L'État peut-il rester tiers garant à l'heure de la blockchain ?

Jean-Gabriel Ganascia

L'État peut-il rester tiers garant à l'heure de la *blockchain* ?

Jean-Gabriel Ganascia[1]

Crypto-anarchie

Pour apprécier la façon dont la *blockchain* — « chaîne de blocs » en français — met en défaut le rôle de l'État comme tiers garant, il n'est pas inutile de commencer par en faire l'archéologie car celle-ci renvoie à une forme d'anarchie, de dislocation des pouvoirs qui semble de prime abord conduire à un affaiblissement de l'État.

Les premières idées paraissent en 1988, un an avant les esquisses du web formulées au CERN, à Genève, par Tim Berners-Lee, et sont émises ensuite sur le réseau Internet et dans les conférences « Crypto'88 » et « Hackers », pour un public de « cyberpunks » qui aspirent à changer l'ordre établi au moyen de programmes informatiques. Des ingénieurs, férus de science-fiction, rêvent de protocoles cryptographiques complexes rendus possible par le perfectionnement des moyens de calcul, et grâce auxquelles les individus et les groupes communiqueront et interagiront de façon totalement anonyme. Selon eux, il s'ensuivra une modification des régulations gouvernementales, en particulier de la capacité des États à contrôler les échanges économiques et à lever l'impôt. De même, en aidant à tenir l'information secrète, cela affectera la confiance et la réputation sur laquelle elle se fonde. Autrement dit, la trame sur laquelle se construit le tissu social en sera transformée. Symptomatique de cet état d'esprit, le *manifeste crypto anarchiste*[2] de Timothy May, ingénieur et chef scientifique dans la société de fabrication de microprocesseurs Intel, commence par ces mots qui font écho au manifeste du parti communiste : « Un spectre hante le monde moderne,

[1] Professeur à la faculté des sciences de Sorbonne Université, membre senior de l'institut universitaire de France, président du comité d'éthique du CNRS
[2] https://www.activism.net/cypherpunk/crypto-anarchy.html

le spectre de la crypto anarchie ». Paru en 1992, un an avant le navigateur *Mosaic* qui va donner son essor au web, ce petit texte d'une page annonce une ère nouvelle où l'emploi généralisé de méthodes cryptographiques conduira à une désintégration sociale due à l'existence d'un marché parallèle, en partie criminel, qui échappera à l'État. En cela, la crypto anarchie revendiquée par Timothy May est non seulement une anarchie sous un faux nez, comme l'avait été en leur temps le cryptocommunisme au communisme ou le crypto-maoïsme au maoïsme, mais aussi une mise à disposition de tous des protocoles cryptographiques, sans égard aux prérogatives traditionnelles des États sur ces matières.

Naissance des crypto-monnaies

Il a fallu attendre 20 ans, et plusieurs essais infructueux, dont la *b-money* de Wei Dai en 1999 et le *bitgold* décrit en 2005 par Nick Szabo, pour que paraisse enfin, en 2008, un article[3] publié sous le pseudonyme Satoshi Nakamoto[4], qui pose les fondements théorique d'une crypto-monnaie fiable s'inspirant des principes de la crypto-anarchie. L'année d'après un logiciel en accès libre mit en œuvre informatiquement cette crypto-monnaie, le *bitcoin*, qui depuis a pris l'essor considérable qu'on lui connaît. Comme toute monnaie[5], elle repose sur l'établissement d'un lien de confiance entre ses détenteurs. Cependant, là où les monnaies traditionnelles recourraient à un tiers qui se portait garant de leur solvabilité, par exemple un prince, une banque, un État, par l'intermédiaire d'une banque centrale, ou éventuellement, comme pour l'Euro, une entité supranationale, dans le cas du *bitcoin*, cela se fonde sur l'établissement d'une confiance distribuée collectivement sur l'ensemble de la société grâce à un livre de compte public que tous peuvent consulter librement, sans être en mesure de le falsifier, et qui pourtant garantit l'anonymat des transactions. C'est ce livre de compte public que réalise la *blockchain*.

Plus précisément, pour qu'une crypto-monnaie inspire confiance, il faut certifier les échanges qu'elle permet en assurant que chaque unité de compte de cette monnaie ne puisse être

---

[3] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, http://www.bitcoin.org/bitcoin.pdf

[4] Jusqu'à présent, et en dépit de revendications fantaisistes, comme celle de Craig Wright en 2016, personne ne sait qui se cache derrière ce pseudonyme.

