# La Blockchain, une philosophie crypto-anarchiste

**Author :** Thibaut Gress

**Categories :** Science & Techno

**Date :** 10 mars 2019

**ANALYSE : Les *Bitcoins* et autres crypto-monnaies, qui reposent sur le principe de la *Blockchain*, sont l'application d'un certain rapport politique voire idéologique au monde, explique le philosophe Thibaut Gress. La *blockchain* substitue l'anonymat du nombre à l'incarnation de l'autorité. Ce crypto-anarchisme veut liquider l'*auctoritas* en son sens classique au profit d'un monde horizontal et sans frontière.**

---

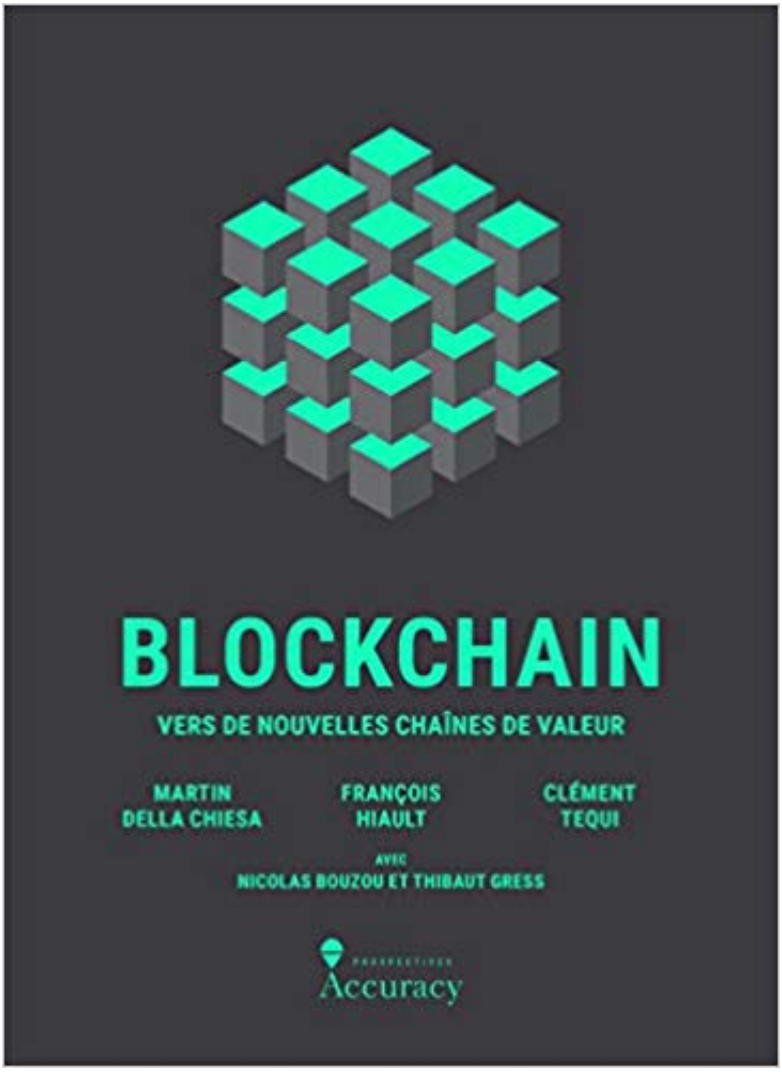
*Ancien élève de l'Ecole normale supérieure, agrégé et docteur en Philosophie,* **Thibaut Gress** *dirige la revue* Actu-Philosophia *et enseigne la philosophie au lycée Charles Péguy. Auteur de plusieurs ouvrages, il a notamment publié* Descartes et la précarité du monde *(éd. CNRS, 2012),*La philosophie au risque de l'intelligence extraterrestre *(avec Paul Mirault, éd. Vrin, 2016),* L'œil et l'Intelligible *(éd. Kimé, 2016) et dernièrement* Blockchain, vers de nouvelles chaînes de valeur *(collectif, éd. Prospectives Accuracy, 2018).*

---

Pour qui s'intéresse à l'actualité économique et technologique, plus un jour ne se passe sans qu'un organe de presse n'annonce la mort du Bitcoin, voire plus généralement celle des cryptomonnaies, à telle enseigne que le journal *Le Temps* eut l'heureuse idée de titrer le 20 novembre 2018 : «Le Bitcoin est mort. Encore [1]». Raillant le nombre anormalement élevé de faireparts médiatiques claironnant le décès de la célèbre «monnaie»,*Le Temps* dénombra pas

moins de 317 articles affirmant prophétiquement sa disparition imminente, et ce quelques semaines avant que les bureaux de tabac soient habilités à vendre des coupons convertibles en bitcoins, en plus des processus classiques d'acquisition sur les plateformes numériques.

