[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, octobre 2008, en ligne en traduction française sur le site Gitbook.com et dans la page « salle de lecture » sur le blog *La Voie du Bitcoin* (http://blog.lavoiedubitcoin.info/public/Bibliotheque/Nakamoto.pdf). Version originale :
https://bitcoin.org/bitcoin.pdf .

[2] John Maynard Keynes, *Théorie Générale,*(1936), Introduction.

[3] « L'empirisme primaire peut être pire que toute autre forme de sottise quand il met les gens en confiance », selon Nassim Taleb, *le Hasard sauvage*, Paris, Les Belles-Lettres, 2008, page 100.

[4] Cité par Andreas Antonopoulos en exergue de son livre *Internet of Money,* 2016.

[5] Philip Zimmermann, *Pourquoi j'ai écrit PGP ?* (première version 1991, réédition 1998), en ligne.

[6] Tim May, *Manifeste crypto-anarchiste*, 1992, traduction en ligne notamment sur le site *La revue des Ressources* ici :
http://www.larevuedesressources.org/manifeste-crypto-anarchiste,2316.html

[7] Eric Hughes, *Manifeste d'un Cypherpunk*, 1993, traduction en ligne notamment sur le site *Terminator Studies* ici :
http://terminatorstudies.org/html/58942231975336345 6.html .

[8] Christian As. Kirtchev, *Cyberpunk Manifesto*, 1997, traduction en ligne notamment sur le site *La Revue des Ressources*, ici :
http://www.larevuedesressources.org/un-manifeste-cyberpunk-le-cyberpunk-manifesto,2317.html .

[9] *Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux*, rapport de la Commission présidée par M. Pierre-Antoine Gally, 2015, en ligne ici :
http://www.lecese.fr/sites/default/files/pdf/Avis/2015/2015_10_nouvelles_monnaies.pdf .

[10] Michel Foucault, *Surveiller et Punir,* 1975.

[11] « Un million de dollars en deux heures pour SuperNET » :
https://le-coin-coin.fr/1205-million-dollars-en-heures-supernet/

[12] Nassim Nicholas Taleb, *Antifragile*, *Things That Gain from Disorder*, 2012, disponible en ligne sur un site dédié à un cours de l'université de Pennsylvania : http://cpor.org/af/Taleb_Antifragile.pdf .

[13] Au commencement, des bugs et des failles ont pu être constatés et réparés avant que Bitcoin n'ait une telle importance financière. On verra, par exemple, celui-ci où Jeff Garzik avait détecté un problème assez sérieux : https://bitcointalk.org/index.php?topic=822.0.

[14] La note blanche de Lamport, Shostak et Pease, publiée en 1982, est en ligne ici :
http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf. Il en existe une présentation en langue française par Aymeric Lesert

(http://aymeric.lesert.pagesperso-orange.fr/expose/dea/byzantin/algorithmes.pdf).
En 1983, Michel Ben-Or avait publié son étude *Another Advantage of Free Choice: Completely Asynchronous Agreement Protocols* qui fait date dans l'histoire du consensus. Enfin on peut aussi lire l'article *Asynchronous Byzantine Agreement Protocols* publié en 1987 par Gabriel Bracha et qui est en ligne ici : http://www.sciencedirect.com/science/article/pii/089054018790054X .

[15] Réunissant, après la dernière guerre, des malfrats mâtinés de collaboration, le « gang des tractions Avant » entre dans la chronique avec l'attaque d'un fourgon du Crédit Lyonnais, le 7 février 1946, avenue Parmentier à Paris. À bord de deux Citroën du modèle éponyme, « Pierrot le Fou » et ses complices s'emparent de trois millions de francs. Le gang commettra cette année-là une dizaine de hold-up. Il a suscité des romans et des films de Jacques Deray (*Le Gang* avec Alain Delon) et Claude Lelouch (*Le Bon et les Méchants* avec Jacques Dutronc) et il est cité par Mc Solaar dans la chanson *Quand le soleil devient froid*. Loin d'être interdite, la Traction-Avant restera produite jusqu'en 1957. Sa notice Wikipedia explique sobrement que « son histoire est liée dans la mémoire collective à l'Occupation, tour à tour voiture de la Gestapo et icône de la Résistance. Elle est également le véhicule préféré des gangsters en raison de qualités routières exceptionnelles pour son époque. »

[16] L'historique de l'idée consistant à contraindre les machines à résoudre des puzzles, énigmes ou problèmes mathématiques pour réduire le spam en rendant le courrier électronique « coûteux » à envoyer comme le courrier physique est reprise ici : http://www.hashcash.org/papers/ ; lire en particulier A. Back, *Hashcash, a denial of service counter-measure* : http://www.hashcash.org/papers/hashcash.pdf , 2002.

[17] Voir note 1.

[18] Nombre de nœuds, ici comptabilisés par la société 21 : https://bitnodes.21.co/ .

[19] http://jasondrowley.com/2015/12/04/the-bitcoin-network-is-11000x-faster-than-the-top-500-supercomputers-combined/#easy-footnote-1. Calcul réactualisé en décembre 2015 par rapport à un calcul de Forbes de 2013 : http://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/.

[20] Ricardo Perez-Marco (CNRS), conférence à la Société Informatique de France le 15 novembre 2016.

[21] Jean-Paul Delahaye (Université Lille I) le même jour à la conférence de la SIF, reprenant par ailleurs une assertion déjà formulée. On trouvera sur le blog de Jean-Paul Delahaye d'intéressants éléments dans les billets :
http://www.scilogs.fr/complexites/lattaque-goldfinder-dune-blockchain/
http://www.scilogs.fr/complexites/contenu-en-calcul/
http://www.scilogs.fr/complexites/epee-de-damocles-bitcoin/.

