @Twetst io](#)

En 2015, la [#JCSA15](#) avait compté 1169 tweets... en 2016
avec 860 à 14h ça sent le record ! [#JCSA16](#)

twetst.io/jcsa16/





Reprise de [#JCSA16](#) après un excellent cocktail. Merci [@AFNIC](#)

[OpenPony @OpenPony](#)



Présentation du Conseil de [@AFNIC #JCSA16](#)

[OpenPony @OpenPony](#)



[#JCSA16 @mathieuweill](#) présente l'[@AFNIC](#) en ce début d'après-midi.

[Récamier @samiamtimet](#)



Reprise de la [#JCSA16](#) avec une allocution de l'[@AFNIC](#) pic.twitter.com/QjfPzpK6o

[Johann @adofou](#)



[#jcsa16](#) reprise avec [@mathieuweill](#) [@ltn22](#) pic.twitter.com/jX1A4tvhmu

[Pierre Beyssac @pbeyssac](#)





l' @AFNIC est une association ouverte à tous ! Pour adhérer : afnic.fr/fr/l-afnic-en-... #JCSA16

[OpenPony @OpenPony](#)



#JCSA16 @mathieuweill invite à adhérer à l'@AFNIC association ouverte : gestion collective d'un bien commun : le . Fr

[Récamier @samiamtimet](#)



Présentation de l'#AFNIC par @mathieuweill. Après-midi au #JCSA16

[BIAOU Ramanou @RamanouB](#)



#jcsa16 un honorable membre de l'auditoire demande si on peut payer son adhésion @AFNIC en Bitcoin :)

[Pierre Beyssac @pbeysac](#)



@mathieuweill est là.
Je suis là aussi.
Bon l'apm des #JCSA16 by @AFNIC peuvent recommencer ☺
#afniclover

[Alexandre SIMON @asimonstweets](#)

[#jcsalover](#)

pic.twitter.com/Q5haxKdUje





[AFNIC @AFNIC](#)

Sur scène @[mathieuweill](#) lance le séminaire #JCSA16. Suivez le live sur [afnic.fr/fr/l-afnic-en-...](#) #Afnic [pic.twitter.com/a0uxRSxosO](#)



[Récamier @samiamtimet](#)

#JCSA16 @[mathieuweill](#) salue les membres du Conseil Scientifique de l'[@AFNIC](#)



[OpenPony @OpenPony](#)

L' [@AFNIC](#) c'est 75 personnes (seulement), il faut partager et échanger #JCSA16 et @[mathieuweill](#) remercie les membres du conseil scientifique



[Récamier @samiamtimet](#)

#JCSA16 @[mathieuweill](#) Hommage particulier aujourd'hui pour @[Mo7sen](#) qui quitte ses fonctions (mais non l'afnic)



[BIAOU Ramanou @RamanouB](#)

Félicitations et Merci à @[Mo7sen](#) #JCSA16



[Alexandre SIMON @asimonstweets](#)

Quoi ??? @[Mo7sen](#) patron de l'[@AFNIC](#) Labs devient RSSI de l'[@AFNIC](#) !!! #félicitation #petitcachotier #JCSA16



[Récamier @samiamtimet](#)

#JCSA16 @[Mo7sen](#) sera remplacé au niveau du Conseil Scientifique par @[bortzmeyer](#) et @[benoit_ameau](#)



[OpenPony @OpenPony](#)

Le conseil scientifique de [@AFNIC](#) permet de dégager des tendances et approfondir les sujets #JCSA16



Pas trop de 2 personnes pour te succéder @Mo7sen ;) Je te souhaite le plein de réussite dans tes nouvelles fonctions à l'Afnic ! #JCSA16

[Benoit Ampeau @benoit_ampeau](#)



Oui, de nouvelles perspectives mais toujours à l'@AFNIC :-)
#JCSA16 [twitter.com/asimonstweets/...](#)

[Mohsen Souissi @Mo7sen](#)



Au conseil scientifique de l'@AFNIC, il y a deux catégories de photo... :-)
#JCSA16 [pic.twitter.com/rwbBiqV026](#)

[Johann @adofou](#)



@benoit_ampeau Merci ! Je suis confiant dans l'avenir de Labs et de JCSA :-)
#JCSA16

[Mohsen Souissi @Mo7sen](#)



Présentation du Conseil Scientifique de l'@AFNIC au #JCSA16

[BIAOU Ramanou @RamanouB](#)



#JCSA16 @ltn22 président du Conseil Scientifique de l'@AFNIC présente les membres du Conseil.

[Récamier @samiamtimet](#)



DNS parle de nom de domaine sans avoir été clairement précisé par RFC #JCSA16

[OpenPony @OpenPony](#)



Que signifie le "S" de "DNS" Service, Système ou Serveur? :) #JCSA16

[BIAOU Ramanou @RamanouB](#)



. @ltn22 revient sur l'histoire du DNS. Et en vient à évoquer la RFC 7686 ".onion" #jcsa16

[Pierre Beyssac @pbeysac](#)



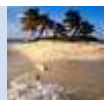
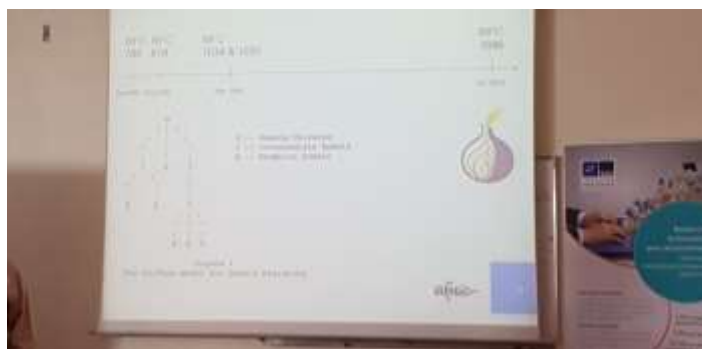
La RFC7686 voit l'apparition du .onion sans respecter les règles pré-établies d'attribution de nom. Il faut donc avancer :) #JCSA16

[OpenPony @OpenPony](#)



Le savez-vous? Le DNS n'a jamais vraiment été explicitement défini dans une RFC #JCSA16 pic.twitter.com/CusLoeZ3jv

[Johann @adofou](#)



À #JCSA16, le #CS #Afnic sz mêle aux .onion cette année :-)

[Mohsen Souissi @Mo7sen](#)



#JCSA16 @ltn22 : "le DNS décrit dans des documents, RFC, écrits à la machine".

[Récamier @samiamtimet](#)



[Mohsen Souissi @Mo7sen](#)

À [#JCSA16](#), le [#CS](#) [#Afnic](#) se mêle aux .onion cette année :-)



[Pierre Beyssac @pbeysac](#)

(Non-)extension du domaine de la lutte [#JCSA16](#)
pic.twitter.com/zgQnGJY9B8



[Récamier @samiamtimet](#)

[#JCSA16](#) Pas de registre centralisé pour le .onion



[OpenPony @OpenPony](#)

DNS est très résistante aux attaques par son infrastructure.
Utilisable pour d'autres services ? [#JCSA16](#)



[Benoit Ampeau @benoit_ampeau](#)

@[ltn22](#) : "Le DNS c'est aussi une infrastructure, pas uniquement les noms de domaine" [#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) la robustesse du DNS pour d'autres usages que les noms de domaine classiques. [#IoT](#) par exemple.



[Pierre Beyssac @pbeysac](#)

.@[ltn22](#) reste indépassable sur les chaussettes. [#bow](#) [#jcsa16](#)
twitter.com/ltn22/status/7...



[Récamier @samiamtimet](#)

[#JCSA16](#) l'enquête de toile de fond technologique, édition 2016.



[Pierre Beyssac @pbeysac](#)

Chers followers vous n'avez pas bossé pour rien en répondant, le résultat enquête toile de fond approche.

[#JCSA16](#) [pic.twitter.com/TYD8DtINFt](#)



[Johann @adofou](#)

Point saillants de l'enquête de toile de fond technologique Afnic 2016 by [@Mo7sen](#) [#JCSA16](#)
[pic.twitter.com/TyZB5dQSXI](#)



[BIAOU Ramanou @RamanouB](#)

Présentation du résultat des Points saillants de l'enquête de toile de fond technologique de l'[@AFNIC](#) 2016 [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

Le questionnaire toile de fond a été sensiblement allégé cette année (cachet d'aspirine moins nécessaire) [#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) la toile de fond technologique 2016, aspirine-free



[Khaled Koubaa @koubaak](#)

[@Mo7sen](#) présentant l'enquête Toile de Fond Technologique 2016 de l' [@AFNIC](#) [#JCSA16](#) [pic.twitter.com/wCA6Py6jvB](#)





[Julien Porschen @JulienPorschen](#)

Numérique, pas digital.
Tsss.

[#JCSA16](#)



[Alexandre SIMON @asimonstweets](#)

@Mo7sen on stage [#JCSA16](#) pour lancer le rendu de l'enquête "de toile de fond technologique Afnic 2016"
pic.twitter.com/aj4bdBRXMm



[J-Philippe CUNNIET @jcunnet](#)

[#Blockchain](#) : Suivez la conférence @AFNIC en direct [#JCSA16](#) avec @bortzmeyer sur afnic.fr/fr/l-afnic-en-...
pic.twitter.com/tQlbRyzahs



[Pierre Beyssac @pbeysac](#)

90% hommes, 10% femmes dans les répondants. Ya du boulot pour la parité dans notre métier, les informaticiens.

[#JCSA16](#)



[OpenPony @OpenPony](#)

Dans les 10 ans, internet restera le réseau de communication électronique dominant fait consensus à 98% [#JCSA16](#)

A simple explanation of a revolutionary technology : learn more about [#Ethereum](#) . youtube.com/watch?v=Clw-qf...
[#JCSA16](#) [#blockchain](#)

[LaBonneNouvelle @Le_Gai_Murmure](#)



[Récamier @samiamtimet](#)

#JCSA16 répondants à l'enquête de toile de fond technologique : 90% d'hommes. Même %age que présents dans la salle [#JamaisSansElles](#) :-)



[OpenPony @OpenPony](#)

Dans les 10 ans, les infrastructures d'internet continueront à évoluer pour répondre aux besoins des applications et service : 97% [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

Internet plébiscité à la Ceaucescu. 98% des répondants pensent qu'il restera le réseau de communication numérique dominant à 10 a. [#JCSA16](#)



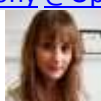
[Johann @adofou](#)

Sylvain Durif à participer à l'enquête de l'[@AFNIC](#) :-)
[#MieuxQuInternet](#) [#JCSA16](#) pic.twitter.com/8xyqwBuwC3



[OpenPony @OpenPony](#)

Le DNS restera le système de nommage et de résolution dominant sur Internet : consensus à 89% [#JCSA16](#)



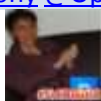
[Charlotte Pommier @PommierCha](#)

[@bortzmeyer](#) excellente présentation ce matin, bravo et merci :) [#JCSA16](#)



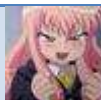
[OpenPony @OpenPony](#)

Les protocoles et algo de routage utilisés aujourd'hui résisteront à la croissance d'internet : consensus à 76% [#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) dans qq années l'internet sera complètement bouché [#joke](#)



Johann @adofou

Pas de crache d'internet dans les 10 ans à venir. Prend ca titre putaclic ! [#JCSA16 pic.twitter.com/PDjGSa7ySq](https://twitter.com/PDjGSa7ySq)



Pierre Beyssac @pbeysac

76% à penser que les protocoles de routage existants supporteront la croissance d'Internet à 10 ans. % en augmentation. [#JCSA16](https://twitter.com/PDjGSa7ySq)



OpenPony @OpenPony

L'exploitation des données personnelles issues des requêtes DNS sera généralisé par les opérateurs de résolveurs DNS : 75% [#JCSA16](https://twitter.com/PDjGSa7ySq)



Lucien Castex @LucienCastex

Séminaire [#JCSA16](https://twitter.com/PDjGSa7ySq), à suivre en direct afnic.fr/fr/l-afnic-en-... @AFNIC



OpenPony @OpenPony

Attention ! ça ne veut pas dire que c'est bien ! C'est juste une problématique qui apparaît :([#JCSA16](https://twitter.com/PDjGSa7ySq) [twitter.com/OpenPony/statu...](https://twitter.com/OpenPony/status...)



Pierre Beyssac @pbeysac

75% à penser que l'exploitation des données perso par les exploitants de résolveurs va se développer. [#JCSA16](https://twitter.com/PDjGSa7ySq)



Récamier @samiamtimet

[#JCSA16](https://twitter.com/PDjGSa7ySq) exploitation des données perso via le DNS par le FAI mise en évidence par l'enquête de toile de fond.



