Journal : Conséquences sociales des cryptomonnaies

Posté par **NumOpen** (**page perso**) le 12/09/17 à 22:30. **Licence CC by-sa**
Tags : **futur**, **crypto-monnaie**, **ethereum**, **bitcoin**

Bonsoir,

J'ai acheté des ethereums il y a quelques mois et je m'intéresse progressivement aux crypto-monnaies, à la blockchain et aux conséquences de l'utilisation de ces technologies.
J'ai l'impression que la masse monétaire mondiale va basculer bien plus vite qu'on ne l'imagine sur ces réseaux d'échange, même si les outils pour les utiliser (paiement, stockage, sécurisation, utilisations dérivées) ne sont pas encore prêts. Je suis aussi persuadé que rien n'arrêtera la blockchain et ses applications car elles se basent sur des technologies libres, et sont mondialisées via internet. Ce sera une révolution très brusque, avec des conséquences encore plus grandes que l'arrivée d'internet. Un signe qui ne trompe pas, les banques et les états commencent à paniquer et tentent de les interdire et de les discréditer à grands coups d'articles de presse pleins de fausses vérités, les associant tantôt aux mafias, aux pirates, aux bulles spéculatives, aux chaînes de Ponzi, j'en passe et des meilleures.
Existe-t-il des études sociales vraiment sérieuses sur les changements à venir ?
Peut-on prédire :
- la fin des paradis fiscaux, des doubles comptabilités, du blanchissement d'argent sale.
- la faillite des banques, des organismes de crédit et autres intermédiaires
- la fin de l'inflation et de l'émission de monnaies par les états, pour réduire leur dette
- des systèmes de prélèvement de TVA, taxes, impôts automatisés
- une accélération folle des échanges commerciaux
- un fossé numérique de plus en plus grand
- un coup de fouet donné aux technologies de chiffrement
autres conséquences ?

En tout cas, si quelqu'un trouve un jour la formule magique pour calculer instantanément un grand nombre premier, ça va faire très mal.
Pour faire son choix, le Distrowatch des cryptommonnaies : http://cryptocoin.cc

Très peu d'articles pour l'instant

Posté par **NumOpen** (**page perso**) le 12/09/17 à 22:55. Évalué à 3 (+2/-1).

Tentatives d'interdiction par les états : https://bitcoin.fr/consequences-economiques-et-societales-de-bitcoin/ , une première prédiction qui pourrait se concrétiser : http://kulturegeek.fr/news-120514/chine-aurait-decide-dinterdire-echanges-bitcoin

Le Canada commence à cogiter : http://www.blockchaindailynews.com/Canada--Les-bitcoins-et-les-chaines-de-blocs-les-consequences-pour-les-services-financiers_a25687.html

Sale temps pour les gros c. :
https://www.lesechos.fr/finance-marches/marches-financiers/030556137592-jamie-dimon-le-patron-de-jp-morgan-qualifie-le-bitcoin-de-fraude-2113681.php
http://www.casinoonlinefrancais.fr/nouvelles/warren-buffet-critique-bitcoin-consequences.html

paradis fiscaux

Posté par **Sytoka Modon** (**page perso**) le 12/09/17 à 23:05. Évalué à 10 (+9/-0).

> *la fin des paradis fiscaux*

Ou vois tu la fin des paradis fiscaux dans les crypto monaie ? Au contraire, je n'ai pas encore vu de TVA ni d'impôt au niveau national et européen dessus donc pour le moment, cela me semble plutôt des parfaits paradis fiscaux…

Re: paradis fiscaux

Posté par **NumOpen** (**page perso**) le 12/09/17 à 23:14. Évalué à 3 (+3/-2). Dernière modification le 12/09/17 à 23:15.

Si l'utilisation de crypto-monnaies avec transactions traçables et l'interdiction d'ouverture de comptes anonymes sont imposées à toutes les banques, il deviendra impossible de masquer les transactions, de faire des doubles comptabilités etc.
http://www.numerama.com/politique/234889-la-police-danoise-arrete-un-narcotrafiquant-grace-au-tracage-de-ses-bitcoins.html

Re: paradis fiscaux

Posté par **pulkomandy** (**page perso**) le 13/09/17 à 08:34. Évalué à 10 (+13/-0).