[22] On verra un peu plus loin, au chapitre 4.2, que l'intervalle entre deux blocs suit une loi exponentielle, et que ce n'est pas sans conséquences (positives) sur la sécurité du protocole.
[23] « Ἀπόδοτε οὖν τὰ Καίσαρος Καίσαρι καὶ τὰ τοῦ Θεοῦ τῷ Θεῷ. » (Rendez donc à César ce qui est à César et à Dieu ce qui est à Dieu) dans les évangiles de Matthieu, XXII,21, Marc, XII, 13-17 et Luc, XX, 25.
[24] D. Bayer, S. Haber, W.S. Stornetta, _« Improving the efficiency and reliability of digital time- stamping »,_ dans *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.
[25] Pierre Noizat, *Bitcoin, mode d'emploi*, 2015, page 54.
[26] Données recueillies sur blockchain.info :
https://blockchain.info/charts/n-transactions-per-block?timespan=all.
[27] R.C. Merkle, _Protocols for public key cryptosystems, dans Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, avril 1980.
[28] Voir note 1.
[29] Au sujet du problème de la « base monétaire », on se reportera avec intérêt à la page 95 de l'ouvrage de Nicolas Bouleau, *Martingales et marchés financiers,* Paris, Odile Jacob, 1998. Faire ses comptes en bitcoin serait un pari probabiliste a priori sur l'avenir. « Dès lors que les devises ont des transactions bruitées les unes par rapport aux autres, faire ses comptes dans une monnaie ou une autre n'est pas indifférent. »
[30] La chose est peut-être ignorée du grand public, mais elle n'est pas secrète. Voir le document « Qui crée la monnaie ? », mis en ligne en septembre 2015 par la Banque de France
https://www.banque-france.fr/uploads/tx_bdfpatchirfaq/NI_Monnaie_09_2015.pdf .
[31] Compte-rendu de la Commission des affaires économiques, mardi 14 juin 2011, séance de 17 heures (Compte rendu n° 77) sur le site de l'Assemblée Nationale.
[32] Zoltan Jakab et Michael Kumhof , *Banks are not intermediaries of loanable funds - and why this matters*, Working paper n°529 de la BoE, mai 2015, en ligne sur son site. Une autre lecture intéressante : Michael McLeay, Amar Radia and Ryland Thomas, *Money in the modern economy : an introduction*, Bulletin de la BoE pour le premier trimestre 2014, en ligne sur le site de la BoE et en traduction française sur le blog d'Alain Grandjean: https://alaingrandjean.fr.
[33] C'est clairement ce que sous-entend André Gide dans *les Faux-Monnayeurs* publiés en 1925. Voir Guillaume Bardet et Dominique Caron, *Les Faux-Monnayeurs*, Paris, Ellipses, 2016.
[34] La position d'Europol a plusieurs fois changé. En janvier 2016 l'organisme relativisait très fortement la réalité d'un usage de Bitcoin par les terroristes :
https://www.europol.europa.eu/sites/default/files/publications/changes_in_modus_operandi_of_is_in_terrorist_attacks.pdf.

En septembre 2016, un partenariat Interpol-Europol-Basel Institute for Governance était annoncé pour lutter contre le blanchiment de bitcoin en relation avec le terrorisme. « There is a clear consensus that digital currencies pose a money laundering and terrorism financing threat » lisait-on dans le communiqué, qui avouait ensuite n'en avoir trouvé que fort peu d'exemples.

[35] Étienne de la Boétie, *Discours de la servitude volontaire*, rédigé en 1549, première édition en 1576. Texte majeur de la philosophie politique, écrit par un humaniste de 18 ans et souvent invoqué dans les écrits anarchistes ou libertaires. À noter que La Boétie établit une relation entre une économie de la rivalité de chacun contre tous et la tyrannie.

[36] Publication du *leak* listant le domaine des adresses piratés ainsi que les mots de passe les plus utilisés :
https://www.leakedsource.com/blog/friendfinder.

[37] Pour être plus précis la clef privée est une suite en hexadécimal (0-9 A-F / base 16) de 64 caractères, mais en caractères lisibles elle fait 51 caractères quand elle est associée à une clef publique non-compressée et 52 caractères quand elle est associée à une clef publique compressée. C'est cet encodage que nous voyons le plus fréquemment, cf. https://en.bitcoin.it/wiki/Private_key.

[38] Pour se rendre compte du nombre de solutions : http://directory.io/ qui est la liste de toutes les clefs privées du monde, et pourtant il n'y a aucun risque de tomber sur la clef de quelqu'un en se baladant sur le site. Voir aussi cette discussion pour imaginer ce vertige :
https://www.reddit.com/r/Bitcoin/comments/3faio9/counting_sand_and_bitcoin_addresses/.

[39] Taille relevée sur blockchain.info :
https://blockchain.info/fr/charts/blocks-size.

[40] Article de *Science* montrant précisément l'aspect non secret de Bitcoin :
http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin.

[41] Voir note 19.

[42] Il s'agit d'une estimation livrée en septembre 2016 par l'un des auteurs du site Bitcoin.fr (article « Bitcoin au Tibet », en ligne ici https://bitcoin.fr/bitcoin-au-tibet/) et qui nous a paru vraisemblable ; il faut toutefois souligner qu'elle repose sur un empilement d'hypothèses (puissance de calcul, âge et efficience des matériels de minage employés). Pierre Noizat (note 82) tablait en novembre 2015 sur 250 MW.

