

NUMÉRO SPÉCIAL
FÉVRIER 2021

REVUE FRANCOPHONE DE LA
PROPRIÉTÉ INTELLECTUELLE



L'ÉTAT AU DÉFI DES BLOCKCHAINS

Régulation(s) et usages publics de la technologie de la blockchain

Direction scientifique :
Franck Macrez, Julien Mouchette
et Raphaël Eckert

 **AFPI**
ASSOCIATION FRANCOPHONE DE
LA PROPRIÉTÉ INTELLECTUELLE

www.revue-rfpi.com

Les conditions de la régulation publique des *blockchains*

La régulation par la blockchain

Amélie Favreau

Maître de conférences, HDR, Université Grenoble-Alpes

« *Decentralization is what allows bitcoin to substitute an army of computer for an army of accountants, investigators and lawyer* ».

Introduction

Internet et la «*pathetic dot theory*». L'environnement numérique a ouvert les portes à de nouvelles formes de régulation, dans lesquelles l'État et les institutions administratives, judiciaires et financières vont occuper une nouvelle place, une place différente. Il demeure pertinent de regarder environ une vingtaine d'années en arrière les conceptions traditionnelles de la régulation d'Internet. Le discours se partageait assez clairement entre les cyber-libertariens, selon lesquels la nature même du cyberspace est ingouvernable par les États et, de l'autre côté, les cyber-paternalistes selon lesquels le cyberspace n'est pas hors d'atteinte de la loi, qui devient un outil de régulation des comportements. Avec le temps, il est apparu que les cyberpaternalistes étaient plus proches de la réalité¹. À cette occasion, le

professeur Lessig avait construit la «*pathetic dot theory*». Le «*pathetic dot*» désigne l'objet de la régulation. À propos d'Internet, il décrit comment les actions individuelles sont contrôlées et affectées par quatre grands mécanismes : la loi établie par les États, les normes sociales dictées par la société, les forces du marché qui dérivent des règles de l'offre et de la demande et enfin l'architecture, ou le «*Code*», c'est-à-dire les systèmes techniques qui siègent dans le monde physique et numérique. Les quatre mécanismes sont évidemment liés, les lois par exemple ont une incidence sur l'évolution des forces du marché et sur l'architecture. «*Code is Law*» selon la célèbre formule du professeur Lessig, désigne justement cette force régulatrice que peut exercer le Code ou l'architecture sur un objet ou une activité². Il devient alors primordial pour chaque société de définir en amont les valeurs primordiales à protéger³. La «*pathetic dot theory*» est

¹ L. Denardis, *The Global War for Internet Governance*, New Haven, CT: Yale University Press, 2014.

² L. Lessig, "Open code and open societies: values of internet governance", 74 *Chi.-Kent L. Rev.* 1405, spéc. 1408. «*Tout d'abord, réfléchissez un peu plus au code - à la manière dont il régleme. Les avocats n'aiment pas beaucoup réfléchir à la manière dont le code régleme. Les avocats aiment penser à la manière dont la loi régleme. Le code, comme les avocats aiment à le penser, n'est que le cadre dans lequel les lois s'appliquent. Mais il manque un point important. Le code du cyberspace - que ce soit l'Internet ou un réseau au sein de l'Internet - définit cet espace. Il constitue cet espace*».

³ L. Lessig, "Open code and open societies: values of internet governance", préc. «*Et comme toute*

constitution, il construit en lui-même un ensemble de valeurs et de possibilités qui régissent la vie dans cet espace. L'Internet tel qu'il était en 1995 était un espace qui rendait très difficile la vérification de l'identité d'une personne ; cela signifie que c'était un espace qui protégeait la vie privée et l'anonymat. L'Internet tel qu'il devient est un espace qui rendra très facile de vérifier qui est quelqu'un ; le commerce l'aime ainsi ; cela signifie qu'il deviendra un espace qui ne protégera pas nécessairement la vie privée et l'anonymat. La vie privée et l'anonymat sont des valeurs, et elles sont respectées, ou non, en raison de la conception du code. Et la conception du code est une chose que les gens font. Ce sont les ingénieurs qui font les choix sur la façon dont le monde sera. En ce sens, les ingénieurs sont des gouverneurs » et p. 1409 : «*Si l'architecture de l'Internet affecte les*

aujourd'hui susceptible d'être étendue à la *Blockchain* pour comprendre comment s'exercent les forces régulatrices sur ce nouvel objet⁴.

