L'Élégance de Bitcoin : notes supplémentaires

Chapitre 1

(page 2) « Satoshi Nakamoto se met à travailler sur Bitcoin au printemps 2007 » : https://bitcointalk.org/index.php?topic=13.msg46#msg46, https://www.metzdowd.com/pipermail/cryptography/2008-November/014863.html.
(page 2) « il rentre en contact avec Adam Back » : Adam Back, *Re: Introduce yourself :)*, 18/04/2013 11:27:49 UTC : https://bitcointalk.org/index.php?topic=15672.msg1873483#msg1873483.
(page 4) « Hal et Ray réalisent alors un examen minutieux du code » : Ray Dillinger, *If I'd Known What We Were Starting*, 20 septembre 2017 : https://www.linkedin.com/pulse/id-known-what-we-were-starting-ray-dillinger/.
(page 4) « Après avoir échangé avec Satoshi » : https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf.
(page 5) « Dustin Trammell communique aussi avec Satoshi par courriel, et reçoit 25 bitcoins de sa part le 15 janvier » : http://web.archive.org/web/20131204164149/http://www.dustintrammell.com/files/Satoshi_Nakamoto.zip.
(page 8) « Certains individus minent en continu » : Ludovic Lars, *Les premiers mineurs de Bitcoin*, 19 juin 2022 : https://journalducoin.com/analyses/premiers-mineurs-bitcoin/.
(page 9) « Les prix sont publiés quotidiennement sur son site » : https://web.archive.org/web/20091229132610/http://newlibertystandard.wetpaint.com/page/Exchange+Rate.
(page 9) « Satoshi annonce la sortie de la version 0.2 du logiciel » : Satoshi Nakamoto, *Bitcoin 0.2 released!*, 16/12/2009 22:45:36 UTC : https://bitcointalk.org/index.php?topic=16.msg73#msg73.
(page 9) « Au début de l'année 2010, le bitcoin est désigné comme une "cryptomonnaie" » : https://web.archive.org/web/20100106082749/http://www.bitcoin.org/
(page 10) « NLS propose que le bitcoin [...] adopte le sigle boursier BTC et le symbole du baht thaïlandais » : NewLibertyStandard, *Bitcoin Currency Symbol ฿*, 05/02/2010 01:48:53 UTC : https://bitcointalk.org/index.php?topic=41.msg238#msg238.
(page 10) « NLS ouvre un magasin en ligne où il propose à la vente des timbres et des autocollants » : Liberty Swap Variety Shop, https://web.archive.org/web/20100414172623/http://newlibertystandard.wetpaint.com/page/Specialty+Shop.
(page 10) « D'autres services acceptant le bitcoin apparaissent » : https://web.archive.org/web/20100517040312/http://www.bitcoin.org:80/trade.
(page 10) « la première partie de poker mettant en jeu des bitcoins est organisée » : Kai Sedgwick, *Bitcoin History Part 14: The 1,000 BTC Poker Game*, 9 août 2019 : https://news.bitcoin.com/bitcoin-history-part-14-the-1000-btc-poker-game/.
(page 11) « Après avoir acheté des bitcoins à NLS » : https://blockchair.com/bitcoin/transaction/faf172f5dc06b0ae03268555dddcd65be47e9a8a8bb44a122b12bfaf735f9a81?o=1
(page 11) « celui-ci programme début mai un logiciel de minage qui s'adapte aux cartes graphiques » : Laszlo Hanyecz, *Generating Bitcoins with your video card (OpenCL/CUDA)*, 10/05/2010, 14:03:57 UTC : https://bitcointalk.org/index.php?topic=133.msg1103#msg1103.
(page 12) « un jeune Californien du nom de Jeremy Sturdivant accepte l'échange sur la messagerie instantanée IRC » : Bitcoin Who's Who, *A Living Currency*, 22 mai 2015 : https://www.bitcoinwhoswho.com/jercosinterview ; archive : https://web.archive.org/web/201505

28074728/http://bitcoinwhoswho.com/jercosinterview/.
(page 12) « un développeur américain de 44 ans, nommé Gavin Andresen, découvre Bitcoin par le biais d'un article publié sur InfoWorld » : Neil McAllister, *Open source innovation on the cutting edge*, 24 mai 2010 : https://www.infoworld.com/article/2627013/open-source-innovation-on-the-cutting-edge.html?page=3.
(page 13) « jusqu'à sa fermeture deux ans plus tard » : Gavin Andresen, *Bitcoin Faucet Hacked*, 2 mars 2012 : https://gavintech.blogspot.com/2012/03/bitcoin-faucet-hacked.html.
(page 13) « Le réseau tient le coup malgré la montée en charge » : Gavin Andresen, *Re: Scalability*, 14/7/2010, 04:22:49 UTC : https://bitcointalk.org/index.php?topic=286.msg2745#msg2745.
(page 13) « Parmi les personnes qui découvrent Bitcoin grâce à Slashdot, il y a Jed McCaleb » : The Ripple Blog, *Interview with Jed McCaleb, inventor of the Ripple protocol and co-founder of OpenCoin*, 17 avril 2013 : https://web.archive.org/web/20130428155220/https://ripple.com/blog/interview-with-jed-mccaleb-inventor-of-the-ripple-protocol-and-co-founder-of-opencoin/.
(page 14) « la plateforme de change Mt. Gox [...] est lancée et annoncée officiellement sur le forum par Jed » : Jed McCaleb, *New Bitcoin Exchange*, 18/07/2010 01:57:19 UTC : https://bitcointalk.org/index.php?topic=444.msg3866#msg3866.
(page 14) « Satoshi s'empresse d'inclure la correction dans la mise à jour 0.3.6 » : Satoshi Nakamoto, **** ALERT *** Upgrade to 0.3.6*, 29/07/2010 19:13:06 UTC : https://bitcointalk.org/index.php?topic=626.msg6451#msg6451.
(page 15) « il publie un correctif créant une chaîne alternative ne contenant pas la transaction incriminée » : Satoshi Nakamoto, *Version 0.3.10 - block 74638 overflow PATCH!*, 15/08/2010 23:48:22 UTC : https://bitcointalk.org/index.php?topic=827.msg9590#msg9590.
(page 15) « la chaîne correcte devient plus longue que l'autre le lendemain à 8 heures 10 du matin » : Satoshi Nakamoto, *Re: overflow bug SERIOUS*, 16/08/2010 12:59:38 UTC : https://bitcointalk.org/index.php?topic=823.msg9734#msg9734.
(page 15) « il a grossi à tel point qu'il devient difficile de diriger le mouvement » : Pete Rizzo, « *The Last Days of Satoshi: What Happened when Bitcoin's Creator Disappeared* », *Bitcoin Magazine*, 26 avril 2021 : https://bitcoinmagazine.com/technical/what-happened-when-bitcoin-creator-satoshi-nakamoto-disappeared.
(page 16) « PayPal gèle le compte de WikiLeaks » : *PayPal statement regarding WikiLeaks*, 3 décembre 2010 : https://web.archive.org/web/20101206112350/https://www.thepaypalblog.com/2010/12/paypal-statement-regarding-wikileaks/.
(page 17) « met en péril la survie financière de l'ONG » : Le 24 octobre 2011, un communiqué de WikiLeaks (*Banking Blockade*, 24/10/2011 13:00 UTC, https://wikileaks.org/Banking-Blockade.html) a indiqué que le blocus financier a fait disparaître de ses 95 % des revenus.
(page 17) « un article est publié sur PC World pour mettre en avant la possibilité d'un usage de Bitcoin par WikiLeaks » : Keir Thomas, *Could the Wikileaks Scandal Lead to New Virtual Currency?*, 11 décembre 2010, 00:30 : https://www.pcworld.com/article/499375/could_wikileaks_scandal_lead_to_new_virtual_currency.html.
(page 17) « Il vendra ses 55 000 bitcoins pour s'acheter un appartement près de Helsinki » : Martti Malmi sur Twitter, 18/12/2020 12:22 UTC : https://twitter.com/marttimalmi/status/1339908783187832834.
(page 17) « Gavin annonce qu'il a été invité par la CIA » : Gavin Andresen, *Gavin will visit the CIA*, 27/04/2011 19:00:26 UTC : https://bitcointalk.org/index.php?topic=6652.msg97181#msg97181.

(page 17) « Cette visite se passe le 14 juin » : Gavin Andresen sur Twitter, 14/06/2011 23:55 UTC : https://twitter.com/gavinandresen/status/80785477342478336.
(page 19) « en aucun cas des cartes bancaires volées, de la pédopornographie ou des services de tueur à gages » : Capture du *Seller's Guide* du 18/9/2012 (GX-120), https://antilop.cc/sr/exhibits/GX-120_Redacted.pdf : « Ne pas mettre en vente les objets dont le but est de nuire ou de frauder, comme les objets ou les informations volés, les cartes de crédit volées, la fausse monnaie, les informations personnelles, les assassinats et les armes de toutes sortes. Ne pas mettre en vente les objets liés à la pédophilie. »
(page 19) « une partie de l'épisode de FreeTalkLive du jour est consacrée à Bitcoin et à Silk Road » : https://soundcloud.com/freetalklive/ftl2011-03-16.
(page 19) « commence à l'accepter avec son entreprise » : Roger Ver, *Re: Earn 131BTC or 12-13BTC for getting shops/organisations to accept Bitcoin!*, 26/04/2011 08:00:52 UTC : https://bitcointalk.org/index.php?topic=4667.msg95746#msg95746.
(page 20) « son fondateur anonyme, Tom Williams, disparaît avec les 154 406 bitcoins présents sur les comptes de ses clients » : shotgun, *mybitcoin down or just me?*, 29/07/2011 22:41:36 UTC : https://bitcointalk.org/index.php?topic=32900.msg411251#msg411251.
(page 21) « Le premier portefeuille pour mobile [...] est lancé par Andreas Schildbach en mars 2011 » : Andreas Schildbach, *Bitcoin Wallet for Android*, 11/03/2011 21:25:51 UTC : https://bitcointalk.org/index.php?topic=4384.msg64142#msg64142.
(page 21) « Thomas Voegtlin crée Electrum en novembre 2011 » : Thomas Voegtlin, *[Electrum] a brainwallet in twelve words*, 10/11/2011 01:06:59 UTC : https://bitcointalk.org/index.php?topic=51397.msg612674#msg612674.
(page 22) « il réalise même une IPO pour son entreprise sur la plateforme roumaine MPEx » : Erik Voorhees, *S.DICE - SatoshiDICE 100% Dividend-Paying Asset on MPEx*, 20/08/2012 04:14:43 UTC : https://web.archive.org/web/20121024050433/https://bitcointalk.org/index.php?topic=101902.0.
(page 22) « Il revendra la plateforme le 17 juillet 2013 pour 126 315 bitcoins, soit 12,4 millions de dollars au moment de l'acquisition » : Erik Voorhees, « *SatoshiDice Sold for $12.4 Million* », *Bitcoin Magazine*, 28 juillet 2012 : https://bitcoinmagazine.com/markets/satoshidice-sold-12-4-million.

Chapitre 2

(page 26) « Bitcoinica, qui connaît une existence tumultueuse entre septembre 2011 et mai 2012 » : Ludovic Lars, *L'affaire Bitcoinica : le succès et la chute de la plateforme de trading*, 17 octobre 2020, https://journalducoin.com/analyses/affaire-bitcoinica-succes-chute-plateforme-trading-bitcoin/.
(page 28) « la place de marché Silk Road, qui représente alors 10 à 20 % de l'activité économique sur la chaîne de blocs » : *Chainalysis in Action: US Government Agencies Seize More Than $1 Billion in Cryptocurrency Connected to Infamous Darknet Market Silk Road*, 5 novembre 2020 : https://blog.chainalysis.com/reports/silk-road-doj-seizure-november-2020/.
(page 29) « est créée la Fondation Bitcoin en septembre 2012 » : Gavin Andresen, *[ANN] Bitcoin Foundation*, 27/09/2012 10:18:51 UTC : https://bitcointalk.org/index.php?topic=113400.msg1224721#msg1224721.
(page 30) « injonctions des sénateurs Chuck Schumer et Joe Manchin appelant à fermer la plateforme » : Joe Manchin, *Manchin Urges Federal Law Enforcement to Shut Down Online Black Market for Illegal Drugs*, 6 juin 2011 : https://www.manchin.senate.gov/newsroom/press-releases/manchin-urges-federal-law-enforcement-to-shut-down-onl

ine-black-market-for-illegal-drugs.
(page 30) « C'est Gary Alford [...] qui débusque la piste » : Nathaniel Popper, *The Unsung Tax Agent Who Put a Face on the Silk Road*, 25 décembre 2015 : https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html.
(page 30) « le serveur de Silk Road est saisi par la police islandaise » : https://antilop.cc/sr/files/2014_09_05_Declaration_of_Tarbell.pdf#page=5.
(page 31) « Mark Karpelès présente ses excuses publiques devant les télévisions japonaises » : https://www.youtube.com/watch?v=NeuCuM9CkBc
(page 31) « ce qui lui vaudra d'être surnommé le "baron du bitcoin" par les médias français » : Pierre Alonso, *En France, le passé trouble de l'ancien « baron du bitcoin »*, 29 juillet 2014 : https://www.lemonde.fr/pixels/article/2014/08/01/en-france-le-passe-trouble-de-l-ancien-baron-du-bitcoin_4464044_4408996.html.
(page 34) « Mike Hearn voit sa proposition d'ajout de la requête de réseau getutxos être rejetée pour cause de non-unanimité dans l'équipe de Bitcoin Core » : https://github.com/bitcoin/bitcoin/commit/70352e11c0194fe4e71efea06220544749f4cd64.
(page 34) « il est contraint de créer Bitcoin XT en décembre 2014 » : Mike Hearn, *[Bitcoin-development] Bitcoin XT*, 28/12/2014 18:04:08 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-December/007057.html.
(page 35) « Gavin Andresen [...] publie une série d'articles à ce sujet sur son blog personnel » : Gavin Andresen, *Time to roll out bigger blocks*, 4 mai 2015 : http://gavinandresen.ninja/time-to-roll-out-bigger-blocks.
(page 36) « L'augmentation de la taille limite des blocs est soutenue par les grandes coopératives minières chinoises » : *Why upgrade to 8MB but not 20MB?*, 12 juin 2015 : https://www.reddit.com/r/Bitcoin/comments/3a0n4m/why_upgrade_to_8mb_but_not_20mb/.
(page 36) « et par une partie des entreprises de l'industrie » : *Industry Letter Regarding Block Size*, 24 août 2015 : https://blog.bitmex.com/wp-content/uploads/2017/09/industry-letter.pdf.
(page 36) « la censure sur les principaux canaux de communication » : John Blocke, *A (brief and incomplete) history of censorship in /r/Bitcoin*, 14 novembre 2016 : https://medium.com/@johnblocke/a-brief-and-incomplete-history-of-censorship-in-r-bitcoin-c85a290fe43.
(page 36) « des attaques par déni de service contre les nœuds utilisant Bitcoin XT et ses successeurs » : Deryk Makgill, *Cyber Attacks Against Scaling Bitcoin* : https://wakgill.github.io/deryk/bitcoin-cyber-attacks.
(page 37) « deux enquêtes indépendantes par Wired et Gizmodo, selon lesquelles il serait probablement le créateur de Bitcoin » : Andy Greenberg, Gwern Branwen, *Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius*, 8 décembre 2015 (https://web.archive.org/web/20151208214655/https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/); Sam Biddle and Andy Cush, *This Australian Says He and His Dead Friend Invented Bitcoin*, 8 décembre 2015 (https://web.archive.org/web/20151208235451/https://gizmodo.com/this-australian-says-he-and-his-dead-friend-invented-bi-1746958692).
(page 38) « Il reconnaîtra plus tard avoir été dupé » : *Déposition de Gavin Andresen dans le cadre de l'affaire Wright / Kleiman*, 19 juin 2020 : https://storage.courtlistener.com/recap/gov.uscourts.flsd.521536/gov.uscourts.flsd.521536.589.3.pdf#page=88.
(page 39) « lancer le signalement de SegWit par les mineurs, qui commence le 15 novembre 2016 » : Bitcoin Core, *Bitcoin Core version 0.13.1 released*, 27 octobre 2016 : https://bitc