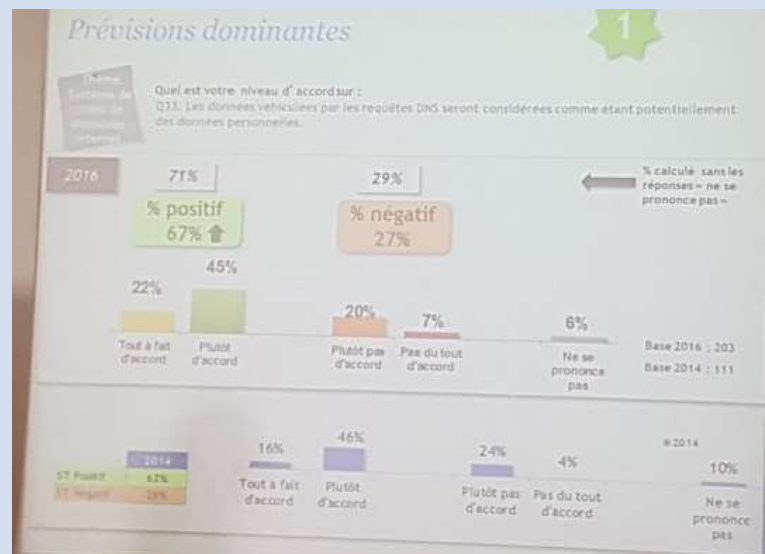
OpenPony @OpenPony

67% à penser que les données véhiculées par les requêtes DNS seront considérées comme étant potentiellement des données personnelles [#JCSA16](https://twitter.com/PDjGSa7ySq)



Johann @adofou

Vos requêtes DNS sont-elles des données personnelle?
Majorité pour un OUI [#JCSA16 pic.twitter.com/FA3tcaBuoW](https://twitter.com/FA3tcaBuoW)



Pierre Beyssac @pbeysac

67% à penser que les données DNS seront considérées comme potentiellement personnelles. [#JCSA16](https://twitter.com/FA3tcaBuoW)



Pierre Beyssac @pbeysac

36% (c'est peu) à penser que les opérateurs DNS s'engageront à ne pas exploiter ces données à des fins portant atteinte vie privée. [#JCSA16](https://twitter.com/FA3tcaBuoW)



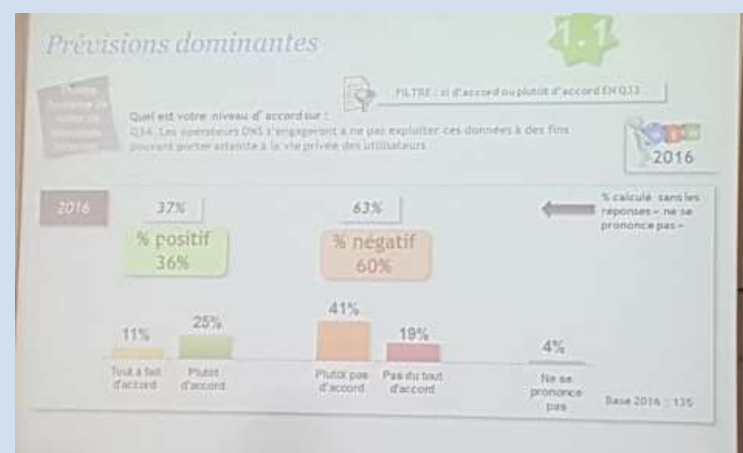
OpenPony @OpenPony

60% ne pensent pas que les opé DNS s'engageront à ne pas exploiter données à des fins pouvant porter atteinte à la vie privée [#JCSA16](https://twitter.com/FA3tcaBuoW)



Johann @adofou

MAIS une majorité pense que les opérateurs DNS ne s'engageront pas ne pas les exploiter [#JCSA16 pic.twitter.com/poUnkTxjh](https://twitter.com/poUnkTxjh)





[Benoît Duchatelet](#)
[@DoubleNumerique](#)

[#JCSA16](#) Journée du Conseil scientifique de l'[@AFNIC](#) à [@TelecomPTech](#) avec [@HasniSEO](#) [🔗🔗🔗](#)
[swarmapp.com/c/kKfCp1TRGoB](#) [pic.twitter.com/l16N7TOyix](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) l'ietf se penche sur le DNS et les fuites de données perso. [#RFC7626](#) et [#RFC7816](#)



Les différents types d'accès à internet sans fil seront neutres : 65% d'avis négatif [#JCSA16](#)

[OpenPony @OpenPony](#)



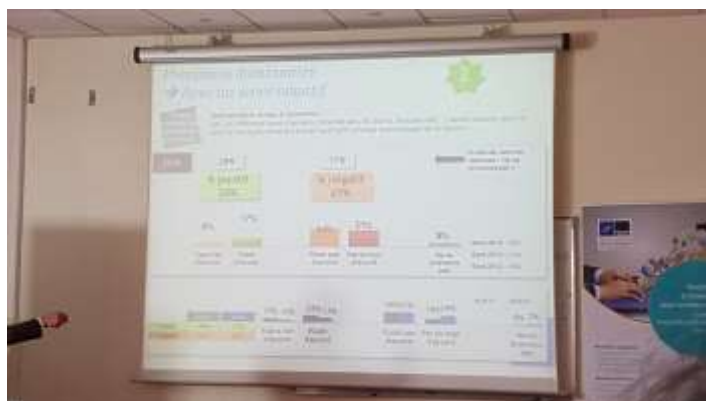
26% seulement pensent que les accès IP sans fil (3G/3G/wifi) seront "neutres". 65% non. [#JCSA16](#).

[Pierre Beyssac @pbeysac](#)



[Johann @adofou](#)

Un accès neutre sur la 3G et 4G dans le futur ?
Majoritairement les gens pensent que non. [#JCSA16](#)
[#DPImonAmour](#) [pic.twitter.com/V2pdfzbZT5](#)





L'espace de nommage internet s'appuiera toujours sur une racine unique : 63% d'accord [#JCSA16](#)

[OpenPony @OpenPony](#)



[#JCSA16](#) 71% des répondants à l'enquête de fond ne croient pas à la [#NeutralitéDuNet](#)

[Récamier @samiamtimet](#)



Racine unique. 63% pensent que oui, 23% non. Opinion stable. [#JCSA16](#).

[Pierre Beyssac @pbeysac](#)



@[pbeysac](#) Je m'étonne de l'emploi du futur: Ces moyens d'accès tels que fournis par les opérateurs mobiles n'ont jamais été neutres [#JCSA16](#)

[Yann Rousse @YRousse](#)



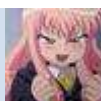
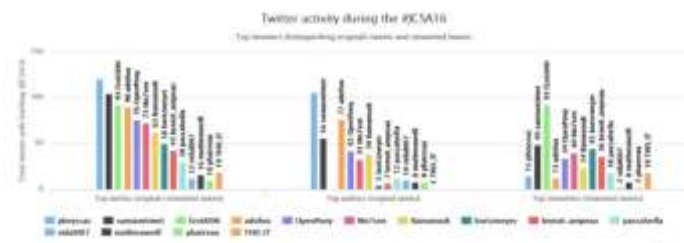
protocoles de routage d'internet intégreront des mécanismes de sécurité au niveau global : 62% plutôt d'accord [#JCSA16](#)

[OpenPony @OpenPony](#)



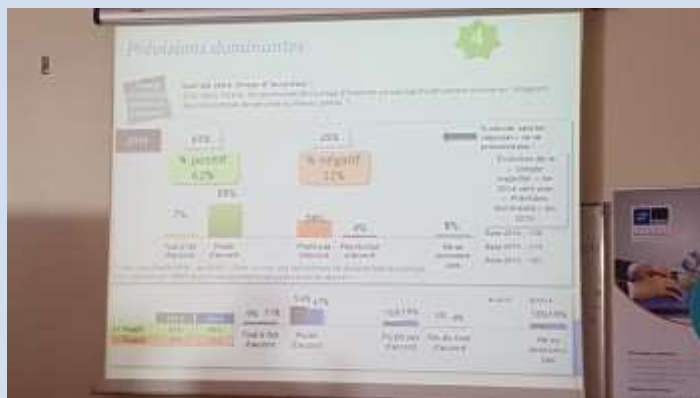
Toutes les stats Twitter de [#JCSA16](#) sont sur [@Twtest io](#) ! Qui tweet le + ? Qui est le + RT ? [twtest.io/jcsa16/pic.twitter.com/9u0bhNOdiU](#)

[Pascal Vella @pascalvella](#)



Question intéressante : les protocoles de routage vont-ils évoluer pour intégrer des mécanismes de sécurité? [#JCSA16](#) [pic.twitter.com/sqOXmPMOzZ](#)

[Johann @adofou](#)





Ivres, 62 % des répondants estiment que la [#RPKI](#) sera déployée :) [#JCSA16](#) [twitter.com/OpenPony/statu...](#) [#FRnog](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[ARHZ @Tutur_Arhz](#)

Il faut torturer les 2% restants ! Ils savent sûrement quelque chose [#disruption](#) [#JCSA16](#) [fr.wikipedia.org/wiki/Chatouill...](#) ... [twitter.com/OpenPony/statu...](#)



[Pierre Beyssac @pbeysac](#)

Sur la neutralité future de l'IP filaire, 47% de positif, 46% négatif (rappel : prédictions à 10 ans). [#jcsa16](#)



[Johann @adofou](#)

Du [#DPI](#) à venir sur votre accès ADSL ou Fibre? L'avis est malheureusement partagé... [#DPImonAmour](#) [#JCSA16](#) [pic.twitter.com/fgE20lutAs](#)



[OpenPony @OpenPony](#)

Accès internet filaires neutre ? 47% positif/46% négatifs [#JCSA16](#) Entre croyances et politiques, le doute persiste même là



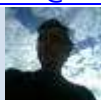
[Stéphane Bortzmeyer @bortzmeyer](#)

[@alexander_band](#) [@OpenPony](#) Next, percentage of *validating* routers. [#JCSA16](#)



[Johann @adofou](#)

Note d'un spectateur : le 49% et 51% sont inversés [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

Recours résolveur alternatif dépassera celui au résolveur FAI ? 45% oui, 41% non. [#JCSA16](#) q politique du filtrage (blocages sans juge...)



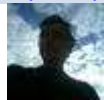
Dans la salle de la [#JCSA16](#) ça ne dort pas ! Une (toute) petite erreur de chiffre sur le transparent et hop ! ça réagit ... ?

[Alexandre SIMON @asimonstweets](#)



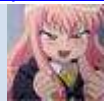
45% seulement pensent que les DNS locaux dépasseront les DNS de FAI ou ouverts contre 41% contre [#JCSA16](#)

[OpenPony @OpenPony](#)



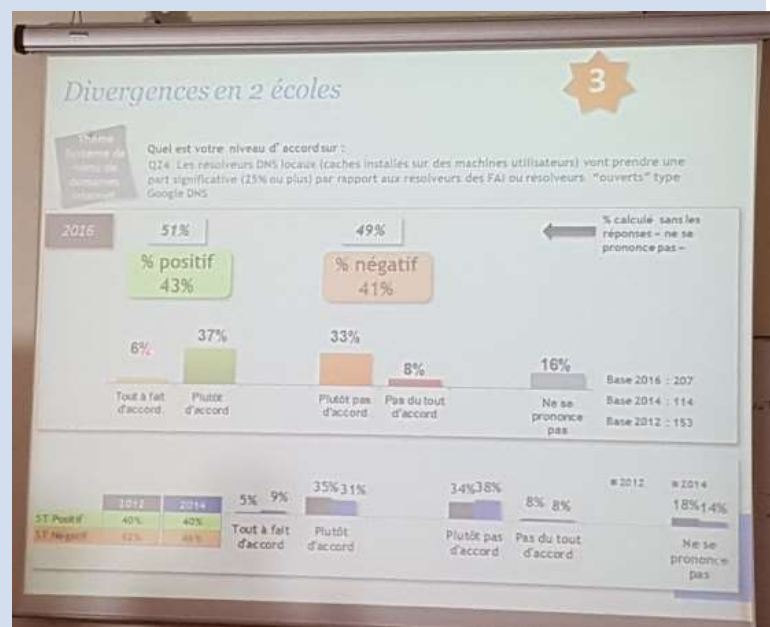
[note perso : on pense à Erdogan DNS plus connu sous le nom de 8.8.8.8] [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Intéressant : Avis partagé entre resolveurs locaux et "ouverts" [#JCSA16 pic.twitter.com/bsVJmGG7eI](#)

[Johann @adofou](#)



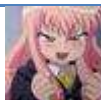
[#JCSA16](#) le resolveur DNS tiers (ie différent de celui de son FAI) va émerger : l'enquête de toile de fond est mitigée.

[Récamier @samiamtimet](#)



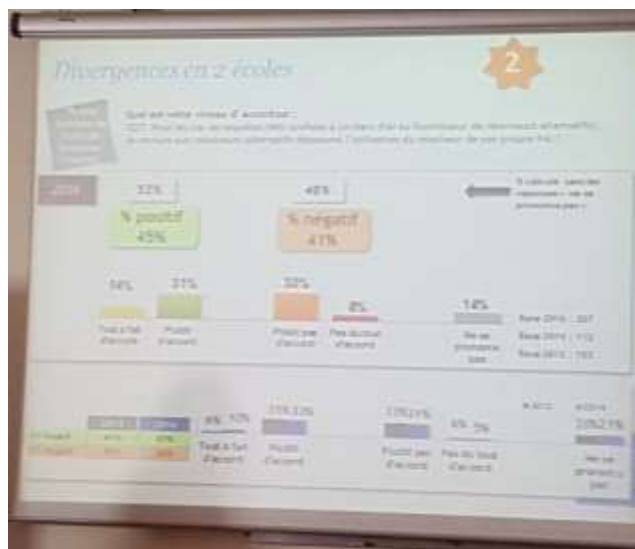
[#JCSA16](#) le rapport de toile de fond technologique 2016 sera publié à la rentrée (septembre 2016).

[Récamier @samiamtimet](#)



Johann @adofou

Avis partagé entre utilisation du résolveur du F.A.I et d'un résolveur local. [#JCSA16](#) pic.twitter.com/6EKnoLHIT3



OpenPony @OpenPony

Le rapport des tendances et pronostics est à venir prochainement : suivez [@AFNIC](#) pour le rapport complet qui viendra prochainement [#JCSA16](#)



Pierre Beyssac @pbeysac

Périodicité enquête : 2 ans. Questions à mettre à jour pour suivre la pertinence. [#JCSA16](#). [@Mo7sen](#) remercie les répondants.



Récamier @samiamtimet

[#JCSA16](#) si vous voulez voir de nouvelles questions apparaître dans la prochaine édition de l'enquête de fond, contacter [@benoit_ampeau](#)



Pierre Beyssac @pbeysac

"Plus on demande aux gens qui ils ont, moins ils ont tendance à répondre". Pb de la segmentation pour mieux évaluer les réponses. [#JCSA16](#)



Stéphane Bortzmeyer @bortzmeyer

Maintenant, un vrai chercheur, pas comme moi. Christian Grothoff sur [@GNUnet](#) "The GNU name system" [#JCSA16](#) [#privacy](#)



Récamier @samiamtimet

[#JCSA16](#) exposé suivant : the GNU name system. Par Christian Grothoff (Inria)



OpenPony @OpenPony

Présentation de GNU Name System in English [#JCSA16](#)



Now Christian Grothoff presents The [#GNU](#) Name system. In English. [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)



[Johann @adofou](#)

The GNU domain system [#JCSA16](#)
pic.twitter.com/gpaSN7kPs0



Since the speaker speaks in english, it'll be easier for me to tweet in english as well. [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



The problem: ICANN decisions (.ir, .xxx), IETF decisions (.onion, .bit), censorship (The Pirate Bay) [#JCSA16](#) [#DNS](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[Alexandre SIMON @asimonstweets](#)

Une idée : proposer les résultats de l'enquête «Toile de fond technologique» by [@AFNIC](#) sur forme [#opendata](#)

[#JCSA16](#)

[@Mo7sen](#)

[@benoit_ampeau](#)

[#JCSA16](#) "they didn't reject .bit, they just sit on it for years"

pic.twitter.com/Ht7I1RRRCr



[Pierre Beyssac @pbeysac](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) Trouble at the root ! pic.twitter.com/F84x7YG0vD





[#DNS](#) used for evil: censorship in China, surveillance (More Cowbell)... [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



"The GNU name system" à la [#JCSA16](#) avec Christian Grothoff

[BIAOU Ramanou @RamanouB](#)



"d-privé solves some problems without adding new ones" which is not usual. [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)



"[#IETF](#) solutions (to [#DNS](#) issues) introduce new problems" [#GNUet](#) [#DPRIVE](#) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[AFNIC @AFNIC](#)

Now at [#JCSA16](#) Christian Grothoff (@Inria) speaks of [#DNS](#) security and the GNU Name System afnic.fr/fr/l-afnic-en-...pic.twitter.com/KfSB8JpXhB



GNU name system is a decentralized name system with secure memorable names [#JCSA16](#)

[OpenPony @OpenPony](#)



The GNU name system solves all the issues of [#DNS](#) (and makes coffee as well?) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[#JCSA16](#) the GNU name system : DNS with privacy

[Récamier @samiamtimet](#)



GNU name system supports globally unique and secure identifiers [#JCSA16](#)

[OpenPony @OpenPony](#)



".gnu is you." "Not a new root, your own zone" [#GNUUnet](#)
[#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



".gnu is you (local)" "www A 5.6.7.8" [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)



Coucou [@AFNIC](#) : On aura moyen de récupérer les supports des [#JCSA16](#) des confs quelque part ?