La blockchain, de l'objet de la régulation à l'outil pour réguler. La technologie *blockchain*⁵ depuis le mouvement des Cypherpunk duquel elle émerge interroge, voire inquiète, sur la capacité des mécanismes traditionnels de régulation à saisir cet objet libertarien. Pour autant, dix ans après le protocole fondateur de bitcoin par Satoshi Nakamoto, les applications de *blockchain* sont au cœur de réglementations plus ou moins contraignantes, plus ou moins perméables à des logiques de marché et plus ou moins respectueuses des écosystèmes dans lesquelles elles évoluent⁶. L'on pense notamment aux cryptomonnaies et plus largement aux actifs numériques. Pour autant, si l'on suit la « *pathetic dot theory* », elle peut également être envisagée comme mécanisme de régulation, en elle-même. La réflexion consiste alors à considérer la technologie *blockchain* non plus comme un objet de régulation, mais comme un outil de la régulation. Cette hypothèse est aujourd'hui soutenue, selon laquelle le meilleur moyen de réguler les

comportements humains, les marchés et les machines serait par le code informatique lui-même. Le protocole *blockchain* grâce à des caractéristiques de décentralisation, de désintermédiation, d'inviolabilité et de résilience permet le développement d'applications susceptibles d'augmenter le droit avec le Code et au-delà, selon les vœux de certains, de substituer le code au Droit. Dit autrement, aux côtés des règles « légales » siègeraient des « règles techniques » qui assumerait le même rôle et les mêmes fonctions. Alors que dans le « Code is Law », le Code exerce une modalité complémentaire de régulation⁷, le « Code as Law »⁸ est une modalité de régulation dans laquelle la technologie est utilisée en soi pour définir et implémenter les « règles de droit », qui sont par analogie désignées par le « Code of Law ». C'est l'articulation « Code is Law », « Code as Law » et « Code of Law » que nous proposons d'étudier dans cette contribution.

La possibilité d'une régulation par la blockchain ? L'idée sous-jacente de configurer les systèmes technologiques pour aider à garantir la conformité de normes juridiques n'est pas nouvelle. Les Digital right management ou les mesures de protections techniques dans le domaine

valeurs aussi bien que les bits - si l'architecture est une sorte de loi - alors, comme dans tout contexte législatif, nous devrions nous demander qui sont ces législateurs et comment ils font la loi. Si le code reflète des valeurs, alors nous devrions identifier les valeurs qui proviennent de notre tradition - la vie privée, la liberté d'expression, l'anonymat, l'accès - et insister pour que ce code les embrasse s'il doit embrasser des valeurs du tout. Que nous devrions nous pencher sur la structure de notre tradition constitutionnelle, en extraire les valeurs qui en sont issues et les transposer dans le monde de la gouvernance de l'internet - que la gouvernance se fasse par le biais d'un code ou par les personnes ».

⁴ Pour une application à la *blockchain*, v. P. de Filippi et A. Wright, *Blockchain and the Law, The Rule of Code*, Harvard University Press, 2018, p. 173 et s.

⁵ Nous employons ce terme générique pour désigner sans distinction particulière le protocole *blockchain* et les applications implémentées sur *Blockchain*, ni les différents types de *Blockchain*.

⁶ Par exemple, les discussions autour de l'impact environnemental de la technologie *blockchain*.

⁷ « La gouvernance au sens où je l'entends est un mélange des règlements du code et des règlements des organismes qui réglementent ce code. C'est à la fois une machine et un homme. » (traduction de : "Thus governance in the sense that I mean is a mix of the regulations of code and the regulations of bodies that regulate this code. It is both machine and man.").

⁸ L'expression ne nous appartient pas. Elle est très fréquente dans la littérature anglo-saxonne, v. l'important article de K. Yeung, "Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law", (2019) 82(2) *Modern Law Review*, 207-239 ou S. Hassan et P. de Filippi, "The Expansion of Algorithmic Governance: From Code is Law to Law is Code", *Field Actions Science Reports*, Special Issue 17 /2017. Sur cette idée: E. Treppoz, « Quelle régulation internationale pour la *blockchain*? Code is Law V. Law will become Code », in *Blockchain et droit*, (dir.) F. Marmoz, Dalloz, coll. Thèmes et commentaires, 2018, p. 55.

musical en sont un exemple⁹. Il s'agit d'une proposition *a minima* dans laquelle la règle technique siège aux côtés des règles de droit. La proposition est régulièrement avancée au sujet de la *Blockchain*, ainsi que l'a récemment observé le conseiller scientifique principal du Royaume-Uni dans un rapport sur les Fintech : « toute innovation technologique pouvant être appliquée à la réglementation ou utilisée dans la réglementation, généralement pour améliorer l'efficacité et la transparence »¹⁰. Coupler les règles de droit traditionnelles avec les caractéristiques inhérentes à la *blockchain* rend ces formes de régulation séduisantes par la sécurité et l'efficacité qu'elles promettent. Aller au-delà de cette proposition en considérant la technologie en soi comme un outil de régulation autonome est une démarche plus sensible. Pour évaluer cette nouvelle régulation *par la blockchain*, plusieurs questions se posent. Tout d'abord, sur l'existence de la règle technique : comment la règle technique est-elle élaborée ? Par qui ? Est-elle nécessairement le décalque ou le complément technique d'une règle préalable juridique ? Ou fonctionne-t-elle de manière autonome au sein d'un ordonnancement propre ? Existe-t-il des applications déployées sur un protocole *blockchain* qui permettraient ce type de régulation ? Mais également, des questions sur l'exercice de la règle technique dans son environnement : comment le « Code as law » s'articule-t-il avec le « Code of law » ? Assistera-t-on à de l'hostilité, de la complémentarité, de la coexistence pacifique ? Verra-t-on dans les années à venir, le droit suppléé, supplanté ou suppléé par la technique ? S'interroger sur la régulation *par la blockchain*, nous invite non seulement à déterminer la place que nous souhaitons accorder à la règle de droit, mais également, à questionner les valeurs fondamentales à préserver, comme y invitait le professeur Lessig à propos de « Code is Law ». En