… et n'importe qui pourra savoir combien d'argent tu as sur ton compte en banque. Pour la protection de la vie privée, on repassera.

à quand le premier site marchand qui augmente les prix tout seul quand il voit que tu es riche?

Re: paradis fiscaux

Posté par **devnewton** (**page perso**) le 13/09/17 à 11:26. Évalué à 3 (+2/-1).

Amazon?

--
http://devnewton.bci.im

Re: paradis fiscaux

Posté par **pulkomandy** (**page perso**) le 13/09/17 à 11:41. Évalué à 1 (+1/-2).

J'ai failli l'écrire dans mon commentaire, mais je me suis dit que ça leur ferait de la pub gratuite.

Re: paradis fiscaux

Posté par **khivapia** le 13/09/17 à 13:44. Évalué à 2 (+0/-0).

à quand le premier site marchand qui augmente les prix tout seul quand il voit que tu es riche?
On peut aller plus loin déjà. Savoir que tu es riche, ça se déduit immédiatement de ta navigation sur internet ("on" est déjà capable de savoir à quoi tu t'intéresses, donc si tu as les moyens ou non en décelant quelques-uns de tes achats).
Il faut donc voir plus grand : les magasins qui, grâce à ton smartphone, savent qui tu es peuvent déjà te proposer un prix personnalisé.

Re: paradis fiscaux

Posté par **maclag** le 13/09/17 à 13:04. Évalué à 4 (+1/-0).

En quoi ça serait plus efficace que l'interdiction des comptes anonymes et la suppression de l'argent liquide?
(c'est une vraie question)

Tu t'emballes

Posté par **Renault** (**page perso**) le 12/09/17 à 23:26. Évalué à 10 (+11/-0).

Je trouve que tu t'emballes un peu vite, il y a beaucoup de soucis liés à ces monnaies à résoudre et certaines critiques, provenant des officiels, restent vrais.

> *Un signe qui ne trompe pas, les banques et les états commencent à paniquer et tentent de les interdire et de les discréditer à grands coups d'articles de presse pleins de fausses vérités, les associant tantôt aux mafias, aux pirates, aux bulles spéculatives, aux chaînes de Ponzi, j'en passe et des meilleures.*

Je n'ai pas l'impression que les institutions dont tu parles paniquent. Ils étudient le sujet, émettent des recommandations contre cet usage, cela ne me paraît pas délirant, d'autant qu'il y a du vrai.

Par exemple, Bitcoin (et sans doute d'autres) sont effectivement une sorte de pyramide de Ponzi, car le premier investisseur a pu amasser plein de Bitcoins presque gratuitement, les autres c'est la guerre. La quantité maximale de Bitcoin disponible dans le système montre aussi ses limites.

Puis une monnaie, c'est surtout une question de confiance pour que cela marche. Et manifestement, nous sommes loin d'être au stade où la population a plus confiance en une cryptomonnaie qu'envers le dollar ou l'euro. Tant que cela ne sera pas acquis, je ne vois pas comment ta généralisation pourrait subvenir.

> *Je suis aussi persuadé que rien n'arrêtera la blockchain et ses applications car elles se basent sur des technologies libres, et sont mondialisées via internet.*

Cela n'est pas un gage de réussite, Linux n'est toujours pas sur le bureau de tout le monde et pourtant c'est aussi libre, dispo et développé à travers Internet. Pour qu'une technologie s'impose il faut surtout que cela apporte quelque chose aux utilisateurs. Personnellement je ne suis pas convaincu du réel gain de cette technologie pour une monnaie (jusqu'ici les temps de traitement semblent longs, énergivores, complexes à comprendre). Bref, faut convaincre ta grand mère de l'intérêt de la chose.

> *En tout cas, si quelqu'un trouve un jour la formule magique pour calculer instantanément un grand nombre premier, ça va faire très mal.*

Si cela est possible. Ce dont on ignore (on sait que les ordinateurs quantiques le peuvent, mais les ordinateurs quantiques ne sont de toute façon pas prévus pour être utilisé par tout le monde donc bon).