[OpenPony @OpenPony](#)



[#JCSA16](#) www.gnu a local domain.

[Récamier @samiamtimet](#)



Alice will really write to bob@LONGCRYPTOHASH.zkey?
[#GNUUnet](#) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



Il s'agit d'une prédiction (pronostic) en aucun cas d'un souhait :-)

[#JCSA16](#) [twitter.com/OpenPony/statu...](#)

[Mohsen Souissi @Mo7sen](#)



If www.gnu is Alice's Web server, www.bob.gnu is Alice's Bob's Web server. [#GNUUnet](#) [#relative](#) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



Clé publique et DHT. Ça se corse. [#JCSA16](#)
[pic.twitter.com/g9u4Agspgs](#)

[Pierre Beyssac @pbeysac](#)



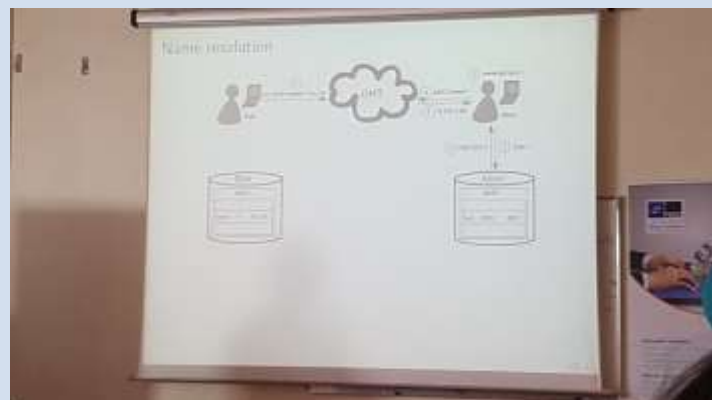
[#JCSA16](#) bon je vais prendre des cours d'anglais et je revient.
:-)

[fzs600 @fzs600N](#)



[Johann @adofou](#)

GNU Domain System avec des clés et du DHT dedans.
[#JCSA16 pic.twitter.com/gSMTtbR3pf](#)



[Fondapol @Fondapol](#)

[#JCSA16](#) Les 5 promesses de la [#Blockchain](#) [goo.gl/aj9jGz](#)
[#Bitcoin](#), [#Primaire2016](#) [#Numerique](#)
[pic.twitter.com/uZOPnPccQR](#)

Les 5 promesses de la blockchain

1. Confiance distribuée
2. Système transactionnel
3. Garanti par une large communauté
4. Absence de tiers de confiance
5. Protocoles complexes

LA BLOCKCHAIN, OU LA CONFIANCE DISTRIBUÉE

FONDATION POUR L'INNOVATION POLITIQUE
[fondapol.org](#)

Julien 2016

Thierry CAILLON
[thierry.cailion@fondapol.org](#)



[Mohsen Souissi @Mo7sen](#)

Les participants sont vigilants à [#JCSA16](#) et ils ont bien raison :-)
[twitter.com/asimonstweets/...](https://twitter.com/asimonstweets/)



[Johann @adofou](#)

Ca ma quand même l'air un chouillat compliqué [#JCSA16](#)
pic.twitter.com/IDG53VX9jf



[Récamier @samiamtimet](#)

[#JCSA16](#) oh la la ça se corse pour de bon. Anglais + Oral + Crypto



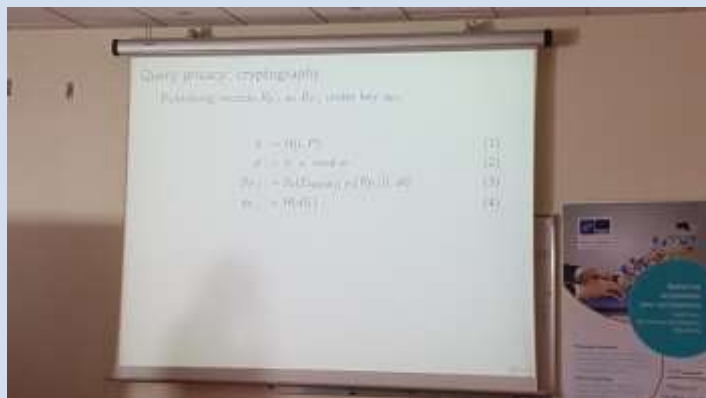
[Pierre Beyssac @pbeysac](#)

Urgh. [#JCSA16](#) pic.twitter.com/6F0xupE7P6



[Johann @adofou](#)

Toute à fait d'accord. Enfin je pense... [#JCSA16](#)
pic.twitter.com/1DNyNydsikk



[Pierre Beyssac @pbeysac](#)

"If somebody doesn't know which label and which zone" "You can check the signature but you can't decrypt" [#gnunet](#)
[#JCSA16](#)



Pierre Beyssac @pbeysac

"With this simple scheme". Yes Christian said "simple".
#jcsa16



Mohsen Souissi @Mo7sen

@asimonstweets C'est une excellente suggestion d'amélioration que mon successeur @benoit_ampeau étudiera avec bcp d'intérêt :-)
#JCSA16



Johann @adofou

Ah mais il y a la suite en dessous! #JCSA16
pic.twitter.com/KD6nzhjUQy



mcabdelAbdel @mcabdel

@Mo7sen #JCSA16 J'ai l'impression qu'on aura plus de mal à trouver des erreurs dans la présentation de Christian Grothoff



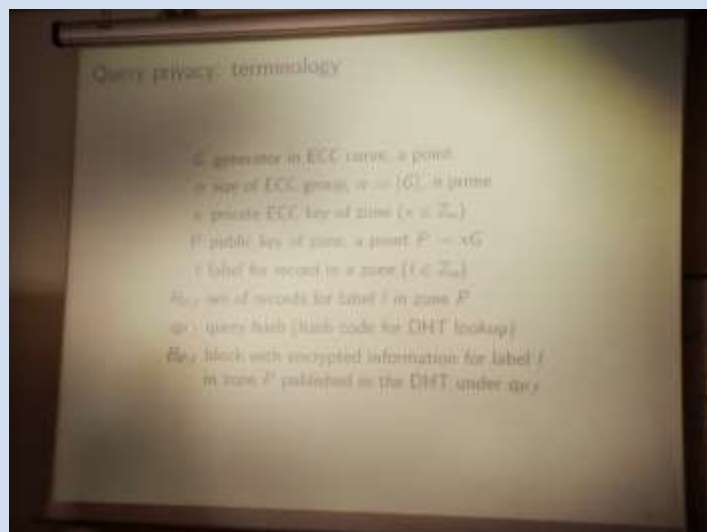
Pierre Beyssac @pbeysac

Même @bortzmeyer ne se risque pas à poser une question.
#jcsa16



Alexandre SIMON @asimonstweets

Ivre, il se promène à @TelecomPTech, entre dans l'amphi de la #JCSA16 et suit un cours de math/crypto en anglais ...
pic.twitter.com/SSVvpokpmN





Zut, je suis inutile [#JCSA16 twitter.com/a_ferron/statu...](https://twitter.com/a_ferron/status/7...)

[Stéphane Bortzmeyer @bortzmeyer](#)



[#JCSA16](#) is there anybody not largued in ze salle [#Crypto](#)
[#GNS](#)

[Récamier @samiamtimet](#)



Pour ceux qui voudraient récupérer les supports de conf des [#JCSA16](#) et qui comme moi savent pas regarder...
twitter.com/AFNIC/status/7...

[OpenPony @OpenPony](#)



"If your nickname is Bob, in the crypto community, you will have conflicts." [#Alice](#) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



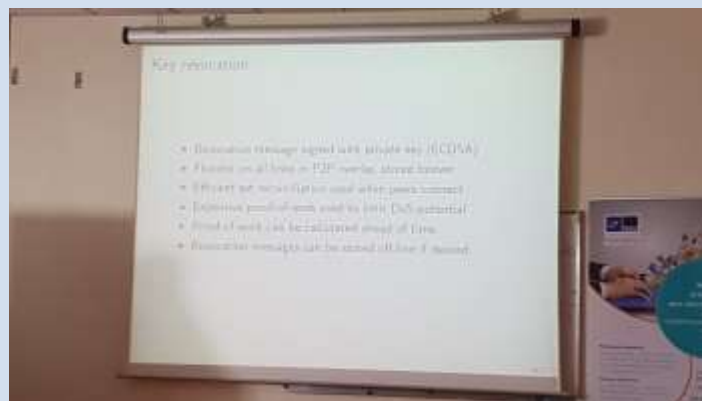
La présentation de GNU Name System par Christian Grothoff pdt [#JCSA16](#) a séché tout le monde. Même [@bortzmeyer](#) ne pose pas de question

[Alexandre SIMON @asimonstweets](#)



Important : gestion de la révocation des clés [#JCSA16](#)
pic.twitter.com/XZrse6FQ0t

[Johann @adofou](#)



[@adofou](#) [@pbeysac](#) Comme c'était arrivé à UUCP (qui avait le même système de nommage), tout le monde se nommait par rapport 1/2 [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[@adofou](#) [@pbeysac](#) aux deux ou trois gros sites de référence. 2/2 [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



Restez bien assis, la ceinture attachée... Christian Grothoff attaque maintenant la partie "Key Revocation" [#JCSA16](#) [#lesyeuxmepiquent](#)

[Alexandre SIMON @asimonstweets](#)



[Pierre Beyssac @pbeysac](#)

"Key revocation, nightmare (stored everywhere forever). We want to avoid that. So we broadcast to the network." (not sure I get it) [#jcsa16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)



[Mohsen Souissi @Mo7sen](#)

Solution for other TLD: slave them in your [#GNet](#) zone... (Check them with [#DNSSEC](#) first) Good privacy [#JCSA16](#)

Chers (e-)participants à [#JCSA16](#), ne vous sentez pas frustrés de ne pas si vs ne comprenez pas les détails de chaque prez. C'est normal :-)



[Pierre Beyssac @pbeysac](#)

"Plan to obsolete the obsolete DNS protocol" [sic] nice but good luck with that; won't happen overnight. [#JCSA16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Last slide "plan to obsolete the obsolete [#DNS](#) protocol" [#boldness](#) [#JCSA16](#)



[Récamier @samiamtimet](#)

[#JCSA16](#) Christian Grothoff " GNS next step : obsolete the obsolete DNS protocol"



[Pascal Vella @pascalvella](#)

Now I feel [#JCSA16](#) pic.twitter.com/WZfmEXaPfx

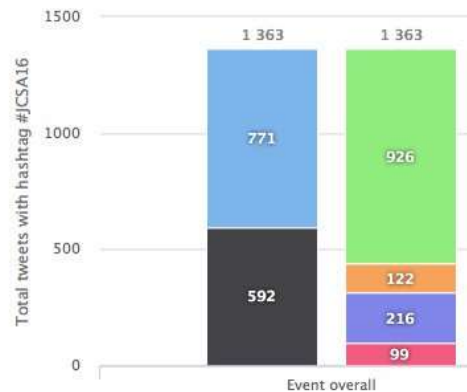




[Twest.io](#) @Twest.io

#JCSA16 beats #JCSA15 !

Les 1169 tweets de 2015 sont largement dépassés par les 1363 de 2016 (et ça continue). pic.twitter.com/vup5ovPiL6



[CryptoParty Rennes](#)
@CryptoPartyRNS



#JCSA16: Bientôt .fr ou .eu.org sur @GNet cc @pbeysac
@Mo7sen @bortzmeyer ? :)

Amélioration continue ! #JCSA16
[twitter.com/Twest.io/statu...](https://twitter.com/Twest.io/status...)

[Mohsen Souissi](#) @Mo7sen



@Twest.io @asimonstweets vous avez les Top #N twittos ?
#JCSA16

[Mohsen Souissi](#) @Mo7sen



#gnunet's global domination plan: hijack (copy) existing TLDs
then work on the copies (?). #JCSA16
pic.twitter.com/om78dly7kv

[Pierre Beyssac](#) @pbeysac



[Johann @adofou](#)

[#JCSA16](#) pic.twitter.com/kfXpHg4FGw

[AFNIC @AFNIC](#)

Et la journée n'est pas finie ! Suivez le live [#JCSA16](#) sur afnic.fr/fr/l-afnic-en-... Prochaine présentation sur [#Tor](#) twitter.com/Twest_io/status...

[Stéphane Bortzmeyer @bortzmeyer](#)

We sommes back en french à [#JCSA16](#). Lunar va parler de cuisine avec des oignons. [#Tor](#) [#JCSA16](#) [#DarkDarkDeep](#)

[Pierre Beyssac @pbeysac](#)

Et bientôt [#gnuparacetamol](#) ? [#jcsa16](#) twitter.com/adofou/status/...

[CryptoParty Rennes @CryptoPartyRNS](#)

[#JCSA16](#) [@GNUnet](#) propose GNS, un système de nom, cleanstate *et* incrémental pouvant intégrer des zones du DNS actuel twitter.com/CryptoPartyRNS...

[Johann @adofou](#)

On va parler de Tor et .onion avec Lunar [#JCSA16](#) pic.twitter.com/Kyh7RX6L6a

[Pierre Beyssac @pbeysac](#)

Lunar présente maintenant Thor et ses .onion. [#JCSA16](#) pic.twitter.com/hTzg6g3C8o



Bon maintenant on parle du project Tor :) au [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



[OpenPony @OpenPony](#)

Lunar va présenter [#Tor](#) à [#JCSA16](#)

Il parle aussi de [@NosOignons](#) qui développe l'infrastructure de Tor en France



Tor : système d'adressage et non pas de nommage [#JCSA16](#)

[Benoit Ampeau @benoit_ampeau](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) Lunar nous parle de [#Tor](#) et ses .onion
pic.twitter.com/3ReTRPMp8z



En ce moment TOR [#JCSA16](#) vidéo en [#Direct](#)

afnic.fr/fr/l-afnic-en-...