somme, le Code n'est pas neutre. L'architecture d'une plateforme dépend de choix spécifiques qui ont été opérés pour réaliser cette plateforme, par exemple, en termes d'identification ou de certification. Les promoteurs ont alors cherché à mettre en avant ou à éviter certains types d'actions. Le Code est éminemment politique. Il a des implications sociales dans la mesure où il aura un impact sur certaines actions et l'influence de certains comportements¹¹. Le sujet est vaste et il sera difficile de répondre à toutes ces questions. Nous commencerons par nous interroger sur l'existence d'une règle technique susceptible de fonder ce mécanisme de régulation *par la blockchain* (I). Admettant cette existence, nous étudierons ensuite ses manifestations dans son environnement, c'est-à-dire ses interactions avec la règle de droit (II).

I. La régulation par la *blockchain*, l'existence d'une règle technique

Il existerait une règle technique issue de la technologie *blockchain*. Il convient d'en rechercher les manifestations (A), avant de s'interroger sur la production de cette règle (B).

A. Les manifestations de règle technique

Loin d'être exhaustives, les deux manifestations étudiées sont les *smart contracts* (1) et les organisations autonomes décentralisées (2).

1. Les « *Smart contracts* »

Définition du *smart contract*. Plusieurs *blockchains* sont aujourd'hui susceptibles de supporter des *smart contracts*. Le *smart contract*, avant d'être un objet de droit, est un outil technique qui permet d'inscrire les transactions des individus dans les blocs de

⁹ M. Filby, "Code is Law? Assessing Architectural File Sharing Regulation in the Online Environment", *Journal of International Commercial Law and Technology* (2013) 8(1): 81-103 at 91.

¹⁰ UK Chief Scientific Adviser, "Fintech Futures: The UK as a World Leader in Financial Technologies", (London, 2015) p. 47.

¹¹ L. Winner, "Do Artefacts Have Politics? ", *Daedalus*, (1980), volume 109, n°1, p. 121-136.

la chaîne. Pour y parvenir, des protocoles informatiques de type « si... [ex. telle condition est vérifiée], alors... [ex. telle conséquence se produira] » (« if... then... »). Le *smart contract* est donc la traduction informatique d'un engagement contractuel, afin d'en assurer son exécution automatique. Dès 1996, Nick Szabo les avait envisagés, et ce, bien avant l'écriture du protocole bitcoin. De ce fait, le dispositif d'un contrat auto-exécuté n'est pas nouveau et préexiste à la *blockchain*. Le terme « *smart contract* » ou « contrat intelligent » est le plus commun, mais non dénué d'ambiguïté. En réalité, le *smart contract*, n'est ni intelligent, car il dépend entièrement de la programmation réalisée, ni un contrat. Un *smart contract* est donc « plutôt un Code de programme informatique qui automatise la vérification, l'exécution et l'application de certaines conditions d'un accord »¹². On pourrait lui préférer selon l'expression revue par Vitalik Butarin celui de « script persistant », qui met en avant le contrôle par des règles incorruptibles et immuables des actions et des transactions. Si le *smart contract* est principalement utilisé dans le domaine de la finance et du transfert de cryptomonnaie¹³, il peut également être un outil de transfert de tout bien immatériel tokenisé. L'on pense notamment à l'initiative d'Ujo Music et d'Imagen Heap utilisant des *smart contract* pour la commercialisation de son titre « *Tiny Human* »¹⁴.

L'intérêt du *smart contract*. Tel que présenté, les *smart contracts* présentent trois séries d'avantages. Pour les parties, tout d'abord, lorsque les clauses sont traduites en *smart contracts*, elles se trouvent alors déchargées de vérifier la bonne exécution de leurs obligations. Si le *smart contract* a été correctement programmé, elles ont l'assurance d'une exécution stable, sans

changement. La barrière du langage et la distance dans les relations contractuelles est vaincue. Ensuite, les transactions sont facilitées. En effet, les parties qui ne se connaissent pas n'ont pas besoin de se faire confiance ou de se prémunir par un lot de garanties inspirées par méfiance. Le *smart contract* est déployé sur une *blockchain* et en prend les caractéristiques, notamment de sécurité et d'immutabilité. La confiance repose sur l'intégrité informatique¹⁵. Enfin, sur le langage, les ambiguïtés du langage naturel sont levées et l'on évite l'inexécution de certaines dispositions complexes, difficiles d'interprétation. Il y a donc peu de place à l'interprétation, les actions sont programmées, anticipées et binaires. Considérant ces nombreux avantages, il est un outil technologique intéressant pour compléter les contrats traditionnels.

