

1. Bitcoin et Ethereum : voir le chapitre suivant.
2. Petit résumé basé sur une illustration du livre *The Business Blockchain* (<http://thebusinessblockchain.com/>) de William Mougayar (<http://www.slideshare.net/OuiShare/william-mougayar-the-promise-of-a-centerless-world>).
3. Lire cet article très instructif sur le sujet : [https://interstices.info/jcms/c\\_8622/les-reseaux-de-pair-a-pair](https://interstices.info/jcms/c_8622/les-reseaux-de-pair-a-pair)
4. Citation de David Daoud (Maltem Consulting) : [http://www.finyear.com/Les-grands-principes-de-la-blockchain-et-son-impact-dans-l-industrie-financiere\\_a36219.html](http://www.finyear.com/Les-grands-principes-de-la-blockchain-et-son-impact-dans-l-industrie-financiere_a36219.html)
5. <http://www.blockchaindailynews.com/glossary/>
6. ASCII (American Standard Code for Information Interchange) ou Code américain normalisé pour l'échange d'information. C'est une norme de codage de caractères en informatique ancienne et connue pour son influence incontournable sur les codages de caractères qui lui ont succédé.
7. Satoshi Nakamoto est l'inventeur du Bitcoin. Pour plus de détails, rendez-vous au chapitre suivant aux paragraphes consacrés à « La blockchain Bitcoin ».
8. Citation de Chris Skinner dans <http://thefinanser.com/2016/07/blockchain-like-internet-browser.html/>
9. Philippe Herlin est économiste et auteur de *La Révolution du bitcoin et des monnaies complémentaires*.
10. [http://www.lemonde.fr/economie/article/2015/09/30/la-revolution-blockchain-legs-du-bitcoin-en-version-seduction\\_4778603\\_3234.html](http://www.lemonde.fr/economie/article/2015/09/30/la-revolution-blockchain-legs-du-bitcoin-en-version-seduction_4778603_3234.html)
11. <http://www.agefi.fr/banque-assurance/actualites/hebdo/20160218/blockchain-prochaine-revolution-159207>
12. <http://santanderinnovations.com/fintech-2-0-paper-highlights-the-multi-billion-dollar-opportunity-open-to-financial-technology-businesses-which-can-help-to-reboot-financial-services/>
13. R3CEV : <http://r3cev.com/>
14. Digital Asset Holdings : <https://digitalasset.com/>
15. Hyperledger : <https://www.hyperledger.org/>
16. Minibons : <https://bitcoin.fr/quelle-blockchain-pour-les-minibons/>
17. Le lecteur trouvera une liste plus détaillée des diverses applications de la blockchain dans le [chapitre 3](#) et en fin d'ouvrage la liste à jour à fin 2016 des principaux projets en cours de développement ou d'utilisation.
18. <http://www.blockchain.vision>
19. <http://www.ibm.com/blockchain/>

## Chapitre 2

1. Nick Szabo, informaticien, juriste et cryptographe, est connu pour ses travaux de recherche dans les contrats numériques et la monnaie numérique. Il est diplômé de sciences informatiques de l'université de Washington.
2. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
3. <https://bitcoin.fr/histoire/>
4. RSA Security est une entreprise dont le sigle est formé à partir des noms de ses fondateurs : Ronald Rivest, Adi Shamir et Leonard Adleman. Ce sont les coinventeurs du cryptosystème à clé publique du même nom : le chiffrement RSA qui est un algorithme cryptographique de cryptographie asymétrique.
5. Ralph C. Merkle est un cryptographe américain et chercheur en nanotechnologies. Il est l'un des pionniers de la cryptographie asymétrique avec Martin Hellman et Whitfield Diffie. En 1974, il a créé les puzzles de Merkle, la première construction (non top secret) à clé publique (publication en 1978).
6. <http://blogchaincafe.com/merkle-roots-et-merkle-trees-expliques#more-110>
7. <https://bitcoin.fr/pages/DigiCash>
8. <https://bitcoin.fr/comment-produire-de-la-monnaie-la-cryptographie-du-cash-electronique-anonyme-2/>
9. <https://bitcoin.fr/Blockchain-et-Sidechains>
10. <https://bitcoin.fr/Le-retour-de-Nick-Szabo>
11. <http://unenumerated.blogspot.fr/2005/12/bit-gold.html>
12. Retrouvez l'histoire du bitcoin sur : <http://historyofbitcoin.org/> et sur <https://bitcoin.fr/histoire/>
13. [http://www.finyear.com/Bitcoin-A-Peer-to-Peer-Electronic-Cash-System-by-Satoshi-Nakamoto\\_a34914.html](http://www.finyear.com/Bitcoin-A-Peer-to-Peer-Electronic-Cash-System-by-Satoshi-Nakamoto_a34914.html)
14. <https://bitcoin.fr/satoshi-nakamoto>
15. [https://en.bitcoin.it/wiki/Main\\_Page](https://en.bitcoin.it/wiki/Main_Page)