[43] Le nombre de liens potentiels dans un réseau comptant n nœuds est n(n-1)/2 et cette fonction est équivalente à ½ n^2 lorsque n tend vers l'infini. L'utilité d'un réseau est donc, selon la remarque de Robert Metcalfe, proportionnelle au carré du nombre de ses utilisateurs. C'est une loi empirique qui a par ailleurs été critiquée.

[44] Gilles Châtelet, *Vivre et penser comme des porcs*, Paris, Exils, 1998, chapitre 11. Merci à Antoine Favier pour la référence.

[45] Maurizio Lazzarato est un sociologue et philosophe italien indépendant, résidant à Paris et auteur notamment de deux ouvrages importants, *La fabrique de l'homme endetté : Essai sur la condition néolibérale* (Editions Amsterdam, 2011) et *Gouverner par la dette* (Les Prairies ordinaires, 2014). Ce dernier livre est évoqué dans le billet n° 18 du blog *La Voie du Bitcoin*.

[46] Les exemples sont innombrables. Les fouilles entreprises par Louis Malleret, dans les années 1940, ont permis de retrouver des pièces romaines dans des tombes du Mékong. Encore en septembre 2016 des fouilles sur l'île d'Okinawa au Japon, ont exhumé des pièces romaines, une première sur le territoire japonais où les anciens Romains n'ont jamais été.

[47] *The limits to growth,* Donella H. Meadows, Dennis L. Meadows, Jorgen Randers William W. Behrens III, Universe Books, 1972, disponible en ligne ici : http://www.donellameadows.org/wp-content/userfiles/Limits-to-Growth-digital-scan-version.pdf.

[48] Dictionnaire numérisé sur ce site : http://www.furetière.eu

[49] Papier décrivant l'algorithme publié par le NIST : http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf.

[50] Bitcoin utilise une courbe elliptique précise, à savoir la courbe secp256k où $y^2 = x^3+7$ dans un corps fini (on dit aussi un champ de Galois) de cardinal p, avec p égal à $2^{256}-2^{32}-2^9-2^8-2^7-2^6-2^4-2^0$ soit un nombre à 78 chiffres, lire : https://en.bitcoin.it/wiki/Secp256k1 .

[51] Toutes les règles du protocole sont bien résumées ici : https://en.bitcoin.it/wiki/Protocol_rules.

[52] Pierre Noizat sur son blog : http://e-ducat.fr/2013-12-21-lattaque-des-selfish-miners/.
Silvio Micali, dans sa publication *Algorand* http://arxiv.org/pdf/1607.01341.pdf

[53] Toutes les données peuvent être vérifiées en ligne au chapitre 7 de Mastering Bitcoin : http://chimera.labs.oreilly.com/books/1234000001802/ch07.html ou à l'aide de cet excellent article : https://codesuppository.blogspot.fr/2014/01/how-to-parse-bitcoin-blockchain.html
ou enfin grâce au wiki Bitcoin : https://en.bitcoin.it/wiki/Block#Block_structure, données réunies dans une infographie très claire traduite en français par BitConseil : http://bitconseil.fr/wp-content/uploads/2016/03/bitcoin-blockchain-infographic-fr.pdf.

[54] Cet « identifiant magique » permet d'identifier le début d'un bloc et correspond à 0xD9B4BEF9. Voir : https://bitcoin.stackexchange.com/questions/2337/how-was-the-magic-network-id-value-chosen.

[55] Cette notion d'extranonce est assez peu connue. Elle est cependant très fine. En effet le nonce de base est beaucoup trop limité (en terme de bits : 2^{32} soit près

de 4 milliards) pour permettre la résolution de la difficulté dans la plupart des cas. Les autres facteurs d'ajustement du hasard sont donc des éléments capitaux de la belle mécanique qu'est Bitcoin, qu'il s'agisse du *timestamp*, de la possibilité de permutations des transactions au sein du bloc (dans l'hypothèse d'un bloc de 1000 transactions il y a factorielle 1000 possibilités, soit un nombre à 2568 chiffres) et enfin de l'extranonce (mais changer la *coinbase* requiert de recalculer tout l'arbre de Merkle, ce qui en fait la solution la plus coûteuse en énergie). On peut voir différents échanges à ce sujet sur des forums, pour approfondir la notion :
https://bitcointalk.org/index.php?topic=1040859.msg11222991#msg11222991
https://bitcointalk.org/index.php?topic=9438.0
et :
https://bitcoin.stackexchange.com/questions/5048/what-is-the-extranonce.
Ces explications non académiques mais exprimées par des membres « légendaires » du forum Bitcointalk ou par des personnalités reconnues comme Pieter Wuille peuvent être considérées comme fiables dans le monde réputationnel qu'est Bitcoin.

[56] La clef privée a été générée à partir de ce site : https://coinb.in/#newAddress non pas aléatoirement mais avec pour *custom seed* « Bitcoin, la monnaie acéphale » et avec l'option de compression des adresses. Vous pouvez essayer et vous devriez tomber sur les mêmes valeurs. N'envoyer cependant aucun bitcoin à cette adresse qui est désormais « grillée » !

[57] Voir ces pages pour plus de détails sur la raison de la variété possible du nombre précis de caractères dans les adresses :
https://bitcoin.stackexchange.com/questions/36944/what-are-the-minimum-and-maximum-lengths-of-a-mainnet-bitcoin-address
ou https://en.bitcoin.it/wiki/Address
ou https://bitcointalk.org/index.php?topic=613068.0. La taille minimale est de 26 caractères pour les adresses connues :
http://pastebin.com/KJmYYmtC. Tout cela dépend en réalité du préfixe d'adresse choisi par Satoshi :
https://en.bitcoin.it/wiki/List_of_address_prefixes .