L'autonomie relative du *smart contract*. Le *smart contract* appelle parfois (non systématiquement) une fonction dynamique appelée « Oracle » pour fonctionner. Des machines ou des hommes enregistrent et transmettent des informations contenues on chain ou off chain qui sont nécessaires à l'exécution du *smart contract*. L'exemple le plus classique est celui de relevés météorologiques pour des contrats d'assurance. Particulièrement vrai pour les Oracles *Off-chain*, le professeur Legeais remarque que « ce recours aux Oracles montre les limites des *smart contracts*. Plus généralement, il démontre la volonté des initiateurs de la *blockchain* de se passer du tiers de confiance est une utopie »¹⁶. La règle purement technique serait donc celle mise en œuvre par un *smart contract* indépendamment de tout recours à des informations *off-chain*.

Du « *smart contract* » au « *smart legal contract* ». La question souvent récurrente en

¹² M. Finck, « Blockchain Regulation », *Max Planck Institute for Innovation and Competition Research Paper Series* No 17-13 SSRN Network (2017) 4.

¹³ Ils servent principalement à exécuter automatiquement des dérivés, des contrats à terme, des swaps et des options.

¹⁴ Sur cette question, v. notamment, A. Favreau, « Les outils technologiques de légitimation de la propriété

intellectuelle. L'exemple de la *blockchain* », *Legipresse*, HS n°62, 2019-2, p. 21, spec. p.28.

¹⁵ C. Zolynski, « Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RD banc. et fin.*, 2017, n°1.

¹⁶ D. Legeais, *Blockchain et actifs numériques*, éd. LexisNexis, 2018, n°171, p. 102.

matière de *smart contract* est l'existence d'un « *smart legal contract* », c'est-à-dire un contrat qui se formerait en plus de s'exécuter de manière automatique sur la *blockchain*¹⁷. Dit autrement, il s'agit de la situation dans laquelle les relations qui sont à la fois définies et automatiquement appliquées par Code, mais qui ne sont liées à aucun contrat ou à aucune forme traditionnelle d'obligation contractuelle. Cette hypothèse ne nous semble pas tenable. La formation d'un contrat par l'échange des consentements reste nécessairement humaine. La question de la formalisation et de la preuve de l'échange des consentements est autrement plus intéressante dans un contexte de *blockchain* où tant l'identité que la signature questionnent. Dès lors, le *smart contract* et le contrat traditionnel forment le plus souvent un ensemble hybride. Certaines stipulations sont facilement traductibles en langage informatique. D'autres comme les notions standards s'y prêtent moins facilement¹⁸. Leur traduction ne serait d'ailleurs pas opportune, car elles perdraient le caractère souple et flexible recherché. Il faut donc comprendre que ce n'est pas systématiquement l'intégralité d'un contrat traditionnel que l'on va traduire en langage informatique.

Le smart contract, manifestation d'une régulation par la blockchain ? Le smart contract permet de traduire des règles de droit en règles techniques et participe au mécanisme de régulation par la *blockchain*. Il s'agit d'une régulation « *ex ante* ». En effet, au lieu d'exercer une contrainte légale sur le cocontractant après l'inexécution de l'obligation, le smart contract prévient l'inexécution ou la violation du contrat. Il devient alors très difficile pour les parties à un *smart contract* d'enfreindre la règle technique telle qu'elle a été écrite. Le développement de *smart contracts* est en pleine expansion. Au cours des dernières

années, plusieurs plateformes ont créé des langages de programmation permettant la création de *smart contracts* de plus en plus sophistiqués. Ces langages sont accessibles, mais la capacité de chacun à les manier est variable (ex. le langage Mickelson). Ceci, pose alors la question de l'intelligibilité de la « règle technique », qui par analogie avec la règle de droit, doit être comprise de tous. Dernier élément, s'il s'agit bien d'un outil de régulation par la *blockchain*, le *smart contract* accompagne le contrat traditionnel. L'on se situerait donc plus dans la manifestation d'un « *Code is Law* » que dans celle d'un « *Code as Law* ».

2. Les organisations autonomes décentralisées

Définition des organisations autonomes décentralisées. Les organisations autonomes décentralisées (DAO) sont un type spécifique d'organisations décentralisées. Elles sont définies comme une entité fonctionnant grâce à un programme informatique qui fournit des règles de gouvernance automatique à une communauté¹⁹. Elles présentent deux principales caractéristiques²⁰. D'une part, elles sont autonomes, ce qui signifie qu'après leur déploiement sur une *blockchain*, elles fonctionnent sans l'intervention de leur créateur. Au-delà même, une fois déployée, il n'est plus possible d'en reprendre le contrôle. Plusieurs *smart contracts* sont liés pour former des DAO, afin de prévoir les règles et les procédures de fonctionnement. La DAO prend alors les caractéristiques d'immutabilité et d'auto-exécution propres au smart contract. D'autre part, elles sont autosuffisantes. En ce sens, elles peuvent accumuler du capital, notamment des cryptomonnaies ou des actifs numériques, mais également facturer les utilisateurs pour des services fournis. Par ce dernier élément, il faut comprendre qu'elle fonctionne indépendamment d'entités juridiques

¹⁷ F. Gillioz, « Du contrat intelligent au contrat juridique intelligent », *Dalloz IP/IT*, 2019, p. 16.

¹⁸ En ce sens, v. not. D. Legeais, *Blockchain et actifs numériques*, préc. n°152, p. 96.