oin.org/en/release/v0.13.1#segregated-witness-soft-fork.
(page 40) «élles exigent en outre qu'elle intègre une protection contre la rediffusion, faute de quoi elle ne sera même pas listée » : Aaron van Wirdum, *Major Exchanges Will Consider Bitcoin Unlimited a "New Asset"*, 17 mars 2017 :https://bitcoinmagazine.com/technical/major-exchanges-will-consider-bitcoin-unlimited-new-asset
(page 40) « l'opposition de Gregory Maxwell » : Gregory Maxwell, *[bitcoin-dev] I do not support the BIP 148 UASF*, 14/04/2017 07:56:31 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-April/014152.html.
(page 41) « ils insistent en particulier sur l'absence de rediffusion des transactions » : Alex Bosworth, *[Bitcoin-segwit2x] Alpha Milestone*, 14/06/2017 17:35:00 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-June/000003.html.
(page 42) « une discussion sur un système distribué de noms de domaine (alors appelé BitDNS) s'engage sur IRC, puis sur le forum de Bitcoin » : appamatto, *BitDNS and Generalizing Bitcoin*, 15/11/2010 03:02:31 UTC : https://bitcointalk.org/index.php?topic=1790.msg22019#msg22019.
(page 42) « Cela donne finalement naissance à Namecoin » : Vincent Durham (vinced), *[announce] Namecoin - a distributed naming system based on Bitcoin*, 18/04/2011 00:52:59 UTC : https://bitcointalk.org/index.php?topic=6017.msg88356#msg88356.
(page 43) « du célèbre Dogecoin en décembre » : Ludovic Lars, *Le dogecoin est-il un concurrent sérieux au bitcoin ?*, 1er mai 2021 : https://www.contrepoints.org/2021/05/01/396380-le-dogecoin-est-il-un-concurrent-serieux-au-bitcoin.
(page 43) « scepticisme qui transparaît dans les réactions de Hal Finney et de Gavin Andresen » : Hal Finney, *Re: Early speculators' reward*, 30/05/2011 18:28:34 UTC : https://bitcointalk.org/index.php?topic=10666.msg152988#msg152988 ; Gavin Andresen, *Alternative Block Chains : be safe!*, 09/09/2011 13:21:18 UTC : https://bitcointalk.org/index.php?topic=42465.msg516789#msg516789.
(page 44) « NXT, une plateforme incluant un grand nombre de fonctionnalités » : Bas Wisselink, *| Nxt | Blockchain Platform | Proof of Stake | Official*, 27/04/2014 19:01:37 UTC : https://bitcointalk.org/index.php?topic=587007.msg6426512#msg6426512.
(page 44) « le Tether USD [...] est lancé sur la chaîne de Bitcoin le 6 octobre sous le nom de Realcoin » : https://www.omniexplorer.info/tx/5ed3694e8a4fa8d3ec5c75eb6789492c69e65511522b220e94ab51da2b6dd53f.
(page 47) « une réglementation ultra-restrictive, imposant à une large part des acteurs de l'écosystème d'obtenir une licence d'exploitation appelée la "BitLicence" » : Davis Polk, *New York's Final "BitLicense" Rule: Overview and Changes from July 2014 Proposal*, 5 juin 2015 : https://www.davispolk.com/sites/default/files/2015-06-05_New_Yorks_Final_BitLicense_Rule.pdf.
(page 47) « l'État français fait passer un décret en novembre 2019 » : *Décret n° 2019-1213 du 21 novembre 2019 relatif aux prestataires de services sur actifs numériques* : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039407517/.
(page 47) « En décembre 2017, il entre même à la bourse de Chicago » : Grégory Raymond, *Le bitcoin débarque à la Bourse de Chicago : un moment historique !*, 8 décembre 2017 : https://www.capital.fr/crypto/le-bitcoin-debarque-a-la-bourse-de-chicago-un-moment-historique-1259946.
(page 48) « servir d'étalon au système monétaire mondial » : Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, mars 2018.
(page 48) « Microstrategy [...] annonce [...] s'être procuré 21 454 BTC, pour un montant d'achat total de 250 millions de dollars » : Business Wire, *MicroStrategy Adopts Bitcoin as Primary*

Treasury Reserve Asset, 11 août 2020, https://www.businesswire.com/news/home/20200811005331/en/MicroStrategy-Adopts-Bitcoin-as-Primary-Treasury-Reserve-Asset.
(page 50) « critiques [...] à l'égard des pratiques autoritaires du président » : Alex Gladstein, « *The Village and the Strongman: The Unlikely Story of Bitcoin and El Salvador* », *Bitcoin Magazine*, 16 septembre 2021 :https://bitcoinmagazine.com/culture/the-polarity-of-bitcoin-in-el-salvador.
(page 50) « de l'imposition du cours légal elle-même qui va à l'encontre de la philosophie de Bitcoin » : Ludovic Lars, *Cours légal du bitcoin au Salvador, la fausse bonne idée*, 21 septembre 2021 : https://www.contrepoints.org/2021/09/21/406280-cours-legal-du-bitcoin-au-salvador-la-fausse-bonne-idee.
(page 50) « l'adoption est loin d'être un succès » : Nessim Aït-Kacimi, *Salvador : le bitcoin peine à s'imposer face au dollar*, 3 mai 2022 : https://www.lesechos.fr/finance-marches/marches-financiers/salvador-ladoption-du-bitcoin-comme-monnaie-officielle-ne-seduit-pas-1404569.
(page 50) « l'initiative Libra, portée par Facebook et annoncée le 18 juin 2019 » : Ludovic Lars, *Analyse du projet Libra : quelles répercussions sur Bitcoin ?*, 6 juillet 2019 : https://cryptoast.fr/analyse-libra-repercussions-bitcoin/.

Chapitre 3

(page 55) « les trois fonctions monétaires classiques, souvent citées par les économistes et dont l'origine est attribuée au philosophe Aristote » : Dans l'*Éthique à Nicomaque*, Aristote énonce ce qui sert de base à ces fameuses trois fonctions. Il fait d'abord de la monnaie une unité de compte permettant d'évaluer la valeur des choses :

> « C'est pourquoi toutes les choses faisant objet de transaction doivent être d'une façon quelconque commensurables entre elles. C'est à cette fin que la monnaie a été introduite, devenant une sorte de moyen terme, car elle mesure toutes choses et par suite l'excès et le défaut. » (trad. de J. Tricot, 1133a)

Il explicite ensuite son rôle d'intermédiaire d'échange, qui est pour lui issu d'une convention légale :

> « Cet étalon n'est autre, en réalité, que le besoin, qui est le lien universel (car si les hommes n'avaient besoin de rien, ou si leurs besoins n'étaient pas pareils, il n'y aurait plus d'échange du tout, ou les échanges seraient différents) ; mais la monnaie est devenue une sorte de substitut du besoin et cela par convention, et c'est d'ailleurs pour cette raison que la monnaie reçoit le nom de νομισμα, parce qu'elle existe non pas par nature, mais en vertu de la loi (νομος), et qu'il est en notre pouvoir de la changer et de la rendre inutilisable. » (trad. de J. Tricot, 1133a)

Il attribue enfin à la monnaie une fonction de réserve de valeur dans le temps :

> « Pour les échanges éventuels, dans l'hypothèse où nous n'avons besoin de rien pour le moment, la monnaie est pour nous une sorte de gage, donnant l'assurance que l'échange sera possible si jamais le besoin s'en fait sentir, car on doit pouvoir, en remettant l'argent, obtenir ce dont on manque. » (trad. de J. Tricot, 1133b)

(page 56) « l'effet Lindy » : Le nom de l'effet Lindy a été créé par l'auteur américain Albert

Goldman, en référence aux restaurants Lindy's à New York où il se disait que « l'espérance de vie d'un comédien de télévision est [inversement] proportionnelle au montant total de son exposition sur les ondes » (Albert Goldman, « *Lindy's Law* », *The New Republic*, pp. 34–35, 13 juin 1964 : `https://gwern.net/doc/statistics/probability/1964-goldman.pdf`). Son sens actuel lui a été donné par Benoît Mandelbrot dans son livre *The Fractal Geometry of Nature* publié en 1982.

(page 58) « la tentative d'instauration d'une monnaie fiat par la dynastie Song entre le XIe et le XIIe en Chine » : Peter St-Onge, *How Paper Money Led to the Mongol Conquest: Money and the Collapse of Song China*, 2017.

(page 61) « la nature mimétique du désir » : René Girard, *Mensonge romantique et vérité romanesque*, 1961.

(page 63) « Les premières pièces frappées sont vraisemblablement apparues au VIIe siècle avant Jésus-Christ en Asie Mineure sous l'impulsion des Lydiens » : John H. Kroll, *The Coins of Sardis*, 2010 : `https://sardisexpedition.org/en/essays/latw-kroll-coins-of-sardis`.

(page 65) « exiger un coût infalsifiable pour sa production » : Nick Szabo, *Antiques, time, gold, and bit gold*, 28 août 2008 : `https://unenumerated.blogspot.com/2005/10/antiques-time-gold-and-bit-gold.html`.

(page 67) « la théorie lockéenne de l'origine de la monnaie » : John Locke, *Some Considerations of the Consequences of the Lowering of Interest and the Raising the Value of Money*, 1691 : « Car l'humanité, ayant consenti à mettre une valeur imaginaire à l'or et à l'argent à cause de leur durabilité, de leur rareté et du fait qu'ils ne sont pas très susceptibles d'être contrefaits, en a fait par consentement général les gages communs, par lesquels les hommes sont assurés, en échange d'eux, de recevoir des choses de même valeur que celles qu'ils ont données pour toute quantité de ces métaux. C'est ainsi que la valeur intrinsèque de ces métaux, qui font l'objet d'un troc commun, n'est rien d'autre que la quantité que les hommes en donnent ou en reçoivent. »

(page 69) « la valeur proviendrait du fait que le bitcoin a été échangé contre du dollar, avançant l'idée que la régression se transmettrait avec cette conversion » : xc, *Bitcoin does NOT violate Mises' Regression Theorem*, 27/07/2010, 02:09:27 AM : `https://bitcointalk.org/index.php?topic=583.msg5984#msg5984` ; AristippusofCyrene, *Bitcoin and the Regression Theorem of Money*, 7 décembre 2012 : `https://voluntaryistreader.wordpress.com/2012/12/07/bitcoin-and-the-regression-theorem-of-money/`.

(page 69) « celle qui ferait résider la valeur initiale du bitcoin dans sa capacité à être un système de paiement » : Brice Rothschild, *Théorème de régression et Bitcoin*, 6 novembre 2013 : `https://www.contrepoints.org/2013/11/06/145305-theoreme-de-regression-et-bitcoin` ; Jeffrey Tucker, *What Gave Bitcoin Its Value?*, 27 août 2014 : `https://fee.org/articles/what-gave-bitcoin-its-value/`.

(page 69) « des individus auraient attribué de la valeur au bitcoin pour sa capacité à servir pour l'horodatage » : Simon Gaines, *Bitcoin: Intrinsically Worthless?*, 24 avril 2019 : `https://medium.com/@ahuroad/bitcoin-intrinsically-worthless-5d626645e1c6`.

(page 71) « Ron Paul [...] proposait notamment d'"abolir la Fed" » : Ron Paul, *End The Fed*, 2009.

(page 73) « droit de résistance [...] reconnu par [...] la révolution américaine » : Thomas Jefferson, *Déclaration unanime des treize États unis d'Amérique*, 4 juillet 1776 : « Lorsqu'une longue suite d'abus et d'usurpations, tendant invariablement au même but, marque le dessein de soumettre [les hommes] au despotisme absolu, il est de leur droit, il est de leur devoir de rejeter un tel gouvernement et de pourvoir, par de nouvelles sauvegardes, à leur sécurité future. »

(page 73) « et la révolution française » : *Déclaration des Droits de l'Homme et du Citoyen*, 26 août 1789 : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à

l'oppression. »
(page 73) « désobéissance civile, conception ébauchée par Étienne de La Boétie au XVIe siècle » : Étienne de La Boétie, *Discours de la servitude volontaire*, 1574.
(page 73) « théorisée par Henry David Thoreau en 1849 » : Henry David Thoreau, *La Désobéissance civile*, 1849.
(page 74) « donations en bitcoins [...] qui, à défaut d'être subtantielles sur le moment, le sont devenues avec la hausse du cours quelques années plus tard » : `https://bitinfocharts.com/bitcoin/address/1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v`
(page 74) « il a participé à la cérémonie d'initialisation [de ZCash] en 2016 » : Zcash Media, *Edward Snowden: I participated in the Zcash ceremony under the pseudonym of John Dobbertin* (vidéo), 28 avril 2022 :`https://www.youtube.com/watch?v=8qSA29vWWds`.
(page 74) « l'équivalent de plusieurs millions de dollars ont transité par son adresse » : `https://bitinfocharts.com/bitcoin/address/3QzYvaRFY6bakFBW4YBRrzmwzTnfZcaA6E`.
(page 74) « cet apport en bitcoin aurait représenté 10 % de leur financement total » : Anton Zverev et Catherine Belton, *Bitcoin donations surge to jailed Kremlin critic Navalny's cause: data*, 11 février 2021 : `https://www.reuters.com/article/us-russia-politics-navalny-crypto-curren-idUSKBN2AB2GR`.
(page 78) « Konkin imaginait alors résoudre le problème par l'utilisation d'une banque illégale » : Samuel Edward Konkin III, *Counter-Economics: From the Back Alleys... To the Stars*, KoPubCo, 2018.
(page 78) « rendre à César ce qui est à César, et à Dieu ce qui est à Dieu » : Mt 22:15-22.
(page 79) « Ross Ulbricht qui a ouvertement admis avoir été influencé par l'école autrichienne d'économie et par la philosophie agoriste » : En mars 2012, Ross Ulbricht a témoigné de son état d'esprit sur le forum de Silk Road sous le pseudonyme de Dread Pirate Roberts. Il écrivait :

> « Pendant des années, j'ai été frustré et démoralisé par ce qui semblait être des barrières insurmontables entre le monde actuel et le monde que je voulais. J'ai longtemps cherché la vérité sur ce qui est bien, mal et bon pour l'humanité. J'ai discuté, appris et lu les œuvres de personnes brillantes à la recherche de la vérité. C'est une chose sacrément difficile à faire avec toute la désinformation et les distractions présentes dans l'océan d'opinions où nous vivons. Mais j'ai fini par trouver quelque chose avec quoi je pouvais être entièrement d'accord. Quelque chose qui avait du sens, qui était simple, élégant et cohérent dans tous les cas. Je parle de la théorie économique autrichienne, du volontarisme, de l'anarcho-capitalisme, de l'agorisme, etc. embrassés par des gens comme Mises et Rothbard avant leur mort, et Salerno et Rockwell aujourd'hui.
>
> Grâce à leurs travaux, j'ai compris les mécanismes de la liberté et les répercutions de la tyrannie. Mais une telle vision était une malédiction. Partout où je posais les yeux, je voyais l'État et l'horrible effet d'étiolement qu'il avait sur l'esprit humain. C'était horriblement déprimant. C'était comme se réveiller d'un rêve agité pour se retrouver dans une cage sans échappatoire. Mais j'ai aussi vu des esprits libres essayant de se libérer de leurs chaînes, faisant tout ce qu'ils pouvaient pour servir leur prochain et subvenir à leurs besoins et à ceux de leurs proches. J'ai vu l'effet magique et puissant de création de richesse du marché, la façon dont il encourageait la coopération, la courtoisie et la tolérance. Comment il transformait les étrangers, ou même les ennemis, en partenaires commerciaux. Comment il coordonnait les actions de chaque personne sur la planète d'une manière trop complexe pour qu'un seul esprit puisse l'imaginer, afin de produire une abondance débordante de richesses, où rien n'est gaspillé et où le pouvoir et la responsabilité sont donnés aux les personnes les plus méritantes et les plus capables. J'ai

> vu une meilleure voie, mais je ne connaissais aucun moyen d'y parvenir.
>
> J'ai lu tout ce que je pouvais pour approfondir ma compréhension de l'économie et de la liberté, mais tout était cérébral et il n'y avait pas d'appel à l'action, si ce n'est dire aux gens autour de moi ce que j'avais appris et espérer leur faire voir la lumière. C'était jusqu'à ce que je lise "Alongside night" et les travaux de Samuel Edward Konkin III. La pièce manquante du puzzle était enfin là ! Tout d'un coup, tout était clair : chaque action qu'on entreprenait en dehors du champ de contrôle du gouvernement renforçait le marché et affaiblissait l'État. J'ai vu comment l'État vivait de façon parasitaire aux dépens des personnes productives du monde, et à quelle vitesse il s'effondrerait s'il n'obtenait pas ses recettes fiscales. Pas de soldats si vous ne pouvez pas les payer. Pas de guerre contre la drogue sans les milliards de dollars détournés des personnes que vous opprimez. »

Dread Pirate Roberts, *chat*, 20 mars 2012 : `https://antilop.cc/sr/users/dpr/threads/20120320-1103-chat.html`.