[Pat F. @rpr8395](#)



[Prunus @OpenPrunus](#)

Lunar nous parle de [#Tor](#) au [#JCSA16](#)



Le projet Tor travaille pour la liberté (d'opinion, d'expression et d'association en autre) et donc l'anonymat [#JCSA16](#)

[Johann @adofou](#)



Vous avez "Tor" de ne pas vous mêler des .Onion de Lunar à [#JCSA16](#) cet après-midi :-)

[Mohsen Souissi @Mo7sen](#)



[OpenPony @OpenPony](#)

La défense des libertés : Opinion, Expression, Association
Pour tout ça : [#Tor](#) offre des garanties pour protéger les communications [#JCSA16](#)



[BIAOU Ramanou @RamanouB](#)

Le Project tor pour la liberté d'opinion et rendre le monde meilleure by Lunar au [#JCSA16](#)



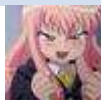
[Khaled Koubaa @koubaak](#)

Lunar présente le .onion du projet Tor [#JCSA16](#) [#Tor](#)
pic.twitter.com/QbWafU0ZSR



[Vidal Chriqui @vidal007](#)

Lunar de [@torproject](#) nous parle du système d'adressage en .onion
[#JCSA16](#) [#freedom](#) [#privacy](#) pic.twitter.com/0xGaV92NO9



[Johann @adofou](#)

Aujourd'hui on sera sérieux. Pas de troll prévient Lunar
[#JCSA16](#) pic.twitter.com/4j0PzFTKTV





Récamier @samiamtimet

#jcsa16 Lunar pic.twitter.com/H3gUVNuFLp



OpenPony @OpenPony

#Tor est un réseau ouvert
#Tor est un logiciel libre
#Tor est une communauté
#JCSA16



Pierre Beyssac @pbeysac

Lunar a un t-shirt "nothing to hide" et nous présente Tor (pas Thor sorry) pour protéger la vie privée. #JCSA16



AFNIC @AFNIC

#JCSA16 Lunar parle de Tor et du .onion "Privacy by design" suivez le live afnic.fr/fr/l-afnic-en-... #privacy #onion pic.twitter.com/XcihO0N86K



OpenPony @OpenPony

7000 relais différents constituent le réseau #Tor #JCSA16



Récamier @samiamtimet

#JCSA16 Tor c'est maintenant 7.000 relais



Stéphane Bortzmeyer @bortzmeyer

Il y a 7000 nœuds Tor. Plus que de nœuds Bitcoin (mais moins qu'Ethereum). #JCSA16



Réseau Tor avec plus de 7000 relais différents. [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



Présentation de Lunar : afnic.fr/medias/documen... [#JCSA16](#)

[OpenPony @OpenPony](#)



[#JCSA16](#) A peu près la moitié de la salle a utilisé le réseau d'anonymisation [@torproject](#)

[Récamier @samiamtimet](#)



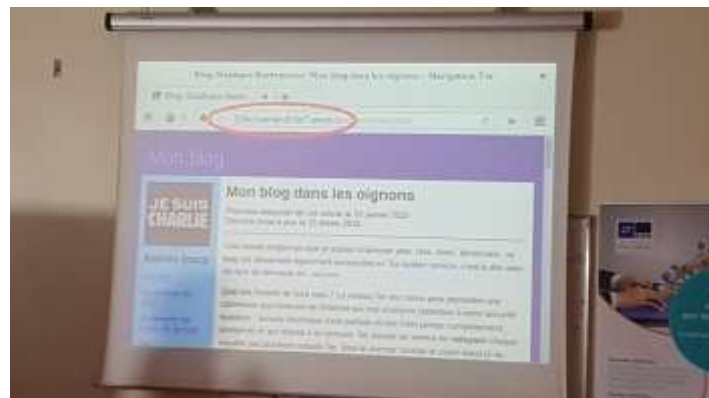
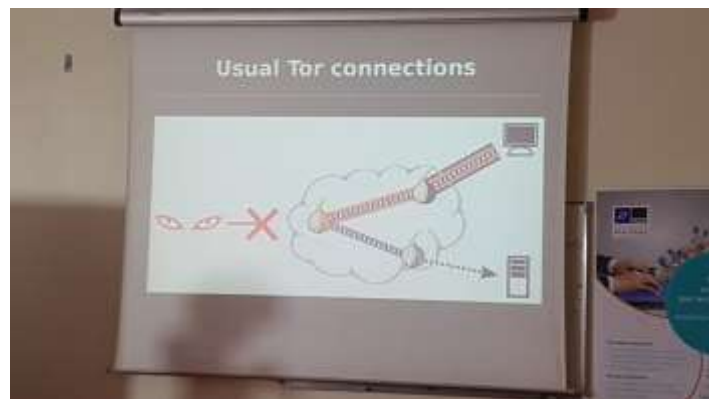
Le blog de [@bortzmeyer](#) en .onion dans la présentation de Lunar [#JCSA16](#)

[OpenPony @OpenPony](#)



Deux types d'utilisation de [#Tor](#) (caché sa connexion OU son service). [#JCSA16](#) pic.twitter.com/SVxwhHtiw

[Johann @adofou](#)



"Une adresse Tor c'est comme une adresse IP, pas facile à retenir" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Le .onion ne fait pas partie du système DNS [#JCSA16](#)

[OpenPony @OpenPony](#)



"Le nom .onion est dérivé du hash de la clé publique du service" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Plus d'info techniques pour la conférence de Lunar ici : [torproject.org](#) [#JCSA16](#)

[OpenPony @OpenPony](#)



Adresse [#Tor](#) ou IPv6 : même combat. [#EnlargeYourMemory](#) [#JCSA16](#) [pic.twitter.com/9dHjD8hiQp](#)

[Johann @adofou](#)



"Avec une adresse .onion ni le client ni le serveur ne savent où l'autre est situé" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Propriété du .onion [#Tor](#) [#JCSA16](#) [pic.twitter.com/T1tzYm06df](#)

[Johann @adofou](#)



Onion Service Properties :

[#JCSA16](#) [pic.twitter.com/EteNkC9qJ4](#)

[Mohsen Souissi @Mo7sen](#)





[#TOR](#) c'est du chiffrement de bout en bout [#JCSA16](#)

[OpenPony @OpenPony](#)



"Chiffrement de bout en bout garanti entre le client et le serveur .onion" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



[#JCSA16](#) les services onion @[torproject](#) permettent une sorte de nommage avec authentification des serveurs .onion

[Récamier @samiamtimet](#)



"Moins de 60 000 serveurs .onion existants" [#jcsa16](#) environ 1 Gbps de trafic (5% du trafic Tor)

[Pierre Beyssac @pbeysac](#)



Un peu moins de 60000 noms/adresses .onion existent. [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



Un peu moins de 60k adresses .onion
Trafic agrégé Tor estimé à 1Gb/s
[#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)



Stats [#Tor](#)
60 000 .onion dans le monde seulement :'
70 Go/s
1 Gb/s pour les .onion [#JCSA16](#)

[OpenPony @OpenPony](#)



Estimation du trafic [#Tor](#). Tor ne sait faire que du TCP par sa construction. Pas UDP. Pour l'instant? [#JCSA16](#)
pic.twitter.com/CWGVBaVCEX

[Johann @adofou](#)



[#JCSA16](#) les services .onion sont là depuis 2004.

[Récamier @samiamtimet](#)



Naissance de Tor en 2004. [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



"Naissance Tor: 2004. 1re utilisation un un peu connue: lancement d'alerte (documents) contre le Zyprexa (médicament)" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Les services .onion (Tor) ont été lancés en 2004. Première utilisation célèbre, en 2006 : (alerte/fuite sur médicament ZYPREXA)

[#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)



"Wikileaks sur .onion: pas pour cacher le serveur mais pour protéger les soumissionnaires de documents." [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Le service .onion à servit à éviter la censure de document mettant en cause des sociétés. Et a été connu pour cela par la presse [#JCSA16](#)

[Johann @adofou](#)



[#WikiLeaks](#) a utilisé [#Tor](#) pour protéger les Whistleblowers avant tout [#JCSA16](#)

[OpenPony @OpenPony](#)



Vie privée et statistiques : Tor protège tellement bien qu'on ne peut pas compter le nombre d'utilisateurs. [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[#JCSA16](#) dans [@torproject](#) impossible de connaître le nbre d'utilisateurs sans casser le "contrat d'anonymisation".

[Récamier @samiamtimet](#)



1 millions d'utilisateurs Facebook utilisent Tor pour accéder au site via le .onion [#JCSA16](#)

[OpenPony @OpenPony](#)



Un million de personne utilise [#Facebook](#) en passant par Tor. Facebook a fini par mettre en place un noeud Onion. [#JCSA16](#)

[Johann @adofou](#)



Hmmm, confusion de Turkish Telecom et Turk Trust, là, je crois. (poke [@squintar](#)) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



L'intérêt du .onion pour facebook est de pouvoir utiliser TOUS les relais [#Tor](#) [#JCSA16](#)

[OpenPony @OpenPony](#)



Au moins 1 Million de personnes utilise Facebook via Tor.
[#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



"Quand on a un .onion on peut utiliser tous les relais Tor quelle que soit leur position dans le réseau, bcp + nombreux"
[#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



OnionBalance est un projet permettant de faire du load balancing over Tor pour répartir la charge [#JCSA16](#)

[OpenPony @OpenPony](#)



Project pour accélérer l'accès à Facebook via [#Tor](#). Des projects d'allègement (évite censure. - anonymation) [#JCSA16](#)
pic.twitter.com/Q1qTxDI7rp

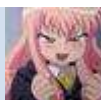
[Johann @adofou](#)





[ARHZ \(@Tutor_Arhz\)](#)

Il me semble qu'il y ait une contradiction là nan ? [#JCSA16](#)



[Johann @adofou](#)

Facebook est l'un des rares à avoir un certificat SSL pour leur .onion (et une adresse simple). [#JCSA16](#)



[OpenPony @OpenPony](#)

Ricochet est une application de chat avec adresses en .onion [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

"Ricochet : application de chat en .onion sans serveur. Pour l'arrêter il faudrait couper tout Tor : difficile." [#jcsa16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

[#Ricochet](#) messagerie instantanée sur [#Tor](#) [ricochet.im](#) [#JCSA16](#)



[Johann @adofou](#)

Plein d'autre service sympa via .onion (chat, partage de fichier, etc). [#JCSA16](#) [#TOR](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Point [#RFC](#) à [#JCSA16](#) [bortzmeyer.org/7686.html](#) [#Tor](#)



[Johann @adofou](#)

RFC7686 sur le .onion [#JCSA16](#) [#Tor](#)
[pic.twitter.com/rPI71FqxVY](#)





[Récamier @samiamtimet](#)

[#jcsa16](#) mettre en place un .onion se fait en 2 coups de cuillères à pot. Vérifier quand même qu'il n'y a pas de leak.



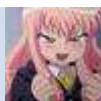
[OpenPony @OpenPony](#)

Les clés, en RSA 1024b, sont faibles [#JCSA16](#)



[Johann @adofou](#)

Problème de sécurité dans [@torproject](#) [#Toe](#) [#JCSA16](#)
pic.twitter.com/NPNlhg5leS



[Johann @adofou](#)

[#Tor](#) utilise une base de donnée distribuée pour toute les informations entre les noeuds. [#JCSA16](#)



[OpenPony @OpenPony](#)

Nouvelle génération de .onion permettant l'ajout d'un nombre aléatoire voté pour 24h afin d'éviter les prédictibilités [#JCSA16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

[@adofou](#) Encore pire avec les nouvelles adresses qu'il vient de présenter. [#JCSA16](#)



[OpenPony @OpenPony](#)

Adresses en .onion : passage de 16 à 52 caractères [#JCSA16](#)



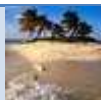
[Johann @adofou](#)

Qlq soucis dans la concept° de la base de donnée distribuée pour les services (basé sur l'heure). Une nouvelle méthode à venir. [#JCSA16](#) [#TOR](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) Bigger Onion Adresses : passage de 16 à 52 caractères



[Mohsen Souissi @Mo7sen](#)

C'est pour ça que c'est "un projet" et non un service éprouvé, en production [#JCSA16 twitter.com/adofou/status/...](#)



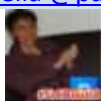
[OpenPony @OpenPony](#)

Trouver processus vérifiés pour authentifier les adresses : GNS, DNSSec, Namecoin, OnionNS, Let'sEncrypt... [#JCSA16](#)



[Pascal Vella @pascalvella](#)

Il vous reste quelques minutes pour poser questions live à Lunar de [@torproject](#) pendant [#JCSA16 afnic.fr/fr/l-afnic-en-... #privacy](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) Fin de la présentation de Lunar sur [@torproject](#) et ses .onions [pic.twitter.com/uTjRHMSiwT](#)



[OpenPony @OpenPony](#)

L'utilisation de [#Tor](#) via le Tor Browser ne donne pas un effort énorme [#JCSA16](#)



[Haelwenn\['elwen'\] @lanodan](#)

[#JCSA16](#) URL pour lecteur multimédia : [live.eyedo.net:1935/w/17832/eyedo ...](#)



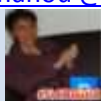
[Johann @adofou](#)

Point pédopornographie de la part d'un spectateur à la [#JCSA16](#). Bien répondu par Lunar



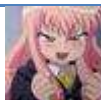
[BIAOU Ramanou @RamanouB](#)

On décortique les .Onions de Lunar après sa présentation et avec des questions [#JCSA16](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) plusieurs annuaires de services en .onion



[Johann @adofou](#)

Facebook à fait un bruteforce et a eu de la chance pour arriver à trouver une URL .onion en "[facebookcorewwi.onion](#)" [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

Après cette présentation .onion, j'ai presque les larmes aux yeux :-) [#JCSA16](#) [@torproject](#)



[Pierre Beyssac @pbeysac](#)

"Quand l'accès à Facebook a été bloqué, les gens ont utilisé Tor pour y accéder" [#jcsa16](#)



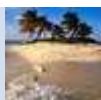
[Pascal Vella @pascalvella](#)

[#JCSA16](#) vient de sortir de la TT France mais toujours bien placé en TT Paris ! [pic.twitter.com/YEk0oC110w](#)



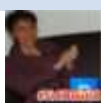
[The Portland Blog @ThePortlandBlog](#)

[#Paris](#) Trends
Eder
Payet
[#14juillet](#)
Theresa May
Lisbonne
[#FausseNote](#)
Graziano Pellè
[#JCSA16](#)
[#RendezNousLaBiscotteSurSnap](#)



[Mohsen Souissi @Mo7sen](#)

[@pascalvella](#) Allez, ecore un effort pour le remettre :-)
[#JCSA16](#)



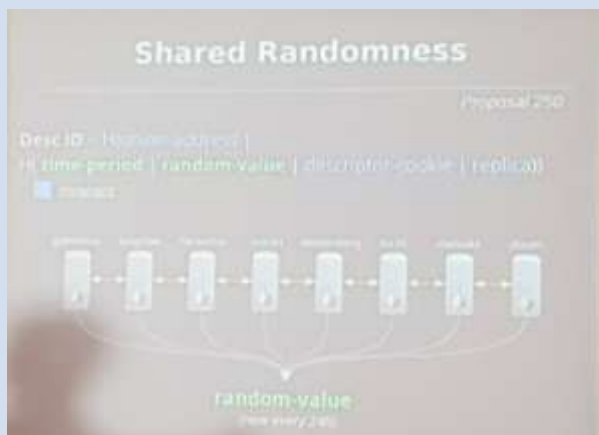
[Récamier @samiamtimet](#)

[#jcsa16](#) [@ltn22](#) président du Conseil Scientifique : "On a besoin d'une pause café, après cette première partie bien touffue".