¹⁹ Sur cette question, A. Maudouit-Ridde, « L'organisation autonome décentralisée », *Bull. Joly Bourse*, 2018, n°3, p. 117.

²⁰ Sur cette question, v. not. A. Wright et P. de Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 10 mars 2015, p.16.

traditionnelles et préexistantes, telles que des sociétés ou des fondations et qu'en cela les DAO sont une véritable réponse au « Code as Law ».

Régulation par la blockchain au sein des DAO. Les deux principaux avantages des DAO sont la réduction des coûts opérationnels et la transparence des décisions, qui diminuent le risque de corruption²¹. La confiance n'est alors plus la base des relations entre les parties. En effet, la confiance ne repose pas sur l'organisation mais sur la sécurité et la fiabilité du code sous-jacent. Les modèles de gouvernance du droit des sociétés peuvent être répliqués, par exemple en répartissant le pouvoir entre plusieurs parties à l'aide d'une technique de signature multiple²², mais sans servir nécessairement de base à la réalisation d'une DAO. Contrairement aux organisations traditionnelles, où la prise de décision est verticale, le processus au sein d'une DAO peut-être horizontal à travers la participation directe d'actionnaires par le biais d'un vote décentralisé.

B. La production de la règle technique

Différents acteurs, différents prescripteurs de la règle technique ? Plusieurs acteurs sont directement impliqués dans leur fonctionnement de la *blockchain*. Si la règle technique est élaborée à partir d'un protocole de *blockchain*, cela signifie que les différents acteurs y œuvrent. Il y a tout d'abord, les développeurs du protocole qui conçoivent, implémentent et contribuent au logiciel *open source* et aux protocoles cryptographiques sur lesquels reposent généralement les *blockchains* publiques. Il y a ensuite les nœuds, c'est-à-dire ceux qui fournissent la puissance de calcul, réalisent les preuves

cryptographiques et stockent une copie du registre. Puis, les prestataires sur actifs numériques, dont les fonctions ont récemment été définies par la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite Loi PACTE. Ce statut couvre un grand nombre d'activités : la conservation d'actifs numériques pour le compte de tiers ; l'achat-vente d'actifs numériques contre une monnaie ayant un cours légal ou contre d'autres actifs numériques (courtage) ; l'exploitation d'une plateforme de négociation d'actifs numériques (bourse) ; d'autres services sur actifs numériques comme la réception et transmission d'ordres pour le compte de tiers, la gestion de portefeuille pour le compte de tiers, le conseil, la prise ferme, le placement garanti et le placement non garanti. Ces acteurs sont largement dispersés dans l'espace et dans le temps, avec pour chacun des intérêts, des opportunités, des formes de participation et des motivations bien distincts. Il est donc difficile d'imaginer une réalisation commune et concertée de la règle technique²³.

Différentes modalités de production de la règle technique. Les protocoles sont publics, tout le monde peut y participer. Bien souvent le modèle est décrit comme « anarchique », ce qui ne signifie pas nécessairement sans règles, mais plutôt sans contrôle vertical. En effet, chaque *blockchain* constituant une base de données distribuée sur un nombre important de nœuds qui peuvent éventuellement être mal intentionnés dans l'enregistrement de données, ces nœuds doivent partager un mécanisme leur permettant de parvenir à un consensus concernant les informations qui doivent être enregistrées dans la *blockchain* et celles qui ne le doivent pas (par exemple, une transaction

²¹ P. de Filippi et R. Mauro, "Ethereum: The Decentralized Platform that Might Displace Today's Institutions", *Internet Policy Review*, 25 août 2014, disponible à l'adresse suivante : <http://policyreview.info/articles/news/ethereum-decentralised-platform-might-displacetodays-institutions/318>.

²² Sur cette question, v. not. A. Wright et P. de Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 10 mars 2015, disponible à

l'adresse suivante : <https://ssrn.com/abstract=2580664> ou <http://dx.doi.org/10.2139/ssrn.2580664>

²³ Rappr. de "Code is Law" : J'ai vendu cette phrase sur le fait que le code est une sorte de loi, et que les auteurs du code - les rédacteurs du code - sont une sorte de gouverneur », L. Lessig, "Open code and open societies: values of internet governance", 74, *Chi.-Kent L. Rev.* 1405, spec. 1409.

impliquant une quantité de cryptomonnaie non disponible pour le débiteur). Il est donc primordial qu'un nœud souhaitant enregistrer une information dans la *blockchain* soit incité à être sincère. Les principaux algorithmes actuellement utilisés sont la preuve de travail, preuve d'enjeu, preuve d'enjeu déléguée, mécanismes à base de vote (comme *Ripple* ou *Stellar*). Et comme cela a été souligné dans le rapport France Stratégie, la question est éminemment stratégique et il s'agit bien ici d'un enjeu de gouvernance²⁴. Les modes de production de la règle technique doivent également veiller à l'évolution ouverte des protocoles. L'objectif est de conserver une base technique simple et laisser les applications développer la part de complexité. Pour cela, le protocole doit le plus neutre possible. C'est un idéal de modularité. Des morceaux du protocole peuvent être modifiés ou supprimés, notamment par le biais de forks qui sont des modes de développement du code. Quant à briser l'architecture, le Code, le professeur Lessig recommandait : « il est illégal d'écrire des logiciels qui visent à briser les protections du code. Ainsi, la loi ne serait pas seulement remplacée par le code ; elle punira les efforts visant à échapper au code »²⁵.