Chapitre 4

(page 84) « illustré par la courbe de Laffer » : Arthur B. Laffer, *The Laffer Curve: Past, Present, and Future*, 1er juin 2004 : `https://www.heritage.org/taxes/report/the-laffer-curve-past-present-and-future`.
(page 84) « approche fiscale de la monnaie » : Tcherneva Pavlina, « *Chartalism and the Tax-Driven Approach to Money* », *A Handbook of Alternative Monetary Economics*, ch. 5, 2007.
(page 86) « Ces pratiques ont notamment été observées par le philosophe chrétien Nicolas Oresme » : Benoît Malbranque, *Oresme et les dangers de la dévaluation monétaire*, 14 juillet 2017 : `https://www.institutcoppet.org/oresme-et-les-dangers-de-la-devaluation-monetaire/`.
(page 87) « la Première guerre mondiale a été majoritairement financée par la création monétaire et par la réduction de la dette liée à l'inflation » : Vincent Duchaussoy et Éric Monnet, *La Banque de France et le financement direct et indirect du ministère des Finances pendant la Première Guerre mondiale : un modèle français ?*, `https://books.openedition.org/igpde/4132`.
(page 89) « Si le phénomène s'emballe, celui-ci peut conduire *in fine* à la destruction de l'unité de compte » : Les cas d'hyperinflation dans l'histoire des siècles précédents sont nombreux. Ils coïncident la plupart du temps avec les premières expériences de papier-monnaie durant une période troublée par la guerre ou par la révolution. Nous pouvons notamment citer les exemples de l'assignat révolutionnaire français qui a connu l'hyperinflation entre 1793 et 1795, du *papiermark* de la république de Weimar dont la valeur s'est effondrée entre 1922 et 1924, du rouble russe dont le pouvoir d'achat a été annihilé entre 1917 et 1922 et du yuan nationaliste chinois qui s'est écroulé entre 1946 et 1949. Dans l'histoire récente, on peut faire mention de l'hyperinflation du rouble soviétique entre 1991 et 1993, de celle du dollar zimbabwéen de 2000 à 2009 et de l'inflation galopante du bolivar vénézuélien qui sévit depuis 2016.
(page 89) « ce qu'on appelle une hyperinflation » : La Commission européenne définit une économie hyperinflationniste par les caractéristiques suivantes : 1) la population en général préfère conserver sa richesse en actifs non monétaires ou en une monnaie étrangère relativement stable ; 2) la population en général apprécie les montants monétaires, non pas dans la monnaie locale, mais dans une monnaie étrangère relativement stable, les prix pouvant être exprimés dans cette monnaie ; 3) les ventes et les achats à crédit sont conclus à des prix qui tiennent compte de la perte de pouvoir d'achat attendue durant la durée du crédit, même si cette période est courte ; 4) les taux d'intérêt, les salaires et les prix sont liés à un indice de prix ; et 5) le taux cumulé de l'inflation sur trois ans approche ou dépasse 100 %. Elle est ainsi liée à la perte des fonctions de

réserve de valeur et d'unité de compte de la monnaie. – Voir IAS 29 : « Information financière dans les économies hyperinflationnistes », 29 octobre 2018 : http://www.focusifrs.com/menu_gauche/normes_et_interpretations/textes_des_normes_et_interpretations/ias_29_information_financiere_dans_les_economies_hyperinflationnistes.

(page 90) « l'éphémère Banque générale, qui s'est développée en France de 1716 à 1720 » : L'exemple de la Banque générale, devenue Banque royale en 1719, est fascinant car cette dernière a contribué à créer l'une des premières bulles financières mondiales de l'histoire. Le système de Law était en effet étroitement lié à la Compagnie du Mississippi, ayant pour but de de prendre en charge la dette à court terme de l'État accumulée par le défunt Louis XIV et de développer le potentiel commercial de la Louisiane française en émettant des actions de la Compagnie. – Antoin E. Murphy, « John Law et la bulle de la Compagnie du Mississippi », *L'Économie politique*, 2010/4 (n° 48), p. 7-22 : https://www.cairn.info/revue-l-economie-politique-2010-4-page-7.htm.

(page 94) « *Digital Currency Electronic Payment* ou DCEP » : Xinyu Liu, Fan Lu, Wanlu Shan, Jiayuan Zhang, *The Progress of Digital Currency Electronic Payment*, 2021 : https://www.atlantis-press.com/article/125965904.pdf.

(page 94) « couronne électronique (ou e-Krona) » : Cecilia Skingsley, *Skingsley: Borde Riksbanken ge ut e-kronor?*, 16 novembre 2016 : https://www.riksbank.se/sv/press-och-publicerat/Tal/2016/Skingsley-Borde-Riksbanken-ge-ut-e-kronor/ ; archive : https://web.archive.org/web/20161117155655/https://www.riksbank.se/sv/press-och-publicerat/Tal/2016/Skingsley-Borde-Riksbanken-ge-ut-e-kronor/.

(page 94) « la Banque d'Angleterre a annoncé former un groupe de travail en avril 2021 » : Bank of England, *Bank of England statement on Central Bank Digital Currency*, 19 avril 2021 : https://www.bankofengland.co.uk/news/2021/april/bank-of-england-statement-on-central-bank-digital-currency.

(page 94) « la BCE a annoncé en juillet 2021 vouloir développer un euro numérique » : https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html

(page 96) « [les banques commerciales] devraient gagner quelque chose au change, par exemple en obtenant à la place un rôle d'intermédiaire dans le système » : C'est le sens de l'idée de MNBC « synthétique » évoquée par Tobias Adrian (économiste du FMI) en 2019. – Tobias Adrian, *Stablecoins, Central Bank Digital Currencies, and Cross-Border Payments: A New Look at the International Monetary System*, 13 mai 2019 : https://www.imf.org/en/News/Articles/2019/05/13/sp051419-stablecoins-central-bank-digital-currencies-and-cross-border-payments). Cette idée a été intégrée dans le prototype Aurum de la Banque des règlements internationaux (BRI) présenté en octobre 2022 (*Project Aurum: a prototype for two-tier central bank digital currency (CBDC)*, 21 octobre 2021 : https://www.bis.org/publ/othp57.htm).

(page 97) « diverses subventions pour encourager l'usage [...] comme cela est déjà fait en Chine dans le cadre du yuan numérique » : China Daily, *E-CNY boosts holiday consumption*, 1er février 2023 : https://www.chinadaily.com.cn/a/202302/01/WS63d9bb3fa31057c47ebac36e.html.

(page 97) « coût de changement de juridiction » : Patri Friedman, *Dynamic Geography: A Blueprint for Efficient Government*, 2002 : https://patrifriedman.com/old_writing/dynamic_geography.html.

(page 100) « la frappe privée de pièces était tout à fait autorisée et pratiquée » : Brian Summers, *Private Coinage in America*, 1er juillet 1976 : https://fee.org/articles/private-coinage-in-america/.

(page 101) « L'IRS a estimé que l'évasion fiscale des clients s'élevait à 24 millions de dollars » :

https://www.latimes.com/archives/la-xpm-2004-mar-10-fi-taxscam10-story.html
(page 101) « NORFED » : NORFED est l'acronyme de *National Organization for the Repeal of the Federal Reserve and Internal Revenue Code*, en français : l'Organisation nationale pour l'abrogation de la Réserve fédérale et de l'*Internal Revenue Code*.
(page 101) « les pièces frappées ressemblaient au dollar ce qui s'apparentait à de la contrefaçon » : *18 U.S. Code § 485 - Coins or bars* : https://www.law.cornell.edu/uscode/text/18/485.
(page 101) « Après une descente du FBI dans les locaux de NORFED en 2007 » : Bernard von NotHaus, *FBI Raids Liberty Dollar*, 14 novembre 2007 : http://www.libertydollar.org/ld/legal/raidday1.htm.
(page 102) « les pièces pouvaient être considérées comme de la contrebande et être saisies comme telles » : https://www.coinworld.com/news/precious-metals/liberty-dollars-may-be-subject-to-seizure.html
(page 102) « Les ventes de ces pièces ont également été interdites sur eBay en décembre 2012 » : Jon Matonis, *U.S. Secret Service Bans Certain Gold and Silver Coins On eBay*, 15 décembre 2012 : https://www.forbes.com/sites/jonmatonis/2012/12/15/u-s-secret-service-bans-certain-gold-and-silver-coins-on-ebay/.
(page 102) « Le troisième cas de monnaie privée est l'e-gold » : Ludovic Lars, *L'e-gold de Douglas Jackson : la cryptomonnaie "or"*, 8 mars 2020 : https://journalducoin.com/analyses/gold-douglas-jackson-cryptomonnaie-or-1996/.
(page 102) « Au terme d'une enquête menée par le Secret Service » : https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads
(page 102) « activité de transfert d'argent sans licence » : *18 U.S. Code § 1960 - Prohibition of unlicensed money transmitting businesses* : https://www.law.cornell.edu/uscode/text/18/1960.
(page 103) « e-gold a dû fermer ses portes définitivement en novembre 2009 » : https://web.archive.org/web/20100103135107/http://blog.e-gold.com/2009/11/egold-update-value-access.html.
(page 103) « le système Liberty Reserve » : Ludovic Lars, *La Liberty Reserve d'Arthur Budovsky : plongée dans l'obscure préhistoire de Bitcoin*, 21 mars 2020 : https://journalducoin.com/analyses/liberty-reserve-bitcoin/.
(page 103) « l'acte d'accusation du département de la Justice étasunienne estimait que Liberty Reserve possédait plus d'un million d'utilisateurs dans le monde, dont plus de 200 000 aux États-Unis, et traitait 12 millions de transactions financières annuellement, pour un volume combiné de plus de 1,4 milliards de dollars » : United States District Court for the Southern District of New York, *Liberty Reserve, et al. Indictment*, 28 mai 2013 : https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Liberty%20Reserve%2C%20et%20al.%20Indictment%20-%20Redacted_0.pdf.
(page 104) Luke Nosek, ancien vice-président de Confinity chargé du marketing, a confirmé la vision originelle de PayPal durant le Forum économique mondial de Davos le 31 janvier 2019 :

> « Beaucoup de gens l'ignorent, mais la mission de PayPal était de créer une monnaie mondiale qui était indépendante de l'ingérence des cartels bancaires corrompus et des États qui dévaluaient leurs monnaies. Nous avons réussi à construire quelque chose de très puissant économiquement, qui a rendu possible de nombreuses petites entreprises, nous en sommes super fiers, mais nous n'avons jamais accompli cette mission. Je ne pense pas que [le problème de la monnaie numérique] soit résolu par PayPal, précisément en raison du fait que [...] PayPal est simplement trop centralisé et trop attaché aux grandes

institutions financières comme Visa, MasterCard, le réseau ACH, le réseau SWIFT. »

Reserve, *Luke Nosek speaks to Nevin Freeman about Reserve and the original vision of PayPal - Davos 2019* (vidéo), 22 mai 2019 : https://www.youtube.com/watch?v=h0e0zh0xeMU&t=40s.

Chapitre 5

(page 108) « la télécommunication, ou la transmission d'information à distance » : Le préfixe télé- vient du grec ancien τῆλε, tēle, « loin ».
(page 110) « Turing-complet » : Alan Turing, *On Computable Numbers, with an Application to the Entscheidungsproblem*, 28 mai 1936 : https://www.cs.virginia.edu/~robins/Turing_Paper_1936.pdf.
(page 111) « Le système libre GNU/Linux a quant à lui été créé en 1991 » : Linus Benedict Torvalds, *What would you like to see most in minix?*, 25/08/1991 20:57:08 UTC : https://groups.google.com/g/comp.os.minix/c/dlNtH7RRrGA/m/SwRavCzVE7gJ.
(page 112) « Clifford Cocks, James Ellis et Malcolm Williamson avaient déjà mis au point un tel cryptosystème [...] mais leurs recherches sont restées classifiées » : James H. Ellis, « *The Possibility of Secure Non-Secret Digital Encryption* », *CESG Report*, janvier 1970 : https://cryptocellar.org/cesg/possnse.pdf ; Clifford C. Cocks, « *A Note on Non-Secret Encryption* », *CESG Report*, 20 November 1973 : https://cryptocellar.org/cesg/notense.pdf ; Malcolm J. Williamson, « *Non-Secret Encryption Using a Finite Field* », *CESG Report*, 21 janvier 1974 : https://cryptocellar.org/cesg/secenc.pdf.
(page 112) « Ralph Merkle avait également décrit l'échange de clés de Diffie et Hellman dans un article écrit en 1974 et publié en 1978 » : Ralph C. Merkle, *Publishing a new idea*, 2005 : https://www.ralphmerkle.com/1974/ ; Ralph C. Merkle, « *Secure Communications over Insecure Channel* », *Communications of the ACM*, avril 1978.
(page 112) « l'algorithme de chiffrement RSA, créé en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman et breveté par le MIT en 1983 » : Ron Rivest, Adi Shamir, Leonard Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, février 1978 : https://people.csail.mit.edu/rivest/Rsapaper.pdf ; archive : https://web.archive.org/web/20070615132925/https://people.csail.mit.edu/rivest/Rsapaper.pdf.
(page 113) « l'algorithme de chiffrement d'ElGamal qui a été présenté par Taher ElGamal en 1984 » : Taher ElGamal, « *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms* », 1984 : https://people.csail.mit.edu/alinush/6.857-spring-2015/papers/elgamal.pdf.
(page 113) « contributions indépendantes de Neal Koblitz et de Victor Miller » : Neal Koblitz, « *Elliptic Curve Cryptosystems* », 1987 : https://community.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf ; Victor S. Miller, « *Use of elliptic curves in cryptography* », 1985.
(page 113) « premières fonctions de hachage cryptographiques, dont les premiers modèles datent de la fin des années 1970 » : Voir en particulier : Michael O. Rabin, « Digitalized Signatures », *Foundations of Secure Computation*, 1978.
(page 113) « Ralph Merkle a mis au point les arbres de hachage qui permettaient d'authentifier un ensemble volumineux de données » : Ralph C. Merkle, « *Protocols for public key cryptosystems* », in *Proceedings of the 1980 IEEE Symposium on Security and Privacy*, IEEE Computer Society, pp. 122–133, avril 1980 : https://www.ralphmerkle.com/papers/Protocols.pdf.
(page 114) « sa thèse de doctorat » : David L. Chaum, *Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups*, 1982 : https://chaum.com/publications/r

esearch_chaum_2.pdf ; archive : https://web.archive.org/web/20151112100526/https://chaum.com/publications/research_chaum_2.pdf.
(page 115) « publié un article dans la revue *IEEE Computer* en 1986 sur RSA » : Philip R. Zimmermann, « *A Proposed Standard Format for RSA Cryptosystems* », in *IEEE Computer*, 1986.
(page 116) « publication d'empreintes dans les petites annonces du New York Times à partir de 1992 » : https://cypherpunks.venona.com/date/1992/11/msg00019.html.
(page 116) « réseau des réseaux international » : Ronda Hauben, *The Internet: On its International Origins and Collaborative Vision (A Work In Progress)*, 2004 : https://www.ais.org/~jrh/acn/ACn12-2.a03.txt.
(page 118) « Le premier courriel a été envoyé en 1971 » : https://web.archive.org/web/20060506003539/https://openmap.bbn.com/~tomlinso/ray/firstemailframe.html.
(page 118) « Le logiciel LISTSERV est ainsi sorti en 1986 » : L-Soft, *History of LISTSERV* : https://www.lsoft.se/corporate/history-listserv.asp.
(page 118) « [le Web] conçu en 1989 par le chercheur Tim Berners-Lee [...] aidé par l'ingénieur Robert Cailliau pour en définir les spécificités » : Tim Berners-Lee, Robert Cailliau, *WorldWideWeb: Proposal for a HyperText Project*, 12 novembre 1990 : https://cds.cern.ch/record/2639699/files/Proposal_Nov-1990.pdf.
(page 118) « rendu public en août 1991 » : Tim Berners-Lee, *Re: Qualifiers on Hypertext links...*, 06/08/1991 14:56:20 UTC : https://www.w3.org/People/Berners-Lee/1991/08/art-6484.txt.
(page 118) « la Toile » : L'image de la toile d'araignée qui a donné son nom au Web vient des hyperliens qui lient les pages web entre elles.
(page 118) « le concept d'hypertexte avait été inventé par Ted Nelson en 1965, dans le cadre de son projet Xanadu » : Theodor H. Nelson, « *A File Structure for The Complex, The Changing and the Indeterminate* », in *ACM Proceedings of the 20th National Conference*, 1965, pp. 84–100 : https://blogs.baruch.cuny.edu/art3057fall2010/files/2010/08/Nelson-AFileStructureForThe-ComplexTheChangingAndTheIndeterminate.pdf.
(page 119) « ce qui représentait une charge considérable pour l'État » : Marc Rees, *Hadopi : 82 millions d'euros de subventions publiques, 87 000 euros d'amendes*, 3 août 2020 : https://www.nextinpact.com/article/30433/109205-hadopi-82-millions-deuros-subventions-publiques-87000-euros-damendes.
(page 120) « les restrictions liées à ce monopole paraissaient totalement absurdes » : Richard M. Stallman, *The GNU Manifesto*, mars 1985 : https://www.gnu.org/gnu/manifesto.en.html.
(page 120) « 'exemple le plus parlant est celui de Bill Gates et de son entreprise Microsoft » : William Henry Gates III, *An Open Letter to Hobbyists*, 3 février 1976 : https://en.wikisource.org/wiki/Open_Letter_to_Hobbyists.
(page 121) « projet GNU » : GNU est un acronyme récursif signifiant « *GNU's Not Unix* ».
(page 121) « courriel diffusé sur le forum Usenet net.unix-wizards » : Richard M. Stallman, *new UNIX implementation*, 27 septembre 1983 : https://groups.google.com/g/net.unix-wizards/c/8twfRPM79u0/m/1xlglzrWrU0J.
(page 121) « raffiné cette définition pour qu'elle inclue quatre libertés fondamentales » : Richard M. Stallman, *What is Free Software?*, v1.11, 21 décembre 2001 : https://www.gnu.org/philosophy/free-sw.en.html.
(page 121) « licence MIT » : Gordon Haff, *The mysterious history of the MIT License*, 26 avril 2019 : https://opensource.com/article/19/4/history-mit-license.
(page 122) « GPL, qui a été créée par Richard Stallman en février 1989 » : Leonard H. Tower Jr.,

New General Public License, 25 février 1989 : https://groups.google.com/g/gnu.announce/c/m0Jjj_64PeQ/m/8xL1xkVKJb8J?pli=1.