[58] Taille relevée sur blockchain.info :
https://blockchain.info/fr/charts/blocks-size.

[59] Benoît Mandelbrot, *Une approche fractale des marchés*, Paris, Odile Jacob, 2004, page 249. La lecture de ce livre antérieur tant à la crise des *subprimes* qu'à l'apparition de Bitcoin reste un antidote indispensable à la vanité et à la suffisance de bien des exposés sur l'efficience des marchés et sur la pertinence des modèles mathématiques qui y sont mis en œuvre.

[60] Ajout réalisé pour compléter des faiblesses de nLocktime à la suite de la *Bitcoin Improvement Proposal* (BIP65) de Peter Todd :
https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki
et intégré fin 2015 dans Bitcoin 0.11.12 :

https://bitcoin.org/en/release/v0.11.2.

[61] Nick Szabo, Smart Contracts :
http://virtualschool.edu/mon/Economics/SmartContracts.html.

[62] Vidéo consultable ici :
https://www.youtube.com/watch?v=N7j8LnBvlp0.

[63] Numérama, *Sandy Bridge : Intel ajoute un DRM dans ses processeurs*, 2011, http://www.numerama.com/magazine/17759-sandy-bridge-intel-ajoute-un-drm-dans-ses-processeurs.html.

[64] S. Haber, W.S. Stornetta, *How to time-stamp a digital document*, dans le *Journal of Cryptology*, Vol. 3, n°2, pages 99-111, 1991 et *op. cit.* note 22.

[65] La probabilité de réussite d'une double-dépense peut être estimée en remplaçant grossièrement une loi binomiale négative par une loi de Poisson. Cela a été expliqué par Meni Rosenfel dans un article de 2012, « Analysis of hashrate-based double-spending » (en ligne : https://bitcoil.co.il/Doublespend.pdf). Cyril Grunspan et Ricardo Perez-Marco, en reprenant ces calculs, ont montré que ladite probabilité peut s'exprimer simplement à l'aide d'une formule fermée mettant en jeu une seule fonction béta régularisée incomplète, et ensuite que cette probabilité tend exponentiellement vers 0 en fonction du nombre de confirmations reçues. Ce résultat était souvent cité mais semble-t-il de manière purement intuitive. Ils ont aussi donné d'autres formules plus fines en prenant en compte les temps de minage. Voir la fin de la conférence du 2 janvier 2017 à Paris 7 en ligne sur :
https://bitcoin.fr/video-paiements-securises-et-non-securises-sur-une-blockchain-2eme-partie.
Voir aussi le résumé en langue française publié par Grunspan :
http://cyrilgrunspan.fr/index.php/2017/02/10/supplement-a-letude-du-bitcoin/

[66] En théorie, du moins, et en l'absence de « famine monétaire » comme celles que connaissaient les hommes de certaines époques au Moyen Âge. On lira avec intérêt le petit ouvrage de jeunesse de Laurent Feller *Faux-Monnayeurs et fausses monnaies en France à la fin du Moyen Âge,* Paris, Le Léopard d'or, 1986.

[67] Article de Marie Lafitte, Florent Brousse, Laurent Noël, Yvan Gaillard et Gilbert Pépin : « Traces de stupéfiants sur les billets, in Revue de la Société française de toxicologie analytique »,
http://cat.inist.fr/?aModele=afficheN&cpsidt=13774974.

[68] Nicolas Oresme, *Traité des Monnaies*, au chapitre VI : « La monnaie est l'étalon de la permutation des richesses naturelles ; elle est donc la possession de ceux auxquels appartiennent ces richesses. En effet, si quelqu'un donne son pain ou le labeur de son propre corps pour de l'argent, une fois qu'il l'a reçu, il est à lui comme l'était le pain ou le labeur de son corps. »

[69] Souvent cité de manière générale, la distinction par Aristote des trois fonctions se déduit du livre I du *Politique* et ne doit pas être confondue avec le cinquième livre de *l'Ethique à Nicomaque* dans lequel il déclare que la monnaie est un fait légal qui n'existe pas dans la nature.