[5] Voir sur ce sujet Michel Aglietta, Pepita Ould Ahmed et Jean-François Ponsot, *La Monnaie : Entre dettes et souveraineté*, Odile Jacob, 2016

dépensée plusieurs fois et qu'elle n'ait pas été introduite frauduleusement, par des faux monnayeurs. Avec les monnaies physiques, pièces ou billets de banque, c'est facile, à condition d'être en mesure d'en vérifier l'authenticité. Avec les monnaies virtuelles, c'est plus délicat, car on peut dupliquer, sans coût, n'importe quelle information.

La *blockchain* résout ce problème grâce à des techniques cryptographiques, en assurant à chaque détenteur de *bitcoins* que l'argent qui est en sa possession est authentique et, surtout qu'il est bien à lui, en ce sens qu'il n'a pas été donné à d'autres et qu'il ne pourra pas l'être sans son consentement, sans pour autant dévoiler l'identité de ceux qui en ont été les possesseurs avant lui.

L'engouement actuel pour le *bitcoin* signifie que des acteurs non étatiques sont désormais en mesure de frapper monnaie, alors qu'il s'agissait, jusqu'à présent d'un attribut régalien de la souveraineté. À cela s'ajoute l'utilisation effective du *bitcoin* qui, tout en étant désormais reconnue, autorise des transactions sur des marchés parallèles pour toutes sortes de commerces illicites, comme celui des armes ou de la drogue. Indubitablement, cela met à mal la puissance des États. Nous devrions donc en conclure que le *bitcoin* et les autres monnaies virtuelles conduiraient, si elles se généralisaient, à une éventuelle disparition de la fonction de garant des États.

Le moment libertarien

Dès à présent, des grands acteurs du web et des technologies de l'information s'en prennent aux institutions étatiques et à l'idée de souveraineté nationale. Ils veulent les dépasser pour instituer une société sans frontières se préoccupant uniquement du bien de l'humanité. En cela, ils revendiquent souvent du « libertarisme », un mouvement politique volontiers antiétatique qui aspire à une extension indéfinie de la propriété privée permettant à chacun d'exercer son plein droit sur ce qu'il possède, en particulier sur lui-même et sur son corps, mais aussi sur ce qu'il a acquis, soit par achat, soit par appropriation originelle d'un bien qui n'appartenait à personne auparavant. Cette doctrine se distingue du libéralisme, dont elle représente une posture extrême, puisqu'elle ne reconnaît pas la souveraineté des États ; elle se dissocie aussi des libertaires, autrement dit des anarchistes puisqu'elle ne repose sur aucun principe de solidarité. La volonté de se désengager de l'influence de l'État conduit même certains de ses adeptes à

créer des îles artificielles dans des eaux internationales pour échapper à toute régulation étatique. C'est le cas d'une micro-nation fondée dans les îles Tonga ou du projet de Patri Friedman financé en parti par Peter Thiel, le fondateur, avec Elon Musk, de la société Paypal.

La logique du *bitcoin* s'inscrit tout à fait dans cette perspective, puisqu'elle ne fait pas appel à un hôtel de monnaies ou à une banque centrale, ou *a fortiori* à un État qui se porterait garant en dernier recours.

Le retour des États

Cependant, les usages de la *blockchain* ne se restreignent pas à la création de monnaies virtuelles, et, dans ce dernier cas, ils ne se limitent pas aux *bitcoins*. Il existe d'autres monnaies virtuelles moins opaques et donc moins facilement utilisables pour des commerces répréhensibles. Qui plus est, il est possible toujours grâce à la *blockchain* de concevoir de nouveaux systèmes d'archivage très fiables, par exemple pour enregistrer les diplômes, les transactions foncières ou les opérations financières. Dans l'éventualité de ce type d'usages, l'influence de l'État qui mettrait en place ces dispositifs ne s'en trouverait par amoindrie, mais plutôt renforcée, puisque l'ensemble de la population de ce même État contribuerait de façon transparente à l'établissement de la confiance collective. Comme nous l'avons vu, la *blockchain* rend infalsifiable un livre de compte contenant un ensemble de transactions, tout en les portant à la connaissance de tous. Certains éléments de ces transactions peuvent être encryptés, comme par exemple le nom des acheteurs et des vendeurs dans le cas du *bitcoin*, tandis que d'autres demeurent transparents. En cela, la *blockchain* ne conduit pas nécessairement à une déstructuration et à un affaiblissement de l'État, même si elle modifie les modalités de l'exercice de sa puissance. Plus généralement, et contrairement à une idée qui a parfois cours, les technologies du numériques ne conduisent pas nécessairement à une forme de libertarianisme ou de libertarisme qui viserait à la dislocation de l'État.

Signe tout à fait révélateur, Peter Thiel, figure emblématique du libertarianisme, a fondé en 2004 la société *Palantir Technologies* qui travaille pour la communauté du renseignement aux États-Unis, en particulier pour la NSA, le FBI et la CIA, ce qui est une curieuse façon de revendiquer son antiétatisme.