[Johann @adofou](#)

Annuaire de [#Thor](#). Hash basé sur 8 machines à travers le monde. Gérer par des personnes diff [#JCSA16](#)
pic.twitter.com/xTDk8YyniY



[BIAOU Ramanou @RamanouB](#)

Des modifications encours qui rendront difficiles les attaques sont annoncées dans le réseau Tor by Lunar [#JCSA16](#)



[Pascal Vella @pascalvella](#)

Stickers et flyers [@torproject](#) disponibles à l'entrée de la salle [#JCSA16](#) [#onion](#) pic.twitter.com/proRipU7eO



[Stéphane Bortzmeyer @bortzmeyer](#)

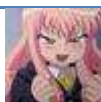
Benno Overeinder (in english) at [#JCSA16](#) on [#DNS](#) security: a secure Internet infrastructure



[Pierre Beyssac @pbeysac](#)

Reprise avec Benno Overeinder, [@NLnetLabs](#) [#JCSA16](#)
pic.twitter.com/9fXk950807





Johann @adofou

From the Ground Up Security DNS-based Security of the Internet Infrastructure [#JCSA16](#) pic.twitter.com/xsqtOIBfxe



Récamier @samiamtimet

[#jcsa16](#) Benno Overeinder de [@NLnetLabs](#) au sujet du DNS pour la sécurité de l'infrastructure de l'internet pic.twitter.com/Dd0jogQzng



Stéphane Bortzmeyer @bortzmeyer

NLnet Labs: making good [#DNS](#) software for [some time] nlnetlabs.nl [#JCSA16](#)



Johann @adofou

About [@NLnetLabs](#) [#JCSA16](#) pic.twitter.com/T4K0k9JFg1



Récamier @samiamtimet

[#jcsa16](#) [@NLnetLabs](#) : NSD, Unbound, OpenDNSSEC et plein d'autres choses



Mohsen Souissi @Mo7sen

By Benno Overeinder from [#NLnetLabs](#)
Welcome to our Dutch partner :-)
[#JCSA16](#) twitter.com/adofou/status/...



[AFNIC @AFNIC](#)

[#DNS](#) Security of the Internet Infrastructure by Benno Overeinder [@NLnetLabs](#) [#JCSA16](#) Webcast [afnic.fr/fr/l-afnic-en-...](#) [pic.twitter.com/vY1IYXIUKB](#)



[@framasky](#) [@bortzmeyer](#) Les présentations [#JCSA16](#) sont sur la page [afnic.fr/fr/l-afnic-en-...](#) La liste en haut à droite. [pic.twitter.com/og6w52V8H6](#)

[Alexandre SIMON @asimonstweets](#)



Hello DNSSEC, Hello DANE, Hello TLS, Hello Internet Security [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



[@NLnetLabs](#) nous parle de la sécurité du DNS et des infrastructures Internet avec Benno au [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



Présentation du modèle de confiance DNS/PKIX/X.509 etc. [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



[#Sobre](#), il présente [@torproject](#) et [@NosOignons](#) d'un point de vue scientifique et non comme [#DeepDarkMarinaAbyssalWeb](#) aux [#JCSA16](#) de [@AFNIC](#)

[CryptoParty Rennes](#)
[@CryptoPartyRNS](#)





[Mohsen Souissi @Mo7sen](#)

J'arrive donc 6e mais avant [@bortzmeyer](#) et [@benoitampeau](#), c'est l'essentiel :- [#compétition](#) [#JCSA16](#) [twitter.com/Twest_io/statu...](#)



[Johann @adofou](#)

Chaîne de certification X.509. Est-ce une bonne chose? [#JCSA16](#) [pic.twitter.com/vuc3DVbYiu](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) the "too many CAs" problem exposed by Benno Overeinder



[OpenPony @OpenPony](#)

DNSSEC validates the authenticity of the DNS data using digital signatures [#JCSA16](#)



[OpenPony @OpenPony](#)

DNSSEC : digital signatures are added to responses by authoritative servers for a zone [#JCSA16](#)



[Johann @adofou](#)

What is the DNSSEC? [#JCSA16](#) [pic.twitter.com/66dp5Tgcle](#)





[Pierre Beyssac @pbeysac](#)

Et maintenant une présentation de haut niveau de [#DNSSEC](#).
[#jcsa16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

"[#DNSSEC](#) in one slide" at [#JCSA16](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) [#DNSSEC](#) THE solution for authenticating data and the source origin for the DNS. No more DNS spoofing



[OpenPony @OpenPony](#)

DNSSEC : Signature validation creates a chain of overlapping signatures from trust anchor to signature of response [#JCSA16](#)



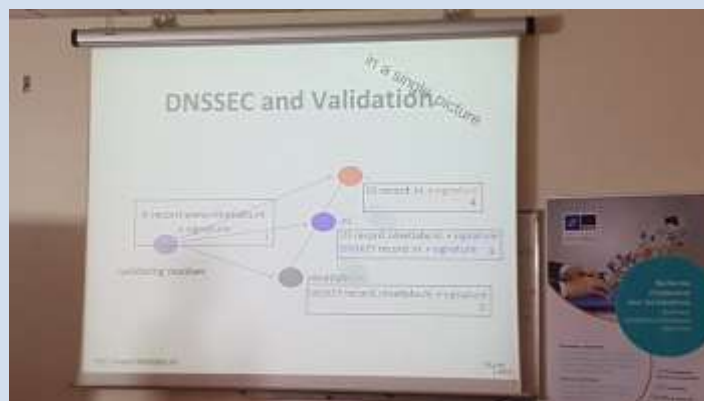
[Régis MASSÉ @remasse](#)

[#JCSA16](#) Describe DNSSEC in only one slide, it's so challenging
@[NLnetLabs](#)



[Johann @adofou](#)

DNSSEC and validation [#JCSA16](#) [pic.twitter.com/AltD8WJvIN](#)



[Pierre Beyssac @pbeysac](#)

[#DANE](#) ([#DNSSEC](#)) offre différentes méthodes pour spécifier des certificats, via TLSA. [#jcsa16](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) DANE is THE solution for the "too many CAs" problem. It securely specifies which certificate an application should use.



[Mohsen Souissi @Mo7sen](#)

@[adofou](#) Non, DANE s'appuie sur DNSSEC, ça ne peut pas être une alternative à DNSSEC :-)
[#synergie](#) [#JCSA16](#)



With DANE, you can securely indicate the X.509 certificate to use. [#DNSSEC](#) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



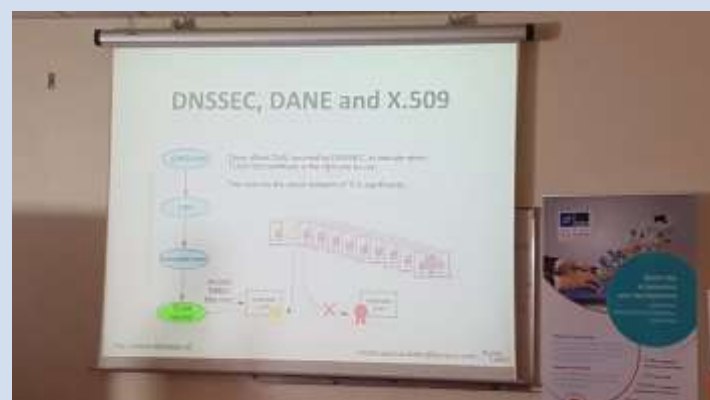
[#jcsa16](#) DANE = a TLSA record published in the DNS

[Récamier @samiamtimet](#)



DANE : solution contre le "too many CA". [#JCSA16](#)
pic.twitter.com/SHkxz2Mzr7

[Johann @adofou](#)



An european speaker saying "the first mile" instead of "the first kilometer". Europe is doomed. [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



Dans le contexte de la préz à [#JCSA16](#), rappel du dossier thématique [@AFNIC](#) sur le sujet de [#DANE](#) : afnic.fr/fr/l-afnic-en-...

[Mohsen Souissi @Mo7sen](#)



"The first mile" host -> resolver. (DNSSEC c'est bien joli mais ça ne traite pas cette étape) [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



[Mohsen Souissi @Mo7sen](#)

And even [#Brexit](#) didn't help :-) [#JCSA16](#)
[twitter.com/bortzmeyer/sta...](https://twitter.com/bortzmeyer/status/728111111111111111)



[Pierre Beyssac @pbeysac](#)

Donc se pose éventuellement la question d'authentifier le
 resolver également. [#jcsa16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

B. Overeinder speaking about securing between machine and
[#DNS](#) resolver ("the first kilometer") Example:
[labs.ripe.net/Members/babak ...](https://labs.ripe.net/Members/babak...) [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

[#DNS](#) over [#TLS](#), ça fait un peu cher la requête, mais ça a bien
 des avantages de nos jours... [#DPRIVE](#) [#Privacy](#) [#JCSA16](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) securing the "first mile" (from a host to its validating
 full resolver) : DNS over TLS Queries & responses encrypted.
[#DPRIVE](#)



[Pierre Beyssac @pbeysac](#)

[#DPRIVE](#): [#DNS](#) over TLS. TLSA records for stub/app to ful
 recursor. DNS queries authenticated over the wire. [#jcsa16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Securing the first kilometer: DNS-over-TLS: encrypt for
 privacy. [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

Open source software for security at all levels host -> resolver
 -> auth name servers / web sites. [#jcsa16](#)



[OpenPony @OpenPony](#)

Dans la lignée des perspectives et de l'enquête de fond de l'
[@AFNIC](#) sur l'avenir du réseau exposé lors de [#JCSA16](#) :
numerama.com/politique/1816...



[Mohsen Souissi @Mo7sen](#)

. [@NLnetLabs](#) has a software solution to all the issues
 presented at [#JCSA16](#) : [#OpenDNSSEC](#), [#NSD](#) & [#Unbound](#) &
[#getdns](#) API [#ldns](#). Kudos!



Summary: encrypt all! [#DNS](#) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[Johann @adofou](#)

Conclusion : déployer DNSSEC et DANE [#JCSA16](#)
pic.twitter.com/N31OH4tOmD



[gum @agumonkey](#)

[#JCSA16](#) Lunar slides afnic.fr/medias/documenten...



[Récamier @samiamtimet](#)

[#jcsa16](#) Benno Overeinder from [@NLnetLabs](#) Conclusion :
 Deploy [#DNSSEC](#) !!! pic.twitter.com/1MeRmaAlqA



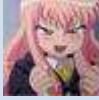
[OpenPony @OpenPony](#)

Encrypt all in face of privacy and confidentiality (RFC7624)
[#JCSA16](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) [@Mo7sen](#) explique que les blocages au déploiement de [#DANE](#) se situe au niveau des navigateurs



Johann @adofou

C'est partie pour deux conférence de l'[@ANSSI_FR](#) à [#JCSA16](#)
pic.twitter.com/chMuXEI4PO



Mohsen Souissi @Mo7sen

De la neutralité de l'Internet sans fil... [#JCSA16](#)
[twitter.com/OpenPony/statu...](https://twitter.com/OpenPony/status...)



BIAOU Ramanou @RamanouB

[@ANSSI_FR](#) est au [#JCSA16](#) pour présenter l'observatoire de la résilience de l'Internet française.