[70] Note en consultation libre :
http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62014CJ0264&from=FR.
[71] Friedrich Hayek, *The denationalization of money*, 1976, traduit en français sous le titre *Pour une vraie concurrence des monnaies*, Paris, PUF, 2015.
[72] Simulation des différents temps de confirmation et leur impact :
https://arthurgervais.github.io/Bitcoin-Simulator/results.html
Résumé des arguments pour et contre :
http://bitcoin.stackexchange.com/questions/1863/why-was-the-target-block-time-chosen-to-be-10-minutes/1864
Avis de Mike Hearn et raison de Satoshi en discours rapporté :
https://www.reddit.com/r/Bitcoin/comments/30lxo4/replace_by_fee_a_counter_argument_by_mike_hearn/cptwk21/
[73] Site s'amusant à recueillir les avis de décès de Bitcoin : https://99bitcoins.com/bitcoinobituaries. Le site recensait 118 avis à fin 2016. Un chiffre fort proche du nombre de BIP (propositions d'amélioration du protocole), et deux raisons de penser que Bitcoin aura raison des oiseaux de mauvais augure.
[74] On trouve des condamnations à mort ou de simples faire-part signés de Paul Krugman, Robert Shiller ou Joseph Stiglitz. Un cryptologue franco-polonais de University College à Londres, Nicolas Tadeusz Courtois, s'est également fait une spécialité de prononcer sans trop de démonstration que Bitcoin est *extrêmement déficient* (lire ici : https://bitcoin.fr/bitcoin-est-un-systeme-extremement-deficient/). Il avait pris en avril 2016 le pari que l'algorithme *ECDSA (Elliptic Curve Digital Signature Algorithm)*, utilisé dans Bitcoin pour la signature des messages de transaction, serait cassé avant la fin de l'année (https://bitcoin.fr/le-pari-manque-de-nicolas-t-courtois/). Ses thèses, que l'on trouvera présentées dans une conférence mise en ligne (https://bitcoin.fr/video-etat-de-lart-de-la-securite-des-blockchains) suscitent des réserves même chez les universitaires.
[75] Voire le documentaire d'Arte sur Ponzi :
http://www.arte.tv/guide/fr/048693-000-A/le-systeme-de-ponzi.
[76] Citation de *Monnayé*, 32ème tome des *Annales du Disque Monde* du défunt Sir Terry Pratchett (titre original : *Making Money,* 2007).
[77] Les transactions en coquillages (en cauris, pour les appeler par leur nom) formant un marronnier de la littérature monétaire, autant se référer aux meilleures sources, les publications de Pierre P. Edoumba, *Aperçu sur les systèmes monétaires africains,* 2001, en ligne sur Persée et de Francis Dupuy, *Les monnaies primitives*, 2009, en ligne sur Cairn-info.
[78] La fameuse citation sur la « relique barbare » mériterait d'être faite avec scrupule. Dans son ouvrage *A Tract on Monetary Reform* (1923) où il plaide contre le retour de l'étalon-or, il souligne le risque de privilégier la stabilité des changes au détriment de celle des prix nationaux. La formule « l'étalon-or est

déjà une relique barbare » ne vise pas le métal mais le système monétaire construit dessus.

[79] Un article résumant bien la question : http://www.bitcoinnotbombs.com/bitcoin-vs-the-nsas-quantum-computer/.

[80] Voir cette article du *Financial Times* qui fait le point sur les avancées des diverses banques centrales : https://www.ft.com/content/f15d3ab6-750d-11e6-bf48-b372cdb1043a.

[81] Voir note 42.

[82] Pierre Noizat, sur son blog : http://e-ducat.fr/2015-11-28-cop21-et-blockchain/, a une estimation (250 MW) un peu basse de la puissance pour bitcoin, nous avons suivi l'estimation de l'ordre de 423 MW (voir note 42).

[83] Fiodor Dostoïevski, dans *Souvenirs de la maison des morts,* 1862.

[84] Voire note 100 pour plus de détails.

[85] Voir le Graphique 1 dans cette étude de Natixis : https://www.research.natixis.com/GlobalResearchWeb/Main/GlobalResearch/DownloadDocument/OX2UPzH-2VJ_z_O_tuopoQ%3D%3D

[86] Au sujet des bitcoins perdus, voir note 111 ci dessous.

[87] On trouve trois fonctions légèrement différentes déduites et énoncées par Jean-Joseph Goux dans *Les monnayeurs du langage*, Paris, Galilée, 1984, pages 50 sqq et 172 : l'archétype, le jeton et le trésor.

[88] Le « Cercle du Coin » a été à l'initiative, en novembre 2016, de la conversion de ce lieu parisien historique et élégant qui est ainsi devenu le premier « Bitcoin Boulevard » français. Toujours dans l'idée de populariser la monnaie cryptographique auprès des publics les plus divers, le Cercle a également encouragé le projet d'un Youtubeur français, Raj, « Autodisciple » qui s'est assigné le défi de « vivre 30 jours en bitcoins ». Cette expérience a été menée en janvier-février 2017, on peut la suivre sur le site https://www.youtube.com/autodisciple

[89] Voltaire, *Candide*, 1759.

[90] Voir note 68.

[91] Voir notamment ce qu'en dit David Graeber au chapitre 2 de son livre *Dette, 5000 ans d'histoire*, Paris, Les liens qui libèrent, 2011, notamment page 34 et note 6.

[92] Maurice Joly, *Dialogue aux enfers entre Machiavel & Montesquieu*, Bruxelles, 1864.

[93] Elle ne fut pas la seule. Un homme d'affaires plein d'humour assurait en privé s'être à l'époque plusieurs fois « réveillé la nuit en sueur en se demandant s'il était assez endetté. »

[94] Bien des discours contre Bitcoin pourraient enrichir l'étude de Laure Belot, *La déconnexion des élites. Comment Internet dérange l'ordre établi,* Paris, Les Arènes, 2015.

[95] Étude de 2010 du Crédit Agricole :

https://www.ca-cotesdarmor.fr/Vitrine/ObjCommun/Fic/CotesdArmor/CondGenBanque/Parlons_clair.pdf, *Alternatives Économiques*, 2011 : http://alternatives-economiques.fr/blogs/gloukoviezoff/2011/11/01/au-moins-5-millions-d%E2%80%99exclus-bancaires-selon-le-gouvernement/, Rapport de l'observatoire de l'inclusion bancaire, Banque de France, 2016 : http://www.lesclesdelabanque.com/Web/Cdb/ActeursSociaux/Content.nsf/DocumentsByIDWeb/AEFDFJ/$File/Rapport-de-l-observatoire-de-l-inclusion-bancaire-2015.pdf .

[96] Le chiffre de 10 millions de *unbanked* aux USA est donné par la Federal Deposit Insurance Corporation (FDIC) dans une étude de janvier 2011 intitulée « Tapping the Unbanked Market », en ligne ici : https://web.archive.org/web/20110102190942/http://www.fdic.gov/consumers/community/unbanked/index.html

[97] https://www.youtube.com/watch?v=BrRXP1tp6Kw.