Admettre l'existence d'une règle technique émanant de *blockchain*, élaborée avec plus ou moins d'autonomie au regard de la règle de droit traditionnelle était un point de départ. Cela conduit à s'interroger sur ses interactions avec la règle de droit. Il reste à étudier comment la régulation par la *blockchain* s'articule avec la régulation par la règle de droit.

II. Régulation par la *blockchain* : exercice de la règle technique

L'autonomie de la règle technique ? Est-il raisonnablement possible de considérer que la régulation par *blockchain* peut opérer sans le recours aux États ou à une quelconque autorité centrale, et à l'extérieur de la règle de droit proprement dite ? La réponse ne peut pas être définitive tant que la technologie et ses applications n'ont pas atteint un seuil de maturité. Il est toutefois très intéressant d'observer le comportement de ces règles techniques dans un environnement juridique, c'est ce que nous nommons l'exercice de la règle technique. En d'autres termes, il s'agit d'étudier les interactions entre la règle de droit et la règle technique. Le professeur Yeung, qui s'est prêté à un exercice similaire, décrivait trois différents types d'intersections entre les dispositions juridiques conventionnelles et les règles issues de la technologie, axées sur la motivation des participants aux *blockchains* à : échapper délibérément aux contraintes de fond des *blockchains* (évasion hostile), compléter le droit conventionnel pour le rationaliser (alignement efficace), et coordonner les actions entre et parmi les multiples participants en évitant les inefficacités procédurales (atténuation des frictions transactionnelles). Elle synthétise les trois propositions par les formules suivantes : « le chat et la souris », « les joies du mariage » et « la coexistence difficile et la suspicion mutuelle »²⁶.

Nous avons fait le choix de concentrer le propos autour de deux propositions : lorsque la règle technique s'exprime indépendamment de la règle de droit (A) et

²⁴ Rapp. France Stratégie, « Les enjeux des *blockchains* », (dir.) J. Toledano, juin 2018, p. 10, v. la définition du Protocole de consensus : « Qui a accès à la *blockchain*, qui définit les modalités d'un ajout sur la chaîne, comment décider d'une évolution du protocole ? Le choix du « protocole de consensus distribué » est une question éminemment stratégique. La *blockchain* peut être publique, avec une architecture ouverte, ou privée, avec un nombre volontairement limité de participants et la

réintroduction d'une forme d'autorité centralisée. L'enjeu technique se fait ici enjeu de gouvernance ».

²⁵ L. Lessig, « Open code and open societies: values of internet governance », préc.

²⁶ K. Yeung, préc. spéc. 210 : "Each of these three motivations can be expected to generate a particular kind of dynamic interaction between law and *blockchain* systems, which I describe as cat and mouse, the joys of marriage and uneasy coexistence and mutual suspicion respectively".

lorsque la règle technique coopère avec la règle de droit (B).

A. La régulation par la *blockchain*, hors de la règle de droit

« Code as Law » contre le « Code of Law » ? Par principe, la *blockchain* repose sur des algorithmes cryptographiques qui assurent la validité de transactions de pair à pair entre des personnes qui ne se connaissent pas, sans le recours à un État ou à un intermédiaire. Il est alors aisé d'imaginer comment la technologie *blockchain* peut devenir un moyen de s'évader des prescriptions légales par des règles techniques. Les autorités judiciaires nationales exercent leur autorité souveraine sur ces activités²⁷. C'est ainsi que lorsque des plateformes sur lesquelles sont utilisées des cryptomonnaies, tel que *bitcoin*, à des fins illégales, c'est la plateforme qui est fermée et non la cryptomonnaie interdite (ex. Silk Road). Comme le soulignent A. Guadamuz et C. Marsden, « l'absence de pression réglementaire significative en faveur de l'interdiction totale des *Bitcoins* (ou d'autres crypto-monnaies) peut être expliquée au motif que les gouvernements ne se sentent pas suffisamment menacés actuellement pour justifier une interdiction et, plus important encore, parce que l'action pourrait s'avérer futile compte tenu de la nature décentralisée des monnaies²⁸. Par exemple, la régulation des cryptomonnaies et des activités financières liées aux cryptomonnaies est avant tout un choix politique, un choix étatique. Cela emporte deux premières conséquences : que la décision de régulation est relative et contingente au régime politique et économique d'un État et qu'il sera difficile à court terme de parvenir à une harmonisation mondiale sur ces activités transnationales.