(page 123) « AMIX [...] une place de marché automatisée dédiée à l'information » : John Walker, *Understanding AMIX*, 7 septembre 1989 : https://www.fourmilab.ch/autofile/e5/chapter2_76.html.

(page 123) « le projet Agorics, un modèle d'échange de calcul informatique » : K. Eric Drexler, Mark S. Miller, « *Markets and Computation: Agoric Open Systems* », in *The Ecology of Computation*, 1988 : https://papers.agoric.com/assets/pdf/papers/markets-and-computation-agoric-open-systems.pdf.

(page 123) « Elle faisait notamment intervenir [...] Ralph Merkle » : Ralph C. Merkle, « *Cryonics, Cryptography, and Maximum Likelihood Estimation* », in *Proceedings of the First Extropy Institute Conference on TransHumanist Thought*, 1994 : https://www.ralphmerkle.com/merkleDir/cryptoCryo.html.

(page 124) « L'extropianisme représentait ainsi un transhumanisme » : Max More, *Transhumanism: A Futurist Philosophy* », *Extropy*, vol. 6, 1er juillet 1990 : https://github.com/Extropians/Extropy/blob/master/ext6.pdf.

(page 124) « une volonté de transcender la nature humaine, déjà envisagée auparavant par des personnes comme Julian Huxley, Robert Ettinger et FM-2030 » : Julian Huxley, *Transhumanism* », in *New Bottles for New Wine*, 1957 ; Robert C. W. Ettinger, *Man Into Superman*, 1972 ; FM-2030, *Upwingers Manifesto*, 1973 ; FM-2030, *Are You a Transhuman?*, 1989.

(page 124) « La philosophie extropienne n'était pas seulement descriptive, mais prescriptive » : En anglais, les initiales des quatre premiers principes extropiens (*Boundless Expansion*, *Self-Transformation*, *Dynamic Optimism*, *Intelligent Technology*) formaient l'acronyme « BEST DO IT », c'est-à-dire « le mieux est de le faire », ce qui montrait la dimension proactive de cette philosophie. – Max More, « *The Extropian Principles* », *Extropy*, vol. 6, 1er juillet 1990 : https://github.com/Extropians/Extropy/blob/master/ext6.pdf.

(page 126) « Le mot [...] a quant à lui a été inventé en 1983 par Bruce Bethke » : Bruce Bethke, *Cyberpunk: a short story by Bruce Bethke*, 1997 : http://www.infinityplus.co.uk/stories/cpunk.htm.

(page 126) « a été popularisé par Gardner Dozois » : Gardner Dozois, *Science Fiction in the Eighties*, 30 décembre 1984 : https://www.washingtonpost.com/archive/entertainment/books/1984/12/30/science-fiction-in-the-eighties/526c3a06-f123-4668-9127-33e33f57e313/.

(page 126) « combinant haute technologie et bassesse humaine, pour reprendre l'expression de Bruce Sterling » : Bruce Sterling, « *Preface* », in William Gibson, *Burning Chrome*, Arbor House, 1986.

(page 126) « Cette nouvelle, qui abordait des thèmes propres au genre cyberpunk sans strictement en faire partie » : Vernor Vinge (interrogé par Michael Synergy), « *Hurtling Towards the Singularity* », in *Mondo 2000*, issue 1, 1989 : https://archive.org/details/Mondo.2000.Issue.01.1989/page/n115/mode/2up.

(page 127) « il avait contribué à résoudre le problème des particules alpha dans les circuits intégrés » : Timothy C. May, Murray H. Woods, *Alpha-Particle-Induced Soft Errors in Dynamic Memories*, janvier 1979 : https://gwern.net/doc/cs/hardware/1979-may.pdf.

(page 127) « Ses discussions avec Salin, ainsi qu'avec d'autres personnes comme Marc Stiegler, l'ont poussé à écrire le *Manifeste crypto anarchiste* en août 1988 » : Timothy C. May, *Cyphernomicon*, 16.3.4.

(page 127) « Ce dernier avait travaillé brièvement pour DigiCash à Amsterdam avant de revenir sur la côte Ouest » : Timothy C. May, *Hackers Conference Report*, 11/11/1992 08:55:26 UTC :

https://cypherpunks.venona.com/date/1992/11/msg00019.html.
(page 128) « Judith Milhon, une femme née en 1939 qui avait participé au mouvement des droits civiques » : Sean Dodson, *Judith Milhon: making the Internet a feminist issue*, 8 août 2003 : https://www.theguardian.com/technology/2003/aug/08/guardianobituaries.obituaries.
(page 128) « courriel de bienvenue » : Eric Hughes, *No Subject*, 22 Sep 92 05:43:46 UTC : https://cypherpunks.venona.com/date/1992/09/msg00001.html.
(page 130) « Adam Back l'a ainsi fait imprimer sur des t-shirts qu'il distribuait aux autres et certains ont été jusqu'à se le tatouer sur leur corps » : http://www.cypherspace.org/adam/rsa/.
(page 130) « Phil Zimmermann a publié la version 2.6.2 de PGP dans un livre » : Philip R. Zimmermann, *PGP: Source Code and Internals*, 1995 : https://philzimmermann.com/EN/essays/BookPreface.html.
(page 131) « grâce au soutien de membres du MIT » : Steven Levy, *Cypher Wars*, 1er novembre 1994 : https://www.wired.com/1994/11/cypher-wars/.
(page 131) « Matt Blaze a découvert une vulnérabilité au sein du dispositif d'autorité de séquestre » : John Markoff, *At AT&T, No Joy on Clipper Flaw*, 3 juin 1994 : https://www.nytimes.com/1994/06/03/business/at-at-t-no-joy-on-clipper-flaw.html ; Matt Blaze, *Paper available via ftp*, 05/06/1994 00:01:57 UTC : https://cypherpunks.venona.com/date/1994/06/msg00319.html.
(page 132) « Le premier serveur de ce type a mis en place par Eric Hughes et Hal Finney pour la liste des cypherpunks dès octobre 1992 » : Hal Finney, *New remailer...*, 13/10/1992 20:31:48 UTC : https://cypherpunks.venona.com/date/1992/10/msg00082.html.
(page 132) « Lance Cottrell a amélioré la chose en proposant le modèle Mixmaster » : Lance Cottrell, *1st Draft Mixmaster chaining instructions*, 21/11/1994 01:07:02 UTC : https://cypherpunks.venona.com/date/1994/11/msg00158.html.
(page 132) « Austin et Hamnett Hill qui ont lancé le réseau Freedom en 1999 » : Chris Oakes, *Zero-Knowledge: Nothing Personal*, 9 février 1999 : https://www.wired.com/1999/02/zero-knowledge-nothing-personal/.
(page 132) « le projet Free Haven » : https://www.freehaven.net/.
(page 132) « programme de serveur de courriel anonyme Mixminion » : George Danezis, Roger Dingledine, Nick Mathewson, *Mixminion: Design of a Type III Anonymous Remailer Protocol*, 2003 : https://git.gnunet.org/bibliography.git/plain/docs/minion-design.pdf.
(page 133) « Cryptome, un site web lancé en 1996 par le cypherpunk John Young » : *Cryptome JYA Archive* : https://cryptome.org/jya/.
(page 133) « un livre à ce sujet » : Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn, Jérémie Zimmermann, *Cypherpunks: Freedom and the Future of the Internet*, OR Books, 2012.
(page 134) « l'utilisation de PGP » : Satoshi Nakamoto, *Re: md5?*, 25/07/2010 22:06:57 UTC : https://bitcointalk.org/index.php?topic=458.msg5772#msg5772.

Chapitre 6

(page 136) « CyberCash » : Peter Wayner, *Cybercash's Lesson in Web Survival*, 10 août 1998 : https://www.nytimes.com/1998/08/10/business/cybercash-s-lesson-in-web-survival.html ; archive : https://web.archive.org/web/20150527080844/https://www.nytimes.com/1998/08/10/business/cybercash-s-lesson-in-web-survival.html.
(page 136) « First Virtual » : https://www.nytimes.com/1994/10/15/business/compan

y-news-a-credit-card-for-on-line-sprees.html
(page 136) « NetBill » : Benjamin Cox, J. D. Tygar, Marvin Sirbu, *NetBill Security and Transaction Protocol*, 1995 : https://people.eecs.berkeley.edu/~tygar/papers/Netbill_securiy_and_transaction_protocol.pdf.
(page 136) « MilliCent » : Martín Abadi, Paul Gauthier, Steve Glassman, Mark S. Manasse, Patrick Sobalvarro, *The Millicent Protocol for Electronic Commerce*, 1995 : https://www.w3.org/Conferences/WWW4/Papers/246/.
(page 137) « Habitat, l'un des premiers MMORPG graphiques, développé en 1985 » : Chip Morningstar, F. Randall Farmer, *The Lessons of Lucasfilm's Habitat*, mai 1990 : http://www.fudco.com/chip/lessons.html.
(page 137) « une économie réelle pouvait émerger d'une monnaie virtuelle » : Julian Dibbell, *The Life of the Chinese Gold Farmer*, 17 juin 2007 : https://www.nytimes.com/2007/06/17/magazine/17lootfarmers-t.html.
(page 137) « le Hawthorne Exchange, lancé le 24 mars 1993 sur la liste de diffusion extropienne » : Brian Holt Hawthorne, *HEX: Introducing the Hawthorne Exchange*, 24/03/1993 06:20:21 UTC : https://diyhpl.us/~bryan/irc/extropians/raided-mailing-list-archives/unzipped/disk-07/DIG30152.
(page 138) « ce type de monnaie numérique était quelque chose d'essentiel dans leur combat » : Eric Hughes, *RANTS: A Cypherpunk's Manifesto*, 17/03/1993 19:51:06 UTC : https://cypherpunks.venona.com/date/1993/03/msg00392.html.
(page 138) « décrit initialement par Chaum en 1982 » : David L. Chaum, « *Blind signatures for untraceable payments* », in *Advances in Cryptology: Proceedings of CRYPTO '82*, 1982, pp. 199–203 : https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.
(page 141) «accueillie favorablement sur la liste, notamment par Hal Finney » : Hal Finney, *Re: Magic Money Digicash System*, 04/02/1994 21:58:18 UTC : https://cypherpunks.venona.com/date/1994/02/msg00251.html.
(page 141) « Tacky Tokens, dont les pièces étaient émises en valeurs de 1, 2, 5, 10, 20, 50 et 100 unités » : Mike Duvos, *Fun With Magic Money*, 26/02/1994 00:51:40 UTC : https://cypherpunks.venona.com/date/1994/02/msg01391.html.
(page 141) « L'activité a très rapidement reculé au cours des semaines » : Mike Duvos, *In Search of Genuine DigiCash*, 16/08/1994 06:06:49 UTC : https://cypherpunks.venona.com/date/1994/08/msg00695.html.
(page 141) « Le concept d'eCash a ensuite été mis en pratique par la société DigiCash B.V. » : La chronologie de DigiCash se retrouve sur le site personnel de David Chaum. – David Chaum, *eCash* : https://chaum.com/ecash/.
(page 141) « présenté en mai 1994 lors de la première conférence internationale sur le World Wide Web au CERN » : DigiCash, *World's first electronic cash payment over computer networks*, 27 mai 1994 : https://chaum.com/wp-content/uploads/2022/01/05-27-94-World_s-first-electronic-cash-payment-over-computer-networks.pdf.
(page 142) « le manque d'adoption dû à la difficulté d'utilisation » : Julie Pitta, *Requiem for a Bright Idea*, 1er novembre 1999 : https://www.forbes.com/forbes/1999/1101/6411390a.html.
(page 143) « l'avait approfondie dans les années qui ont suivi » : Nick Szabo, « *Smart Contracts: Building Blocks for Digital Markets* », *Extropy*, vol. 16, 1er janvier 1996 : https://github.com/Extropians/Extropy/blob/master/Extropy-16.pdf ; Nick Szabo, « *Smart Contracts: Formalizing and Securing Relationships on Public Networks* », *First Monday*, vol. 2, no. 9, 1er septembre 1997 : https://firstmonday.org/ojs/index.php/fm/article/view/548/469.

(page 144) « Ayant fui la Chine communiste et émigré aux États-Unis avec sa famille à l'âge de 10 ans » : Wei Dai, *A tale from Communist China*, 18/10/2020 17:37 UTC : https://www.lesswrong.com/posts/osYFcQtxnRKB4F4HA/a-tale-from-communist-china ; Wei Dai, *Re: Tell Your Rationalist Origin Story*, 15/09/2009 02:53 UTC : https://www.lesswrong.com/posts/BHMBBFupzb4s8utts/tell-your-rationalist-origin-story?commentId=ByhZPzBDyYdYs9SRN.
(page 144) « participé à l'élaboration de plusieurs brevets » : Voir les brevets US5724279A et US5724279 assignés à Microsoft. Wei Dai est donc *a priori* son nom civil.
(page 144) « Pipenet, un protocole de communication anonyme » : Wei Dai, *PipeNet description*, 20/01/1998 07:53:25 UTC : https://cypherpunks.venona.com/date/1998/01/msg00878.html ; Wei Dai, *PipeNet 1.1*, 26/11/1998 23:33:49 UTC : http://www.weidai.com/pipenet.txt.
(page 144) « un modèle de crédit anonyme en 1997 » : Wei Dai, *anonymous credit*, 12/04/1997 09:08:04 UTC : https://cypherpunks.venona.com/date/1997/04/msg00398.html.
(page 145) Ronald L. Rivest, Adi Shamir, « *PayWord and MicroMint: Two Simple Micropayment Schemes* », in *Security Protocols Workshop*, 1996 : pp. 69–87 : https://people.csail.mit.edu/rivest/pubs/RS96a.pdf. Voir aussi https://people.csail.mit.edu/rivest/pubs/RS96a.slides.pdf.
(page 145) « Wei Dai a travaillé sur son idée à partir de 1995 » : Wei Dai, *Re: AALWA: Ask any LessWronger anything*, 16/03/2014 06:14 UTC : https://www.lesswrong.com/posts/YdfpDyRpNyypivgdu/aalwa-ask-any-lesswronger-anything?commentId=ZvJDryrskf2Gy6nhG.
(page 145) « Le texte descriptif de b-money a été publié le 26 novembre 1998 par Wei Dai sur sa page personnelle » : Wei Dai, *b-money*, 26/11/1998 23:33:49 UTC, archive : https://web.archive.org/web/19990219124653/http://www.eskimo.com/~weidai/bmoney.txt.
(page 147) « un registre public de titres de propriété » : Nick Szabo, *Secure Property Titles with Owner Authority*, 1998, archive : https://web.archive.org/web/20020202165211/http://szabo.best.vwh.net/securetitle.html.
(page 147) « le *Byzantine Quorum System* de Malkhi et Reiter » : Dahlia Malkhi, Michael Reiter, « *Byzantine quorum systems* », in *Proceedings of the 29th Annual ACM Symposium on Theory of Computing*, 1997.
(page 148) « les morceaux de bit gold [...] devaient donc être évalués sur un marché » : Nick Szabo, *Bit gold markets*, 10 avril 2008 : https://unenumerated.blogspot.com/2008/04/bit-gold-markets.html.
(page 149) « Il s'agissait, en somme, d'une mise en œuvre partielle du bit gold de Nick Szabo » : À propos du bit gold de Nick Szabo, Hal Finney écrivait :

> « Le chercheur en sécurité Nick Szabo a inventé le terme bit gold pour désigner un concept similaire de jetons qui représentent intrinsèquement un certain niveau d'effort. Le concept de Nick est plus complexe que le système simple des RPOW, mais son idée s'applique : à certains égards, un jeton de RPOW peut être considéré comme ayant les propriétés d'une substance rare comme l'or. Miner et frapper des pièces d'or demande un effort et une dépense, ce qui les rend intrinsèquement rares. Les pièces d'or peuvent alors être transmises d'une personne à une autre, et chaque bénéficiaire peut vérifier l'authenticité de la frappe monétaire.
>
> De la même manière, la création de jetons de RPOW demande un certain degré d'effort et de dépense. Ils débutent tous avec une collision hashcash qui, au plus haut degré, prendra des heures voire des jours de calcul pour être créée. Les jetons de RPOW peuvent être validés et vérifiés à la réception en étant échangés contre un nouveau jeton de RPOW

> sur un serveur RPOW. Cela leur permet d'être transmis d'une personne à une autre tout comme des pièces.
>
> Plus important encore, le système RPOW est conçu dans un but primordial : empêcher quiconque, y compris le propriétaire du serveur RPOW et le développeur du logiciel RPOW, de violer les règles du système et de falsifier des jetons de RPOW. Sans cette garantie contre la falsification, les jetons de RPOW ne représenteraient pas de manière crédible le travail effectué pour les créer. Des jetons falsifiables ressembleraient davantage à du papier-monnaie qu'à du bit gold. Mon objectif avec ce projet était de donner vie à une concrétisation simple qui démontre la puissance du concept de bit gold. Pour ce faire, une résistance à la falsification est nécessaire, et c'est cet objectif qui a dominé tous les aspects de la conception. »