[98] Chiffres calculés par la Banque Mondiale, cités par Wikipedia. Détail en ligne ici : http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1199807908806/4549025-1450455807487/Factbookpart1.pdf.

[99] Emmanuel Kant, *Vers la paix perpétuelle*, 1795.

[100] Plusieurs études de cabinets spécialisés convergent autour de ces chiffres : voir ces rapports sur : https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, https://www.ericsson.com/au/res/region_RASO/docs/2010/ericsson_50_billion_paper.pdf, https://www-ssl.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html ou ce résumé des prédictions contradictoires de *Structure Connect* : http://www.structureconnect.com/prediction-there-wont-be-50b-connected-iot-devices-by-2020/.

[101] Éclairage intéressant sur la difficulté de faire adopter des objets connectés : http://tempsreel.nouvelobs.com/economie/20161209.OBS2448/les-objets-connectes-n-interessent-personne.html

[102] Les messages de Satoshi dans l'ordre chronologique inversé : https://bitcointalk.org/index.php?action=profile;u=3;sa=showPosts.

[103] https://bitcoin.org/en/alert/2016-11-01-alert-retirement La « clef d'alerte » ayant été trop dévoilée au fur et à mesure du développement de Bitcoin, il a été choisi de la supprimer. De plus, le réseau Bitcoin est désormais épaulé par de nombreux relais médiatiques, il n'a plus semblé nécessaire de maintenir un affichage de message urgent dans le client.

[104] Calcul du nombre de bitcoins possédés par Satoshi : https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/.

[105] Papier de 2005 de Nick Szabo sur Bitgold : https://unenumerated.blogspot.fr/2005/12/bit-gold.html
[106] Réponse de Satoshi : http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:52186.
[107] L'équipe d'une quarantaine d'étudiants du *Aston University Centre for Forensic Linguistics* de l'Université de Birmingham était dirigée par le Professeur Jack Grieve. Elle confirmait au demeurant l'étude publiée par le bloggeur Skye Grey en décembre 2013, en ligne ici : https://likeinamirror.wordpress.com/2013/12/01/satoshi-nakamoto-is-probably-nick-szabo/.
[108] http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate Estimation du prix du Bitcoin à partir de 2009.
[109] Le message en question sur Bitcointalk : https://bitcointalk.org/index.php?topic=137.0.
[110] Article de la BBC sur le sujet : http://www.bbc.com/news/uk-wales-south-east-wales-25134289.
[111] Étude en langue anglais en ligne ici : https://letstalkbitcoin.com/blog/post/rise-of-the-zombie-bitcoins.
[112] A la fin de l'année 2012, la banque britannique HSBC a été condamnée à payer un montant record de 1,9 milliard de dollars) pour mettre fin à des poursuites des autorités américaines dans une affaire de blanchiment. « Nous assumons la responsabilité de nos erreurs passées. Nous avons déjà dit que nous en sommes profondément désolés et nous le disons une nouvelle fois », déclarait alors Stuart Gulliver, directeur général de HSBC.
[113] http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main Le *White Paper* intitulé « The Deep Web : Surfacing Hidden Value », publié en 2001, dresse un portrait de ce que pourrait être ce Web « profond ».
[114] Cours relevés sur blockchain.info.
[115] Volumes relevés sur blockchain.info.
[116] Ross Ulbricht a continué d'entretenir la chronique judiciaire. De nouveaux éléments tendant à prouver, atténuer ou contester sa culpabilité sont régulièrement publiés. Il semble notamment que des connexions suspectes usant de l'identité de Dread Pirate Roberts aient eu lieu depuis l'incarcération d'Ulbricht.
[117] Un exemple parmi d'autres, avec ce fâcheux raccourci du titreur du Figaro : http://www.lefigaro.fr/flash-actu/2015/08/21/97001-20150821FILWWW00037-l-ex-patron-francais-de-bitcoin-reste-en-prison.php.
[118] La BCE donne de nombreux détails (en anglais) ici : http://www.ecb.europa.eu/stats/money/euro/circulation/html/index.en.html. et quant aux chiffres en valeur, là : http://sdw.ecb.europa.eu/reports.do?node=1000004112.
[119] https://www.federalreserve.gov/paymentsystems/coin_currcircvalue.htm.