16. Entre autres plateformes, voir la liste en fin d'ouvrage.
17. Acquérir des bitcoins : <https://bitcoin.fr/obtenir-des-bitcoins/>
18. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
19. « D'où vient la valeur des bitcoins ? », <http://e-ducat.fr/links/value/>
20. Source : <https://blockchain.info/fr/charts/market-price?timespan=all>
21. CPU : voir glossaire : <http://www.blockchaindailynews.com/glossary/>
22. Minage : une « mine » d'informations sur <https://bitcoin.fr/minage/>
23. Les algorithmes de hachage sont SHA-256 et RIPEMD-160. Un double hash en SHA-256 est utilisé pour obtenir le hash des blocs et donc la preuve de travail, tandis qu'un SHA-256 suivi d'un RIPEMD-160 est utilisé pour construire les adresses bitcoin.
24. Bitcoin Core est un projet *open source* qui maintient et publie le logiciel client Bitcoin dénommé « Bitcoin Core ». C'est un descendant direct du logiciel client Bitcoin original créé par Satoshi Nakamoto suite à la publication du fameux livre blanc du Bitcoin. Il est téléchargeable ici : <https://bitcoin.org/fr/telecharger>
25. Minage et consommation électrique : [https://karlodwyer.github.io/publications/pdf/bitcoin\\_KJOD\\_2014.pdf](https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf)
26. Lire « Plaidoyer pour le Bitcoin » (<http://www.scilogs.fr/complexites/plaidoyer-pour-le-bitcoin/>) pour découvrir les fausses informations publiées par les médias et les banques en 2013 à propos du Bitcoin...
27. Pierre Noizat, e-ducat : <http://e-ducat.fr/2015-11-28-cop21-et-blockchain/>
28. « The Byzantine Generals Problem », *ACM Transactions on Programming Languages and Systems*, vol. 4, n° 3, juillet 1982.
29. Extrait d'un article d'Hubert de Vauplane publié sur Finyear.
30. M. Correia, G.S. Veronese, N.F. Neves et P. Verissimo, « Byzantine consensus in asynchronous message-passing systems : a survey », *International Journal of Critical Computer-Based Systems*, vol. 2, n° 2, 2011, p. 141–161.
31. Ancien nom de la DARPA (Defense Advanced Research Projects Agency), l'agence du département de la Défense des États-Unis chargée des nouvelles technologies militaires et à l'initiative de ARPAnet.
32. Paxos est un algorithme qui résout le consensus dans les systèmes répartis par passage de messages en deux étapes de communication.
33. <https://tendermint.com/>
34. Lire également « La tyrannie des mineurs », [http://www.blockchaindailynews.com/La-Tyrannie-des-Mineurs\\_a24751.html](http://www.blockchaindailynews.com/La-Tyrannie-des-Mineurs_a24751.html)
35. Pour en savoir plus, vous pouvez vous rendre sur le forum dédié : <http://bitcoin.stackexchange.com/questions/658/what-can-an-attacker-with-51-of-hash-power-do>
36. Si un utilisateur mal intentionné essaie de dépenser ses bitcoins auprès de deux destinataires différents au même moment, il s'agit d'une double dépense. Le minage et la chaîne de blocs existent pour créer un consensus dans le réseau afin de décider laquelle des deux transactions sera confirmée et considérée valide. (Voir glossaire : <http://www.blockchaindailynews.com/glossary/>)
37. La puissance de calcul d'un mineur est exprimée en Hash/s (quantité de hash calculée à la seconde) (Kilo Hash / Mega Hash / Giga Hash / Terra Hash).
38. Procédure suite à une attaque : [https://en.bitcoin.it/wiki/Contingency\\_plans](https://en.bitcoin.it/wiki/Contingency_plans)
39. Note rédigée par David Teruzzi (voir page de remerciements).
40. <http://www.blockchain.info>
41. Dash (anciennement connue sous le nom de Darkcoin) est une crypto-monnaie créée en 2012 par Evan Duffield, et présentée au grand public le 18 janvier 2014. Son nom initial, Darkcoin, a été changé le 25 mars 2015 en Dash, mot-valise de *digital* et de *cash*, c'est-à-dire « argent liquide numérique ». Voir <https://www.dash.org/>
42. <http://zerocoin.org/>
43. <http://zerocash-project.org/>
44. <https://z.cash/>
45. <https://getmonero.org/>

46. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
47. <https://www.oreilly.com/ideas/blockchain-scalability>
48. Sur ce point, voir plus loin les paragraphes consacrés au « Lightning Network ».
49. <http://altcoins.com/>
50. Monnaie virtuelle interne à une blockchain permettant des transferts de valeurs de compte à compte. C'est une forme de monnaie numérique basée sur les mathématiques, où les techniques de cryptage sont utilisées pour réguler la production d'unités de la monnaie et vérifier le transfert de fonds. En outre, les crypto-monnaies fonctionnent indépendamment d'une banque centrale.
51. Source CoinMarketCap : <http://coinmarketcap.com/all/views/all/>
52. <http://www.wikiberal.org/wiki/Monnaie-fiat> -
53. <http://www.riksbank.se/en/>
54. <https://litecoin.org/fr/>
55. <https://namecoin.org/> et <https://wiki.namecoin.org/index.php?title=Welcome>
56. <http://www.onecoin.eu/>
57. <http://www.potcoin.com/>
58. <http://mazacoin.org/>
59. <https://bitshares.org/>
60. <https://www.dash.org/>
61. <http://blackcoin.co/fr/>
62. <https://viacoin.org/>
63. <https://z.cash/> – Voir également : [http://www.blockchaindailynews.com/What-is-Zcash\\_a24678.html](http://www.blockchaindailynews.com/What-is-Zcash_a24678.html)
64. <https://www.georgetown.edu/>
65. « Cryptocurrency with a Conscience : Using Artificial Intelligence to Develop Money that Advances Human Ethical Values », <http://www.finyear.com/attachment/641777/>
66. « Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox? », [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2393537](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393537)
67. <http://coloredcoins.org/>
68. <https://counterparty.io/>
69. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
70. Pierre Noizat : <http://e-ducat.fr>
71. Gavin Andresen est le scientifique en chef de la Fondation Bitcoin. Il possède une clé cryptographique qui lui permet de publier une alerte à tous les clients Bitcoin. Son site perso : <http://gavinandresen.ninja/>
72. <https://bitcoin.fr/quel-est-lenjeu-du-debat-sur-la-taille-minimale-des-blocs-de-transactions/>
73. Site personnel : <http://www.cypherspace.org/adam/>
74. 1997 : Adam Back invente HashCash, un système de preuve de travail à partir d'une idée introduite par Cynthia Dwork et Moni Naor dans un rapport publié en 1993, « Pricing *via* Processing or Combatting Junk Mail ». Adam Back deviendra plus tard le premier interlocuteur de Satoshi Nakamoto puis récemment le cofondateur de Blockstream.
75. <http://www.hashcash.org/>
76. <https://blockstream.com>
77. <https://blockstream.com/technology/#sidechains>
78. <https://blockstream.com/technology/sidechains.pdf>
79. Voir également le projet « Éléments » ou « Elementsproject » (<https://elementsproject.org/sidechains/>) initié par Blockstream et une communauté. Vous pouvez rejoindre ce projet et créer votre propre sidechain (<https://elementsproject.org/sidechains/creating-your-own.html>).

80. Pour plus de détails sur le fonctionnement des sidechains, vous pouvez consulter un article de Pierre Noizat dédié aux sidechains (<http://e-ducat.fr/2014-11-08-blockchain-et-sidechains/>).
81. <http://www.rsk.co/#1>
82. Projet Rootstock sur [bitcoin.fr](http://bitcoin.fr) : <https://bitcoin.fr/rootstock-bitcoin-pour-les-smart-contracts/>
83. Turing-complet : machine de Turing universelle qui a potentiellement la capacité de calculer tout ce qui est calculable. En informatique théorique, une machine de Turing est un modèle abstrait du fonctionnement des appareils mécaniques de calcul, tels un ordinateur et sa mémoire. Ce modèle a été imaginé par Alan Turing en 1936, en vue de donner une définition précise au concept d'algorithme ou de procédure mécanique.
84. <https://interledger.org/>
85. <https://lightning.network/>. Voir aussi : <https://bitcoin.fr/lightning-network-la-solution-pour-bitcoin/> et <http://blogchaincafe.com/the-lightning-network-pour-un-reseau-bitcoin-totalement-scalable>
86. <https://lightning.network/lightning-network-paper.pdf>
87. <http://bitfury.com/>
88. <http://acinq.co/>
89. Interview ACINQ : [http://www.blockchaindailynews.com/Blockchain-Bitcoin-Eclair-et-reseau-Lightning\\_a24530.html](http://www.blockchaindailynews.com/Blockchain-Bitcoin-Eclair-et-reseau-Lightning_a24530.html)
90. « Flare : An Approach to Routing in Lightning Network » (fruit de la collaboration entre le coauteur Olaoluwa Osuntokun et le reste de l'équipe du réseau Lightning), <http://bitfury.com/content/5-white-papers-research/whitepaper-flare-an-approach-to-routing-in-lightning-network-7-7-2016.pdf>
91. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
92. Unité de mesure de stockage en informatique équivalent à un milliard de bytes.
93. <https://www.bigchaindb.com>
94. <https://www.ascribe.io/>
95. <https://www.rethinkdb.com/>
96. Source : <http://www.bortzmeyer.org/ethereum.html>
97. <https://about.me/vitalik-buterin>
98. Livre Blanc / White Paper Ethereum – Traduction française : <https://www.ethereum-france.com/livre-blanc-white-paper-ethereum-traduction-francaise/>
99. Ether : monnaie de la blockchain Ethereum.
100. Bloc genesis : la genèse d'une blockchain, c'est-à-dire le premier bloc d'une blockchain.
101. Étapes du lancement d'Ethereum sur Ethereum France : <https://www.ethereum-france.com/etapes-du-lancement-dethereum/> ; sur Blogchain Café : <http://blogchaincafe.com/les-differentes-etapes-du-lancement-dethereum>
102. En informatique ou en logique, un système Turing-complet est un système formel ayant une puissance de calcul au moins équivalente à celle des machines de Turing. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
103. <https://www.ethereum.org/>
104. Ethereum Foundation : <https://ethereum.org/foundation>
105. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
106. The Mauve Revolution : <https://www.ethereum-france.com/%EF%BB%BFethereum-2-0-mauve-paper-traduction-francaise/>
107. Voir CoinMarketCap : <http://coinmarketcap.com/#EUR>
108. Pour obtenir les informations complètes sur les deux solutions, rendez-vous sur <https://www.ethereum-france.com/comment-acheter-des-ethers-eth/>
109. <https://www.coinhouse.io/>
110. Smart contracts par Szabo : <http://www.virtualschool.edu/mon/Economics/SmartContracts.html> et [http://szabo.best.vwh.net/smart\\_contracts\\_idea.html](http://szabo.best.vwh.net/smart_contracts_idea.html)