**Lire aussi :** *Ce que l'argent ne saurait acheter* **(Jean-Pierre Dupuy)**




A cela s'est ajoutée dès juillet 2018 une campagne de presse visant à dénoncer le caractère excessivement énergivore de la technologie sous-tendant les cryptomonnaies, à savoir la technologie *Blockchain*, laquelle suppose en effet une puissance de calcul considérable particulièrement coûteuse en énergie. A titre d'illustration, nombre de publications ont indiqué que le fonctionnement du *Bitcoin* impliquait une consommation d'électricité égale à celle de la Hongrie en une année [2], estimation toutefois sujette à caution en raison de l'absence de données précises et quantifiables sur le sujet.

De là un discours médiatique volontiers anxiogène en la matière, voire teinté de moralisme, qui vise moins à expliquer les enjeux concrets de cette nouvelle technologie qu'à dissuader les lecteurs et les auditeurs d'y avoir recours. Cela peut surprendre car, parallèlement à ces innombrables articles, se développe toute une réflexion au sein des entreprises sur sa portée et ses vertus, réflexion dont le rapport du *Capgemini Research Institute* [3] de 2015 s'était fait l'écho en annonçant que, d'ici 2025, une grande majorité d'entreprises auront fait appel à cette technologie pour garantir et sécuriser leurs échanges à l'échelle mondiale.

**Lire aussi :** *Levinas et les robots* **(Julien de Sanctis)**

Une sorte de schizophrénie s'est ainsi installée à l'endroit de la *Blockchain* en général, et du symbole du *Bitcoin* en particulier, schizophrénie parfaitement résumée par l'attitude de Jamie Dimon, PDG de JPMorgan ; le 20 septembre 2017, il lançait en effet une diatribe sévère contre le *Bitcoin*, le qualifiant de «fraude» et d'«arnaque à grande échelle», et annonçant à ses employés qu'il licencierait tous ceux qui s'essaieraient à échanger cette crypto-monnaie. Mais, en février 2017, la même holding financière s'alliait avec Microsoft pour lancer l'*Enterprise Ethereum Alliance*, une association à but non lucratif regroupant de très grands groupes (on y trouve plus de 150 membres tels que Toyota, BBVA, Samsung, etc.) et visant à «développer la confidentialité, la souplesse et la sécurité» d'Ethereum, blockhain dont l'une des applications les plus célèbres est la crypto-monnaie *Ether*. Fin 2018, on apprenait en outre que JPMorgan souhaitait «tokeniser» ses lingots d'or, c'est-à-dire sécuriser les données concernant ces derniers mais aussi pouvoir procéder à des échanges se dispensant d'intermédiaires, en l'occurrence de courtiers.

Comprendre les contradictions apparentes que charrient ces quelques exemples introductifs suppose d'investiguer le fonctionnement d'une technologie révolutionnaire apparue en 2008 en même temps que le *Bitcoin*, et les potentialités qu'elle détient, sans pour autant statuer sur l'avenir : il est en effet très difficile de prédire quel sera son développement réel ni sa capacité à surmonter les obstacles énergétiques et idéologiques qui se dressent devant elle. Paraît en revanche certain ce qu'avait noté le très médiatique et très jeune Vitalik Buterin, à savoir qu'un trop grand nombre d'entreprises, grisées par la nouveauté de la chose, se sont lancées dans la course sans avoir d'objectifs ni même de besoins précis, avec la seule crainte de passer à côté d'une mode séduisante, précipitation qui put occasionner de grandes et précoces déceptions et qui ne furent peut-être pas pour rien dans l'hallali médiatique des dernières années.

## Présentation rapide de la technologie *blockchain* : l'exigence de certification

Commençons donc par présenter le principe sous-tendant la blockchain, dont la traduction en français est chaîne de blocs. De manière basique, elle peut être pensée comme une base de données où les informations envoyés par les utilisateurs sont vérifiées à intervalle régulier et, partant, certifiées. C'est une technologie qui permet de stocker et transmettre des informations de manière transparente, sécurisée et sans organe central de contrôle, la décentralisation étant sans

doute l'élément décisif du processus. Métaphoriquement, on peut la décrire comme un registre contenant l'historique de tous les échanges réalisés entre les utilisateurs depuis la création de la chaîne.

