Consommation énergétique des technologies blockchain

Pierre Boulet

Université de Lille

Consommation énergétique des technologies blockchain

Pierre Boulet

Mis à jour le 5 novembre 2021

Nous expliquons dans cet article que la consommation d'énergie des technologies blockchains dépend principalement du protocole de consensus choisi. Si la preuve de travail (du Bitcoin) est extrêmement gourmande, il existe de nombreuses alternatives bien moins énergivores.

1 De quoi parle-t-on ?

Dans le rapport 1092 de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) [1], les auteurs proposent la définition suivante des technologies blockchains : « ce que l'on appelle par métonymie blockchains (ou chaînes de blocs) désigne des technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués (distributed ledgers), sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers. Dans leur diversité, les standards que recouvre ce concept visent à assurer le stockage, la conservation et la transmission d'informations de toute nature dans le cadre d'un réseau décentralisé, dépourvu d'intermédiaire ou d'organe central de contrôle. » Ces technologies permettent donc d'enregistrer des échanges d'information horodatés (par exemple des transactions) de manière sûre et inflasifiable sans tiers de confiance au sein d'un réseau de pairs. Pour assurer la confiance et la sécurité des informations, ces technologies reposent sur un assemblage de techniques informatiques : les réseaux pairs-à-pairs, la cryptographie et les algorithmes de consensus distribués.

Toutes ces techniques sont évidemment consommatrices d'énergie mais ce sont de loin les algorithmes de consensus distribués qui sont les plus problématiques de ce point de vue. Les réseaux pairs-à-pairs supposent un haut degré de réplication des informations et des calculs ; il faut donc multiplier par ce degré de réplication la consommation d'énergie d'un des nœuds du réseau (par exemple environ 250 Go de stockage sont nécessaires pour chaque nœud du réseau bitcoin au moment de l'écriture de cet article). Les opérations de chiffrement nécessaires pour chaîner les blocs et identifier les participants aux transactions sont aussi consommatrices d'énergie. La consommation d'énergie de ces deux composants (réseaux pairs-a-pairs et chiffrement) sont nécessaires mais restent dans des ordres de grandeurs habituels des systèmes

informatiques, à tel point qu'il n'existe pas aujourd'hui, à la connaissance de l'auteur, d'étude précise de ces coûts. Nous ne parlerons donc en détail dans la suite que de ces algorithmes de consensus, le lecteur est invité à se rapporter au rapport de l'OPECST précité ou à des ouvrages généraux sur les technologies blockchains [2, 3] pour plus d'informations sur leurs autres aspects.

On peut classer les technologies blockchains en plusieurs catégories :

— les technologies de blockchains publiques où n'importe qui peut participer au réseau ;
— les technologies de blockchains de consortium où seuls les membres du consortium peuvent participer, les données sont en général en accès limité aux membres du consortium mais peuvent être éventuellement lisibles publiquement ;
— les technologies de blockchains privées où une entité contrôle le réseau, on est alors très près des bases de données répliquées traditionnelles.

Ce sont les technologies de blockchains publiques qui nécessitent le plus de sécurité et qui font participer le plus grand nombre d'entités. C'est donc dans leur cas qu'on est obligé de recourir à des algorithmes de consensus particuliers qui innovent par rapport aux algorithmes de consensus classiquement utilisés dans les systèmes distribués (cloud computing, big data, etc). La complexité de ces algorithmes classiques (BFT, PAXOS, RAFT et leurs variantes) est connue et maîtrisée et ne conduit pas à des impacts environnementaux excessifs. Leur problème est le passage à l'échelle d'un réseau public de taille mondiale, ce qui les rend inapplicables pour les réseaux blockchains publics (Bitcoin compterait environ 11 000 nœuds actifs début 2020 selon [4], mais d'autres estimations donnent un nombre bien plus élevé). Nous ne parlerons donc dans la suite que des algorithmes de consensus utilisés dans les technologies de blockchains publiques.