Hal Finney, *RPOW Theory*, 15 août 2004 : `http://rpow.net/theory.html` ; archive : `https://web.archive.org/web/20040815154951/http://rpow.net/theory.html`.
(page 149) « Hal Finney l'a annoncé sur la liste des cypherpunks » : Hal Finney, *RPOW - Reusable Proofs of Work*, 15/08/2004 17:43:09 UTC : `https://lists.cpunks.org/pipermail/cypherpunks-legacy/2004-August/134945.html`.
(page 149) « l'annonce a été retransmise sur la liste de Metzdowd.com par Robert Hettinga » : Robert Hettinga, *FW: RPOW - Reusable Proofs of Work*, 15/08/2004 18:36:51 UTC : `https://www.metzdowd.com/pipermail/cryptography/2004-August/007362.html`.
(page 150) « comptait notamment multiplier le nombre de serveurs autour du monde » : Hal Finney, *World of RPOW*, 15 août 2004 : `http://rpow.net/world.html` ; archive : `https://web.archive.org/web/20040816004128/http://rpow.net/world.html`.
(page 150) « Fugger lui-même avait participé à un tel système à Vancouver » : Bailey Reutzel, *Disruptor Chris Larsen Returns with a Bitcoin-Like Payment System*, 7 décembre 2012 : `https://www.americanbanker.com/news/disruptor-chris-larsen-returns-with-a-bitcoin-like-payment-system` ; archive : `https://web.archive.org/web/20140323151243/http://www.paymentssource.com/news/disruptor-chris-larsen-returns-with-bitcoin-like-payments-system-3012580-1.html?zkPrintable=1&nopagination=1`.
(page 151) « une preuve de concept appelée Ripplepay » : `https://web.archive.org/web/20070702210719/http://ripplepay.com/`.
(page 151) « Ryan Fugger a également créé un Google Group en janvier 2007 » : Ryan Fugger, *Welcome...*, 14/01/2007 23:47:26 UTC : `https://groups.google.com/g/rippleusers/c/oRDaKz-qPjQ/m/zHV3hMPwMg0J`.
(page 151) « Ryan Fugger a laissé les rênes de son projet entre les mains des dirigeants de l'entreprise OpenCoin Inc., Chris Larsen et Jed McCaleb, en novembre 2012 » : Ryan Fugger, *Ripple.com and taking the project to the next level*, 28/11/2012 21:21:12 UTC : `https://groups.google.com/g/rippleusers/c/IVin3Qwrp7k/m/urzaH_VrQcQJ`.
(page 151) « Ryan Fugger a finalement modifié le nom de sa preuve de concept en Rumplepay en 2020 pour éviter la confusion » : Ryan Fugger, *New Name*, 26 août 2020 : `https://rumplepay.com/`.
(page 153) « La référence à bit gold a fini par être ajoutée sur la page web de Bitcoin.org au début de l'année 2009 » : `https://web.archive.org/web/20090303195936/http://bitcoin.org/`.
(page 154) « Nick Szabo courant 2009 » : Nick Szabo, *Liar-resistant government*, 07/05/2009 23:13 UTC : `https://unenumerated.blogspot.com/2009/05/liar-resistant-government.html`.
(page 154) « ils ont tous les trois démenti la chose » : Wei Dai : « Ce que je comprends c'est

que le créateur de Bitcoin, qui se fait appeler Satoshi Nakamoto, n'a même pas lu mon article avant de réinventer l'idée lui-même. Il l'a appris par la suite et m'a crédité dans son papier. Donc ma connexion avec le projet est assez limitée. » – Wei Dai, *Re: Making money with Bitcoin?*, 25/02/2011 15:27 UTC : https://www.lesswrong.com/posts/ijr8rsyvJci2edxot/making-money-with-bitcoin?commentId=hbEu9ue9eymNzaF2J.

Nick Szabo : « Comme je l'ai déclaré à plusieurs reprises auparavant, toute cette spéculation est flatteuse, mais incorrecte – je ne suis pas Satoshi. » – Nathaniel Popper, *Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin*, 15 mai 2015.

Hal Finney : « Aujourd'hui, la véritable identité de Satoshi est devenue un mystère. Mais à l'époque, je pensais avoir affaire à un jeune homme d'origine japonaise, très intelligent et sincère. » – Hal Finney, *Bitcoin and me*, 19/03/2013 20:40:02 UTC : https://bitcointalk.org/index.php?topic=155054.msg1643833#msg1643833.

(page 154) « il répondait à Martien van Steenbergen qui y faisait référence » : Martien van Steenbergen faisait aussi référence à d'autres projets issus de la communauté P2P : Pekunio et Wizard Rabbit Treasurer. – Martien van Steenbergen, *[p2p-research] Re: Bitcoin open source implementation of P2P currency*, 12/02/2009 20:01:03 UTC : https://diyhpl.us/~bryan/irc/bitcoin-satoshi/p2presearch-again/p2pfoundation.net/backups/p2p_research-archives/2009-February.txt.gz.

(page 154) « il avait été l'une des premières personnes à intervenir sur le Google Group nouvellement créé » : Mike Hearn, *Hello from a Ripple fan*, 06/05/2007 12:20:53 UTC : https://groups.google.com/g/rippleusers/c/i8OyR5yLC0Q/m/SyztfhBGYJEJ.

Chapitre 7

(page 160) « de détecter la présence d'erreurs de frappe mais aussi de les localiser » : Samuel Dobson, *(Some of) the math behind Bech32 addresses*, 2 septembre 2019 : https://medium.com/@meshcollider/some-of-the-math-behind-bech32-addresses-cf03c7496285.

(page 160) « Dans Electrum par exemple, les clés privées sont chiffrées par le biais de l'algorithme symétrique AES-256-CBC » : Electrum Documentation, *Frequently Asked Questions*, 3 octobre 2021 : https://electrum.readthedocs.io/en/latest/faq.html#how-is-the-wallet-encrypted.

(page 166) « Il est supposé que ce doublement mis en place par Satoshi avait pour rôle la protection contre les attaques par extension de longueur » : https://bitcoin.stackexchange.com/questions/6037/why-are-hashes-in-the-bitcoin-protocol-typically-computed-twice-double-computed/6042#6042.

(page 167) « la perte d'au moins 55,82 bitcoins » : Burt Wagner, *Bad signatures leading to 55.82152538 BTC theft (so far)*, 10/08/2013, 22:53:13 UTC :https://bitcointalk.org/index.php?topic=271486.msg2907468#msg2907468.

(page 174) « l'infrastructure matérielle des portefeuilles Trezor » : *Hardware design of Trezor* :https://github.com/trezor/trezor-hardware.

(page 174) « Le concept a été développé pour Bitcoin à partir de 2011 » : Gregory Maxwell, *Deterministic wallets*, 18/06/2011 21:27:29 : https://bitcointalk.org/index.php?topic=19137.msg239768#msg239768.

(page 174) « Il a été élargi aux autres cryptomonnaies en 2014 » : *SLIP-0044 : Registered coin types for BIP-0044* : https://github.com/satoshilabs/slips/blob/master/slip-0044.md.

(page 181) « la plateforme Mt. Gox qui a connu de multiples piratages entre 2011 et 2013 ayant mené à la volatilisation de 650 000 bitcoins, et qui a fait faillite en 2014 » : Ludovic Lars, *Mt. Gox et ses 842 109 bitcoins disparus, la lente descente aux enfers d'un géant du bitcoin*, 24 décembre 2020 :https://journalducoin.com/analyses/mt-gox-lente-descente-enfers/.

(page 184) « les propriétaires sont attaqués physiquement pour être extorqués » : Jameson Lopp maintient un registre (non exhaustif) des attaques physiques connues contre les propriétaires de bitcoins, où ceux-ci subissent des menaces de violences voire de torture afin de transférer des fonds : *Known Physical Bitcoin Attacks*, https://github.com/jlopp/physical-bitcoin-attacks/blob/master/README.md.
(page 184) « La famille de Hal Finney a ainsi été ciblée par un maître-chanteur » : Robert McMillan, *An Extortionist Has Been Making Life Hell for Bitcoin's Earliest Adopters*, 29 décembre 2014 : https://www.wired.com/2014/12/finney-swat/.
(page 184) « C'est une fonctionnalité que Ledger intègre dans ses produits » : Ledger Documentation, *Comment configurer une passphrase ?* : https://support.ledger.com/hc/fr-fr/articles/115005214529-Comment-configurer-une-passphrase-?.
(page 185) « graver ses mots sur une plaque d'acier forgée à cet effet » : Jameson Lopp, *Metal Bitcoin Seed Storage Reviews* : https://jlopp.github.io/metal-bitcoin-storage-reviews/.

Chapitre 8

(page 191) « l'algorithme de consensus PBFT [...] mis au point par Miguel Castro et Barbara Liskov en 1999 » : Miguel Castro, Barbara Liskov, *Practical Byzantine Fault Tolerance*, février 1999.
(page 193) « attaque Sybil » : Voir John R. Douceur, « *The Sybil Attack* », in *Peer-to-Peer Systems*, 2002, pp. 251–260. La pratique a été décrite en 1993 par le cypherpunk L. Detweiler sous le nom de *pseudospoofing* : https://cypherpunks.venona.com/date/1993/10/msg00760.html.
(page 196) « décrite en 1991 par Stuart Haber et Scott Stornetta dans le cas particulier de l'horodatage de documents » : Stuart Haber, Wakefield Scott Stornetta, « *How to time-stamp a digital document* », *Journal of Cryptology*, 1991 : http://www.staroceans.org/e-book/Haber_Stornetta.pdf.
(page 196) « Haber et Stornetta, qui avaient publié chaque semaine une empreinte cryptographique dans les petites annonces du *New York Times* » : Daniel Oberhaus, *The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995*, 27 août 2018 : https://www.vice.com/en/article/j5nzx4/what-was-the-first-blockchain.
(page 201) « ne doit pas dépasser l'horloge des nœuds récepteurs de deux heures » : https://github.com/bitcoin/bitcoin/blob/24.x/src/validation.cpp#L3483-L3490.
(page 204) « la fonction CalculateNextWorkRequired dans le fichier pow.cpp » : https://github.com/bitcoin/bitcoin/blob/24.x/src/pow.cpp#L49-L72.
(page 205) « Elle est bien évidemment inscrite dans le code » : https://github.com/bitcoin/bitcoin/blob/24.x/src/validation.cpp#L1473-L1484
(page 207) « la chaîne possédant le plus de travail accumulé » : Ce principe a été redéfini le 25 juillet 2010 au sein de la version 0.3.3 du logiciel : https://github.com/bitcoin/bitcoin/commit/3b7cd5d89a226426df9c723d1f9ddfe08b7d1def.
(page 209) « Le délai sur le réseau BTC est aujourd'hui de 101 confirmations » : https://github.com/bitcoin/bitcoin/blob/23.x/src/consensus/consensus.h#L18-L19
(page 213) « Ethereum Classic qui a subi plusieurs recoordinations agressives entre 2019 et 2020 » : Plus précisément : le 7 janvier 2019, le 31 juillet 2020, le 6 août 2020 et le 29 août 2020.
(page 214) « En 2011, est apparu le premier circuit logique programmable FPGA consacré au minage » : fpgaminer, *Official Open Source FPGA Bitcoin Miner (Spartan-6 Now Tops Performance per $!)*, 20/05/2011 02:33:56 UTC : https://bitcointalk.org/index.php?topic=9047.msg130885#msg130885.
(page 214) « la sortie de l'Avalon ASIC » : ngzhang, *"Avalon" ASIC, announcement & pre-order*,

17/09/2012 07:48:26 UTC : https://bitcointalk.org/index.php?topic=110090.msg1197494#msg1197494.
(page 216) « Le premier relai [...] a été lancé en 2013 » : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-November/003596.html.
(page 216) « [il] est devenu pleinement fonctionnel en 2015 » : https://web.archive.org/web/20150628233706/https://bitcoinrelaynetwork.org/.
(page 216) « Un concurrent était le réseau Falcon » : https://web.archive.org/web/20160609081540/https://www.falcon-net.org/
(page 217) « P2Pool qui est un protocole de minage coopératif basé sur un réseau pair à pair de mineurs » : http://p2pool.in/.
(page 217) « le procédé est mis en œuvre sur Monero » : https://p2pool.io/.

Chapitre 9

(page 221) « C'est aussi le sens que lui donne l'*Electronic Frontier Foundation* » : Electronic Frontier Foundation, *Financial Censorship* : https://www.eff.org/issues/financial-censorship.
(page 222) « la bancarisation de la société, qui a eu lieu à partir des années 1960 en Occident » : https://books.openedition.org/pur/121053?lang=fr ; https://www.the-american-interest.com/2019/02/25/bigger-fewer-riskier-the-evolution-of-u-s-banking-since-1950/.
(page 223) « la première directive de l'Union Européenne relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux » : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31991L0308&from=FR.
(page 223) « le secret bancaire [...] a fini par disparaître » : Anthony Amicelle, Jean Bérard, *Vers la fin du secret bancaire ou de la vie privée ?*, 2019 : https://journals.openedition.org/conflits/21291.
(page 223) « y compris en Suisse » : Mathilde Damgé, *Comment la Suisse a renoncé au secret bancaire*, 11 février 2015 : https://www.lemonde.fr/evasion-fiscale/article/2015/02/11/comment-la-suisse-a-renonce-au-secret-bancaire_4572485_4862750.html.
(page 224) « le blocus financier avait fait disparaître 95 % de ses revenus » : WikiLeaks, *Banking Blockade*, 24/10/2011 13:00 UTC, https://wikileaks.org/Banking-Blockade.html.
(page 224) « opération Choke Point mise en place entre 2013 et 2017 par le département de la Justice des États-Unis » : https://en.wikipedia.org/wiki/Operation_Choke_Point ; https://www.wsj.com/articles/SB10001424127887323838204578654411043000772, archive : https://archive.is/bF8KZ.
(page 224) « en subissant une fermeture de ses comptes par Chase, PayPal et Strip » : Kelsey Bolar, *Firearms Sellers Say They're Being Choked Off From Payment Processors*, 12 janvier 2015 : https://www.dailysignal.com/2015/01/12/firearms-sellers-say-theyre-choked-off-payment-processors/.
(page 225) « Alex Jones [...] a vu son compte PayPal être clôturé » : Brian Fung, *PayPal bans Alex Jones, saying Infowars 'promoted hate or discriminatory intolerance'*, 21 septembre 2018 : https://www.washingtonpost.com/technology/2018/09/21/paypal-bans-alex-jones-saying-infowars-promoted-hate-or-discriminatory-intolerance/
(page 225) « chassé de PayPal, Stripe Cash App et Coinbase » : https://www.bitcoininsider.org/article/44690/after-coinbase-paypal-bans-social-media-platform-gab-just-because.
(page 225) « banni de PayPal pour avoir fait un salut nazi » : https://www.timesofisrael.

com/paypal-suspends-milo-yiannopoulos-over-nazi-based-trolling-of-jewish-journalist/.
(page 225) « chassé de Patreon suite à la pression de Mastercard » : https://twitter.com/Patreon/status/1029551216886341634.
(page 225) « L'association a également vu plusieurs de ses comptes bancaires (Banque postale, BNP Paribas, Banque populaire) être fermés » : Égalité et Réconciliation, *Soutenez-nous : la Banque populaire ferme le compte en banque d'Égalité & Réconciliation*, 6 février 2022 : https://www.egaliteetreconciliation.fr/Soutenez-nous-la-Banque-populaire-ferme-le-compte-en-banque-d-Egalite-Reconciliation-67155.html.
(page 225) « elle a gelé le compte du démocrate Ted Hui en décembre 2020 » : https://hongkongfp.com/2020/12/07/hsbc-re-freezes-accounts-belonging-to-family-of-exiled-democrat-ted-hui-amid-hong-kong-police-money-laundering-probe/.
(page 225) « elle refusait aux Hongkongais ayant fui au Royaume-Uni d'accéder légitimement à leurs fonds de pension, pour un montant s'élevant à 2,2 milliards de livres sterling » : https://www.lefigaro.fr/flash-eco/hsbc-complice-de-violation-des-droits-humains-a-hong-kong-selon-un-rapport-parlementaire-20230208, https://www.telegraph.co.uk/business/2023/08/07/hsbc-exececutive-apologises-calling-uk-weak-on-china/.
(page 225) « Viruswaarheid [...] a ainsi vu son compte bancaire utilisé pour recevoir des donations être fermé par ING Bank en février 2021 » : Andreas Kouwenhoven et Wilmer Heck, *De complotdenker bankiert maar elders, zegt de bank*, 17 août 2021 : https://www.nrc.nl/nieuws/2021/08/17/de-complotdenker-bankiert-maar-elders-zegt-de-bank-a4055125 ; archive : https://archive.is/8LI0k.
(page 226) « celle de GoFundMe, ayant réuni 10 millions de dollars canadiens, a été retirée le 4 février » : Radio-Canada, *La campagne de sociofinancement du convoi des camionneurs retirée de GoFundMe*, 4 février 2022 : https://ici.radio-canada.ca/nouvelle/1859918/retrait-campagne-gofundme-convoi-camionneurs-2022.
(page 226) « les fonds récupérés par les campagnes organisées sur la plateforme chrétienne GiveSendGo [...] ont été gelés par le gouvernement ontarien » : Stephanie Taylor, *Ontario court freezes access to donations for truckers' protest from GiveSendGo*, 10 février 2022 : https://www.ctvnews.ca/canada/ontario-court-freezes-access-to-donations-for-truckers-protest-from-givesendgo-1.5776674.
(page 226) « 280 comptes contenant 8 millions de dollars au total ont été gelés de le sorte » : Bill Curry, Marsha McLeod, *Deputy Minister of Finance describes race against time to prevent economic damage from border blockades*, 17 novembre 2022 : https://www.theglobeandmail.com/politics/article-emergencies-act-inquiry-michael-sabia/.
(page 226) Les sanctions économiques internationales qui concernent le domaine financier rentrent dans la catégorie de la censure financière. Celles-ci ont en effet pour but premier d'empêcher le commerce avec la population gouvernée par un État ennemi. Le cas des Russes n'est pas un cas isolé, et de nombreuses autres populations n'ont pas accès aux services financiers disponibles pour les Occidentaux, comme les Palestiniens par exemple. Voir à ce sujet Electronic Frontier Foundation, *Why Is PayPal Denying Service to Palestinians?*, 12 octobre 2021 : https://www.eff.org/deeplinks/2021/10/why-paypal-denying-service-palestinians.
(page 226) Ben Canton, *Un an de guerre en Ukraine : la petite histoire de Valériia et de Binance*, 24 février 2023 : https://journalducoin.com/analyses/un-an-guerre-ukraine-petite-histoire-valeriia-binance/.
(page 226) « RT France [...] a ainsi subi le gel de ses avoirs » : Le Parisien, *RT France, branche française de la chaîne russe, annonce sa fermeture*, 23 janvier 2022 : https://www.leparisi

en.fr/international/rt-france-branche-francaise-de-la-chaine-russe-annonce-sa-fermeture-21-01-2023-YMOTSTASWZAF3KSGCYHAFFMG6U.php.