Récamier @samiamtimet

[#jcsa16](#) Guillaume Valandon présente l'observatoire de la Résilience de l'internet en France.
pic.twitter.com/dMCCDuuF2x



OpenPony @OpenPony

Présentation de l'Observatoire de la résilience de l'internet Français par [@ANSSI_FR](#) ssi.gouv.fr/agence/rayonne...
[#JCSA16](#)



Johann @adofou

Les outils utilisés par [@ANSSI_FR](#) pour leurs observations sont open source et disponibles sur Github [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

Guillaume Valadon & Maxence Tury de l'[@ANSSI_FR](#) présentent l'étude annuelle de l'obs. de la résilience de l'Internet français. [#jcsa16](#)



[Mohsen Souissi @Mo7sen](#)

Intro par [@guedou](#), puis zoom [#TLS](#) par Maxence Tury (ANSSI)
[#JCSA16](#) [twitter.com/RamanouB/statu...](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Outils ANSSI pour les analyses [#BGP](#) : Mabo et Tabi
[github.com/ANSSI-FR](#) [#OcamlRulez](#) [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

Les URL présentées même sur Github sont en http plutôt que https, tradition ANSSI pour imiter son propre site :-P ?
[#jcsa16](#)



[OpenPony @OpenPony](#)

Des outils ont été développés par [@ANSSI_FR](#) pour détecter les erreurs : [github.com/ANSSI-FR/mabo](#) [github.com/ANSSI-FR/tabi](#) [#JCSA16](#)



[Johann @adofou](#)

Quelques chiffres sur les annonces BGP d'acteurs Français.
[#JCSA16](#) [pic.twitter.com/z5SqvGotlv](#)



[Récamier @samiamtimet](#)

[#jcsa16](#) Rapport de l'Observatoire de la Résilience de l'Internet en France publié par l'[@ANSSI_FR](#) en juin. Version anglaise en septembre



[AFNIC @AFNIC](#)

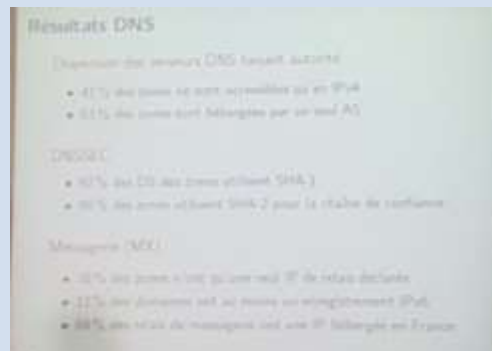
[#JCSA16](#) [@guedou](#) ([@ANSSI_FR](#)) présente l'Observatoire de la résilience Internet français 2015 [afnic.fr/fr/l-afnic-en-...](#)
[pic.twitter.com/hV20JPpvhE](#)





Johann @adofou

Quelques chiffres sur les DNS des .fr [#JCSA16](#)
pic.twitter.com/DrU9zksQc7



Pierre Beyssac @pbeysac

41% des zones DNS ne sont accessibles qu'en IPv4 (en France). 10% des zones utilisent DNSSEC. 92% avec SHA-1, 98% avec SHA-2. [#jcsa16](#)



Stéphane Bortzmeyer @bortzmeyer

"69 % des domaines en .fr ont un MX en France" Tournant sur l'[@ossouverain](#) ? [#JCSA16](#)



BIAOU Ramanou @RamanouB

41 % des zones ne sont accessibles qu'en IPv4 [#JCSA16](#)



OpenPony @OpenPony

6392 conflits d'annonces détectés
 26 usurpations avérées détectées
 avec les outils tabi et mabo de [@ANSSI_FR](#)
[#JCSA16](#)



Pierre Beyssac @pbeysac

Pour la première fois, l'étude s'est intéressée à SSL/TLS.
[#jcsa16](#)



Mohsen Souissi @Mo7sen

Pour la première fois [#TLS](#) est introduit dans l'ensemble des indicateurs de résilience étudiés par l'Observatoire ([#ODRIF](#)).
[#JCSA16](#)



Récamier @samiamtimet

[#jcsa16](#) Maxence Tury de l'[@ANSSI_FR](#) partie TLS du rapport de l'Observatoire de la Résilience de l'internet en Fr.
pic.twitter.com/QITNzEYbvj





[Pierre Beyssac @pbeysac](#)

Jolie présentation d'une négociation TLS avec github :)

[#JCSA16 pic.twitter.com/mACqweGiBG](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

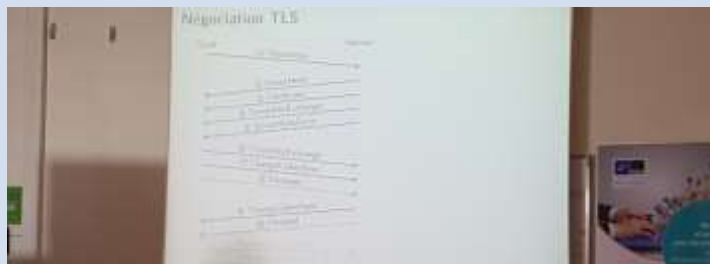
"Je ne vais pas rentrer dans les détails, vous pouvez consulter les RFC." [#TLS](#) [#JCSA16](#)

Comment que ca marche [#TLS?](#) [#JCSA16](#)

[pic.twitter.com/ijO4ICDbCF](#)



[Johann @adofou](#)





Pierre Beyssac @pbeysac

"J'en ai une preuve merveilleuse mais elle ne rentre pas dans la marge" [#famouslastwords](#) [#jcsa16](#)
[twitter.com/bortzmeyer/sta...](https://twitter.com/bortzmeyer/status/7711111111)



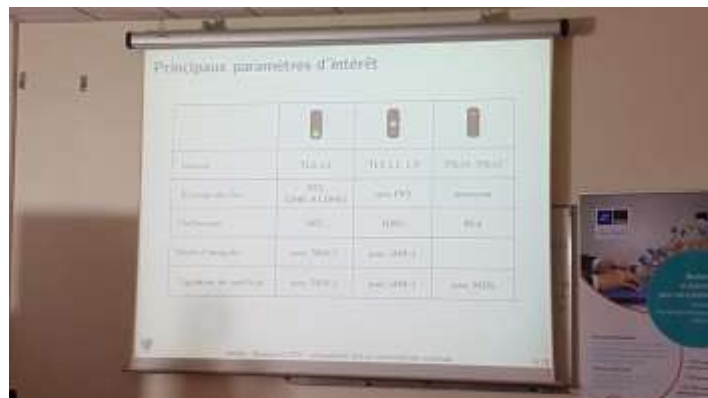
AFNIC @AFNIC

L'Observatoire complet dont parle Maxence Tury de l'@ANSSI_FR est sur afnic.fr/fr/l-afnic-en-... [#JCSA16](#) [#Afnic](#)
pic.twitter.com/HUZt7iHlIT



Johann @adofou

Tu utilises encore SSLv2, SSLv3? Carton rouge! [#JCSA16](#)
pic.twitter.com/i4EO0Ar16



Pierre Beyssac @pbeysac

PFS = "confidentialité persistante". Si la clé privée est compromise, cela ne compromet pas les messages échangés auparavant. [#jcsa16](#)



Pierre Beyssac @pbeysac

La négociation de la version TLS se fait au moment des échanges ClientHello/ServerHello. [#jcsa16](#)



Mohsen Souissi @Mo7sen

Le simple fait même de dire ou d'écrire "SSL" t'expose à des risques juridiques et opérationnels ;-) [#JCSA16](#)
[twitter.com/adofou/status/...](https://twitter.com/adofou/status/7711111111)



Méthodologie : envoyer des TLS ClientHello à plein de serveurs [www.\\$DOMAINE.fr](http://www.$DOMAINE.fr) et regarder les réponses.

[#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



Extraire zone .fr, ajout de www, résolution DNS, randomisation des IP, si port 443 ouvert : négociation TLS ClientHello. [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Ca ressemble bcp a SSLScan ce que raconte l'orateur aux

[#JCSA16](#)

[Sebdraven @Sebdraven](#)



On parse avec parsifal, disponible sur le github de l'[@ANSSI_FR](#), puis base SQL. [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Entre 2014 et 2015 : fort adoption de TLS1.2 [#JCSA16](#)
pic.twitter.com/iAWeuB5yet

[Johann @adofou](#)



Résultats : TLS 1.2 en forte croissance (54% en 2014 -> 75% en 2015). (NB c'est le seul TLS qui ne soit pas grossièrement troué) [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



75 % des serveurs interrogés gèrent le TLS 1.2 (en rapide progrès). 16 % de mauvaises réponses (timeout, SSH...)

[#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[#jcsa16](#) TLS 1.2 augmentation significative courant 2015 : 75% des serveurs web.

[Récamier @samiamtimet](#)



L'étude a aussi trouvé du http "en clair" ainsi que du SSH sur port 443. [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Juste au passage...

C'est moche la limitation des champs certs x.509 ☹

Abréviation @AFNIC

#JCSA16 pic.twitter.com/Xsh9AWWOn4

[Alexandre SIMON @asimonstweets](#)



Près de 3/4 des serveurs https interrogés (en .fr) supportent la #TLS 1.2

Cool :-) Mais faut poursuivre l'effort ! #JCSA16

[Mohsen Souissi @Mo7sen](#)



Encore 18 % des serveurs qui répondent en SSLv2... (En légère baisse) #JCSA16

[Stéphane Bortzmeyer @bortzmeyer](#)



#jcsa16 "SSL v2 obsolète et dangereux" Maxence Tury de l'@ANSSI FR

[Récamier @samiamtimet](#)



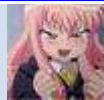
SSLv2 (officiellement obsolète) accepté par trop de sites (baisse de 22% à 18%). [note de service : se sortir les doigts du..] #jcsa16

[Pierre Beyssac @pbeysac](#)



1 serveur sur 5 parlait encore SSLv2 en 2015 ! "C'est quand même relativement gênant" dixit l'orateur. #JCSA16

[Mohsen Souissi @Mo7sen](#)



En 2015. Encore 1/5 serveurs prennent en charge SSLv2 (ultra obsolète et dangereux). #JCSA16

[Johann @adofou](#)



MaBo - MRT and BGP parser in OCaml github.com/ANSSI-FR/mabo #jcsa16

[Guillaume Valadon @guedou](#)



1 serveur sur 5 qui soit capable de parler SSLv2 [#JCSA16](#)

[Haelwenn\['elwen'\] @lanodan](#)



TaBi - Track BGP Hijacks github.com/ANSSI-FR/tabi [#jcsa16](#)

[Guillaume Valadon @guedou](#)



Prise en charge de la PFS : de 50% à 74% \o/ "la PFS n'est pas un mythe, elle existe bel et bien" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Solution de PFS (Confidentialité persistance) : Passage de 50 à 74% des serveurs compatibles entre 2014 et 2015 [#JCSA16](#)

[Johann @adofou](#)



Parsifal : an OCaml-based parsing engine github.com/ANSSI-FR/parsi... [#jcsa16](#)

[Guillaume Valadon @guedou](#)



Près de 3/4 des serveurs https offraient la [#PFS](#) en 2015. Plutôt positif. [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)



Scapy: the python-based interactive packet manipulation program & library github.com/secdev/scapy [#jcsa16](#)

[Guillaume Valadon @guedou](#)



55% des certificats observés (avant : 3%) signés avec SHA-2. Bonne progression. Chute symétrique de SHA-1. [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Bonne augmentation de l'utilisation de SHA-2 à 55% en 2015. Mais encore 44% des serveurs sont compatibles SHA-1 [#JCSA16](#)

[Johann @adofou](#)



[#jcsa16](#) signature basées sur SHA-2 en progression : 55% des signatures en 2015.

[Récamier @samiamtimet](#)

[Mohsen Souissi @Mo7sen](#)

La proportion des certificats TLS utilisant SHA-2 est passée de 3% à 55% entre 2014 et 2015. [#JCSA16](#)

[Johann @adofou](#)

L'essentiel des certificats émis en 2015 sont maintenant chiffrés en SHA-2 (89%) [#JCSA16](#)

[Pierre Beyssac @pbeysac](#)

Nombreux param pour juger d'un serveur TLS. Longue réflexion sur ce qui était pertinent. [#jcsa16](#). TLS 1.2 DHE SHA-2 ont le vent en poupe.

[BIAOU Ramanou @RamanouB](#)

SSLv2 persiste alors qu'il faut l'abandonner. Idem pour SSLv3 [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)

En conclusion :

[#JCSA16 pic.twitter.com/QipJavs9gt](#)

Conclusion

- Nombreux paramètres à observer pour juger d'un serveur TLS
- SSLv2 persiste alors qu'il faut l'abandonner (comme SSLv3)
- TLS 1.2, DHE et les signatures SHA-2 se répandent bien

[Pierre Beyssac @pbeysac](#)

Points à ajouter : automatisation, prise en charge des suites cryptographiques, guide de reco TLS [v/o], reversement scapy-TLS [#jcsa16](#)

[Récamier @samiamtimet](#)

[#jcsa16](#) conclusion de Maxence Tury : TLS 1.2, DHE, signatures SHA-2 préconisés et en cours d'adoption [pic.twitter.com/FBJffRflmr](#)





L'attaque utilisant SSLv2 dont parle Maxence est DROWN
[#jcsa16](https://drownattack.com)

Guillaume Valadon @guedou



Je dirais même plus, il faudrait ne garder que TLS 1.2 [les
gourous complèteront/me corrigeront le cas échéant]
@Mo7sen #icsa16

Pierre Beyssac @pbeysac



リアルパンダさん mark 2.2
@real_panda3

英語以外だと全く分からんでござる。
何語だかも分からんでござる。あとで動画(スライド付きで)上がるみたいだから動画見よう。
NLnetLabsさんは英語でDNSSEC/DANE/DPRIVEとか使おうぜ的なお話をされていたのかな。動画カクカク&聞き取れずワロタ。
#JCSA16



[#jcsa16](#) Guide de recommandations de sécurité [#TLS](#) sera publié cet été par l'[@ANSSI](#) FR

Récamier @samiamtimet



@[ANSSI_FR](#) envisage l'automatisation des mesures pour faire plus de mesures et avoir plus de précisions. #JCSA16

BIAOU Ramanou @RamanouB



Q : "Envisagez-vous de rendre publiques les données collectées" "pas vraiment, il y a scans.io" #jcsa16

Pierre Beyssac @pbeysac



Point [#opendata](#) suite à la conf @[ANSSI_FR](#) : pas d'intérêt de publier les datas [#JCSA16](#)

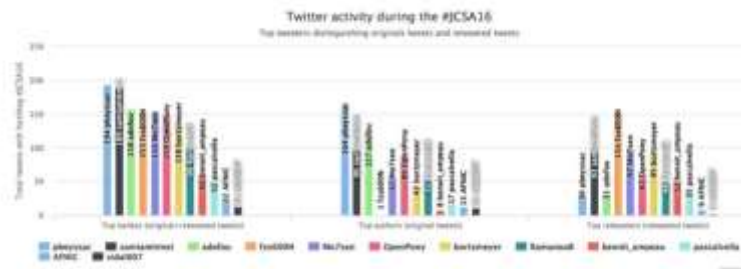
OpenPony @OpenPony



Et hop, je viens de gagner une place :-)
twest.io/jcsa16/

Mohsen Souissi @Mo7sen

#JCSA16 pic.twitter.com/63grMHY6Gd





Un serveur sur 5 continuait à faire du SSLv2 et la moitié des certificats restaient en SHA-1 en 2015 [#JCSA16](#)

[OpenPony @OpenPony](#)



J'ai 5 tweets de retard sur [@pbeysac](#). Faut que je m'active :) [#jcsa16 twitter.com/Mo7sen/status/...](#)

[Récamier @samiamtimet](#)



Le [#TagCloud](#) de [#JCSA16](#) : [pic.twitter.com/2hwJfuvH7](#)

[Mohsen Souissi @Mo7sen](#)

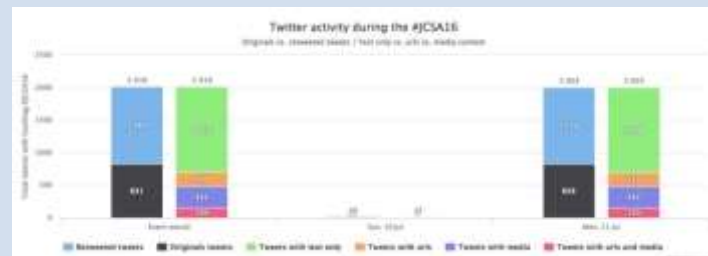
Words cloud of most tweeted words during the event



Go go go [@Mo7sen](#) !