[120] Concernant l'or des particuliers, on ne peut que risquer des estimations. Celle-ci provient du site :
http://www.orargent.com/OrArgentvaleur.asp.
Il est probable qu'elle soit assez prudente.
[121] Les statistiques touchant à l'or sont toujours assez opaques, même en ce qui concerne celui détenu par les Banques Centrales. Leurs réserves seraient selon l'inventaire du World Gold Council, de 32 702 tonnes au 1er janvier 2016. Un chiffre qui paraît plausible.
[122] Il s'agit de l'application *Bitcoin Ticker*, selon le site américain spécialisé dans les technologies mobiles BGR. Ce n'est naturellement pas le seul exemple.
[123] https://bitcoin.fr/hausse-du-cours12/.
[124] C'est ce qu'avance Patrice Bernard sur son blog C'*est pas mon idée* le 10 décembre 2016 :
http://cestpasmonidee.blogspot.fr/2016/12/bitcoin-dans-une-prevision-choc-de-saxo.html.
[125] Sur ce qui suit, lire https://le-coin-coin.fr/3071-bitcoin-in-tempore-belli/.
[126] En page 7 du rapport du 18 janvier 2016 « Changes in modus operandi of IS in terrorist attacks ». Le rapport en ligne sur le site d'Europol (voir note 34 plus haut) étant régulièrement complété ou réécrit en palimpseste, on trouvera sa version d'origine sur le site Bitcoin.fr à l'adresse https://bitcoin.fr/europol-bitcoin-ne-finance-pas-les-terroristes.
[127] Site avec la liste la plus exhaustive conservant les monnaies « mortes » : http://cryptoguru.tk/.
[128] Petit historique des premières cryptomonnaies :
https://github.com/ppcoin/ppcoin/wiki/History-of-cryptocurrency.
[129] Toutes les capitalisations et leurs historiques sont issus de https://coinmarketcap.com/ .
[130] Adresse de l'ICO d'Ethereum :
https://blockchain.info/address/36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2.
[131] Adresse de l'ICO de NXT :
https://blockchain.info/address/1BCN1ugdKdWd9pQ8Am9hMhtHZfmbXzxE8a.
[132] Q3 Blockchain State par Coindesk :
http://www.coindesk.com/research/state-of-blockchain-q3-2016/.
[133] On les trouvera sur des sites comme
https://www.worldcoinindex.com.
[134] Sur l'anonymat des cryptomonnaies, lire « Sur la fongibilité, Bitcoin, Monero et pourquoi zCash est une mauvaise idée » en ligne ici : https://steemit.com/bitcoin/@dnaleor/on-fungibility-bitcoin-monero-and-why-zcash-is-a-bad-idea.
[135] Au total à la fin 2016, il y a eu 123 BIP (Bitcoin Improvement Proposals) dont une vingtaine a été définitivement acceptée. Et nul ne prétend que Satoshi Nakamoto ait été omniscient et infaillible. On a souligné qu'il avait notamment sous-estimé les chances d'un attaquant (sans grande conséquence d'ailleurs car

elles décroissent bien exponentiellement vers zéro comme cela a été montré par Ricardo Perez-Marco et Cyril Grunspan).

[136] Historique des forks Bitcoin : https://blog.blockchain.com/2016/02/26/a-brief-history-of-bitcoin-forks/.

[137] Fork Ethereum vs Ethereum Classic : frise historique sur le site https://ethereumclassic.github.io/.

[138] Voir note 18.

[139] On peut lire notamment l'étude prépubliée en octobre 2016 par G. Bissias, B. N. Levine, A. P. Ozisik, et G. Andresen, *An Analysis of Attacks on Blockchain Consensus* : https://arxiv.org/pdf/1610.07985v2.pdf .

[140] Lire en particulier l'étude *Eclipse Attacks on Bitcoin's Peer-to-Peer Network* de E. Heilman A. Kendler A. Zohar et S. Goldberg : https://eprint.iacr.org/2015/263.pdf .

[141] Pour en savoir un peu plus sur les signatures de Schnorr https://bitcoinmagazine.com/articles/the-power-of-schnorr-the-signature-algorithm-to-increase-bitcoin-s-scale-and-privacy-1460642496.

[142] Il est possible de constater encore aujourd'hui cette modification sur le lien suivant, à la ligne 17 de main.sh : https://github.com/bitcoin/bitcoin/commit/8c9479c6bbbc38b897dc97de9d04e4d5a5a36730.

[143] « "Argument from Authority" is a logical fallacy, so "Because Satoshi Said So" isn't a valid reason. However, staying true to the original vision of Bitcoin is very important. That vision is what inspires people to invest their time, energy, and wealth in this new, risky technology. » in https://bitcoinfoundation.org/a-scalability-roadmap/.

[144] Voir ici la répartition des différents nœuds : https://coin.dance/nodes. Voir également les prises de positions ici : https://coin.dance/poli

[145] *The Resolution of the Bitcoin experiment*, un véritable article hégelien : https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7.

[146] Une étude en langue anglaise fait un point complet sur le « fees market » : https://dl.dropboxusercontent.com/u/43331625/feemarket.pdf

[147] Le papier d'origine mise à jour en 2016 : https://lightning.network/lightning-network-paper.pdf.

[148] Un bon résumé de cela est disponible sur Wikipedia : https://fr.wikipedia.org/wiki/Six_degrés_de_séparation, et pour approfondir ces questions de chemins au sein d'un réseau : https://www.franceculture.fr/emissions/la-conversation-scientifique/les-reseaux-quils-soient-sociaux-ou-non-sont-ils.

[149] Papier décrivant le principe des sidechains : https://blockstream.com/sidechains.pdf.

[150] Couverture correspondante : http://www.economist.com/printedition/covers/2015-10-29/ap-e-eu-la-me-na-uk. Les plus attentifs noteront en bas à droite que le canonique « *vires in*

numeris » a été remplacé par « *in blockchain we trust* » absolument révélateur du glissement. Dans l'article premier du magazine :
http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine
il est intéressant de noter que blockchain apparaît 26 fois et Bitcoin seulement 13 fois.

[151] Voir cet article du *International Business Times* :
http://www.ibtimes.com/amazon-nearly-20-years-business-it-still-doesnt-make-money-investors-dont-seem-care-1513368.

[152] Voir cet article de *The Atlantic* :
https://www.theatlantic.com/business/archive/2009/09/facebook-turns-a-profit-users-hits-300-million/26721/.

[153] Voir cet article de *CNNMoney* :
http://money.cnn.com/2016/03/21/technology/twitter-10th-anniversary/.