(page 227) « L'achat de cryptomonnaies est entravé par les banques qui interdisent régulièrement à leurs clients [...] d'envoyer des fonds vers les plateformes de change » : Jean-Luc (Bitcoin.fr), *Les banques et Bitcoin — Classement de janvier 2023*, 9 janvier 2023 : https://bitcoin.fr/bitcoin-et-les-banques-classement-de-janvier-2023/.

(page 227) « C'est le cas de l'auteur de cet ouvrage » : Ludovic Lars sur Twitter, 15/02/2022 10:42 UTC : https://twitter.com/lugaxker/status/1493536121678147586.

(page 228) « un système panoptique, où la surveillance se ferait à l'insu du surveillé » : Le panoptique (en anglais, *panopticon*) était un type d'architecture carcérale imaginée par le philosophe utilitariste Jeremy Bentham et son frère Samuel à la fin du XVIII^e siècle. L'objectif de la structure panoptique était de permettre à un gardien, logé dans une tour centrale, d'observer tous les prisonniers, enfermés dans des cellules individuelles autour de la tour, sans que ceux-ci puissent savoir s'ils étaient observés.

(page 228) « C'est le cas de la Suède [...] où l'État fait tout pour mettre à disposition des moyens de paiement numérique innovants » : sweden.se, *A cashless society* : https://sweden.se/life/society/a-cashless-society.

(page 228) « Narendra Modi a ainsi démonétisé les billets de 500 et 1000 roupies » : Ninon Renaud, Michel De Grandi, *En Inde, la démonétisation des grosses coupures provoque l'émoi*, 13 novembre 2016 : https://www.lesechos.fr/2016/11/en-inde-la-demonetisation-des-grosses-coupures-provoque-lemoi-216048.

(page 228) « la limitation des retraits et la démonétisation des grosses coupures » : Simi Jolaoso, *Nigeria's naira shortage: Anger and chaos outside banks*, 14 février 2023 : https://www.bbc.com/news/world-africa-64626127.

(page 230) « où il n'y aurait plus besoin de lois formelles » : George Orwell, *1984*, 1949 : « Ce qu'il allait commencer, c'était son journal. Ce n'était pas illégal (rien n'était illégal, puisqu'il n'y avait plus de lois), mais s'il était découvert, il serait, sans aucun doute, puni de mort ou de vingt-cinq ans au moins de travaux forcés dans un camp. »

(page 231) « la liste dressée par l'*Office of Foreign Assets Control* » : U.S. Department of the Treasury, *Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity*, 14 septembre 2022 : https://home.treasury.gov/news/press-releases/jy0948 ; https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220914.

(page 231) « les processeurs de paiement » : Depuis le début de l'année 2021, BitPay demande par exemple à ses clients européens de s'inscrire et de vérifier leur identité avant de pouvoir effectuer un achat.

(page 232) « en refusant des bitcoins provenant de mélanges de pièces et geler les comptes des personnes le faisant » : Jamie Redman, *As FATF Regulations Galvanize, Crypto Mixing Applications Are Targeted*, 27 décembre 2019 : https://news.bitcoin.com/as-fatf-regulations-galvanize-crypto-mixing-applications-are-targeted/ ; 6102bitcoin, *CoinJoin Flagging* : https://6102bitcoin.com/coinjoin-flagging/.

(page 236) « lorsque les frais médians par transaction ont dépassé les 30 $ » : https://bitinfocharts.com/comparison/bitcoin-median_transaction_fee.html#alltime.

(page 237) « l'activation de l'EIP-1559 en août 2021 » : Ludovic Lars, *Ethereum face à une catastrophe annoncée ? Censure et volatilité : l'EIP-1559, le cauchemar des mineurs*, 15 juillet 2021 : https://journalducoin.com/analyses/eip-1559-changement-nefaste-ethereum/.

(page 239) « l'apparition d'une version modifiée de la "règle du voyage", recommandée par le

GAFI et déjà imposée par la FINMA suisse » : https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf – Recommandation 16 du GAFI, mise à jour en juin 2019 pour inclure le transferts d'actifs virtuels : https://www.fatf-gafi.org/fr/publications/Recommandationsgafi/Recommandations-gafi.html. – https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/ – https://aopp.group/.
(page 239) « consensus social » : Arthur Breitman parlait de *social consensus* dès août 2014 dans la première description formelle de Tezos. – Arthur Breitman, *Tezos: A Self-Amending Crypto-Ledger*, 3 août 2014 : https://tezos.com/position-paper.pdf.
(page 240) « invalidation directe » : Cette méthode peut par exemple être mise en place dans l'esprit de l'*User Resisted Soft Fork* proposé par Michael Folkson en avril 2022 en réaction à la menace d'activation de la mise à niveau OP_CHECKTEMPLATEVERIFY. – Michael Folkson, *[bitcoin-dev] User Resisted Soft Fork for CTV*, 21/04/2022 16:45:20 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2022-April/020262.html.
(page 240) « implémenté dans le logiciel de Bitcoin dès juillet 2010 » : Satoshi Nakamoto, *Bitcoin 0.3.2 released*, 17/07/2010 21:35:51 UTC : https://bitcointalk.org/index.php?topic=437.msg3807#msg3807.
(page 240) « certains de ces points de contrôle sont encore présents dans Bitcoin Core » : https://github.com/bitcoin/bitcoin/blob/24.x/src/chainparams.cpp#L148-L164.
(page 241) « soutenue par les développeurs luke-jr et Gregory Maxwell » : https://www.reddit.com/r/Bitcoin/comments/3fg0jw/could_a_cartel_of_pool_operators_collude_to/ctoat0d/ ;https://www.reddit.com/r/bitcoinxt/comments/41pbmf/maxwell_considers_changing_the_pow_algorithm_in/.
(page 242) « le minage combiné » : Aljosha Judmayer, Alexei Zamyatin, Nicholas Stifter, Artemios G. Voyiatzis, Edgar Weippl, *Merged Mining: Curse of Cure?*, 22 août 2017 : https://eprint.iacr.org/2017/791.
(page 244) « la preuve d'espace » : Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, Krzysztof Pietrzak, *Proofs of Space*, 2013 : https://eprint.iacr.org/2013/796.
(page 244) « intégrée au sein de Tenebrix en septembre 2011 » : Lolcust, *[ANNOUNCE] Tenebrix, a CPU-friendly, GPU-hostile cryptocurrency*, 26/09/2011 00:09:44 UTC : https://bitcointalk.org/index.php?topic=45667.msg544675#msg544675.
(page 244) « héritée plus tard par Litecoin » : Charlie Lee, *Re: [ANN] Litecoin - a lite version of Bitcoin. Be ready when is launches!*, 09/10/2011 06:14:28 UTC : https://bitcointalk.org/index.php?topic=47417.msg564414#msg564414.
(page 244) « ETHash » : https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/mining-algorithms/ethash/.
(page 244) « GHOST » : *Ethereum Whitepaper*, consulté le 11 mars 2023 : https://ethereum.org/en/whitepaper/#modified-ghost-implementation.
(page 244) « ETCHash » : https://github.com/eth-classic/etchash/blob/main/README.md.
(page 244) « RandomX » : https://github.com/tevador/RandomX.
(page 244) « Chia Network » : Ludovic Lars, *Face à la preuve de travail de Bitcoin, la preuve d'espace, une fausse solution écologique*, 19 mai 2021 : https://journalducoin.com/analyses/preuve-espace-fausse-solution-ecologique/.
(page 245) « protection contre la recoordination profonde » : Bitcoin ABC, *Bitcoin ABC 0.18.5 Released*, 20 novembre 2018 : https://www.bitcoinabc.org/2018-11-20-bitcoin-abc-0-18-5/.
(page 245) « MESS » : Dean Pappas, *An Elegant MESS – The Fast Solution to 51% attacks and Low Hash Rate*, 18 septembre 2020 : https://medium.com/ethereum-classic-labs/an-elega

nt-mess-the-fast-solution-to-51-attacks-and-low-hash-rate-4e8f8347bdfe.
(page 246) « slashing » : Vitalik Buterin, *Slasher: A Punitive Proof-of-Stake Algorithm*, 15 janvier 2014 : https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm.
(page 247) « par le biais de leur protocole PPCoin » : Sunny King, Scott Nadal, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, 19 août 2012, archive : https://web.archive.org/web/20121021014644/http://www.ppcoin.org/static/ppcoin-paper.pdf.
(page 247) « preuve d'enjeu déléguée » : Dan Larimer, *DPOS Consensus Algorithm - The Missing White Paper*, 29 mai 2017 : https://hive.blog/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper.
(page 247) « preuve d'enjeu liquide » : Jacob Arluck, *Liquid Proof-of-Stake*, 30 juillet 2018 : https://medium.com/tezos/liquid-proof-of-stake-aec2f7ef1da7.
(page 247) « le coût d'une attaque est un ordre de grandeur plus élevé » : https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/pos-vs-pow/#security.
(page 248) « une scission entre le protocole Steem contrôlé par la Fondation Tron et la plateforme Hive » : Tim Copeland, *Steem vs Tron: The rebellion against a cryptocurrency empire*, 18 août 2020 : https://decrypt.co/38050/steem-steemit-tron-justin-sun-cryptocurrency-war.
(page 249) « proposition de l'abandon de la preuve de travail, telle que celle faite par Greenpeace en 2022 » : Tyler Kruse, *Change The Code: Not The Climate — Greenpeace USA, EWG, Others Launch Campaign to Push Bitcoin to Reduce Climate Pollution*, 29 mars 2022 : https://www.greenpeace.org/usa/news/change-the-code-not-the-climate-greenpeace-usa-ewg-others-launch-campaign-to-push-bitcoin-to-reduce-climate-pollution/.

Chapitre 10

(page 252) « la syntaxe des messages de transmission de données » : Bitcoin Wiki, *Protocol documentation: Common structures* : https://en.bitcoin.it/wiki/Protocol_documentation#Common_structures.
(page 254) « l'implémentation principale utilisée par plus de 99 % des nœuds en novembre 2023 » : https://coin.dance/nodes.
(page 254) « une diversité d'implémentations » : https://clientdiversity.org/#distribution.
(page 254) « Les distributions Linux sont ainsi formées de distributions antérieures » : Andreas Lundqvist, Donjan Rodic, Mohammed A. Mustafa, Muhammad Herdiansyah, Fabio Loli, *Linux Distribution Timeline*, 27 février 2021 : https://commons.wikimedia.org/wiki/File:Linux_Distribution_Timeline_27_02_21.svg.
(page 254) « le logiciel a été renommé en bitcoind / Bitcoin-Qt en 2011 » : Gavin Andresen, *Bitcoin-Qt/bitcoind version 0.5.0*, 21/11/2011 17:17:04 UTC : https://bitcointalk.org/index.php?topic=52480.msg626275#msg626275.
(page 254) « en Bitcoin Core le 19 mars 2014 » : Bitcoin Core, *Bitcoin Core version 0.9.0 released*, 19 mars 2014 : https://bitcoin.org/en/release/v0.9.0#rebranding-to-bitcoin-core.
(page 255) « la liste de diffusion bitcoin-dev » : The bitcoin-dev Archives : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/.
(page 255) « Ryan Ofsky » : https://github.com/bitcoin/bitcoin/commit/59ebee3fb4181baf20fab263cf1b587ece1bd5e2.
(page 255) « la voie de mainteneurs emblématiques » : Andrew Chow, *List of people who have had commit access to Bitcoin Core*, 07/07/2022 20:05:39 UTC : https://bitcointalk.org/

index.php?topic=1774750.msg17700787#msg17700787.
(page 256) « hébergé sur un dépôt GitHub géré par Bitcoin Core » : https://github.com/bitcoin/bips
(page 257) « SLIP-44 » : https://github.com/satoshilabs/slips/blob/master/slip-0044.md
(page 257) « les CHIP » : https://bch.info/en/chips.
(page 257) « les LIP » : https://github.com/litecoin-project/lips.
(page 259) « prévoyaient de doubler la taille limite des blocs sans protection contre la rediffusion afin que les portefeuilles à vérification de paiement simplifiée suivent simplement la chaîne la plus longue » : Mike Belshe, *[Bitcoin-segwit2x] Strong 2-Way Replay Protection*, 08/10/2017 20:16:02 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-October/000323.html « Aujourd'hui, nous sommes en bonne voie pour déployer segwit2x avec une grande majorité de mineurs qui le signalent encore. En plus de cela, 99,94 % des nœuds et des clients SPV suivront automatiquement la chaîne la plus longue (segwit2x). »
(page 259) « Satoshi pensait que le système pourrait perdurer avec une vérification centralisée entre les mains de quelques nœuds vérificateurs » : Satoshi Nakamoto a conservé cette vision jusqu'à son départ, comme en témoigne son courriel à Mike Hearn du 29 décembre 2010 :

> « Un jour, lorsque nous aurons des implémentations fonctionnant uniquement en mode client, la taille de la chaîne de blocs n'aura plus beaucoup d'importance. D'ici là, tant que tous les utilisateurs ont toujours à télécharger la chaîne de blocs entière pour commencer, il est bon de pouvoir la maintenir à une taille raisonnable. »

Satoshi Nakamoto, *Re: More BitCoin questions*, 29/12/2010 21:42 UTC : https://plan99.net/~mike/satoshi-emails/thread3.html.
(page 260) « pas ton nœud, pas tes règles » : L'adage « *not your node, not your rules* » a été naturellement calqué sur l'adage « *not your keys, not your coins* » (voir par exemple ce tweet de Udi Wertheimer : https://twitter.com/udiWertheimer/status/936215582487261184). Il a été popularisé par le panel du même nom lors de la conférence Understanding Bitcoin, le 5 avril 2019. Le projet RaspiBlitz en a fait son slogan en 2020 : https://github.com/rootzoll/raspiblitz/blob/bbeb5b21a982eeeb93306537e0aca2474bd23e03/README.md.
(page 264) « celui qui a eu lieu sur Ethereum en juillet 2016 » : Simon Polrot, *The DAO : post mortem*, 24 janvier 2017 : https://www.ethereum-france.com/the-dao-post-mortem/ ; Casey Detrio, *EIP-779: Hardfork Meta: DAO Fork*, 26 novembre 2017 : https://eips.ethereum.org/EIPS/eip-779.
(page 264) « celui qui a mené à la création de Bitcoin Cash en août 2017 » : Ludovic Lars, *Bitcoin Cash : la branche minoritaire issue du débat sur la scalabilité*, 30 janvier 2022 : https://journalducoin.com/analyses/bitcoin-cash-branche-minoritaire-debat-scalabilite/ ; *BCH-UAHF: Bitcoin Cash User-Activated Hard Fork*, 24 juillet 2017 : https://reference.cash/protocol/forks/bch-uahf.
(page 266) « la version 0.3.6 du logiciel [...] publiée le 29 juillet » : Satoshi Nakamoto, *** *ALERT* *** *Upgrade to 0.3.6*, 29/07/2010 19:13:06 UTC : https://bitcointalk.org/index.php?topic=626.msg6451#msg6451.
(page 267) « Les développeurs de Bitcoin SV ont ainsi désactivé P2SH en février 2020 » : Jon Southurst, *Final Genesis specs released—bye P2SH*, 10 janvier 2020 : https://coingeek.com/final-genesis-specs-released-bye-p2sh/.
(page 267) « bloc auxiliaire » : https://bitcointalk.org/index.php?topic=283746.msg3036293#msg3036293.
(page 267) « bloc d'extension » : https://lists.linuxfoundation.org/pipermail/bi

tcoin-dev/2015-May/008356.html.
(page 267) « soft fork généralisé » : ZoomT, *Increasing the blocksize as a (generalized) softfork.*, 20/12/2015 11:12:48 UTC : https://bitcointalk.org/index.php?topic=1296628.msg13305141#msg13305141.
(page 267) « dette technique » : Ward Cunningham, « The WyCash Portfolio Management System », *Addendum to the Proceedings of OOPSLA 1992*, octobre 1992 : https://dl.acm.org/doi/pdf/10.1145/157710.157715.
(page 267) « avant que le développeur luke-jr ne décrive en 2015 comment en faire un soft fork » : Aaron van Wirdum, *The Long Road to SegWit: How Bitcoin's Biggest Protocol Upgrade Became Reality*, 23 août 2017 : https://bitcoinmagazine.com/technical/the-long-road-to-segwit-how-bitcoins-biggest-protocol-upgrade-became-reality.