2 Cas du Bitcoin

Le Bitcoin [5, 6] est le premier réseau de blockchain public et encore aujourd'hui la cryptomonnaie qui domine largement le marché. Cette domination repose sur le fait que depuis sa mise en place en 2009 et malgré la grande quantité de monnaie qu'il porte, le Bitcoin n'a jamais été attaqué avec succès. Cette très grande sécurité est la raison pour laquelle il a été conçu : pour résister à la censure d'un état et permettre des échanges monétaires le plus librement possible. Cette sécurité repose sur un grand nombre de facteurs : robustesse du SHA-256, redondance des calculs et du stockage, et sur son algorithme de consensus, *la preuve de travail* où, pour valider un bloc, les différents validateurs sont en compétition pour résoudre un problème cryptographique dont la difficulté est ajustée automatiquement pour qu'en moyenne, un bloc soit validé toutes les 10 min. Ce problème cryptographique sert à tirer au hasard le validateur du prochain bloc qui sera récompensé par l'émission de bitcoins. C'est pour cette raison qu'on appelle ces validateurs des mineurs, ils créent les nouveaux bitcoins par leur travail. Et c'est bien ce processus de minage qui est extrêmement gourmand en énergie. Ajoutons que le validateur est récompensé par la création de bitcoin, mais aussi par les commissions payées par les utilisateurs du réseau qui l'utilisent pour certifier leurs transactions. Pour des explications plus détaillées, voir les articles de Jean-Paul Delahaye [7-9].

Plusieurs études ont essayé de chiffrer la consommation d'énergie ou plus généra-

lement l'impact environnemental du Bitcoin [10-17] et au moins 2 sites web donnent des visualisations graphiques de la variation de cette consommation d'énergie au cours du temps [18, 19]. Les méthodes d'estimation varient entre ces articles ; les plus fines prennent en compte le mix énergétique dans les pays des différents mineurs mais toutes donnent des ordres de grandeur comparables : *le réseau Bitcoin a une consommation électrique en 2019 entre 30 et 90 TWh par an et a une empreinte carbone de 15 à 40 $MtCO_2$-eq, comparables à celle de pays comme l'Autriche, la Belgique ou le Danemark.* De plus l'augmentation du cours du bitcoin depuis fin 2020 augmente les récompenses accordées aux mineurs, et donc l'intensité de la compétition dans le minage. Plusieurs études confirment l'augmentation de l'impact environnemental du minage du bitcoin avec l'augmentation des cours [9, 20] avec des estimations d'une consommation annualisées de 80 à 130 TWh en mars 2021.

D'autres auteurs ont tenté la comparaison du coût énergétique du minage des cryptomonnaies et des métaux. Les auteurs de [21] estiment que le minage d'un US$ de cryptomonnaie produit à peu près la même quantité de gaz à effet de serre que celui d'un US$ d'or, de cuivre ou de platine, l'aluminium en produisant beaucoup plus. A contrario, l'étude [22] affirme que le bitcoin serait moins coûteux à produire que l'or. D'autres auteurs argumentent même que le bitcoin serait bon pour l'environnement [23] en argumentant sur sa valeur en tant que monnaie alternative au système bancaire, sur son intérêt dans la promotion de la production d'énergies renouvelables et sur des optimisations à venir. Toutes les études citées négligent les autres impacts environnementaux liés à l'infrastructure informatique utilisée, en particulier les impacts liés à la fabrication des ordinateurs plus ou moins spécialisés utilisés pour le minage (au sens du consensus). Or, le minage (physique cette fois-ci) des multiples métaux utilisés pour la fabrication des équipements électroniques compte pour une très grande part dans leur impact environnemental [24].

Le problème est que cet impact environnemental ne sert qu'à assurer la sécurité du système, et à rien d'autre. La puissance de calcul nécessaire pour attaquer par la force brutale le Bitcoin nécessite au moins la moitié de la puissance de minage (ou seulement 25 % pour certaines attaques particulières), ce qui est, par construction, prohibitif. Certains proposent de remplacer le problème cryptographique au cœur de la preuve de travail par un problème utile [25] mais l'une des solutions les plus évidentes est de remplacer la preuve de travail par un autre algorithme de consensus.

3 Alternatives à la preuve de travail

De nombreuses technologies de blockchains publiques reposent sur la preuve de travail. C'est le cas des nombreux dérivés du Bitcoin ainsi que de son plus grand concurrent, Ethereum. Cependant, des alternatives à la preuve de travail existent [26-29].