Par la même occasion, la [#JCSA16](#) vient de passer les 2000 tweets (dont 831 originaux) [pic.twitter.com/nYHvwUOuvv](#)

[Twest io @Twest io](#)



[@adofou](#) [@pbeysac](#) carrément [#jcsa16](#) :p

[Récamier @samiamtimet](#)



[@pbeysac](#) Cela élimine, par exemple, une moitié des Android (Google a mis longtemps à inclure TLS 1.2) [#JCSA16](#)

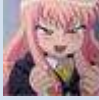
[Stéphane Bortzmeyer @bortzmeyer](#)



[@samiamtimet](#), [@pbeysac](#) a triché en commençant la course avt tt le mde... Je demande à l'arbitre [@asimonstweets](#) de le disqualifier !

[#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)



Johann @adofou

Beaucoup de question sur les mesures et la méthodologie
[#JCSA16](#)

CryptoParty Rennes
@CryptoPartyRNS

[#JCSA16](#) en plus de l'[@ANSSI_FR](#), les éditeurs de navigateurs publient de outils pr générer des confs TLS "solides":
mozilla.github.io/server-side-tl...



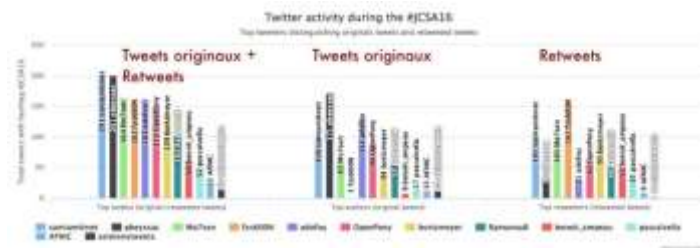
Récamier @samiamtimet

[#JCSA16](#) 1 campagne de mesures TLS c'est de l'ordre de 1 Go mais toute la zone. Fr n'est pas prise en compte.



Twest io @Twest_io

@adofou @samiamtimet @pbeysac Checkez bien les graphes : la 2ème colonne donne le top twittos "originaux"
[#JCSA16](#) pic.twitter.com/ARcXmq5nuS



Stéphane Bortzmeyer @bortzmeyer

Dernière présentation, @X_Cli sur "Certificate transparency" et le groupe [#IETF](#) "trans". Encore trop d'AC [#JCSA16](#)



Pierre Beyssac @pbeysac

Dernière présentation : Florian Maury @X_Cli de l'[@ANSSI_FR](#), sur "public notary transparency" [#jcsa16](#)



Johann @adofou

Dernière conférence de l'[@ANSSI_FR](#) à la [#JCSA16](#)
pic.twitter.com/d9G61UKcZ1





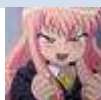
+600 autorités de certification : nombreux rapports d'incidents. Changer système de confiance, réduire nombre ? renforcer ? [#JCSA16](#)

[OpenPony @OpenPony](#)



[#JCSA16](#) Florian Maury de l'[@ANSSI_FR](#) à propos d'un groupe de travail de l'[@ietf](#) pic.twitter.com/mZKjyJely

[Récamier @samiamtimet](#)



Plus de 600 autorité de certifications! Autant de possibilité d'avoir un problème de sécurité [#JCSA16](#)

[Johann @adofou](#)



Un système apparemment un peu inspiré de la [#blockchain](#) (aspect public) :-P [note perso] [#icsa16](#)

[Pierre Beyssac @pbeysac](#)



[#FlorianMaury](#) de l'[@ANSSI_FR](#) nous parle des registres publics en ajout seul et leurs usages avec TLS. [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



Journalisation publique des certificats émis répond aux problématiques [#JCSA16](#)

[OpenPony @OpenPony](#)



Solution : mettre les certificats émis dans une base de données publique et vérifiable. [#tousÀpoil](#) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



Surprise, on retrouve les arbres de Merkle. [#icsa16](#) Usages : Git, Bitcoin, Bittorrent.

[Pierre Beyssac @pbeysac](#)



[#JCSA16](#) @X_Cli présente l'arbre de Merkle (1979). Utilisé dans [#Bitcoin](#) et [#Bittorrent](#)

[Récamier @samiamtimet](#)



Arbre de Merkel revient. Hachage Cryptographiques [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)



"Vous utilisez de la crypto tous les jours sans le savoir" [#fear](#) [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



La boucle est bouclée ! On revient à l'arbre de Merkle ! [#JCSA16](#)

[OpenPony @OpenPony](#)



[#JCSA16](#) Certificate Transparency draftcRFC 6962 bis

[Récamier @samiamtimet](#)



Le RFC décrivant actuellement "Certificate Transparency" bortzmeyer.org/6962.html [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



Stockage des certificats dans une base de donnée avec une possibilité d'ajout seul. Pas de suppression possible. [#JCSA16](#)

[Johann @adofou](#)



"journaliser les certificats émis par les AC publiques, permettre détection émissions frauduleuses." [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



La journalisation des certificats permet la détection des émissions défectueuses ou frauduleuses [#JCSA16](#)

[OpenPony @OpenPony](#)



Acteurs TLS : client, serveur, AC. Nouveaux : mainteneur de journaux, moniteurs, auditeurs. [#jcsa16](#) [sent la [#blockchain](#) en tech classique]

[Pierre Beyssac @pbeysac](#)



[OpenPony @OpenPony](#)

Tout le monde peut soumettre un certificat valide, les autorités de certification le font, mieux de le faire sur plusieurs journaux [#JCSA16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Et, sur l'idée de vérification publique
bortzmeyer.org/tousapoil.html [#JCSA16](#) [#jeHijackeLesConfs](#)



[Pierre Beyssac @pbeysac](#)

"Journalisation effective après délai" "engagement de journal." (objet crypto) remis au soumissionnaire. Peut constituer preuve dysf [#jcsa16](#)



[OpenPony @OpenPony](#)

Engagements de journalisation distribués aux navigateurs permettant les vérifications [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

"Si l'engagement est absent/futur/invalidé alors erreur" (dès la transaction TLS) [#jcsa16](#)



[OpenPony @OpenPony](#)

Si engagement absent ou émis dans le futur ou signatures invalides : ERREUR ! [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

Ceux qui s'intéressent à l'Arbre de Merkle (rien avoir avec Angela !), wikipedia en parle :
fr.wikipedia.org/wiki/Arbre_de_...
[#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

"Le navigateur joue rôle de l'auditeur" "partage preuve de journalisation par rumeur" protection contre partitionnements de vue [#jcsa16](#)



[OpenPony @OpenPony](#)

Vérification de l'honnêteté du journal pour s'assurer que tout le monde a bien la même preuve d'insertion : rôle d'auditeur
[#JCSA16](#)



[Johann @adofou](#)

Il y a connexion entre les navigateurs et les journaux. Un niveau de sécurité en plus dans la détection de faux certificats [#JCSA16](#)



@[bortzmeyer](#) Merkle plutôt ... :)
je l'invite au [#JCSA16](#) :-)

[BIAOU Ramanou @RamanouB](#)



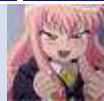
"Les titulaires de sites web vont devoir télécharger
l'intégralité des journaux" [euh wait, what ?] [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



[#JCSA16](#) seules implémentations de Certificate Transparency
: Chrome et Chromium pour l'instant.

[Récamier @samiamtimet](#)



Malheureusement seul Chrome et Chromium sont
partiellement compatible pour l'instant. [#JCSA16](#)

[Johann @adofou](#)



Seul client TLS compatible de Certificate Transparency :
Chrome/Chromium : pas de vérif asynchrone, stockage en
cache... [#JCSA16](#)

[OpenPony @OpenPony](#)



"Seul client TLS compatible à ce jour : Chrom(e|mium)"
"Implém partielle" "Rumeur mais réservée GG" "Dur pour
application tierce" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Déjà qu'ils ne testent pas leurs configs DNS, qu'ils ne
supervisent pas... [twitter.com/pbeysac/statu...](#) [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



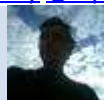
"Au moins un engagement émis par Google et un autre par
un tiers" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



En cas d'échec de vérification d'engagement : Perte du statut
EV. Aucun impact sur DV et OV [#JCSA16](#)

[OpenPony @OpenPony](#)



"La barre rouge prouve que le système marche" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



Toutes les AC dont le statut EV est reconnu par Chromium participent à la Certificate Transparency [#JCSA16](#)

[OpenPony @OpenPony](#)



Symantec (qui a eu de gros pb) et CNNIC soumettent tous leurs certificats à ce système. [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



"9 journaux utilisés dont 3 administrés par Google." "C'est déjà mieux que 600 AC". [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



[#JCSA16](#) Certificate Transparency : 9 journaux utilisés dont 3 administrés par Google

[Récamier @samiamtimet](#)



Ça commence à me poser problème cette conf niveau neutralité du net cette histoire de journalisation administrée par Google [#JCSA16](#)

[OpenPony @OpenPony](#)



9 journaux existant. Environ 40Go de donnée compressé pour 22M de certificats dans la base de donnée. [#JCSA16](#)

[Johann @adofou](#)



Plus gros journal 22M de certificats, qqes dizaines de Go compressés (raté le nombre) à stocker. [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)



nginx → 1.9 // Apache → encore dans les versions de dev (pour une fois) [#JCSA16](#)

[Haelwenn 'elwen' @lanodan](#)



[@OpenPony](#) Ce n'est pas différent de Google ayant un "exit node" Tor ou bien Google ayant des mineurs Ethereum. [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[@OpenPony](#) L'important, c'est qu'il y ait pluralisme. [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)



[Pierre Beyssac @pbeysac](#)

[#DANE](#) d'un côté, AC X.509 & Google & Chrome de l'autre.
[#jcsa16](#) [twitter.com/OpenPony/statu...](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Je découvre que le certificat X.509 de l'[@AFNIC](#) est dans un journal "Certificate Transparency" [#JCSA16](#)



[Haelwenn\['elwen'\] @lanodan](#)

Un lien du truc pas compilable ? [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

C'est 40 Go (compressés par Gzip)

[#JCSA16](#) [twitter.com/pbeysac/statu...](#)



[BIAOU Ramanou @RamanouB](#)

[@OpenPony](#) effectivement [#JCSA16](#)



[Pierre Beyssac @pbeysac](#)

"Petit problème : la vie privée car tous les certificats sont visibles. Exemple, Google en a 2048" [#jcsa16](#)



[Johann @adofou](#)

Google à 2048 certificats enregistré dans digicerts
[#BlagueDeGeek](#) [#JCSA16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

[@pbeysac](#) C'est aussi le cas avec SSL Observatory, non ?
[#JCSA16](#)



[Johann @adofou](#)

Grâce à CT, Google à pu voir que Symantec avait sous estimé le nombre de certificats généré frauduleusement [#JCSA16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

Grâce à Certificate Transparency, on a détecté le certificat LE demandé par le stagiaire, en violation des règles de \$CORPORATION. [#JCSA16](#)

[Johann @adofou](#)

Grâce à CT, détection d'une violation des politiques interne de Facebook pour la génération de deux certificats par un prestataire [#JCSA16](#)

[Stéphane Bortzmeyer @bortzmeyer](#)

Titulaires de noms de domaine : surveillez les journaux Certificate Transparency, conseille [@X_Cli](#) [#JCSA16](#)

[Récamier @samiamtimet](#)

[#JCSA16](#) conclusion lrs certificats EV apportent des assurances supplémentaires avec

[Pierre Beyssac @pbeysac](#)

"Certificate Transparency" "déjà déployé [si vous utilisez Chrom*]" "ça fait une barre verte" "assurances supplémentaires" [#jcsa16](#)

[Pierre Beyssac @pbeysac](#)

"General Transparency" "2 journaux + 1 arbre de Merkle creux" CRL, publication de politiques, remplacement DNS (!) [#jcsa16](#)

[Récamier @samiamtimet](#)

[#JCSA16](#) l'arbre de Merkle creux permettrait de remplacer tout le DNS.

[Pierre Beyssac @pbeysac](#)

Est-ce que c'est X.509 qui va tuer le DNS, ou DNS+DANE qui va tuer X.509 :-P [note perso] [#icsa16](#)

[Johann @adofou](#)

[#JCSA16](#) [@Mo7sen](#) est ravi d'avoir autant d'intervenant qui proposent des solutions de remplacement de [#DNS](#) :-)

[Récamier @samiamtimet](#)

[#JCSA16](#) [@Mo7sen](#) "Aujourd'hui plusieurs OPA sur le [#DNS](#)"

[Stéphane Bortzmeyer @bortzmeyer](#)

[@tzim](#) Un seul logiciel libre, que [@X_Cli](#) n'a pas réussi à compiler. Sinon, des sites Web (genre "looking glass"). [#JCSA16](#)

[BIAOU Ramanou @RamanouB](#)

Eventuelle offre de remplacement de DNS = forçement problème avec ICANN. Le chemin est long ... [#JCSA16](#)



Pierre Beyssac @pbeysac

Parce qu'en plus il va falloir surveiller les logs :-D [#jcsa16](#)
[twitter.com/bortzmeyer/sta...](https://twitter.com/bortzmeyer/status/724444444444444444)



Récamier @samiamtimet

[#JCSA16](#) rejoignez l' @AFNIC pic.twitter.com/NeN3PiBNTk



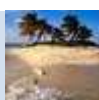
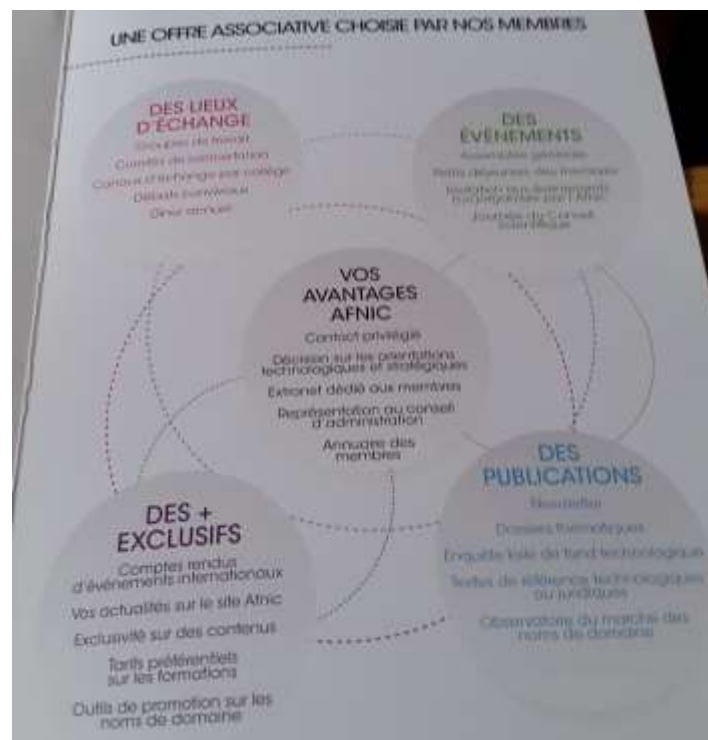
Pierre Beyssac @pbeysac

"On résout le problème du "too big too fail", si un journal fait mal son travail, on le vire" [et si c'est Google ?] [#jcsa16](#)



Récamier @samiamtimet

[#JCSA16](#) rejoignez l' @AFNIC pic.twitter.com/tnPOgEMHxQ



Mohsen Souissi @Mo7sen

Oui, il faut tout surveiller :-D [#JCSA16](#)
[twitter.com/pbeysac/statu...](https://twitter.com/pbeysac/status/724444444444444444)



[suinot remi @rsuinux](#)

@[pbeysac](#) @[bortzmeyer](#) #jcsa16 est ce qu'on pourrait voter démocratiquement avec la blockchain (ie +qu'avec les machins à voter) ?