Les États font alors face à un trilemme : ne pas introduire de cadre juridique pour réguler l'existence et la circulation des cryptomonnaies, introduire un cadre régulateur souple favorisant le développement de la technologie et définir précisément les risques liés aux cryptomonnaies pour introduire une législation stricte de protection du secteur financier. La France a fait le choix d'une régulation souple. Il s'agit dans cette hypothèse de laisser les cryptomonnaies et les plateformes se développer dans l'espace virtuel. Si réglementation il y a, elle doit être claire et attractive pour inciter les entreprises à venir s'installer sur le territoire français. Comme le souligne le rapport de M. LANDAU : « à long terme, l'attractivité d'un cadre réglementaire ne s'apprécie pas à l'aune de sa permissivité, mais bien au regard de la sécurité juridique qu'il apporte aux acteurs du marché »²⁹. Hors de cette possibilité, et telle est la conclusion du professeur Yeung, « à moins que les systèmes juridiques conventionnels ne tentent explicitement d'aborder des activités fondées sur des chaînes de blocs, la coexistence qui en résulte entre le Code en tant que loi et le Code de droit peut être qualifiée de suspicion et d'incertitude mutuelles »³⁰.

Exercice de la règle technique en inadéquation avec la règle de droit. Si l'on s'attache aux *smart contracts*, la règle technique peut s'opposer à certaines prescriptions légales. Par exemple, la transparence de la *blockchain* sur laquelle sont implémentés les *smart contracts* perturbe le besoin de confidentialité de certaines transactions (en droit du travail ou en finance). Des solutions existent sur des protocoles ZCash ou Monero utilisant le Zero Knowledge Proof. Second exemple, le *smart contract*, et *a fortiori* dans les DAO, les

²⁷ E. Treppoz, « Quelle régulation internationale pour la *blockchain*? Code is Law V. Law will become Code », préc., selon qui, le droit n'a pas vocation à saisir la technologie, mais ses applications. L'auteur apporte des réponses en droit international privé.

²⁸ A. Guadamuz et C. Marsden, "Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies", *First Monday Review*, 2015.

²⁹ Rapport au Ministère de l'Économie et des Finances de J.-P. Landau, *Les cryptomonnaies, La documentation française*, 4 juil. 2018, p. 45.

³⁰ K. Yeung, préc. spéc. 217.

cryptomonnaies peuvent couvrir des activités illicites, comme se soustraire à une obligation fiscale ou à d'autres obligations réglementaires, telles que celles visant à identifier et à réduire le risque de blanchiment de capitaux. Les autorités judiciaires nationales ont exercé leur autorité souveraine sur ces activités en fermant les interfaces publiques (ex. Silk Road). D'ailleurs, des chercheurs au Royaume-Uni et aux États-Unis travaillent également sur l'hypothèse où des *smart contracts* faciliteraient des crimes complexes comme l'assassinat d'une personne publique.

B. La régulation par la *blockchain*, avec la règle de droit

Complémentarité de la règle de droit et de la règle technique. Règle technique et règle de droit ont des buts similaires : il s'agit de guider les comportements et d'orienter les actions. Tout d'abord, transposer les règles de droit en code contribue à réduire l'incertitude autour de l'interprétation et l'application des règles. Parce que les langages informatiques sont stricts et formalisés, il est possible de prédire la manière dont ils vont s'appliquer. Un autre avantage est pour l'État de réduire les coûts liés à une régulation traditionnelle. La perspective de voir naître un corpus appelé « *Lex cryptographia* » apparaît prometteuse³¹. Selon de Filippi et Wright, elle est une émanation/extension de la « *Lex mercatoria* » médiévale, cet ensemble de règles informelles qui régissaient les relations entre les commerçants pour les échanges internationaux ou interrégionaux. Pour la régulation d'Internet, nous avons vu apparaître une « *Lex electronica* » hors des cadres juridiques nationaux et émanant d'une communauté internationale

d'utilisateurs. La *Lex electronica* est la première forme de régulation par le Code. La *Lex Cryptographia* instaurerait un nouveau corpus de règles administrées et exécutées automatiquement à travers les *smart contracts* et la DAO. Ainsi, à mesure que les technologies de *blockchain* évolueront et que de nouvelles applications apparaîtront, *Code of Law* et *Code as Law* cohabiteront avec plus ou moins d'antagonisme ou de coopération.

Interaction de la règle de droit et de la règle technique sur l'écriture informatique du droit. Comme les juristes le constatent depuis longtemps, l'écriture de la règle de droit n'est pas toujours parfaite, même si l'on doit remarquer la résistance au temps de nombreuses dispositions. Parallèlement, la manière dont les règles informatiques sont rédigées interroge sur leur résistance aux dysfonctionnements et sur leur pérennité dans le temps³². Autre question, le débat d'interprétation de la règle technique nécessitera un jugement humain, comme l'illustre parfaitement The DAO Hack. Le 26 mai 2016, un projet DAO a levé près de 12 millions d'éthers, la cryptomonnaie attachée à la *blockchain* Ethereum. Un pirate a profité d'une faille dans l'écriture du *smart contracts* pour détourner plusieurs millions d'unités de la cryptomonnaie. Le bloc une fois validé a corrompu la chaîne et par un consensus de la majorité un fork (une bifurcation) a été réalisée pour aboutir à une nouvelle *blockchain* renommée Ethereum Classic. Cet exemple, nous permet de remarquer qu'il n'a pas été fait de recours au droit et à la justice traditionnelle pour remédier à l'injustice perçue³³. Des systèmes juridiques étrangers ont cherché à reconnaître la validité des transactions effectuées sur la *blockchain*, telle que la loi de l'Arizona (US) en 2017³⁴.