Les alternatives les plus courantes sont la preuve d'enjeu [30-33] et la preuve d'enjeu déléguée [34]. Dans la preuve d'enjeu, la probabilité d'être choisi comme validateur d'un bloc est proportionnelle à la quantité de cryptomonnaie possédée (et/ou à la durée de cette possession), et plus à la quantité de travail fourni (et donc d'électricité consommée). Par conséquent, la résistance aux attaques repose sur la valeur possédée (en cryptomonnaie) et pas sur la capacité de calcul mobilisée. Notons cependant que dans certaines variantes de la preuve d'enjeu, une preuve de travail reste utilisée mais avec une difficulté bien moins grande, et donc une consommation d'énergie très

significativement réduite. Dans la preuve d'enjeu déléguée, les participants élisent un petit nombre de validateurs (quelques dizaines) qui se coordonnent avec un algorithme simple. Ces deux familles d'algorithmes, comme d'autres, suppriment donc la source de la consommation excessive d'énergie de la preuve de travail.

Le choix d'un algorithme de consensus pour un réseau blockchain public repose sur plusieurs critères antagonistes : la sécurité, la scalabilité (capacité à passer à l'échelle mondiale), la rapidité, la décentralisation, et la consommation d'énergie. Cette dernière prend de plus en plus d'importance au point qu'Ethereum passe d'un algorithme de consensus reposant sur la preuve de travail à un algorithme reposant sur la preuve d'enjeu [35]. Dans [22], les auteurs estiment à 3 ou 4 ordres de grandeur le gain en consommation d'énergie en passant de la preuve de travail à la preuve d'enjeu. Des billets et rapport récents [36-38] estiment que les blockchains publiques n'utilisant pas la preuve de travail consomment entre 4 et 6 ordres de grandeur de moins d'électicité que le réseau bitcoin et que le gain par transaction peut même atteindre 8 ordres de grandeur pour devenir négligeable (de l'ordre de la consommation du chargement d'une page web ou de l'envoi d'un mail par exemple).

Dans le contexte des crypto-monnaies la sécurité reste encore l'objectif principal et une façon intéressante de la mesurer est d'intégrer la quantité d'actifs sécurisés au cours du temps. Selon cette mesure, qu'on appelle la résilience publique, la preuve de travail du bitcoin est de loin la plus résilente sur ces 11 années d'existance. L'avenir nous dira si une crypto-monnaie à base de preuve d'enjeu (déléguée ou non) réussira à atteindre une résilence publique comparable. Pour une comparaison plus technique de la sécurité des différents protocoles de consensus, voir [26-28].

4 Conclusion

La consommation d'énergie excessive de certaines technologies blockchains publiques comme le Bitcoin ou Ethereum n'est pas une fatalité. Cette consommation de l'ordre de celle d'un petit pays européen vient de l'algorithme de consensus utilisé : la preuve de travail. Depuis l'apparition du Bitcoin en 2008, de nouveaux algorithmes de consensus ont été proposés qui offrent un autre compromis entre la sécurité, la décentralisation et la consommation d'énergie. Avec la migration en cours d'Ethereum vers la preuve d'enjeu, c'est une étape très importante qui sera franchie vers des technologies blockchain plus durables.

Notons enfin que de nombreuses applications des technologies blockchain existent au delà des cryptomonnaies et qu'elles peuvent reposer sur d'autres compromis entre sécurité, décentralisation et consommation d'énergie. Un exemple de tel projet est l'infrastructure européenne de services sur la blockchain (EBSI, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi) dédiée aux services publics transfrontaliers.

Remerciements

Merci à Jean-Paul Delahaye, François-Xavier Thoorens, Fabrice Flipo, Olivier Ridoux et Perrine de Coëtlogon pour leurs commentaires très constructifs sur cet article.

Références

[1] Valéria Faure-Muntian, Claude de Ganay et Ronan Le Gleut. *Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies*. 1092. Assemblée nationale, 20 juin 2018, p. 189. URL : http://www.assemblee-nationale.fr/dyn/15/dossiers/enjeux_technologiques_blockchains_rap-info (visité le 26/12/2019).

[2] Primavera De Filippi. *Blockchain et cryptomonnaies*. Que sais-je ? puf, 19 sept. 2018. 128 p. ISBN : 978-2-13-081145-9. URL : https://www-cairn-info.ressources-electroniques.univ-lille.fr/blockchain-et-cryptomonnaies--9782130811459.htm (visité le 26/01/2020).

[3] Imran Bashir. *Mastering Blockchain : Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition*. 2nd Revised edition. Birmingham : Packt Publishing, 30 mar. 2018. 656 p. ISBN : 978-1-78883-904-4. URL : http://univ.scholarvox.com.ressources-electroniques.univ-lille.fr/catalog/book/docid/88842714.

[4] *Global Bitcoin nodes distribution*. URL : https://bitnodes.earn.com/ (visité le 19/01/2020).