Re: Tu t'emballes

Posté par **modr123** le 13/09/17 à 00:48. Évalué à 2 (+1/-0).

pour le blockchain ça intéresse beaucoup de banque
https://fr.wikipedia.org/wiki/Blockchain W

> > *En tout cas, si quelqu'un trouve un jour la formule magique pour calculer instantanément un grand nombre premier, ça va faire très mal.*

je vois pas le rapport :)
si on veut casser RSA

> > *Choisir p et q, deux nombres premiers distincts ;*
> > *calculer leur produit n = pq, appelé module de chiffrement ;*
> > *calculer φ(n) = (p - 1)(q -1) (c'est la valeur de l'indicatrice d'Euler en n) ;*
> > *choisir un entier naturel e premier avec φ(n) et strictement inférieur à φ(n), appelé exposant de chiffrement ;*
> > *calculer l'entier naturel d, inverse de e modulo φ(n), et strictement inférieur à φ(n), appelé exposant de déchiffrement ; d peut se calculer efficacement par l'algorithme d'Euclide étendu.*

avec notre ordinateur quantique on calcul p et q ce qui permet d'avoir d et donc de déchiffrer le
message

Re: Tu t'emballes

Posté par **PsychoFox** le 13/09/17 à 08:13. Évalué à 4 (+3/-1).

> *Puis une monnaie, c'est surtout une question de confiance pour que cela marche. Et manifestement, nous sommes loin d'être au stade où la population a plus confiance en une cryptomonnaie qu'envers le dollar ou l'euro. Tant que cela ne sera pas acquis, je ne vois pas comment ta généralisation pourrait subvenir.*

Et il faut surtout se demander ce que veut tout un chacun. Une nouvelle monnaie ? Bof.

Le public en général ce qu'il veut c'est éventuellement se débarasser de la mitraille qui reste dans le porte-monnaie et que des virements soient faciles à faire. Et en cela des services comme apple/google pay, paypal, twint et cartes de paiements sans contact sont intéressantes et finalement il n'y a pas forcément besoin de blockchains pour cela. L'anonymisation des transactions intéresse peu de monde, d'une part parce que c'est des fois bien pratiques d'avoir une preuve de l'identité de la personne à qui tu a payé (je pense aux petites annonces et ventes aux enchères en ligne), d'autre part parce que ça ne dérange pas grand monde que leur institution financière soit au courant de chacune de leur transaction ou qu'un commerce puisse savoir si untel préfère le jambon cru ou cuit.

Si on prend en compte les considérations écologiques liées au minage, le fait que les cryptomonnaies ont une image - un peu à raison - de monnaie fortement spéculative et du darkweb pour acheter des armes, de la drogues et des services sexuels sur des petits nenfants, je doute que ça prenne tel quel en tant que monnaie.

Par contre la technologie des blockchains pourrait être utilisée comme intermédiaire pour les processus de transactions, on l'a vue aussi utiliser dans des projets de cadastres…

Re: Tu t'emballes

Posté par **Sytoka Modon** (**page perso**) le 13/09/17 à 10:57. Évalué à 1 (+1/-2).

> *Le public en général ce qu'il veut c'est éventuellement se débarasser de la mitraille qui reste dans le porte-monnaie*

Je pense que c'est surtout l'état qui souhaite qu'on utilise la carte sans contact. Avec elle, il y a une VRAI trace dans la caisse. Le problème de la mitraille n'est pas du coté des clients mais du coté des commerçants qui trichent éperdument et ne déclarent rien ou très peu derrière.

Re: Tu t'emballes

Posté par **Xavier Claude** (**page perso**) le 13/09/17 à 11:06. Évalué à 6 (+4/-1).

> *Le problème de la mitraille n'est pas du coté des clients*

Si clairement. La mitraille, ça me fait bien chier. Je me retrouve avec des kilos de pièces dans les poches. Pour payer, ça ne suffit jamais. Du coup, tu sors un billet et tu te retrouve avec encore plus de pièce. Ce n'est pas pour rien que les magasin qui échangent les pièces contre des bons d'achat ont du succès.

--
« Rappelez-vous toujours que si la Gestapo avait les moyens de vous faire parler, les politiciens ont, eux, les moyens de vous faire taire. » Coluche

Re: Tu t'emballes

Posté par **chimrod** (**page perso**) le 13/09/17 à 12:41. Évalué à 4 (+3/-1).

J'ai mon boulanger pour ça : je sais combien coute le prix d'un pain, et je prépare l'appoint chez moi avant d'aller lui rendre visite, ça me permet d'écouler mon stock.