[Stéphane Bortzmeyer @bortzmeyer](#)

"Certificate Transparency *est* une blockchain"
[#blockchainEverywhere](#) [#JCSA16](#)



[Mohsen Souissi @Mo7sen](#)

Non sans une pointe d'humour sur les OPA multiples sur le [#DNS](#) :-)



[Pierre Beyssac @pbeysac](#)

[#JCSA16](#) [twitter.com/adofou/status/...](#)

"[#Firefox](#) a un patch ouvert depuis 2013 et qui est très actif donc bientôt tout le monde va l'avoir" [#jcsa16](#)



[Stéphane Bortzmeyer @bortzmeyer](#)

@[tzim](#) @[X_Cli](#) vient de préciser : aller en [crt.sh](#) ou [digicert.com/secure/monitor...](#) ou un truc équivalent.
[#JCSA16](#)



[CryptoParty Rennes @CryptoPartyRNS](#)

[#JCSA16](#). En conclusion: "Vérifiez vos certificats, c'est ça la surveillance". Merci !' @[ANSSI_FR](#) ;)



[Mohsen Souissi @Mo7sen](#)

Je finis #4 du Top [#N](#) twittos de [#JCSA16](#), c'est honorable. Je félicite les gagnants !
[twtest.io/jcsa16/](#)



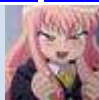
[OpenPony @OpenPony](#)

Fin de [#JCSA16](#) Merci à @[AFNIC](#) pour cette super journée :)



[Sebdraven @Sebdraven](#)

Merci aux organisateurs [#JCSA16](#) pour cette journée. C'était vraiment très instructif. Etrange qu'il n'y ait pas plus de CERT qui soient venus



[Johann @adofou](#)

Fin de la [#JCSA16](#). Très bonne journée. Riche et enrichissante.



Pierre Beyssac @pbeysac

[#jcsa16](#) terminé, fin ou quasi fin du flood, merci de votre patience :)



noueP lueinel @lpenou

[#JCSA16](#) Merci à @AFNIC & Talkeurs pour cette super journée :)



Récamier @samiamtimet

[#jcsa16](#) @ltn22 remercie l'auditoire, les présents et Télécom Paris



Guillaume Valadon @guedou

Merci pour ces [#jcsa16](#) !



BIAOU Ramanou @RamanouB

Donner votre avis sur le [#JCSA16](#)
fr.surveymonkey.com/r/EngSatisfJCS...



BIAOU Ramanou @RamanouB

Très belle journée du [#JCSA16](#) rendez-vous en 2017 :) Merci à @AFNIC



Régis MASSÉ @remasse

Bravo à @Mo7sen pour ces années d'animation du Conseil Scientifique et bon courage à @benoit_ampeau et @bortzmeyer pour la suite [#JCSA16](#)



fzs600 @fzs600N

[#JCSA16](#) merci pour ces conférences très intéressants a l'année prochaine



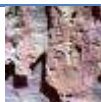
AFNIC @AFNIC

[#JCSA16](#) c'est fini ! Merci à tous pour votre présence & vos tweets ! En attendant l'an prochain le replay demain sur afnic.fr/fr/l-afnic-en-...



Pascal Vella @pascalvella

[#JCSA16](#) c'est fini merci à tous les participants !



[DataPrivacy @privacy_data](#)

ICYMI Supports de conf @AFNIC afnic.fr/fr/l-afnic-en-... & dossier thématique sur protocole #DANE afnic.fr/medias/documen... h/t @Mo7sen #JCSA16



[CryptoParty Rennes @CryptoPartyRNS](#)

#JCSA16: Grand merci à @ltn22 @Mo7sen @pascalvella @AFNIC pour l'orga et les talks originaux sur la #cryptographie #sécurité & #privacy !



[Twest.io @Twest.io](#)

Clap de fin sur la #JCSA16 by @AFNIC. Quelques chiffres sur cette journée de folie :
2369 tweets (942 originaux)
+202% p/r à 2015
1/7



[Twest.io @Twest.io](#)

Clap de fin sur la #JCSA16 by @AFNIC. Quelques chiffres sur cette journée de folie :
🐦twittos :
1 @fzs600N
2 @pbeysac
3 @samiamtimet
2/7



[Twest.io @Twest.io](#)

Clap de fin sur la #JCSA16 by @AFNIC. Quelques chiffres sur cette journée de folie :
👤auteurs:
1 @pbeysac
2 @adofou
3 @samiamtimet
3/7



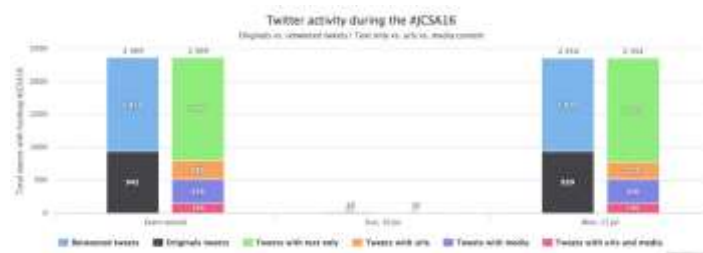
[Pierre Beyssac @pbeysac](#)

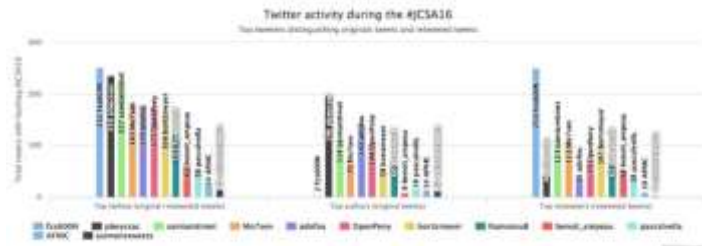
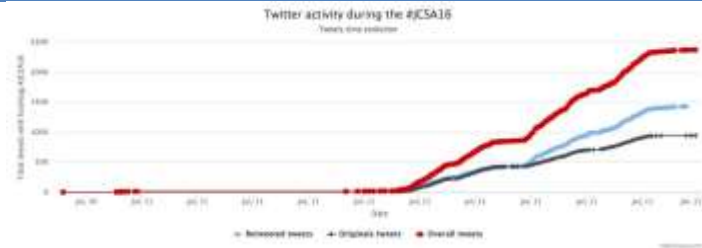
Votre serviteur coiffé au poteau. #jcsa16. Bravo @fzs600N mais aussi @samiamtimet @Mo7sen @adofou @bortzmeyer. [twitter.com/Twest.io/statu...](https://twitter.com/Twest.io/status...)



[Twest.io @Twest.io](#)

Clap de fin sur la #JCSA16 by @AFNIC. Quelques images sur cette journée de folie.
twest.io/jcsa16/
6/7 pic.twitter.com/SHeAVh56VZ





Twist io @Twist io

Clap de fin sur la [#JCSA16](#) by [@AFNIC](#). Arrêt des stats [#Twext](#) io demain (mardi) à 12h.

Encore un peu de temps causer [#JCSA16](#) !
7/7



@pbeysac @samiamtimet @Mo7sen @adofou
@bortzmeyer Merci.

C'était amusant et les conférences intéressantes #JCSA16

fzs600 @fzs600N



Alexandre SIMON @asimonstweets

Ma journée [#JCSA16](#) by [@AFNIC](#) :

- accueil ?
- prés ? (niveau tech +++)
- discussions off ?

Le roi @Mo7sen part, vive le roi @benoit ampeau !



X Cli Public @X Cli Public

@pbeysac @lhirlimann @X_Cli @firefox Je disais juste qu'une fois dans NSS, d'autres pourraient l'utiliser : bugzilla.mozilla.org/show_bug.cgi?id=105416 #JCSA16



X Cli Public @X Cli Public

#JCSA16 Thanks @Mo7sen and @AFNIC for this event.
Thanks to the speakers for their time and efforts! :)

[Mohsen Souissi @Mo7sen](#)

Mais [#OverTheTop](#), c'était ton excellente animation de la twittosphère [#JCSA16](#) avant et pendant l'évènement ! :-)
[twitter.com/asimonstweets/...](https://twitter.com/asimonstweets/)

[Mohsen Souissi @Mo7sen](#)

@[X_Cli_Public](#) Merci à toi et à tous les orateurs et participants à [#JCSA16](#) @[AFNIC](#)

[X_Cli_Public @X_Cli_Public](#)

@[pbeyssac](#) À noter que l'idée de remplacement du DNS n'est pas basé sur les certs X.509. Juste sur General Transparency ;) [#Merkle](#) [#JCSA16](#)

[Mohsen Souissi @Mo7sen](#)

Je vous demande d'arrêter de mettre la pression sur [@benoit_ampeau](#) ! Il suffit :-)
[#JCSA16](#)
twitter.com/remasse/status...

[X_Cli_Public @X_Cli_Public](#)

Yep. Tout ce que je sais de Bitcoin est dans ce bouquin !
[#JCSA16](#) twitter.com/samiamtimet/st...

[Prunus @OpenPrunus](#)

Une Bonne journée au [#JCSA16](#) aujourd'hui. On a appris tout plein de chose avec de la blockchain, du Tor et du RFC :)
Merci @[AFNIC](#)

[Mohsen Souissi @Mo7sen](#)

@[X_Cli](#) Merci ! Je note cette amélioration et je la transmets à mon successeur [@benoit_ampeau](#) pour les prochaines éditions [#JCSA16](#) :-)

[Mohsen Souissi @Mo7sen](#)

[#Raccourci](#) [#JCSA16](#) : [#Bitcoin](#) emploie des "mineurs" (enfants ? :-)) qui produisent des zéros et qui sont (sous-)payés en [#BTC](#) [#okjesors](#)

[Stéphane Bortzmeyer @bortzmeyer](#)

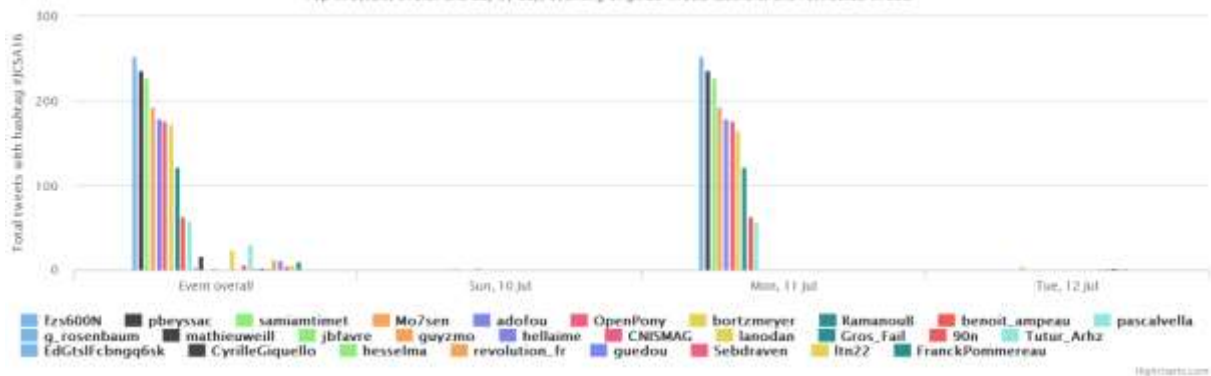
Zéro [#bitcoin](#) reçu malgré le QR-code et l'adresse montrés à [#JCSA16](#) blockchain.info/address/1HtNJ6... [#FAIL](#)

[Stéphane Bortzmeyer @bortzmeyer](#)

Maintenant que [#JCSA16](#) est fini, j'ai eu le temps de finir la saison 6 de [#GoT](#). [#blockchainIsComing](#)

Twitter activity during the #JCSA16

Top tweeters, overall and day by day, counting original tweets (authors) and retweeted tweets



Top retweeted tweets

1

2

3

Luxurious Adventure @LuxuriousAdv
#Paris Trends
Eder
Payet#14juillet
Theresa May
Lisbonne#FausseNote
Graziano
Pelle#JCSA16#RendezNousLaBiscotteSurSnap
4:03 PM - 11 Jul 2016
31 retweets, 2 likes

afnic @AFNIC
Que faire de rigolo avec la blockchain ?
AFNIC
Les slides de @bortzmeyer à #JCSA16 sur la #blockchain sont disponibles sur afnic.fr/fr/l-afnic-en-... #Afnic
9:47 AM - 11 Jul 2016 - Paris, France, France
38 retweets, 26 likes

Luxurious Adventure @LuxuriousAdv
#Paris Trends#Eder
Payet#FausseNote#LouisHasABeautifVoice#JC
Andy Delort
Srebrenica
2:10 PM - 11 Jul 2016
25 retweets, 3 likes

Top favorited tweets

1

2

3

afnic @AFNIC
Suivez #JCSA16 ce matin avec le tuto #blockchain par @bortzmeyer à suivre en direct sur afnic.fr/fr/l-afnic-en-...
9:17 AM - 11 Jul 2016
19 retweets, 14 likes

afnic @AFNIC
Que faire de rigolo avec la blockchain ?
AFNIC
Les slides de @bortzmeyer à #JCSA16 sur la #blockchain sont disponibles sur afnic.fr/fr/l-afnic-en-... #Afnic
9:47 AM - 11 Jul 2016 - Paris, France, France
38 retweets, 26 likes

Alexandre SIMON @asimonstweets
Trop bonne la photo de @adofou... on dirait que @bortzmeyer est en impression sur l'affiche @AFNIC #JCSA16 !
11:01 AM - 11 Jul 2016
8 retweets, 13 likes