Partant, alors qu'internet transfère des paquets de données, la *Blockchain* enregistre les données dans un registre ouvert à tous, car distribué sur un grand nombre d'ordinateurs. Néanmoins, certaines blockchains sont publiques, et ainsi accessibles à tout «individu» désireux de devenir membre du réseau, tandis que d'autres sont privées réservant leur accès à certains acteurs spécifiques. Grâce à elle peuvent être effectués des transferts d'actifs, peuvent être exécutés automatiquement des contrats – appelés *Smart Contracts* – ou encore obtenues des données sur la traçabilité d'actifs ou de produits commerciaux. L'enregistrement des données peut être utilisé selon de multiples directions, l'une des plus impressionnantes étant celle de la garantie des cadastres : le Honduras a récemment fait appel à un enregistrement certifié dans la blockchain pour garantir les registres cadastraux et les soustraire ainsi à la corruption galopante.

Plus techniquement parlant, la décentralisation de cette technologie signifie qu'elle n'est pas hébergée par un serveur unique mais qu'elle est partagée par tous ses utilisateurs, aucun ne disposant donc d'un pouvoir central capable de contrôler l'ensemble ; parmi les utilisateurs se trouvent de «nœuds» capables de «miner», c'est-à-dire de certifier en vertu de la puissance de calcul de leur ordinateur la validité d'une transaction et donc du bloc conservant la trace de celle-ci. Le bloc peut ainsi être défini comme l'agglomération de plusieurs opérations valides, et le fait de miner permet de valider la création d'un nouveau bloc grâce à la puissance de calcul de l'ordinateur, et c'est cette puissance de calcul que d'aucuns jugent excessivement énergivore.

## L'idéal *trustless*

La technologie *Blockchain* se présente comme une technologie *trustless,*comme une technologie permettant de se dispenser de la confiance dans le cadre des transactions ; cela tient au fait que toute procédure fondée sur la confiance est faillible, précaire, incertaine. Parler de confiance, c'est aussitôt envisager la possibilité de la *rupture* de confiance, prendre en compte l'éventualité d'une faillite de ce en quoi avait été placée la confiance. Plus généralement, nous pouvons considérer qu'*il n'y a de confiance que là où il y a incertitude et relative précarité de la relation* : autrui peut être défaillant, ne pas tenir sa parole, le temps peut corrompre son engagement, celui en qui j'avais placé ma confiance peut aussi soudainement mourir et, au-delà de l'échelle individuelle, l'autorité souveraine qu'est l'État peut se révéler plus faible que prévu ; même envers Dieu, l'homme peut rompre sa confiance – définition du péché. En d'autres termes, *il n'y a de sens à parler de confiance que là où l'incertitude liée à la faillibilité de l'individu ou du système demeure possible et envisageable*. Cela revient à dire que l'exigence de garantie et d'assurance est incompatible avec la confiance, celle-ci ne pouvant s'exercer qu'à la condition que l'on ait renoncé à exiger la présence de celles-là.

Il se trouve que la technologie *Blockchain* se prétend *trustless* donc sans confiance requise ; à

partir du moment où la confiance implique la précarité de la relation, on peut par contraposition dire qu'une relation fiable implique l'inutilité de la confiance. Prenons l'application des *bitcoins* pour comprendre cela : à chaque fois qu'un nœud envoie des *bitcoins* à un autre nœud, la transaction est sécurisée en même temps que certifiée à l'aide de l'envoi d'une clé cryptographique dont le déchiffrement permet de confirmer en retour ladite transaction. Or, un tel procès de chiffrement-déchiffrement (le chiffrement est une technique de cryptographie par laquelle on rend impossible l'accès au sens d'un document sans la clé) est répété un nombre indéfini de fois par les différents nœuds du réseau, la transaction recevant ainsi un nombre croissant de confirmations au cours du temps ; cela signifie donc que la technologie *blockchain* ne fait pas tant appel à la confiance qu'elle ne permet de *certifier* la validité de l'échange en la *confirmant* à chaque fois. Elle est, en théorie du moins, *trustless*. Dès lors, le domaine de la *fermeté* impliqué par la *confirmation* substitue à la confiance prise *stricto sensu* le cadre de l'assurance et de la certitude. S'insérer dans la chaîne permet ainsi de s'extraire de la confiance qui est toujours un pari et d'y substituer une forme de *savoir* en ceci qu'aucune technologie connue à l'heure actuelle n'est davantage certifiante que celle rendue possible par la technologie.