[5] Satoshi Nakamoto. *Bitcoin : A peer-to-peer electronic cash system*. 2008. URL : https://bitcoin.org/bitcoin%20pdf.

[6] Andreas Antonopoulos. *Mastering Bitcoin*. Independently published, 8 mai 2019. 284 p. ISBN : 978-1-09-722800-3.

[7] Jean-Paul Delahaye. *La dépense électrique des crypto-monnaies | Bitcoin.fr*. URL : https://bitcoin.fr/la-depense-electrique-des-crypto-monnaies/ (visité le 26/12/2019).

[8] Jean-Paul Delahaye. *Ne nions pas le problème électrique du Bitcoin | Bitcoin.fr*. URL : https://bitcoin.fr/ne-nions-pas-le-probleme-electrique-du-bitcoin/ (visité le 26/12/2019).

[9] Jean-Paul Delahaye. « La folie électrique du Biticoin ». In : *Pour la science* 484 (fév. 2018), p. 80-84.

[10] Harald Vranken. « Sustainability of bitcoin and blockchains ». In : *Current Opinion in Environmental Sustainability*. Sustainability governance 28 (1er oct. 2017), p. 1-9. ISSN : 1877-3435. DOI : 10.1016/j.cosust.2017.04.011. URL : http://www.sciencedirect.com/science/article/pii/S1877343517300015 (visité le 29/09/2019).

[11] Alex de Vries. « Bitcoin's Growing Energy Problem ». In : *Joule* 2.5 (16 mai 2018), p. 801-805. ISSN : 2542-4351. DOI : 10.1016/j.joule.2018.04.016. URL : http://www.sciencedirect.com/science/article/pii/S2542435118301776 (visité le 26/12/2019).

[12] Michel Zade et al. « Is Bitcoin the Only Problem ? A Scenario Model for the Power Demand of Blockchains ». In : *Frontiers in Energy Research* 7 (2019). ISSN : 2296-598X. DOI : 10.3389/fenrg.2019.00021. URL : https://www.frontiersin.org/articles/10.3389/fenrg.2019.00021/full (visité le 26/12/2019).

[13] Michel Rauchs et al. *2nd Global Cryptoasset Benchmarking Study*. SSRN Scholarly Paper ID 3306125. Rochester, NY : Social Science Research Network, 12 déc. 2018. URL : https://papers.ssrn.com/abstract=3306125 (visité le 26/12/2019).

[14] Hass McCook. *The Cost & Sustainability of Bitcoin (August 2018)*. URL : https://www.academia.edu/37178295/The_Cost_and_Sustainability_of_Bitcoin_August_2018_ (visité le 26/12/2019).

[15] Christian Stoll, Lena Klaaßen et Ulrich Gallersdörfer. « The Carbon Footprint of Bitcoin ». In : *Joule* 3.7 (17 juil. 2019), p. 1647-1661. ISSN : 2542-4785, 2542-4351. DOI : 10.1016/j.joule.2019.05.012. URL : https://www.cell.com/joule/abstract/S2542-4351(19)30255-7 (visité le 06/10/2019).

[16] Susanne Köhler et Massimo Pizzol. « Life Cycle Assessment of Bitcoin Mining ». In : *Environmental Science & Technology* (20 nov. 2019). ISSN : 0013-936X. DOI : 10.1021/acs.est.9b05687. URL : https://doi.org/10.1021/acs.est.9b05687 (visité le 02/12/2019).

[17] Alex de Vries. « Bitcoin's energy consumption is underestimated : A market dynamics approach ». In : *Energy Research & Social Science* 70 (1er déc. 2020), p. 101721. ISSN : 2214-6296. DOI : 10.1016/j.erss.2020.101721. URL : http://www.sciencedirect.com/science/article/pii/S2214629620302966 (visité le 05/01/2021).

[18] *Bitcoin Energy Consumption Index*. Digiconomist. URL : https://digiconomist.net/bitcoin-energy-consumption (visité le 29/09/2019).

[19] *Cambridge Bitcoin Electricity Consumption Index (CBECI)*. URL : https://www.cbeci.org/ (visité le 03/11/2019).

[20] Alex de Vries. « Bitcoin boom : What rising prices mean for the network's energy consumption ». In : *Joule* 5.3 (17 mar. 2021). Publisher : Elsevier, p. 509-513. ISSN : 2542-4785, 2542-4351. DOI : 10.1016/j.joule.2021.02.006. URL : https://www.cell.com/joule/abstract/S2542-4351(21)00083-0 (visité le 25/03/2021).