111. « Bitcoin is not just digital currency. It's Napster for finance », *Fortune*, janvier 2014.
112. Voir S. Bourque et S. Fung Ling Tsui, « A Lawyer's Introduction to Smart Contracts », *Scientia Nobilitat Reviewed Legal Studies*, 2014.
113. Pour une explication technique du projet, voir <http://www.bortzmeyer.org/ethereum.html>
114. Comme tout système de registre décentralisé, la vérification coûte cher et les pairs doivent être incités à travailler ; d'où le développement des jetons (« token ») ou des points spécifiques à Ethereum, l'ether : il n'y a donc pas de mineurs contrairement au système Bitcoin dans lequel les mineurs sont rémunérés par des bitcoins.
115. <https://solidity.readthedocs.io/en/develop/> et <https://github.com/ethereum/wiki/wiki/The-Solidity-Programming-Language>
116. Le code utilisé dans le projet Ethereum est différent de celui utilisé par le Bitcoin, même s'il s'en inspire. Le code a été réécrit à partir de zéro. La principale différence par rapport à Bitcoin est que les transactions stockées dans la blockchain ne sont pas limitées à envoyer et recevoir de l'argent. Ethereum dispose d'un quasi-langage de Turing et est donc un système de calcul réparti : les pairs dans le réseau Ethereum ne se contentent pas de vérifier l'intégrité de la blockchain et d'ajouter de la monnaie, ils exécutent du code arbitraire, celui des applications que vous ou moi développons et envoyons sur le réseau.
117. Pour en savoir plus sur la programmation de *smart contracts*, voici un lien pédagogique : <http://blogchaincafe.com/la-programmation-de-smart-contract-une-operation-hautement-delicate>
118. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
119. <http://www.oraclize.it/>
120. Oracle – Ethereum France : <https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/>
121. <https://www.codius.org/>
122. <https://www.ethereum-france.com/decentralized-autonomous-organization-dao-blockchain/> et « Qu'est-ce qu'une DAO ? », <https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/>
123. Pour en savoir plus sur la DAO, reportez-vous à l'article « DAO : Contractors et Curators », <http://blogchaincafe.com/dao-contractors-et-curators>
124. <https://bitnation.co/>
125. Assurance récolte : <https://www.ethereum-france.com/livre-blanc-white-paper-ethereum-traduction-francaise/>
126. « Les organisations distribuées autonomes : quel statut juridique ? », maître Thibault Verbiest, avocat associé du cabinet De Gaulle Fleurance & Associés.
127. <https://www.ethereum-france.com/dao-link-permet-a-des-entreprises-de-contracter-avec-des-dao/>
128. « Qu'est-ce qu'une DAO ? » : <https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/>
129. Informaticien qui recherche à exploiter les faiblesses de la sécurité informatique.
130. Maître Pascal Agosti, avocat, Caprioli Avocats – <http://www.caprioli-avocats.com/>
131. L'Usine digitale, juillet 2016, <http://www.usine-digitale.fr/article/la-blockchain-pose-de-serieux-problemes-de-confiance-de-droit-et-de-securite.N401527>
132. *Hard fork*, voir « fork » : objet ayant une racine commune avec un second. Ces deux objets, jumeaux au départ, suivent chacun, après séparation, leur évolution propre.
133. Lire à ce sujet l'article « Editing the Uneditable Blockchain : Why distributed ledger technology must adapt to an imperfect world », <https://acnprod.accenture.com/us-en/insight-editing-uneditable-blockchain>
134. Lire à ce sujet Vitalik Buterin, « On Public and Private Blockchains », <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
135. Néologisme de Vitalik Buterin (Ethereum).
136. NXT Whitepaper : [https://nxtwiki.org/wiki/Whitepaper:Nxt#Proof\\_of\\_Stake](https://nxtwiki.org/wiki/Whitepaper:Nxt#Proof_of_Stake)
137. Source : KPMG, George Samman.