Re: Tu t'emballes

Posté par **Mimoza** le 13/09/17 à 13:51. Évalué à 2 (+0/-0).

Perso je préfère la mitraille a une carte … au moins tu te rend vraiment compte de ce que tu dépenses.

Quand je voie l'évolution des tickets resto je me demande dans combien de temps ça va arriver sur les CB classique. D'un bout de papier que tu pouvais donner/utiliser comme bon te semble, là tu es limité temporellement, géographiquement et en valeur.
Déjà que l'on te pique des € sur ta paye pour te forcer a consommer dans les resto, ça devient une vrai galère a écouler. Tu peux même plus payer le resto de toute la famille pour écouler en fin d'année le stock de tickets que tu n'as pas pu utiliser. Et bien sûr ceux que tu as oublier/perdu/pas eu le temps d'utiliser ce n'est pas perdu pour tout le monde.
Me parle pas de les écouler dans les supermarchés, la liste de produit éligible se rétréci tous les trimestres.

Re: Tu t'emballes

Posté par **passant** le 13/09/17 à 11:31. Évalué à 4 (+2/-0).

Oui toutafé d'accord. L'optimise c'est bien mais il ne faut pas perdre raison pour autant.

Le foirage de TheDAO W qui sacralisait le principe de "Code is Law" (Le Code c'est la loi) est un exemple ou l'humain a dû vite intervenir dans le protocole pour protéger les intérêts de ceux qui avaient placé des millions pour ne pas briser la confiance dans ethereum.

Il y a un emballement - personne ne veut rater le prochain grand TRUC - et du coup c'est le farwest des crypto monnaies : il y en a pour n'importe quel occasion (dogecoin W)… Il faudra attendre quelques explosions de bulle avant de savoir ce qui sera durable.

À moins que...

Posté par **Sylvain Briole** (**page perso**) le 13/09/17 à 01:37. Évalué à 4 (+4/-1).

… les limites soient du côté de l'énergie consommées par ces technos:
https://usbeketrica.com/article/bitcoin-peut-on-arreter-ce-monstre-energivore
https://blogrecherche.wp.imt.fr/2016/07/28/bitcoin-blockchain-gouffres-energetiques/
Après, il faut mettre cela en face des technos/méthodes actuelles potentiellement supplantables, qui ne sont pas neutres du point de vue énergétique.

Re: À moins que...

Posté par **pulkomandy** (**page perso**) le 13/09/17 à 08:40. Évalué à -1 (+1/-4).

Ce n'est pas forcément un problème de technos/méthodes. Dans bitcoin en tout cas, c'est volontaire que des calculs intensifs (et énergivores) soient nécessaires. Le but est d'empêcher que quelqu'un puisse valider tout plein de blocs et construire sa propre blockchain, en ayant plus de 50% de la capacité totale de calcul (ce serait un genre d'attaque brute force de la blockchain). Pour éviter ça, le bitcoin fait en sorte que les calculs soient trop coûteux pour que quelqu'un puisse avoir 50% de la capacité totale de calcul.

Si on fait une blockchain qui n'a pas cette contrainte, il faut trouver autre chose pour se protéger de ce genre d'attaque. Si on veut garder la décentralisation et la distribution des calculs, je ne vois pas trop d'autre solution, mais peut-être que quelqu'un avec plus de connaissance en cryptograhpie pourrait donner quelques pistes?

Re: À moins que...

Posté par **Moonz** le 13/09/17 à 09:20. Évalué à 2 (+0/-0).

https://en.wikipedia.org/wiki/Proof-of-stake W
https://filecoin.io/

Re: À moins que...

Posté par **Harvesterify** (**page perso**) le 13/09/17 à 12:55. Évalué à 2 (+2/-0).

Le problème de ces calculs, c'est qu'ils ne servent à rien, d'où les récentes propositions de se servir de cette puissance "perdue" à des fins utiles : https://blog.acolyer.org/2017/09/06/rem-resource-efficient-mining-for-blockchains/

--
Mes messages engagent qui je veux.

Re: À moins que...

Posté par **ǝpɐlƃu∀ nǝıɥʇʇɐW-ǝɹɹǝıԀ** (**page perso**) le 13/09/17 à 13:19. Évalué à 2 (+0/-0).