[21] Max J. Krause et Thabet Tolaymat. « Quantification of energy and carbon costs for mining cryptocurrencies ». In : *Nature Sustainability* 1.11 (nov. 2018), p. 711-718. ISSN : 2398-9629. DOI : 10.1038/s41893-018-0152-7. URL : http://www.nature.com/articles/s41893-018-0152-7 (visité le 19/01/2020).

[22] Luisanna Cocco, Roberto Tonelli et Michele Marchesi. « An Agent Based Model to Analyze the Bitcoin Mining Activity and a Comparison with the Gold Mining Industry ». In : *Future Internet* 11.1 (jan. 2019), p. 8. DOI : 10.3390/fi11010008. URL : https://www.mdpi.com/1999-5903/11/1/8 (visité le 19/01/2020).

[23] Laurent Benichou. *Bitcoin, a gift to environment*. Medium. 10 mar. 2021. URL : https://laurentbenichou.medium.com/bitcoin-a-gift-to-environment-f7e676107dd9 (visité le 11/03/2021).

[24] *Lean ICT - Les impacts environnementaux du Numérique*. The Shift Project. URL : https://theshiftproject.org/lean-ict/ (visité le 19/01/2020).

[25] P. Fairley. « Blockchain world - Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous ». In : *IEEE Spectrum* 54.10 (oct. 2017), p. 36-59. DOI : 10.1109/MSPEC.2017.8048837.

[26] Z. ZHENG et al. « An Overview of Blockchain Technology : Architecture, Consensus, and Future Trends ». In : *2017 IEEE International Congress on Big Data (BigData Congress)*. 2017 IEEE International Congress on Big Data (BigData Congress). Juin 2017, p. 557-564. DOI : 10.1109/BigDataCongress.2017.85.

[27] D. MINGXIAO et al. « A review on consensus algorithm of blockchain ». In : *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Oct. 2017, p. 2567-2572. DOI : 10.1109/SMC.2017.8123011.

[28] L. M. BACH, B. MIHALJEVIC et M. ZAGAR. « Comparative analysis of blockchain consensus algorithms ». In : *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Mai 2018, p. 1545-1550. DOI : 10.23919/MIPRO.2018.8400278.

[29] Wenbo WANG et al. « A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks ». In : *IEEE Access* 7 (2019), p. 22328-22370. ISSN : 2169-3536. DOI : 10.1109/ACCESS.2019.2896108. arXiv : 1805.02707. URL : http://arxiv.org/abs/1805.02707 (visité le 05/11/2021).

[30] Sunny KING et Scott NADAL. « PPCoin : Peer-to-peer crypto-currency with proof-of-stake ». In : *self-published paper, August* 19 (2012).

[31] *Proof-of-stake (PoS)*. ethereum.org. URL : https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (visité le 26/03/2021).

[32] *Proof-of-Stake in Blockchain Technology : All You Need To Know*. URL : https://proofofstake.com/ (visité le 27/12/2019).

[33] *What Is Proof of Stake ?* ConsenSys. URL : https://consensys.net/blog/blockchain-explained/what-is-proof-of-stake/ (visité le 26/03/2021).

[34] Daniel LARIMER. *Bitshares - Delegated Proof-of-Stake Consensus*. URL : https://bitshares.org/technology/delegated-proof-of-stake-consensus/ (visité le 26/12/2019).

[35] *The Eth2 upgrades*. ethereum.org. URL : https://ethereum.org/en/eth2/ (visité le 26/03/2021).

[36] *Combien d'énergie consomment les cryptomonnaies comme le Bitcoin ?* Adan. 29 sept. 2021. URL : https://adan.eu/article/classification-protocoles-blockchain-empreinte-energetique (visité le 30/09/2021).

[37] T. Q. TEZOS. *Proof of Work vs. Proof of Stake : the Ecological Footprint*. Medium. 16 mar. 2021. URL : https://medium.com/tqtezos/proof-of-work-vs-proof-of-stake-the-ecological-footprint-c58029faee44 (visité le 24/03/2021).

[38] *Energy Efficiency of Blockchain Technologies*. The European Union Blockchain Observatory & Forum, 30 sept. 2021. URL : https://www.eublockchainforum.eu/sites/default/files/reports/Energy%20Efficiency%20of%20Blockchain%20Technologies_1.pdf (visité le 30/09/2021).