S'opèrent de ce fait deux déplacements d'importance, l'un visible, l'autre plus indirect.

- Le premier est celui de la neutralisation de la faillibilité inhérente à la confiance ; l'idéal *trustless* n'est pas une condamnation de la confiance comme telle mais bien plutôt la tentative de trouver une parade à la précarité structurelle de celle-ci.
- La certification se substituant à la confiance procède d'une réitération indéfinie de la confirmation de la validité de la transaction ; c'est donc la *quantité* de confirmations qui cimente la certification et qui met fin à l'*autorité qualitative d'un organe central*. Pour le dire autrement, le *quantitatif se substitue au qualitatif*, la qualité des agents n'étant ici d'aucune importance, contrairement au nombre d'itération de la confirmations.

## Soubassement anarchique de la *blockchain* : le crypto-anarchisme

Les deux points précédents méritent d'être mis en perspective ; loin de n'être qu'une technologie, la *blockchain* est l'application concrète et efficiente d'un certain rapport politique voire idéologique au monde, rapport parfaitement assumé par ses promoteurs.

Le premier point saillant porte sur la représentation des organes centraux fiduciaires ; en cherchant un moyen de soustraire des transactions de toute nature au contrôle centralisé, les concepteurs de cette technologie ont agi à partir d'une représentation négative de ces organes, refusant donc la légitimité de l'autorité politique, bancaire, et même législative. Au fond, se joue une volonté de liquider l'*auctoritas* en son sens classique et de liquider un monde verticalisé au sein duquel des différences de compétences légitimeraient un système hiérarchique de pouvoir, de contrôle et d'organisation. Contre ce monde verticalisé est promu un univers horizontal où n'existent plus que des différences intensives de puissance de calcul, de chiffrement/déchiffrement, aucune entité du réseau n'étant plus *légitime* qu'une autre pour certifier la validité d'une transaction.

Structurellement parlant, la *blockchain* substitue l'anonymat du nombre à l'incarnation de l'autorité, et évacue l'idée d'une différenciation qualitative entre les êtres, au moins quant à la souveraineté et à la décision. Chacun est aussi souverain que les autres, l'accumulation seule pouvant engendrer des différences au sein de la chaîne.

**Lire aussi :** *Menace numérique : Big Mother is watching you* **(Philippe Granarolo)**

Cela permet de cerner la nature de la philosophie inhérente à cette technologie ; il s'agit d'une philosophie anarchiste ou, plus exactement encore, d'une philosophie *crypto-anarchiste*, proposant d'utiliser les techniques de cryptographie pour échapper dans le cadre du *cyber-espace* au contrôle et à la maîtrise des États. Dotée d'un Manifeste [4] parodiant par sa première phrase le *Manifeste du Parti communiste* de Marx et Engels et rédigé par l'ingénieur informaticien Timothy C. May décédé prématurément en décembre 2018, cette philosophie craint par-dessus tout la puissance de contrôle des États et recherche les conditions d'une préservation de l'intimité à travers des moyens de soustraction au contrôle chaque jour croissant qu'exerce la puissance publique sur les citoyens. Voulant par des protocoles cryptographiques «modifier en intégralité la nature de la réglementation gouvernementale, la capacité de taxer et de contrôler les interactions économiques, mais aussi la capacité de conserver des informations secrètes» [5], cette pensée élabore les conditions d'un «devenir-invisible» des individus au sein du*cyber-espace* afin de contourner l'utilisation étatique de la surveillance informatique.

Classiquement anarchistes par leur refus radical d'une autorité supérieure à celle de l'individu – qu'elle fût politique, religieuse, traditionnelle ou encore sociale –, ces penseurs élaborent une réponse non politique au problème politique de l'hyperpuissance ou, plus exactement, de l'hypercontrôle étatique que rend aujourd'hui possible la technologie informatique. Pour le dire autrement, la *blockchain* apparaît comme une *solution technologique d'un problème politique et même anthropologique*. Il faut ajouter à cette philosophie crypto-anarchiste quelque chose de l'ordre du refus de la séparation, de la limite, de ce que les Grecs appelaient un *horizon*. Le monde de la technologie *blockchain* est un monde sans frontières, délivré des différences qualitatives inhérentes au réel, délivré des territoires, des lois positives, du droit, de la surveillance de la puissance publique, autant d'éléments distinguant le crypto-anarchisme de l'anarcho-capitalisme qui nécessite une sorte de législation positive destinée au moins à faire respecter les contrats [6]. Enfin, jusqu'à un certain point, ce monde est délivré des limites de l'individualité et de la singularité puisque seuls peuvent échanger des pseudonymes sans identité délimitante ni déterminante.