Il m'avait semblé comprendre qu'au contraire ces calculs permettait de valider la blockchain. On m'aurait menti ?

le seul truc

Posté par **dark_star** le 13/09/17 à 07:46. Évalué à 7 (+5/-0).

gênant a mon gout, c'est la nécessite d'avoir un internet mondial fiable pour pouvoir les utiliser. Genre en ce moment a saint martin, le gars avec sa clé USB et ses 5 000 B$ il ne peut rien en faire. Qui lui achèterai sa clé USB, a par nous :)

cela me fait plus penser a de l'or dématérialiser, pas super pratique pour acheter de la bière mais permet de transférer pas mal d'argent sans employer des camions de la banque de france. Ou de garder au chaud ses économie afin d'éviter que les banques se servent :).

par la suite si il ne reste que quelques pays qui permettent la conversion vers de la monnaie réel, cela risque d'etre difficile de récupérer ses sous pour celui en ayant acheté.

Bof

Posté par **Olivier** le 13/09/17 à 10:23. Évalué à 10 (+9/-0).

> *Peut-on prédire :*
> *- la fin des paradis fiscaux, des doubles comptabilités, du blanchissement d'argent sale.*

Non. Peut-être. Non.

> - *la faillite des banques, des organismes de crédit et autres intermédiaires*

Elles n'ont pas besoin des cryptomonnaies pour ça.

> - *la fin de l'inflation et de l'émission de monnaies par les états, pour réduire leur dette*

Non.

> - *des systèmes de prélèvement de TVA, taxes, impôts automatisés*

Peut-être.

> - *une accélération folle des échanges commerciaux*

Non, les cryptomonnaies en vogue ayant tendance à renforcer l'inégalité de répartition de l'argent.
Par ailleurs, le Bitcoin incite à ne pas dépenser son argent (puisque celui-ci est très limité).
Et leur système est incapable de suivre en volume les échanges faits actuellement par le système bancaire.
La taille de stockage de la blockchain est déjà énorme. Je n'ose pas envisager ce que ça va devenir.

> - *un fossé numérique de plus en plus grand*

Bitcoin, c'est pas facile pour madame Michu. C'est une usine à gaz superlente et consommatrice de ressources (même quand on ne mine pas). Stockage de données gigantesque. J'ai essayé. À l'usage, c'est pas pratique.

Alors certes, on peut se passer d'installer le logiciel Bitcoin sur son PC et faire confiance à des intermédiaires qui vont gérer ça pour nous. Du coup, ça n'a plus aucun intérêt, puisqu'on se retrouve avec des tiers qui ne sont pas plus dignes de confiance que des banquiers et probablement même moins.

La blockchain va peut-être se généraliser, mais probablement pas chez les particuliers qui ont autre chose à faire que stocker toutes ces données. Et même chez les banquiers, je ne vois pas comment ça peut se gérer sur le long terme, à moins de prévoir des resets de la blockchain de temps en temps. Je me demande si on a des DD assez gros pour stocker une blockchain des transactions mondiales du système bancaire.

Au 27 mai 2017 (je n'ai pas relancé Bitcoin depuis lors), la blockchain de Bitcoin pesait 128 Go… alors que cette monnaie ne traite probablement pas le millième des transactions mondiales.

> - *un coup de fouet donné aux technologies de chiffrement*

Non. On n'a pas besoin des cryptomonnaies pour ça.
Et ça ne va pas inciter les gens à utiliser GPG ou abandonner Gmail.

> *autres conséquences ?*

Spéculation intensive basée en partie sur les rançongiciels.

Le Bitcoin me semble trop mal pensé pour gérer les finances mondiales (ou trop bien pensé pour enrichir les spéculateurs).

L'Ethereum, je connais moins. Ça a l'air mieux pensé globalement, vu de loin. Les contrats intelligents, ça a probablement de l'avenir. Ça a aussi l'air compliqué. Pas sûr que ça motive les foules s'il faut être un spécialiste pour ne pas se faire enfumer.

Si on veut démocratiser la genèse de l'argent et que le peuple retrouve le pouvoir sur la monnaie, ce n'est pas en laissant celle-ci à des spécialistes en informatique et des mineurs prêts à investir des fortunes en consommation électrique pour se retrouver rois de la montagne.