- [138](#). Le calcul distribué consiste à répartir un calcul ou un traitement sur plusieurs microprocesseurs et plus généralement sur toute unité centrale informatique.
- [139](#). Les mécanismes de consensus sont utilisés pour s'assurer que l'ensemble des nœuds du réseau disposent des mêmes informations et que seules les transactions valides soient enregistrées dans les registres distribués.
- [140](#). Adam Back, « HashCash – A Denial of Service Counter-Measure », <http://www.hashcash.org/hashcash.pdf>
- [141](#). Système qui lie la capacité du minage à la puissance de calcul.
- [142](#). <https://decred.org>
- [143](#). Méthode par laquelle une chaîne de blocs d'une crypto-monnaie vise à atteindre un consensus distribué.
- [144](#). Projet Sharding : <http://ethereum.stackexchange.com/questions/573/what-is-a-shard>
- [145](#). <https://peercoin.net/index.php?locale=fr>
- [146](#). PoW vs PoS : <http://blogchaincafe.com/les-consensus-proof-of-work-vs-proof-of-stake#more-559>
- [147](#). OCTO : <http://blog.octo.com/quel-consensus-dans-une-blockchain-privee/>
- [148](#). <https://bitshares.org/>
- [149](#). <https://bitshares.org/blog/2015/06/15/the-history-of-graphene/>
- [150](#). <https://steem.io/>
- [151](#). <https://raft.github.io/>
- [152](#). <http://www.the-blockchain.com/docs/JP-Morgan-Juno-Distributed-Cryptolledger.pdf>
- [153](#). [http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland\\_zhong.pdf](http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf)
- [154](#). Voir glossaire : <http://www.blockchaindailynews.com/glossary/> La théorie des graphes acycliques détermine, dans un ensemble d'objets distants les uns des autres et espacés de façon variable, le chemin optimal pour aller de tel objet à tel autre.
- [155](#). <https://lisk.io/>
- [156](#). Voir l'article de David Teruzzi, « Lisk : un concurrent d'Ethereum ? », [http://www.finyear.com/Lisk-un-concurrent-d-Ethereum\\_a35894.htm](http://www.finyear.com/Lisk-un-concurrent-d-Ethereum_a35894.htm)
- [157](#). Pour en savoir plus sur les Dapps : <http://blogchaincafe.com/les-dapps-applications-distribuees-decentralisees#more-443>
- [158](#). SCP Stellar : <https://www.stellar.org/>
- [159](#). <https://ripple.com/>
- [160](#). The Ripple Protocol Consensus Algorithm : [https://ripple.com/files/ripple\\_consensus\\_whitepaper.pdf](https://ripple.com/files/ripple_consensus_whitepaper.pdf)
- [161](#). <https://www.iotatoken.com/>
- [162](#). Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
- [163](#). Si vous souhaitez en savoir plus sur IOTA et IOTA token, nous vous conseillons la lecture des deux articles suivants : « IOTA, pour en finir avec la blockchain », <http://www.blockchaindailynews.com/IOTA-pour-en-finir-avec-la-blockchain-a24438.html> et « IOTA token : une tangle crypto-currency », <http://blogchaincafe.com/iotatoken-une-tangle-crypto-currency#more-1057>
- [164](#). Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
- [165](#). Dans ce cercle fermé des DAG, IOTA présente quelques similitudes avec la solution française beAchain qui est en cours de développement et prévoit de lancer sa version 1 en février 2017.
- [166](#). <https://www.hyperledger.org>
- [167](#). <https://www.hyperledger.org/announcements/2016/11/30/hyperledger-hits-100-member-milestone>
- [168](#). <https://interledger.org/>
- [169](#). TLA+, acronyme de Temporal Logic of Actions (« logique temporelle des actions »), est un système de méthode formelle pour les algorithmes parallèles et distribués.
- [170](#). <https://tendermint.com/>

171. « Tendermint: Consensus without Mining », <http://the-blockchain.com/docs/TendermintConsensuswithoutMining.pdf>
172. <https://monax.io/>
173. <https://www.corda.net/>
174. R3CEV : [http://www.blockchaindailynews.com/Goldman-Sachs-confirme-son-depart-de-R3\\_a24794.html](http://www.blockchaindailynews.com/Goldman-Sachs-confirme-son-depart-de-R3_a24794.html)
175. <http://www.beachain.com>
176. Groupes d'objets associés, voir glossaire : <http://www.blockchaindailynews.com/glossary/>
177. Quick Virtual Organization, voir glossaire : <http://www.blockchaindailynews.com/glossary/>
178. <http://beachain.com/BEACHAIN-QVO-Paris-NewYork.pdf>
179. Pour les bitconistes historiques, il n'existe qu'une seule blockchain. Pour certains éthereumiens, il n'y en a que deux. Pour tous les autres, il en existe autant qu'il y a de registres distribués (DLT) à transactions horizontales P2P consensuelles, qu'elles soient publiques, hybrides ou privées.

