

The DAO : « code is law » of the jungle ?

L'expérience des monnaies virtuelles, et plus particulièrement de *bitcoin*, a surtout suscité l'intérêt du monde économique en raison des possibilités qu'offre la technologie Blockchain.

Fondées sur un système de gouvernance décentralisée, les monnaies virtuelles ont soulevées des problématiques nouvelles (déterritorialité, responsabilité dans une gouvernance décentralisée, transparence et données personnelles, lutte contre le blanchiment et le financement des activités interdites, etc.). Face à ces questions, trois attitudes se sont opposés : il y a ceux qui pensent qu'un encadrement juridique spécifique est nécessaire, ceux qui pensent que moyennant leur interprétation les règles existantes sont suffisantes, et enfin ceux qui considèrent que le protocole informatique qui en régit le fonctionnement est suffisant.

Ainsi pour cette monnaie, parfois qualifiée de monnaie de singe, l'incantation « code is law » serait suffisante (L. Lessig, « Code Is Law. On Liberty in Cyberspace », *Harvard Magazine*, 2000 (disponible en ligne : <http://harvardmagazine.com/2000/01/code-is-law-html>). Alors que dans cet appel, la théorie de Lessig n'en sort pas indemne, l'importance financière croissante de Bitcoin nécessite d'investir cette question. En effet, à l'examen on peut craindre que cette loi informatique soit finalement celle de la jungle.

Investir cette question est d'autant plus nécessaire que le développement de la blockchain démultiplie son importance et que les promoteurs des projets en cours se prévalent généralement de l'idée d'une innovation « hors sol juridique », libérée du contrôle étatique.

Le projet porté par la communauté d'Ethereum semble aujourd'hui à cet égard le plus avancé (le *White Paper* qui accompagne ce projet est disponible à l'adresse suivante : <https://slock.it/dao.html>). Il consiste à promouvoir une nouvelle forme d'association digitale de partenaires porteurs de fonds. La « *decentralized autonomous organization* » est toutefois conçue comme un conseil d'administration géant, au sein duquel la prise de décision est ouverte et transparente (« auditable ») grâce à l'utilisation du registre d'Ethereum (il est possible de faire des liens entre ce projet et le mouvement « *democracy by design* » – P. de Filippi et D. Bourcier, *op. cit.*, p. 48).. La structure se comporte ensuite comme un fond d'investissement ouvert (il est possible d'y entrer librement), qui répond aux offres présentées par des membres ou des tiers (*TheDAO*, premier essai, a été mis en œuvre à très grande échelle puisqu'il aurait réuni jusqu'à 130 millions d'euros) ou elle peut avoir été créée afin de

répondre à un objectif spécifique (projets de *Slock.it* et de *Freeftopia*). Cette entité est supposée être dépourvue de statut juridique : elle serait davantage un programme qu'un organisme susceptible de se voir reconnaître une personnalité morale (la position des initiateurs de ce projet sur ce point mériterait toutefois d'être discutée, car la qualification de société de fait semble difficilement pouvoir être exclue et il en va de même pour la notion d'entreprise retenue en droit de l'Union européenne). Les participants sont liées entre eux et avec leurs cocontractants par des *smart-contracts*, intégrés à Ethereum, et dont la bonne exécution pourrait être certifiée par des tiers.

Le projet a connu toutefois une crise majeure depuis le 16 juin 2016, à la suite d'un vol de tokens (c'est-à-dire de parts des associés de *TheDAO*) pour un montant de 3,6 millions d'Ether. Les 11,6 millions restants ont été bloqués à la suite d'un *soft fork*, de sorte que ni *TheDAO*, ni les participants ne pouvaient les utiliser. Après un débat difficile, il a été convenu de réécrire le registre d'Ethereum, à la faveur d'un *hard fork*, afin de reprendre les Ether volés au pirate et de les restituer à leurs détenteurs initiaux.

Cette affaire illustre les dangers de l'investissement dans ces nouvelles technologies. Les porteurs de *TheDAO* ont mis en place une procédure de remboursement pour les participants qui souhaiteraient se retirer, et craignent désormais que les régulateurs comme l'*AMF* (*Autorité des Marchés Financiers*) ou la *SEC* (*Securities Exchanges Commission*) américaine ne s'intéressent à la régulation des projets adossés à une Blockchain – venant ainsi couper l'élan d'innovation.

Cette solution, en apparence la plus juste, fut difficile à accepter dans la mesure où elle remettait en cause un principe fondateur de la technologie Blockchain : l'immutabilité¹. Cet épisode montre que l'immutabilité ne tient que dans la mesure où elle bénéficie du consensus de la communauté. Non seulement, quiconque parvient à convaincre 51% des participants peut induire la réécriture du code qui gouverne le fonctionnement du système, mais en outre quiconque possède ou parvient à réunir 51% de la puissance de calcul du réseau peut bel et bien réécrire le registre des transactions.

¹ Un désaccord a conduit à une scission avec la création d'une chaîne minoritaire (*Etheruem classic*), dans laquelle les tokens volés n'ont pas été retournés. Elle se présente donc comme réellement immuable et affirme faire une exacte application de la maxime « *code is law* » en partant du principe que les investisseurs auraient dû être plus vigilants et découvrir la faille dans le code de *TheDAO*. Cet épisode a plus largement été l'occasion de revivifier le débat sur la portée de cette doctrine (voir, par exemple, <http://www.coindesk.com/code-is-law-not-quite-yet/>).

Les opposants du *hard fork* ont dénoncé avec cet épisode une violation du principe « code is law ». Selon eux, ceux qui avaient tiré profit d'une faille du code originel étaient les possesseurs légitimes des tokens. Mais à l'inverse ne peut-on pas penser que la possibilité de réécrire le ledger au terme d'une procédure de vote « démocratique » est justement une application du principe précité (le consensus est en effet la source de la confiance dans le système) ? Cependant, cette solution a remis en cause le principe qui semblait jusque là fondamental de l'immutabilité (sur lequel repose normalement la sécurité du système).

En réalité, l'affirmation selon laquelle c'est le code qui définit la loi soulève pour le juriste une infinité de questions. D'abord de quel type de loi parle-t-on ? Est-ce de la *soft law*, ou faut-il y voir un ordre juridique au sens d'un ensemble de normes doté d'une logique et destiné à régir une institution ? On pourra encore se demander si les critères utilisés par Hart pour identifier un système juridique peuvent être satisfaits (règle d'appartenance, d'adjudication, et de changement). Ensuite, on doit s'interroger sur l'existence au sein du code d'une hiérarchie, d'une distinction entre des règles primaires et des règles secondaires, etc. qui seraient de nature à permettre le changement des règles de fonctionnement tout en assurant la régularité de ces changements. Enfin, c'est la réalité de la décentralisation de la gouvernance qui doit être examinée (initiative, partage de l'information, transparence, application d'un principe démocratique du type « one computer, one vote », etc.), ainsi que la nécessité d'en assurer via le code ou une autre source de contrainte, le bon fonctionnement.

Si comme le prétend Lawrence Lessig, il est nécessaire de laisser dans un premier temps les innovations du monde de l'Internet se développer loin des rigidités d'une régulation d'origine étatique, il reste possible et souhaitable