Les cryptomonnaies, ce n'est pas une révolution, c'est juste une tentative de transfert de pouvoir. Et les gens qui œuvrent à tout ça ne se soucient pas plus de nos intérêts que nos banquiers actuels.

Il faudrait envisager une genèse de monnaie équitablement répartie pour sortir du cycle infernal. Mais les riches et leurs larbins n'y ont pas intérêt. Pas plus que les spéculateurs sur les cryptomonnaies.

Re: Bof

Posté par **pulkomandy** (**page perso**) le 13/09/17 à 11:44. Évalué à 2 (+1/-1).

> *Les cryptomonnaies, ce n'est pas une révolution, c'est juste une tentative de transfert de pouvoir.*

C'est pas justement ça, une révolution?

Re: Bof

Posté par **Olivier** le 13/09/17 à 12:13. Évalué à 3 (+1/-0). Dernière modification le 13/09/17 à 12:14.

> *C'est pas justement ça, une révolution?*

C'est plus qu'un simple transfert de pouvoir. C'est aussi un changement de paradigme, et dans mon esprit, c'était aussi porté par une volonté populaire. Ce qui n'est pas le cas ici.
Mais qu'importe, révolution, c'est un mot polysémique, on peut y mettre un peu ce qu'on veut. Faut pas s'attarder sur ça. :)

Quel nombre d'utilisateurs ?

Posté par **goom** (**page perso**) le 13/09/17 à 10:25. Évalué à 6 (+4/-0).

Quelle est la part des consommateurs qui utilisent ces monnaies ? Quelle confiance les consommateurs vont-ils accorder à ces monnaies ?

Je crois, et je peux largement me tromper, qu'on est loin - même très loin - d'une révolution.

Aucune raison de s'emballer

Posté par **arnaudus** le 13/09/17 à 13:50. Évalué à 2 (+0/-0).

> *la fin des paradis fiscaux, des doubles comptabilités, du blanchissement d'argent sale.*

J'ai l'impression que c'est *exactement* le contraire. On est en train de se débarrasser peu à peu du secret bancaire, et les crypto-monnaies sont une aubaine pour le blanchiment, le marché noir, la corruption, etc.

> *la faillite des banques, des organismes de crédit et autres intermédiaires*

Par quel miracle? Comment tu fais pour emprunter en Bitcoins?

> *la fin de l'inflation et de l'émission de monnaies par les états, pour réduire leur dette*

C'est déja le cas en Europe, du fait de la politique de la BCE. Pas besoin d'artifice monnétaire pour ça. De toutes manières, une inflation contrôlée est souhaitable puisqu'elle incite à la circulation monnétaire (mieux vaut acheter aujourd'hui que d'attendre demain). Les monnaires comme le Bitcoin sont (fortement) déflationnistes, et sont blocantes pour l'économie (tout le monde garde sa monnaie). Techniquement, le Bitcoin n'est pas viable comme monnaie, parce que dépenser en Bt a un coût. C'est plus comme l'or, c'est un instrument spéculatif ou de réserve (en cas de coup dur), pas une monnaie au jour le jour.

> *des systèmes de prélèvement de TVA, taxes, impôts automatisés*

Heureusement que les impôts sont un peu plus compliqués que de prélever un forfait fixe sur les rentrées d'argent sur un compte… Sans compter que tu peux avoir autant de comptes Bt que tu souhaites, et que si l'anonymat est levé, n'importe qui peut tout connaitre de tes transactions financières.

> *une accélération folle des échanges commerciaux*

Pas attendu le Bitcoin…

De toutes manières, la futurologie est par définition foireuse. Les cryptomonnaies seront ce qu'elles seront : peut-être un feu de paille, peut-être un instrument de spéculation financière supplémentaire, peut-être un système généralisé de traffic d'argent et de blanchiment… Mais elles ne sont rien de plus qu'une monnaie électronique, qui a un coût réel et un coût environnemental plusieurs ordres de grandeurs supérieurs aux réseaux bancaires traditionnels.

À mon avis, le seul truc intéressant et innovant avec les cryptomonnaies, c'est la blockchain. L'aspect "monnaie", c'est totalement foireux ; c'est lent, inefficace, archi-anti-écologique, obscur, coûteux… bref, c'est un instrument financier, construit au profit de leur concepteur, et au détriment de leurs utilisateurs.