Chapitre 11

(page 272) « établie par Satoshi Nakamoto lors du lancement du prototype le 8 janvier 2009 » : Satoshi Nakamoto, *Bitcoin v0.1 released*, 08/01/2009 19:27:40 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html.
(page 272) « l'exigence d'unanimité communautaire » : River Financial, *Can Bitcoin's Hard Cap of 21 Million Be Changed?* : https://river.com/learn/can-bitcoins-hard-cap-of-21-million-be-changed.
(page 272) « le caractère juridique du décret de Satoshi » : https://craigwright.net/blog/law-regulation/forking-and-passing-off/.
(page 276) « TCP/IP a prévalu sur le modèle concurrent de l'époque, le modèle OSI » : Andrew L. Russell, « *"Rough Consensus and Running Code" and the Internet-OSI Standards War* », in *IEEE Annals of the History of Computing*, vol. 28, no. 3, juillet-septembre 2006, pp. 48–61 : https://courses.cs.duke.edu/common/compsci092/papers/govern/consensus.pdf.
(page 279) « modèle de gouvernance » : La gouvernance (mot venant du latin *gubernare*, « diriger un navire ») désigne la manière dont est dirigée une entité sociale, qu'elle se rapporte à un groupe humain spécifique (famille, tribu, entreprise, nation) ou à autre chose (projet, réseau, langue). Popularisée par son usage en entreprise, la gouvernance n'implique pas nécessairement le gouvernement et peut être issue de l'interaction volontaire entre les individus.
(page 282) « Jeremy Rubin, qui a menacé de faire activer le BIP-119 (soft fork) par les mineurs en 2022 » : Jeremy Rubin, *7 Theses on a next step for BIP-119*, 17 avril 2022 : https://rubin.io/bitcoin/2022/04/17/next-steps-bip119/ ; archive : https://web.archive.org/web/20220419172825/https://rubin.io/bitcoin/2022/04/17/next-steps-bip119/. – On peut rapprocher son cas de celui de Paul Sztorc, qui travaille sur son concept de Drivechain depuis 2017, mais dont les propositions d'amélioration (BIP-300 et BIP-301) n'ont pas été intégrées par Bitcoin Core.
(page 282) « la suggestion des mineurs de procéder à un soft fork pour rediriger une partie de la récompense de bloc vers les équipes de développement » : Jiang Zhuoer, *Infrastructure Funding Plan for Bitcoin Cash*, 22 janvier 2020 : https://medium.com/@jiangzhuoer/infrastructure-funding-plan-for-bitcoin-cash-131fdcd2412e ; archive : https://web.archive.org/web/20200123082358/https://medium.com/@jiangzhuoer/infrastructure-funding-plan-for-bitcoin-cash-131fdcd2412e.
(page 282) « a fini en novembre par tenter d'imposer ce changement via une intégration dans Bitcoin ABC » : Amaury Séchet, *Bitcoin ABC's plan for the November 2020 upgrade*, 6 août 2020 : https://amaurysechet.medium.com/bitcoin-abcs-plan-for-the-november-2020-upgrade-65fb84c4348f.
(page 282) « Une implémentation alternative, Bitcoin Cash Node, a alors été créée pour faire

face à ce changement » : Notamment grâce aux deux développeurs anonymes freetrader et imaginary_username. – freetrader, *Bitcoin Cash Node*, 20 février 2020 : https://read.cash/@freetrader/bitcoin-cash-node-662e4737.
(page 283) « C'est également ce qu'a fait le mineur pro-BCHN face à Bitcoin ABC en novembre 2020 en censurant la chaîne » : https://decrypt.co/49819/bitcoin-cash-rebels-launch-51-attack-to-destroy-bch-hard-fork.
(page 283) « fork maléfique » : https://www.reddit.com/r/Bitcoin/comments/3yrsxt/bitcoindev_an_implementation_of_bip102_as_a/cyg4m39/.
(page 284) Satoshi Nakamoto, *Re: BitDNS and Generalizing Bitcoin*, 10/12/2010 17:29:28 UTC, https://bitcointalk.org/index.php?topic=1790.msg28917#msg28917 : « Les utilisateurs de Bitcoin pourraient devenir de plus en plus sectaires à propos de la limitation de la taille de la chaîne pour que son accès reste facile pour beaucoup d'utilisateurs et pour les petits appareils. »
(page 284) « appelés thésauriseurs » : Daniel Krawisz, *I'm Hoarding Bitcoins, and No You Can't Have Any*, 12 février 2014 : https://nakamotoinstitute.org/mempool/im-hoarding-bitcoins-and-no-you-cant-have-any/.
(page 287) « Twitter, lieu privilégié pour la communication sur Bitcoin » : Cette dépendance à Twitter a poussé les bitcoineurs à développer leur propre protocole de média social décentralisé : Nostr.
(page 287) « le salaire versé aux personnes chargées de l'écriture et de la révision du code dans Bitcoin Core provient principalement » : https://blog.bitmex.com/wp-content/uploads/2022/10/Bitcoin-Grant-Presentation-1.pdf

Chapitre 12

(page 295) « Tim May estimait que la chose était impossible » : Timothy C. May, *Cyphernomicon*, 12.3.8.
(page 297) « Ce modèle est donc particulièrement adapté à l'utilisation monétaire » : Ludovic Lars, *Pièces et comptes : deux modèles de représentation*, 20 juillet 2019 : https://viresinnumeris.fr/pieces-comptes-modeles-representation/.
(page 299) « Le langage est constitué de plus d'une centaine d'opérateurs » : La liste des opérateurs et de leurs actions est disponible sur la page de Bitcoin Wiki consacrée à Script : https://en.bitcoin.it/wiki/Script.
(page 302) « CVE-2010-5137 » : NIST, *CVE-2010-5137*, 8 juin 2012 : https://nvd.nist.gov/vuln/detail/CVE-2010-5137.
(page 302) « P2PK, P2PKH, P2MS, P2SH, NULLDATA, P2WPKH, P2WSH et P2TR » : https://github.com/bitcoin/bitcoin/blob/22.x/src/script/standard.h#L59-L71.
(page 304) « la sortie de la version 0.6.0 du logiciel » : Gavin Andresen, *Version 0.6.0 released*, 30 mars 2012 : https://bitcointalk.org/index.php?topic=74737.msg827484#msg827484.
(page 305) « par l'intermédiaire de plusieurs propositions » : Mike Caldwell (casascius), *Proposal to modify OP_CHECKSIG*, 22/09/2011 02:21:17 UTC : https://bitcointalk.org/index.php?topic=45211.msg538756#msg538756 ; jimrandomh, *Proposed extensions to the transaction protocol: Receiver scripts, OP_TIME, more*, 01/10/2011 16:56:47 UTC : https://bitcointalk.org/index.php?topic=46429.msg553217#msg553217 ; Gavin Andresen, *Re: Proposal to modify OP_CHECKSIG*, 02/10/2011 00:26:42 UTC : https://bitcointalk.org/index.php?topic=45211.msg553668#msg553668.
(page 305) « fonction VerifyScript de l'interpréteur » : https://github.com/bitcoin/bitcoin/blob/25.x/src/script/interpreter.cpp#L2005-L2062.

(page 305) « l'opposition notable de luke-jr » : Amir Taaki, *The Truth behind BIP 16 and 17*, 29 janvier 2012 : http://bitcoinmedia.com/the-truth-behind-bip-16-and-17/ ; archive : https://web.archive.org/web/20120202032835/http://bitcoinmedia.com/the-truth-behind-bip-16-and-17/.
(page 306) « l'arrivée de la version 0.9.0 de Bitcoin Core en mars 2014 » : Bitcoin Core, *Bitcoin Core version 0.9.0 released*, 19 mars 2014 : https://bitcoin.org/en/release/v0.9.0#opreturn-and-data-in-the-block-chain.
(page 307) « BIP-118 » : Christian Decker, Anthony Towns, *BIP-118: SIGHASH_ANYPREVOUT for Taproot Scripts*, 28 février 2017 : https://github.com/bitcoin/bips/blob/master/bip-0118.mediawiki.
(page 308) « Elle a également amélioré l'algorithme de signature pour éviter les hachages redondants durant la vérification et pour rendre plus sûre la signature hors-ligne » : https://github.com/bitcoin/bips/blob/master/bip-0143.mediawiki.
(page 308) « problème identifié depuis janvier 2012 » : Gavin Andresen, *[Bitcoin-development] Extending IsStandard() to transaction scriptSigs*, 19/1/2012 16:29:29, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2012-January/001066.html.
(page 309) « proposée initialement par Gregory Maxwell en août 2013 sur IRC » : Gregory Maxwell, IRC, 29/08/2013 20:21 UTC : https://download.wpsoftware.net/bitcoin/wizards/2013/08/13-08-29.log : « Je suggère de ne jamais hacher cette valeur dans le protocole. En gros, je dis que les scriptsigs pour une [transaction] seraient un arbre de hachage séparé. Il est toujours engagé dans la chaîne de blocs mais ce serait une branche séparée. »
(page 309) « version alpha du modèle de sidechain Elements, annoncée le 8 juin 2015 » : Adam Back, *Announcing Sidechain Elements: Open-Source Code and Developer Sidechains for Advancing Bitcoin*, 8 juin 2015 : https://blog.blockstream.com/en-714/.
(page 314) « nul ne peut prétendre exercer une activité complètement secrète qui échapperait absolument à la surveillance » : Les premiers utilisateurs de Bitcoin ont ainsi été bien imprudents, à l'instar de Hal Finney qui a révélé des informations entre 2013 et 2014 permettant de déduire qu'il possédait plus de 10 000 bitcoins en 2011. – Hal Finney, *Bitcoin and me*, 19/03/2013 20:40:02 UTC : https://bitcointalk.org/index.php?topic=155054.msg1643833#msg1643833 ; Andy Greenberg, *Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius*, 25 mars 2014 : https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/.
(page 315) « BitLaundry, une plateforme qui a été lancée en septembre 2010 par Peter Vessenes » : Peter Vessenes, *Announcing: BitLaundry – decorrelated payment service*, 01/09/2010 05:52:25 UTC : https://bitcointalk.org/index.php?topic=963.msg11823#msg11823.
(page 317) « protocole de paiement Pay-to-EndPoint » : Adam Ficsor, *Pay To EndPoint*, 31 juillet 2018 : https://nopara73.medium.com/pay-to-endpoint-56eb05d3cac6.
(page 317) « transactions Stowaway de Samourai Wallet » : Samourai Wallet, *Stowaway* : https://samouraiwallet.com/stowaway. – Il y a également protocole Bustapay qui a été proposé dans le BIP-79 en août 2018.
(page 317) « 2019 pour les transactions Stowaway » : Samourai Wallet, *Collaborative Transactions - "Cahoots"*, 11 mars 2019 : https://blog.samouraiwallet.com/post/183378923792/collaborative-transactions-cahoots.
(page 317) « 2020 pour P2EP » : Samson Mow, Daniel Williams, *Bitcoin Privacy Improves With BTCPay Server's P2EP Implementation*, 16 avril 2020 : https://blog.blockstream.com/en-bitcoin-privacy-improves-with-btcpay-servers-p2ep-implementation/.
(page 318) « formalisé en 2001 par Ronald Rivest, Adi Shamir et Yael Tauman » : Ronald L. Rivest, Adi Shamir, Yael Tauman, « *How to Leak a Secret* », *Advances in Cryptology — ASIACRYPT*

2001, 2001, pp. 552–565 : https://people.csail.mit.edu/rivest/pubs/RST01.pdf.
(page 318) « signature de groupe » : Satoshi faisait référence à ces signatures de groupe dans l'un de ses messages écrits sur le forum en 2010. – Satoshi Nakamoto, *Re: Not a suggestion*, 13/08/2010 19:28:47 UTC : https://bitcointalk.org/index.php?topic=770.msg9074#msg9074.
(page 319) « BIP-47 » : Justus Ranvier, *Reusable Payment Codes for Hierarchical Deterministic Wallets*, 24 avril 2015 : https://github.com/bitcoin/bips/blob/master/bip-0047.mediawiki.
(page 320) « grâce au travail de Shen Noether » : Shen Noether, *Ring Confidential Transactions*, 2015 : https://eprint.iacr.org/2015/1098.pdf.
(page 320) « Mimblewimble » : Le nom du concept et le pseudonyme du créateur sont issus de l'univers d'Harry Potter : Mimblewimble est la formule du sortilège à la langue de Plomb qui interdit à l'adversaire de parler en faisant des nœuds avec sa langue (Mimblewimble est censé « empêcher la chaîne de blocs de parler des informations personnelles de ses utilisateurs ») et Tom Elvis Jedusor est le vrai nom de Voldemort dans la traduction française.
(page 320) « proposé le 1er août 2016 par un inconnu se faisant appeler Tom Elvis Jedusor au sein du canal IRC #bitcoin-wizards » : Bitcoin-wizards logs, 1er août 2016 : https://gnusha.org/bitcoin-wizards/2016-08-01.log. Lien originel : http://5pdcbgndmprm4wud.onion/mimblewimble.txt.
(page 320) « OWAS » : Horas Yuan Mouton, *Increasing Anonymity in Bitcoin*, 9 septembre 2013 : https://www.dropbox.com/s/nkh22cibel8stb4/horasyuanmouton.pdf ; archive : https://download.wpsoftware.net/bitcoin/wizardry/horasyuanmouton-owas.pdf.
(page 320) « sectionnage des transactions » : Gregory Maxwell, *Transaction cut-through*, 26/08/2013 22:17:19 UTC : https://bitcointalk.org/index.php?topic=281848.msg3014613#msg3014613.
(page 321) « *Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge* » : On peut traduire ce terme par « argument de connaissance succinct et non interactif à divulgation nulle de connaissance » en français.

Chapitre 13

(page 325) « l'exemple de deux personnes qui ne se connaissent pas, Alice et Bob, et qui veulent réaliser une transaction en ligne » : Une description de ce contrat est faite dans le BIP-65 : https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki.
(page 326) « contrats de garantie » : Mike Hearn, *Bitcoin Wiki: Contracts*, 23 juin 2011 : https://en.bitcoin.it/wiki/Contract#Example_3:_Assurance_contracts : « Un contrat de garantie est une manière de financer la création d'un bien public, c'est-à-dire d'un bien qui, une fois créé, bénéficie à tous gratuitement. L'exemple typique est celui d'un phare : bien que tout le monde puisse être d'accord sur le fait qu'il doit être construit, c'est bien trop cher pour justifier qu'un marin individuel en construise un, étant donné qu'il bénéficiera à tous ses concurrents. Une solution est que tout le monde promette de payer pour la création du bien public, de sorte à ce que les promesses soient appliquées seulement si la valeur totale des promesses dépasse le coût de création. Si le nombre de personnes qui contribuent n'est pas assez élevé, personne ne doit payer quoi que ce soit. »
(page 327) « Flipstarter » : Ludovic Lars, *Flipstarter, le financement participatif pour Bitcoin Cash*, 24 avril 2020 : https://viresinnumeris.fr/flipstarter-financement-participatif-bitcoin-cash/.
(page 329) « l'idée d'un canal de paiement était envisagée dès les origines » : Satoshi Nakamoto, *Re: Open sourced my Java SPV impl*, 09/03/2011 16:15 UTC : https://plan99.net/~mike/satoshi-emails/thread4.html ; hashcoin, *Instant TX for established business relationships*

(need replacements/nLockTime), 04/07/2011 02:16:23 UTC : https://bitcointalk.org/index.php?topic=25786.msg320931#msg320931 ; Meni Rosenfeld, *Trustless, instant, off-the-chain Bitcoin payments*, 05/07/2012 13:37:19 UTC : https://bitcointalk.org/index.php?topic=91732.msg1010405#msg1010405 ; Jeremy Spliman, *[Bitcoin-development] Anti DoS for tx replacement*, 20/04/2013 01:48:11 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002433.html ; Alex Akselrod, *Bitcoin Wiki: Draft*, 12 mars 2013, https://en.bitcoin.it/wiki/User:Aakselrod/Draft ; Christian Decker, Roger Wattenhofer, *A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels*, août 2015 : https://www.researchgate.net/publication/277991245_A_Fast_and_Scalable_Payment_Network_with_Bitcoin_Duplex_Micropayment_Channels.