[154] Il y aurait une thèse à écrire sur le très efficace marketing mis en œuvre par les initiateurs de la start-up R3CEV autour d'un projet de « blockchain consortiale » qui après avoir été vanté comme l'esprit de la blockchain enfin objectivé dans le monde réel et sérieux, celui des banques, n'avait, en fin 2016, délivré qu'un projet de base de donnée distribuée dont les concepteurs durent avouer à mi-mot qu'il n'était pas stricto sensu une blockchain. À la fin de l'année, trois des premières banques à avoir rejoint le consortium en sortaient assez bruyamment.

[155] Tous ces différents graphiques peuvent être consultés ici : https://blockchain.info/charts.

[156] Voir notes 73 et 74.

[157] Le Rapport de la BCE *Virtual currency schemes –a further analysis* (février 2015) est en ligne ici :
https://fr.scribd.com/document/257441572/Virtual-Currency-Schemes-A-Further-Analysis?ad_group=Online+Tracking+Link&campaign=Skimbit%2C+Ltd.&content=10079&irgwc=1&keyword=ft500noi&medium=affiliate&source=impactradius.

[158] Déclaration de David Andolfatto, vice-président de la Federal Reserve Bank de St. Louis.

[159] Tout cela est disponible dans la note du secrétaire général de la SEC, Robert W. Errett :
https://www.sec.gov/rules/sro/batsbzx/2016/34-79084.pdf.

[160] Voir note 70.

[161] On trouvera le poids des mots et le choc des photos en ligne sur Bloomberg ici :
https://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything.

[162] « Il n'existe en réalité aucun pouvoir au monde capable d'assurer l'honnêteté d'une banque qui ne tient pas à rester honnête », comme le note Sir Terry Pratchett dans l'ouvrage fondamental déjà cité en note 76.
[163] Lire ceci :
http://www.theaustralian.com.au/business/opinion/alan-kohler/asxs-blockchain-plans-may-have-been-hacked/news-story/5427ce8ebc8f44387bc1c966e86817bc
et entre les lignes ici :
https://www.ft.com/content/45851b58-62d1-11e6-8310-ecf0bddad227.
[164] La fin de l'année 2016 a vu, avec de premiers signes de désenchantement devant les résultats concrets des entreprises fondées sur la « technologie blockchain » un sensible retournement d'opinion, chez les plus pragmatiques, envers un bitcoin qui ne cesse de survivre à ses fossoyeurs. En décembre, les experts de la Saxo Banque incorporaient dans leurs dix prédictions choc pour 2017 un bitcoin propulsé à 2000 euros par l'aventurisme de la nouvelle administration américaine. Lire le document de Saxo Banque ici : http://fr.saxobank.com/Documents/Prévisions%20choc%202017%20FR.pdf.
[165] Source déjà citée en note 85.
[166] Stéphane Laborde, *Théorie Relative de la Monnaie 2.718*, 2016 : http://trm.creationmonetaire.info/.
[167] Article détaillant les problèmes de transmissions de données terre-mars : http://www.astrosurf.com/luxorion/mars-communication3.htm.
[168] Voir notes 73 et 74.
[169] Site reprenant les prédictions de personnalité du milieu en 2014 : https://foundersgrid.com/bitcoin-price/, site prenant des prédictions volontaires : https://www.hedgeable.com/research/bitcoin/estimator.
[170] Sans compter que la monnaie classique, régalienne si l'on puit dire par sa gravure, a été vue par une tradition longue et bien établie, comme de nature commune autant que publique. Citons ici Oresme, au chapitre V du Traité des Monnaies : « La monnaie, l'impression du coin, doit être faite par une personne publique ou par plusieurs, désignées pour cela par la communauté, parce que, comme on l'a déjà dit, la monnaie est, par nature, instituée et inventée pour le bien de la communauté. Et en son chapitre VI : L'argent appartient donc à la communauté et à chacune des personnes qui la composent. »
[171] Salvador Dalí, *Journal d'un génie*, Paris, Gallimard, 1994.
[172] Conférence donnée à Zurich en mars 2016. Texte dans *The Internet of Money*, page 55 et vidéo sur
www.youtube.com/watch?v=5ca70mCCf2M.
[173] Jean-Joseph Goux, *Les monnayeurs du langage*, Paris, Galilée, 1984.
[174] On a parfois l'impression que certains orateurs (même nés avant le 15 août 1971) n'ont ou ne veulent avoir aucune idée de ce qui existait auparavant : « Nous nous basons trop sur l'histoire récente (en particulier lorsque nous nous exclamons: "on n'a jamais vu ça!") et pas assez sur l'histoire dans sa globalité. En d'autres termes, l'histoire nous enseigne que ce qui ne s'est jamais produit finit

par arriver. Elle nous apprend beaucoup de choses en dehors des séquences temporelles étroites : plus notre vision est élargie, plus ces leçons s'avèrent enrichissantes. Bref, l'histoire nous prévient contre l'empirisme naïf qui consiste à apprendre des faits superficiels », Nassim Taleb, *op. cit.*, p.133.

[175] Jean-Joseph Goux, *Le trésor perdu de la finance folle*, Paris, Blusson, 2013, page 127. Goux parle d'un « moment inouï, dont on mesure encore mal les conséquences et la signification historique. » dans *Dette*, (*op. cit.* page 441). Graeber parle aussi d'une « phase nouvelle de l'histoire financière, une phase que personne ne comprend tout à fait. »

[176] En particulier pour nous avoir communiqué avant publication le support de sa présentation du 12 janvier 2017 au Séminaire de Cryptologie de l'Université Paris 7, « The Mathematics Behind Bitcoin Double Spend Race… » et avoir patiemment répondu à nos questions.