## Chapitre 3

1. Ces organisations distribuées sont au cœur du projet DAO d'Ethereum. Pour la première fois, nous voyons apparaître une forme de société entièrement décentralisée mais qui, à ce jour, n'existe que sur la blockchain Ethereum et ses participants n'interagissent entre eux que sur la blockchain. Ce type de société est 100 % transparente, les comptes et les échanges entre participants étant publics.
2. <https://openbazaar.org/>
3. <https://arcade.city/>
4. Voir glossaire : <http://www.blockchaindailynews.com/glossary/>
5. Gilles Babin est serial-entrepreneur et Digital Champion de la France à la Commission européenne. Voir <https://blockchainfrance.net/2016/01/22/la-blockchain-pour-horizontaliser-le-monde/>
6. Vous pouvez aussi lire à ce sujet l'article « Une épée de Damoclès sur le Bitcoin », <http://www.scilogs.fr/complexites/epée-de-damocles-bitcoin/>
7. Pour en savoir plus, lisez « Transparency Overlays and Applications » (<http://dl.acm.org/citation.cfm?id=2978404>), une étude très intéressante à propos de la transparence dans des environnements distribués et en particulier la blockchain Bitcoin.
8. Lire, à propos de l'immutabilité, l'article portant sur la tentative d'Accenture d'« effacer » des données dans certains cas exceptionnels : « Accenture tue l'innovation », [http://www.blockchaindailynews.com/Blockchain-Accenture-tue-l-innovation\\_a24489.html](http://www.blockchaindailynews.com/Blockchain-Accenture-tue-l-innovation_a24489.html)
9. <http://cambridge-blockchain.com/>
10. PoC ou *proof of concept* (preuve de concept) est une démonstration de faisabilité, une réalisation courte ou incomplète d'une certaine méthode ou idée pour démontrer sa faisabilité. C'est une étape importante pour aboutir à un prototype pleinement fonctionnel.
11. <http://www.wma.net/fr/20activities/10ethics/10helsinki/>
12. <http://www.blockness.io>
13. <https://symbiont.io/>
14. Vous pouvez retrouver les liens web des acteurs travaillant à ces applications et plus encore dans l'annexe en fin d'ouvrage.
15. Voir également le « Top 250 des compagnies & startups blockchain » mis à jour régulièrement : [http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups\\_a24712.html](http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html)
16. Si nous devons anticiper sur la vision prospective que nous avons de la blockchain (voir le chapitre suivant), nous ajouterions que le *smart grid*, s'il est associé à un système distribué de très nombreuses microcentrales, est désigné comme l'un des cinq piliers de la « troisième révolution industrielle » annoncée, notamment par Jeremy Rifkin. Ce qui revient à dire que la révolution blockchain qui se profile passera par le monde de l'énergie.
17. <https://www.rwe.com/web/cms/en/8/rwe/>
18. Partenariat Slock.it et RWE : <https://blog.slock.it/partnering-with-rwe-to-explore-the-future-of-the-energy-sector-1cc89b9993e6#.cxxx17p5m>

19. *Micro-grid* : microréseaux électriques intelligents (produire de l'électricité à l'échelle de son quartier).
20. <http://lo3energy.com/>
21. <https://consensus.net/>
22. <http://www.navigantresearch.com/newsroom/worldwide-microgrid-market-will-surpass-40-billion-in-annual-revenue-by-2020>
23. <http://www.ponton.de/>
24. <http://enerchain.ponton.de/>
25. <http://www.h4ckenergy.com/>
26. <http://www.yuso.be/index-fr.html>
27. <http://priogen.com/>
28. <http://www.electricchain.org/>
29. <http://www.chainofthings.com/>
30. [http://www.blockchaindailynews.com/IBM-et-WalMart-explorent-la-blockchain-pour-la-securite-alimentaire\\_a24646.html](http://www.blockchaindailynews.com/IBM-et-WalMart-explorent-la-blockchain-pour-la-securite-alimentaire_a24646.html)
31. <https://scripts.veredictum.io/>
32. <http://revelator.com/>
33. Lire également « Music On The Blockchain (Foreword by Nick Mason, Pink Floyd) » :  
[http://www.blockchaindailynews.com/Music-On-The-Blockchain-Foreword-by-Nick-Mason-Pink-Floyd\\_a24414.html](http://www.blockchaindailynews.com/Music-On-The-Blockchain-Foreword-by-Nick-Mason-Pink-Floyd_a24414.html)
34. La tokenisation est le procédé qui permet de remplacer une donnée critique par un élément équivalent (jeton ou *token*) qui n'aura aucune valeur intrinsèque ou signification exploitable une fois sorti du système.
35. <http://www.blockpharma.com/>
36. <https://blockchainhealth.co/>
37. <https://www.pubpub.org/pub/medrec>
38. <http://www.enigma.co/>
39. <http://landing.bitland.world/>
40. <http://epigraph.io/>
41. <https://shocard.com/>
42. <https://onename.com>
43. Avocat, Caprioli Avocats, <http://www.caprioli-avocats.com/> Voir aussi sur le sujet É. Caprioli, *Signature électronique et dématérialisation (Droit et pratiques)*, LexisNexis, 2014.
44. CJUE, gde ch., 13 mai 2014, aff. C-131/12, Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos e.a. : JurisData n° 2014-009597.
45. <https://ripple.com/>
46. <https://setl.io/>
47. Par Léo Lemordant, CEO Enerfip, [www.enerfip.fr](http://www.enerfip.fr) et maître Diane Hervey, avocat au barreau de Paris.
48. <http://www.crowdlending.fr/assises-financement-participatif/>
49. Cité dans le communiqué de presse de l'association professionnelle Financement participatif France.
50. Article L.223-12 du Code monétaire et financier (« CMF ») issu de l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.
51. Xavier Delpech, « Le régime juridique des bons de caisse modernisé », *Dalloz actualité*, 10 mai 2016.
52. Du moins pour les blockchains fonctionnant en preuve de travail (*proof of work*) et non en preuve de détention (*proof of stake*).
53. Olivier Hielle, « La technologie Blockchain : une révolution aux nombreux problèmes juridiques », *Dalloz actualité*, 31 mai 2016.