(page 333) « diverses méthodes d'inscription » : Andrew Sward, Ivy Vecna, Forrest Stonedahl, *Data Insertion in Bitcoin's Blockchain*, in *Ledger*, vol. 3, avril 2018 : https://doi.org/10.5195/ledger.2018.101.

(page 333) « message de bienvenue pour Shuya Yang » : *Welcome to the world, Shuya Yang!*, https://blockchair.com/bitcoin-cash/block/478559.

(page 333) « Le bloc précédant le troisième halving sur BTC en 2020 [...] incluait le titre d'un article du New York Times » : https://blockchair.com/bitcoin/block/629999.

(page 333) « le critère qui a permis d'identifier les bitcoins de Satoshi » : Sergio Lerner, *The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius*, 17 avril 2013 : https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/.

(page 334) « un point de vue approuvé par Satoshi » : Satoshi Nakamoto, *Re: [bitcoin-list] Bitcoin v0.1.5 released*, 04/03/2009 16:59:12 UTC, archive : https://web.archive.org/web/20131016004648/http://sourceforge.net/p/bitcoin/mailman/bitcoin-list/?viewmonth=200903 : « En effet, Bitcoin est un serveur d'horodatage sécurisé et distribué pour les transactions. Quelques lignes de code pourraient créer une transaction avec une empreinte supplémentaire de tout ce qui doit être horodaté. Je devrais ajouter une commande pour horodater un fichier de cette façon. »

(page 335) « l'hommage à Len Sassaman [...] inscrit sur la chaîne par les développeurs Dan Kaminsky et Travis Goodspeed » : Cet hommage peut être retrouvé dans la transaction d'identifiant 930a2114cdaa86e1fac46d15c74e81c09eee1d4150ff9d48e76cb0697d8e1d72 confirmée le 30 juillet 2011.

(page 335) « Un logo Bitcoin inscrit le 13 mai 2011 peut par exemple être retrouvé » : Transactions ceb1a7fb57ef8b75ac59b56dd859d5cb3ab5c31168aa55eb3819cd5ddbd3d806 et 9173744691ac25f3cd94f35d4fc0e0a2b9d1ab17b4fe562acc07660552f95518

(page 335) « Un hommage à Nelson Mandela accompagné d'une photo a été publié le 7 décembre 2013, quelques jours après sa mort » : Voir transaction 8881a937a437ff6ce83be3a89d77ea88ee12315f37f7ef0dd3742c30eef92dba.

(page 336) « un document » : Le PDF du livre blanc de Bitcoin a été inscrit sous forme de sorties P2MS au sein de la transaction 54e48e5f5c656b26c3bca14a8c95aa583d07ebe84dde3b7dd4a78f4e4186e713, le 6 avril 2013.

(page 336) « un jeu » : Nicholas Carlini, *Yet Another Doom Clone*, 1er février 2023 : https://ordinals.com/inscription/521f8eccffa4c41a3a7728dd012ea5a4a02feed81f41159231251ecf1e5c79dai0, https://nicholas.carlini.com/writing/2019/javascript-doom-clone-game.html.

(page 336) « données météorologiques » : Helen Partz, *98% of BSV Transactions Used for Writing Weather Data on Blockchain: Report*, 24 juin 2019 : https://cointelegraph.com/news/98-of-bsv-transactions-used-for-writing-weather-data-on-blockchain-repor

t.
(page 337) « Ils font usage de l'inscription de données arbitraires sur la chaîne pour inclure des instructions qui sont interprétées par des implémentations logicielles spécifiques » : C'est en ce sens que les métaprotocoles peuvent être appelés des surcouches, même si on préfère généralement utiliser ce terme pour parler des systèmes comme Lightning par exemple.
(page 337) « ChromaWallet » : Alex Mizrahi, *ChromaWallet (colored coins): issue and trade private currencies/stocks/bonds/..*, 07/09/2012 12:46:12 UTC : https://bitcointalk.org/index.php?topic=106373.msg1167516#msg1167516.
(page 338) « Mastercoin » : Le mot *master* dans le nom de Mastercoin est l'acronyme de « *Metadata Archival by Standard Transaction Embedding Records* », d'après les spécifications techniques : https://github.com/OmniLayer/spec/blob/master/OmniSpecification-v0.6.adoc.
(page 338) « « le livre blanc, intitulé "*The Second Bitcoin Whitepaper*", a été publié le 6 janvier 2012 par J.R. Willett » : J.R. Willett, *[It's here] The Second Bitcoin Whitepaper*, 06/01/2012 22:42:24 UTC : https://bitcointalk.org/index.php?topic=56901.msg678427#msg678427.
(page 338) « une multitude de collections de tels objets » : Vlad Costea, *Bitcoin NFTs On Counterparty (And How To Get Or Create Your First One)*, 29 décembre 2021 : https://bitcoin-takeover.com/bitcoin-nfts-on-counterparty-and-how-to-get-or-create-your-first-one/.
(page 338) « Le protocole s'appelait Memo et consistait à publier de courts messages visibles publiquement sous un profil défini et à pouvoir suivre les autres utilisateurs, à aimer et répondre à leurs messages » : https://memo.cash/protocol.
(page 339) « Le protocole Ordinals » : https://docs.ordinals.com/.
(page 339) « STAMPS » : STAMP est l'acronyme de *Secure, Tradeable Art Maintained Permanently*. – Mike In Space, *STAMPS: A Protocol for Storing Images On-Chain in Transaction Outputs Immutably on Bitcoin*, 6 avril 2023 : https://github.com/mikeinspace/stamps/tree/main.
(page 340) « Comparé à ECDSA, le schéma de signature de Schnorr possède quelques avantages » : Pieter Wuille, Jonas Nick, Tim Ruffing, *BIP-340: Schnorr Signatures for secp256k1*, 19 janvier 2020 : https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki.
(page 340) « MuSig2 » : Jonas Nick, Tim Ruffing, Yannick Seurin, *MuSig2: Simple Two-Round Schnorr Multi-Signatures*, 14 octobre 2020 : https://eprint.iacr.org/2020/1261.pdf.
(page 340) « *Discreet Log Contracts* » : Thaddeus Dryja, *Discreet Log Contracts*, 2017 : https://adiabat.github.io/dlc.pdf.
(page 340) « BIP-341 » : Pieter Wuille, Jonas Nick, Anthony Towns, *BIP-341: Taproot: SegWit version 1 spending rules*, 19 janvier 2020 : https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki.
(page 341) « BIP-342 » : Pieter Wuille, Jonas Nick, Anthony Towns, *BIP-342: Validation of Taproot Scripts*, 19 janvier 2020 : https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki.
(page 342) « deux primitives techniques conceptualisées en 2016 par le développeur Peter Todd » : https://petertodd.org/2016/state-machine-consensus-building-blocks#uniqueness-and-single-use-seals ; https://petertodd.org/2016/closed-seal-sets-and-truth-lists-for-privacy.

(page 345) « entre la facilité de transaction et la facilité de vérification » : Sosthène, *Apologie des petits blocs*, 2 août 2018 : https://www.sosthene.net/apologie-petits-blocs/.
(page 345) « Ce compromis se manifeste généralement par une limite de capacité transactionnelle » : Dans le cas où elle n'est définie nulle part, cette limite est de toute manière inférieure à la limite de marché du mineur le plus efficace, car aucun mineur économiquement rationnel ne traiterait de transaction gratuitement.
(page 347) « augmenter progressivement la limite de taille des blocs dans le but d'accompagner l'accroissement de l'activité » : Dans Monero, la pénalité (P) liée à la taille d'un bloc (B) est calculée à partir la taille médiane des 100 derniers blocs (M) et la subvention de base (R) qui est de 0,6 XMR par bloc depuis 2022. Si $B < M_0 = 300$ ko, alors $P = 0$. Sinon :

$$P = R\left(\frac{B}{M} - 1\right)^2 .$$

La taille du bloc ne peut pas dépasser $2M$ (taille qui correspond à une pénalité maximale).
(page 347) « C'était la solution soutenue par Satoshi Nakamoto » : Satoshi Nakamoto, *Re: [PATCH] increase block size limit*, 04/10/2010 19:48:40 UTC : https://bitcointalk.org/index.php?topic=1347.msg15366#msg15366.
(page 349) « Cette méthode présente un défaut de vérification (au moins temporaire) de sorte que l'opérateur est exposé à la tromperie, mais le risque est considéré comme acceptable » : Les risques liées à AssumeValid et à AssumeUTXO sont discutés dans le chapitre 5 de l'ouvrage *Bitcoin: A Work in Progress* de Sjors Provoost publié en 2022.
(page 349) « vaguement envisagée par les développeurs de Bitcoin Cash » : Amaury Séchet, *Using Merklix tree to shard block validation*, 6 novembre 2016 : http://www.deadalnix.me/2016/11/06/using-merklix-tree-to-shard-block-validation, archive : https://web.archive.org/web/20170716220359/https://www.deadalnix.me/2016/11/06/using-merklix-tree-to-shard-block-validation/ ; Joannes Vermorel, Amaury Séchet, Shammah Chancellor, Jason Cox, *Merklix tree for Bitcoin*, juillet 2018 : https://blog.vermorel.com/pdf/merklix-tree-for-bitcoin-2018-07.pdf.
(page 349) « le danksharding qui pourrait être implémenté dans Ethereum » : https://ethereum.org/en/roadmap/danksharding/.
(page 350) « Cette thèse a été par la suite développée par d'autres personnes comme Nik Bhatia » : Nik Bhatia, *Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies*, 2021.
(page 352) « OpenDime » : Les clés Opendime de Coinkite sont les produits les plus réputés pour l'échange physique en dehors de la chaîne. L'utilisateur peut vérifier que le scellé d'une clé n'a pas été brisé et que le contenu de celle-ci correspond au montant indiqué, de sorte qu'il peut l'accepter en tant que moyen de paiement. L'un des inconvénients majeurs est que la perte et le vol sont beaucoup plus faciles que dans le cas d'une portefeuille numérique bien géré. – Voir https://opendime.com/.
(page 352) « le protocole Rumple » : Fiatjaf, *idea: Rumple* 16/10/2020 21:42 UTC : https://fiatjaf.com/rumple.html.
(page 352) « les statechains » : Ruben Somsen, *Statechains: Non-custodial Off-chain Bitcoin Transfer*, 4 juin 2019 : https://medium.com/@RubenSomsen/statechains-non-custodial-off-chain-bitcoin-transfer-1ae4845a4a39.
(page 352) « les ZK-rollups » : Rollkit, *Sovereign rollups on Bitcoin with Rollkit*, 5 mars 2023 : https://rollkit.dev/blog/sovereign-rollups-on-bitcoin-with-rollkit ; archive : http://web.archive.org/web/20230511021256/https://rollkit.dev/blog

/sovereign-rollups-on-bitcoin/.
(page 352) « le protocole Ark » : Kudzai Kutukwa, « *Introducing Ark: An Alternative Bitcoin Scaling Solution Focused on Preserving Privacy* », *Bitcoin Magazine*, 11 juin 2023 : https://bitcoinmagazine.com/technical/how-ark-plans-to-scale-private-bitcoin-payments.
(page 352) « une fédération de participants qui se méfient les uns des autres » : Johnny Dilley, Andrew Poelstra, Jonathan Wilkins, Marta Piekarska, Ben Gorlick, Mark Friedenbach, *Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks*, 2016 : https://blockstream.com/strong-federations.pdf.
(page 353) « la chaîne latérale SmartBCH de Bitcoin Cash » : CheapLightning, *The Resolution of the smartBCH Experiment*, 2 août 2022 : https://read.cash/@CheapLightning/the-resolution-of-the-smartbch-experiment-b06eb075.
(page 354) « BIP-300 » : Paul Sztorc, CryptAxe, *BIP-300: Hashrate Escrows*, 23 mai 2017 : https://github.com/bitcoin/bips/blob/master/bip-0300.mediawiki.
(page 354) « BIP-301 » : Paul Sztorc, CryptAxe, *BIP-301: Blind Merged Mining*, 23 juillet 2019 : https://github.com/bitcoin/bips/blob/master/bip-0301.mediawiki.
(page 355) « le sigle LNP/BP a émergé pour désigner l'ensemble des protocoles intervenant dans le passage en surcouche » : Giacomo Zucco, *LNP/BP: A gentle introduction*, 21 juillet 2020, archive : https://web.archive.org/web/20200820123506/https://alzashop.com/lnp-bp-lightning-netowrk-and-bitcoin-protocols.
(page 356) « en novembre 2023, une capacité totale de 5 400 BTC, équivalant à environ 200 millions de dollars » : https://bitcoinvisuals.com/ln-capacity.
(page 356) « MiniMint » : Kiara Bickers, *Blockstream Sponsors Federated E-Cash as a Bitcoin Scaling Technology*, 26 octobre 2021 : https://medium.com/blockstream/blockstream-sponsors-federated-e-cash-as-a-bitcoin-scaling-technology-637ba05de7b3.
(page 357) « SCRIT » : https://github.com/scritcash/scrit-whitepaper/blob/master/scrit-whitepaper.pdf.
(page 357) « Open Transactions » : fellowtraveler, *Open Transactions: untraceable digital cash*, 17/08/2010 20:58:05 UTC : https://bitcointalk.org/index.php?topic=847.msg9976#msg9976.
(page 357) « certificats aveugles au porteur » : theymos, *Blinded bearer certificates*, 28/12/2016 21:44:24 : https://www.reddit.com/r/Bitcoin/comments/5ksu3o/blinded_bearer_certificates/.
(page 357) « Cashu » : callebtc sur Twitter, 14/09/2022 09:47 UTC : https://twitter.com/callebtc/status/1569986110272540674.
(page 358) « HBBFT » : Il s'agit du sigle de *Honey Badger Byzantine Fault Tolerant*.
(page 359) « ce ratio or-argent a été relativement stable au cours de l'histoire en variant entre 10 et 18 » : William Jacob, *An Historical Inquiry Into the Production and Consumption of the Precious Metals*, 1831.

Chapitre 15

(page 367) « Nous ne parlerons pas des risques techniques, que des personnes mieux informées ont déjà traités » : Voir par exemple Sjors Provoost, *Bitcoin: A Work in Progress*, 2022.
(page 369) « dépositaires institutionnels comme Coinbase Custody qui détiennent un pourcentage non négligeable des bitcoins en circulation » : https://platform.arkhamintelligence.com/explorer/entity/coinbase, https://twitter.com/brian_armstrong/status/1595126425371414528.
(page 371) « hyperbitcoinisation » : Daniel Krawisz, *Hyperbitcoinization*, 29 mars 2014 : ht

tps://nakamotoinstitute.org/mempool/hyperbitcoinization/ ; Pierre Rochard, *Speculative Attack*, 4 juillet 2014 : https://nakamotoinstitute.org/mempool/speculative-attack/.

(page 371) « La culture est l'ensemble des aspects matériels, intellectuels, affectifs et spirituels, qui caractérisent une société ou un groupe social » : UNESCO, « *Déclaration de Mexico sur les politiques culturelles* », *Conférence mondiale sur les politiques culturelles*, 26 juillet – 6 août 1982 : https://www.culture.gouv.fr/Media/Thematiques/Egalite-et-diversite/College-de-la-Diversite/Declaration-de-Mexico : « Dans son sens le plus large, la culture peut aujourd'hui être considérée comme l'ensemble des traits distinctifs, spirituels et matériels, intellectuels et affectifs, qui caractérisent une société ou un groupe social. Elle englobe, outre les arts et les lettres, les modes de vie, les droits fondamentaux de l'être humain, les systèmes de valeurs, les traditions et les croyances. »

(page 372) « la part de la culture que l'on pourrait qualifier de religieuse » : Émile Durkheim, *Les formes élémentaires de la vie religieuse*, 1912 : « Une religion est un système solidaire de croyances et de pratiques relatives à des choses sacrées, c'est-à-dire séparées, interdites, croyances et pratiques qui unissent en une même communauté morale, appelée Église, tous ceux qui y adhèrent. »

(page 372) « infini sur 21 » : Knut Svanholm, *Bitcoin: Everything divided by 21 million*, 2022.

(page 372) « HODL » : GameKyuubi, *I AM HODLING*, 18/12/2013 10:03:03 UTC : https://bitcointalk.org/index.php?topic=375643.msg4022997#msg4022997 ; Coindesk, *Maybe Don't HODL Bitcoin... – Hodl Guy*, 11 janvier 2019 : https://www.youtube.com/watch?v=6lAPU2yP6rw.

(page 372) « le taureau du marché haussier » : Vijay Boyapati, *The Bullish Case for Bitcoin*, 2021.

(page 373) « nous nous adressons au reste » : Albert Jay Nock, *Isaiah's Job*, 1936 : https://www.theatlantic.com/magazine/archive/1936/06/isaiahs-job/652293/.

(page 373) « travaillant pour l'adversaire » : Upton Sinclair, *I, Candidate for Governor, and How I Got Licked*, 1934 : « Il est difficile de faire comprendre quelque chose à un homme lorsque son salaire dépend précisément du fait qu'il ne la comprenne pas. »