## *Blockchain* et posthumanité

Ces principes théoriques, trouvant leur débouché dans une technologie appliquant concrètement et fidèlement ces derniers, doivent ainsi être pensés selon les modifications concrètes de la vie sociale et politique qu'ils s'apprêtent consciemment à introduire. Outre les aspects économiques

consistant à rendre obsolètes – à supposer que la technologie *Blockchain* soit pérenne – bien des métiers, l'organisation sociale pourrait connaître de profonds bouleversements, ne serait-ce que par la réduction drastique de la place de la confiance au sein des relations humaines. Non seulement pourraient disparaître les professions destinées à certifier les transactions – pensons aux notaires – mais, de surcroît, certaines révolutions récentes dans les modes de vie seraient elles-mêmes frappées d'obsolescence plus rapidement que prévu ; le cas le plus emblématique concerne Uber qui est tout à la fois le symbole de la mise en contact relativement directe des clients et des professionnels et en même temps l'ersatz de l'ancien monde dans la mesure où la plateforme d'Uber demeure contrôlée par un organe central. Là-contre, un système comme Arcane City supprime le contrôle central et donc supprime tout intermédiaire en vue de créer une relation vraiment directe entre l'usager et le conducteur, ce que condense le célèbre slogan : «Uber t'es foutu, la blockchain est dans la rue».

Le monde que dessinent les blockchains est donc un monde qui cherche à conjurer l'incertitude, le contingent ; mais, ce faisant, c'est le domaine propre de l'humain qui s'efface progressivement au profit de procédures automatisées fondées non sur la délibération – laquelle suppose que l'on ait affaire au contingent – mais bien plutôt sur une *certification* d'autant plus forte qu'elle aura réussi à éliminer l'incertitude que fait toujours régner l'intervention de la délibération humaine, domaine spécifique des hommes ainsi que l'avait relevé Aristote [7].

**Lire aussi :** *Les marivaudages du réel et du virtuel* **(Bruno Jarrosson)**

A cet égard, les blockchains doivent être pensées comme un élément crucial de la post-humanité qui vient. Il est vrai que cette technologie semble plus extérieure et moins intrusive que celles que véhicule le trans- ou post-humanisme, et paraît de ce fait moins spectaculaire ; pourtant, en rendant caduques deux éléments déterminants du cadre humain – confiance et délibération – elle transforme en profondeur ce que l'on entend par «humanité» et, si elle n'affecte pas sa constitution biologique, elle n'en atténue pas moins sa dimension sociale et politique. De ce point de vue, la technologie *blockchain* ne soustrait pas tant l'homme au contrôle étatique et centralisé qu'elle ne cherche à libérer l'homme de l'humanité, qu'elle ne cherche à le libérer du fardeau d'être lui-même et d'entretenir des relations incertaines. Dans ces conditions, la question n'est sans doute plus de se demander *où* va l'homme mais bien plutôt de déterminer *si c'est encore un homme*qui y va.

**[1]« Le Bitcoin est mort. Encore », *Le Temps*, 20 novembre 2018.** https://www.letemps.ch/economie/bitcoin-mort
**[2]Une étude d'octobre 2018 parue dans *Nature*prenait la consommation de l'Autriche comme élément comparatif.**
**[3]Le rapport est consultable ici :** https://www.capgemini.com/fr-fr/news/la-blockchain-technologie-incontournable-des-chaines-logistiques-mondiales-dici-2025/
**[4]**https://www.theyliewedie.org/ressources/biblio/fr/C.May_Timothy_-_Le_manifeste_crypto_anarchiste.html
**[5]**http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html
**[6]Nous nous permettons de renvoyer à notre analyse de la singularité du crypto-anarchisme qu'il convient de distinguer de l'anarcho-capitalisme et du monétarisme dans l'ouvrage collectif suivant : Martin della Chiesa, François Huault, Clément Téqui (dir.), *Blockchain.Vers de nouvelles chaînes de valeur*, Chapitre B, Accuracy, 2018, pp. 41-65.**
**[7]Aristote*, Éthique à Nicomaque*, 1112a34-35**