54. <https://enerfip.fr/>
55. Le livre blanc publié par Enerfip intitulé « La Blockchain, nouveau levier du financement participatif » est disponible gratuitement au téléchargement sur <https://blockchain-explorer.enerfip.fr/livre-blanc>
56. Communiqué de presse : <https://group.bnpparibas/communiquede-presse/bnp-paribas-securities-services-renforce-plateforme-blockchain-titres-entreprises-cotees>
57. Voir également par extension « L'Assemblée nationale habilite le gouvernement à légiférer sur la blockchain par ordonnance » : [http://www.finyear.com/L-Assemblee-Nationale-habilite-le-gouvernement-a-legiferer-sur-la-blockchain-par-ordonnance\\_a36403.html](http://www.finyear.com/L-Assemblee-Nationale-habilite-le-gouvernement-a-legiferer-sur-la-blockchain-par-ordonnance_a36403.html)
58. Voir aussi É. Caprioli, « Consécration légale de la "blockchain" dans les bons de caisse », *Comm. com. électr.* juin 2016, comm. 58 ; P. Agosti, « La blockchain a sa première définition légale » (<http://www.usine-digitale.fr/article/la-blockchain-a-sa-premiere-definition-legale.N392352>) ; H. de Vauplane, « La blockchain et la loi » ([http://www.finyear.com/La-Blockchain-et-la-loi\\_a35403.html](http://www.finyear.com/La-Blockchain-et-la-loi_a35403.html))
59. [http://www.blockchaindailynews.com/La-blockchain-promesse-de-lendemain-radieux-pour-la-democratie\\_a24726.html](http://www.blockchaindailynews.com/La-blockchain-promesse-de-lendemain-radieux-pour-la-democratie_a24726.html)
60. Par ailleurs, dans un article paru sur [Cryptos.net](http://www.cryptos.net/technologie-block-chain-lavenir-democratie-numerique/) (<http://www.cryptos.net/technologie-block-chain-lavenir-democratie-numerique/>), on pouvait lire : « En 2012, lors des dernières élections aux États-Unis, une inscription sur huit était invalide ou incorrecte ; tandis que seulement 2,7 millions d'électeurs se sont inscrits dans différents États du pays. Ces statistiques sont terribles pour un système qui est utilisé dans le but de déterminer l'avenir d'une nation, surtout pour un pays aussi puissant que les États-Unis. »
61. [http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_ATA\(2016\)581918](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2016)581918)
62. <http://www.frenchweb.fr/voter-via-la-blockchain-experimentations-et-retours-dexperience/240683>
63. <http://vote.belem.io/>
64. <https://voatz.nimsim.com/>
65. <http://www.kinno.fi/en>
66. Keeex, solutions de confiance blockchain : <https://keeex.me/fr/>
67. Learning on the block : <http://www.knowledgeworks.org/learning-block-smart-transactional-models> D'après l'étude : « Il est important pour les éducateurs et les autres parties prenantes de réfléchir à tous les impacts possibles, tant positifs que négatifs, que la blockchain pourrait avoir sur l'avenir de l'apprentissage. [...] Du suivi des absences à la gestion des délais des devoirs, les nouvelles technologies sont souvent tournées vers la résolution d'un problème dans une école ou une classe. Mais, si au lieu de résoudre un problème, la technologie permettait d'ouvrir des portes pour l'apprentissage ? »
68. <https://blockchainedu.org/>
69. UIT : Organisation des Nations unies pour les télécommunications. Fondée en 1865, elle compte quelque 180 pays membres. Son rôle est d'harmoniser le développement des télécommunications dans le monde. Le siège de l'UIT est à Genève.
70. Dirigeant du cabinet de conseil Xavier Dalloz Consulting spécialisé dans le suivi des technologies de l'information, <http://www.dalloz.com/>
71. Organisation qui utilise les technologies financières innovantes pour fournir ou soutenir des services financiers.
72. Organisation qui utilise les technologies blockchain : France Blocktech, <http://www.franceblocktech.org>
73. PoC (*proof of concept* ou preuve de concept) est une démonstration de faisabilité, une réalisation courte ou incomplète d'une certaine méthode ou idée pour démontrer sa faisabilité. C'est une étape importante pour aboutir à un prototype pleinement fonctionnel.
74. FOMO, acronyme de l'anglais Fear Of Missing Out (peur de manquer quelque chose).
75. Lean Startup : concept développé en 2008 par Eric Ries sur la base de la pensée Lean dans des entreprises high-tech de la Silicon Valley. Cette approche repose sur la vérification de la validité des concepts, l'expérimentation scientifique et le design itératif. Elle permet de réduire les cycles de commercialisation des produits, de mesurer régulièrement les progrès réalisés, et d'obtenir des retours de la part des utilisateurs.
76. Certains consultants de la start-up Blockness (voir acteurs en fin d'ouvrage) sont très actifs sur ce sujet.
77. Lawrence Lessig (juriste américain), « Code is law, On Liberty in Cyberspace », *Harvard magazine*, janvier 2000, <http://harvardmagazine.com/2000/01/code-is-law-html>

78. Pour une explication très complète des aspects juridiques de la blockchain, voir Quinn DuPont et Bill Maurer, « Ledgers and Law in the Blockchain », *The King's Review*, 2015 : <http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/>
79. Voir l'excellent ouvrage de Jean-François Blanchette, *Burdens of proof, Cryptographic Culture and Evidence Law in the Age of Electronic Documents*, Hardcover, 2012.
80. La question de l'utilisation de la blockchain dans les opérations de règlement/livraison dans l'industrie financière illustre les bouleversements que cette technologie peut apporter : un registre décentralisé privé peut demain remplacer les dépositaires centraux tels que Euroclear, DTCC et autres, sous réserve de régler préalablement la question juridique du droit de propriété des titulaires de titres. Voir Pascal Bouvier, « Distributed Ledgers Part II : Clearing, Settlements and Legal frameworks » : <http://finiculture.com/distributed-ledgers-part-ii-clearing-settlements-and-legal-frameworks/>
81. Il est désormais possible d'enregistrer sur la blockchain la preuve horodatée, irréfutable et indélébile de l'existence d'un document sans avoir à en révéler le contenu. L'expérimentation proposée par *proof of existence* n'intègre évidemment pas le document lui-même dans le registre, mais une simple empreinte qui permet de prouver que le document existait à une époque donnée et qu'il est lié à une adresse précise.

## Chapitre 4

1. Source : Carlota Perez, « Technological Revolutions and Techno-economic Paradigms », *Technology governance*, janvier 2009 : <http://technologygovernance.eu/files/main//2009070708552121.pdf>
2. Jeremy Rifkin, essayiste américain, spécialiste de prospective (économique et scientifique). Jeremy Rifkin and the Foundation on Economic Trends : <http://www.foet.org/>
3. Arnaud Péchoux, société Wavestone : <https://www.wavestone.com/fr/>
4. <http://dontapscott.com/books/blockchain-revolution/>. C'est le 3<sup>e</sup> ouvrage significatif de Don Tapscott après *Digital Economy* en 1994 sur le travail et la production collaborative *via* les technologies récentes de communication comme Internet, et *Wikinomics : How Mass Collaboration Changes Everything* en 2006 où il traite de l'intelligence collaborative.
5. Citation de Hubert de Vauplane, avocat, extraite d'un article publié dans Finyear.
6. Extrait du rapport téléchargeable en fin d'ouvrage : « Blockchain : 5 propositions pour transformer les services financiers ».
7. Le libertarianisme ou libertarisme est une philosophie politique issue du libéralisme qui prône, au sein d'un système de propriété et de marché universel, la liberté individuelle en tant que droit naturel.
8. Économiste américain : <http://scholar.harvard.edu/rogoff>
9. <http://press.princeton.edu/titles/10798.html>
10. Par Sébastien Bourguignon (voir remerciements en fin d'ouvrage).
11. <http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>
12. <http://www.fondapol.org/wp-content/uploads/2016/06/083-SOUODOPLATOF-2016-05-26-webDEF.pdf>
13. Un pic des espérances exagérées peut être défini comme « un emballement médiatique qui aboutit à des attentes exagérées et non réalistes. Des start-up se créent pour développer et commercialiser des produits basés sur la nouvelle technologie » (source : Wikipédia).
14. Par Alain Brégy (voir remerciements en fin d'ouvrage).
15. Lire ce texte intégral : <https://medium.com/@beAchain/blockchain-comme-révolution-mais-révolution-de-quoi-8acc059bf316#.fb4ynqv44>

## Conclusion

1. La génération X regroupe les personnes nées entre 1966 et 1976 (environ), la génération Y, celles nées entre le début des années 1980 et le milieu des années 1990.
2. Philippe Herlin, économiste et auteur de *La Révolution du bitcoin et des monnaies complémentaires*.
3. <http://www.trustnomics.net>
4. Citation d'Alain Brégy (voir remerciements en fin d'ouvrage).