³¹ Le premier texte sur cette question : A. Wright et P. de Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", 10 mars 2015. Disponible à l'adresse suivante : <https://ssrn.com/abstract=2580664> ou <http://dx.doi.org/10.2139/ssrn.2580664>.

³² A. Diallo, *La formalisation de la règle de droit en langage informatique. L'exemple des smart contracts*. Thèse en cours, Université de Grenoble.

³³ Sur cette question, v. not. D. Legeais, *Blockchain et actifs numériques*, préc. n°175, p. 104.

³⁴ J.-C. Roda, « Smart contracts, dumb contract », *Dalloz IP/IT*, 2018, p. 397, selon qui la logique même du smart contract peut être rapprochée de l'École de Chicago, avec une logique de réduction des coûts, une tentative d'écarter le juge ou les intermédiaires tels que les notaires et les avocats.

Interaction de la règle de droit et de la règle technique sur la standardisation du droit. La traduction des stipulations les plus simples en *smart contracts* et la constitution de bibliothèques conduisent nécessairement à une standardisation du droit. En soi, la cohabitation ne poserait pas de difficulté dans la mesure où la règle de droit continue à intervenir pour régir les relations contractuelles complexes. Toutefois, la plupart des *smart contracts* exécutent automatiquement des dérivés de *smart contracts* préexistants. Cela multiplie les risques de bogue ou d'introduction de biais cognitifs. Des chercheurs ont mis en avant ce phénomène en créant une typologie des *smart contracts* sur Ethereum³⁵. Quelques statistiques ressortent de leur étude : les *smart contracts* ont trois fois de plus chance d'être créés à partir d'autres *smart contracts* ; plus de 60% des *smart contract* ne sont pas utilisés (*smart contract* dormants) ; surtout, ils soulignent que les *smart contracts* déployés sur Ethereum présentent peu de diversité entre eux : parmi les *smart contract* créés par des utilisateurs, moins de 10% sont « uniques ». Concrètement, le *smart contract* le plus connu est le ERC20 qui permet l'interopérabilité des *tokens* fongibles créés à l'occasion des ICO. Ce *smart contract* a été énormément repris et constitue un standard dans le milieu des fournisseurs d'actifs numériques.

Interaction de la règle de droit et de la règle technique : sur le caractère supplétif des règles techniques. Les réseaux de *blockchain* ne peuvent pas en pratique fonctionner comme des systèmes hermétiquement isolés de la communauté. Même si les règles techniques édictées sur la *blockchain* peuvent assurer avec succès une sécurité transactionnelle fiable et efficace, les systèmes juridiques classiques devront veiller à ce que les droits, les intérêts et les

attentes de la communauté au sens large soient protégés. La règle technique apparaît alors nécessairement supplétive. En effet, le code est sujet aux bogues et, à l'instar d'une règle de droit, doit être mis à jour pour les éviter. Ce travail sur le Code renvoie à la question de la production de la règle technique. Il y a alors fort à parier que le règlement des litiges issus d'une programmation incorrecte et préjudiciable se résoudra devant le juge, ce dernier incarnant l'indispensable marge d'appréciation et d'interprétation pour résoudre les litiges, à côté d'un « Code informatique » immuable et d'un « Code légal » pérenne.

Interaction de la règle de droit et de la règle technique : sur les valeurs fondamentales véhiculées par le Code. Le Code n'est pas neutre. Le développeur qui rédige un *smart contract* est susceptible de l'influencer par sa subjectivité et son interprétation, déformant possiblement la commune intention des parties. L'opinion générale est plutôt de laisser l'État en dehors de la technologie, afin de la laisser se développer sans contrainte et de ne pas opérer de choix technologique. Tel a été le choix fait par le législateur français dans l'écriture du décret n°2018-1226 du 24 décembre 2018 relatif à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibons (art. R. 211-9-7 du CMF)³⁶. Ce n'est pas entre régulation et absence de régulation technique ou étatique que nous devons aujourd'hui choisir. Le code informatique régule et il implémente un certain nombre de valeurs. Les seules questions sont de savoir si nous aurons collectivement un rôle dans le choix des valeurs garanties et comment garder un regard sur la production du code pour ne pas perdre de rôle dans ce choix. En d'autres termes, les systèmes *blockchain* peuvent

³⁵ L. Kiffer, D. Levin, A. Mislove, "Analyzing Ethereum's Contract Topology", IMC '18: Proceedings of the Internet Measurement Conference, oct. 2018, p. 494-499 : <https://doi.org/10.1145/3278532.3278575>

³⁶ CMF, art. R. 211-9-7 : « Le dispositif d'enregistrement électronique partagé mentionné à

l'article [L. 211-3](#) est conçu et mis en œuvre de façon à garantir l'enregistrement et l'intégrité des inscriptions et à permettre, directement ou indirectement, d'identifier les propriétaires des titres, la nature et le nombre de titres détenus ».

assurer avec succès une sécurité transactionnelle fiable et efficace, il faut toutefois s'en remettre aux règles de droit pour garantir certaines valeurs essentielles, les droits et libertés fondamentaux.

Conclusion

Particulièrement sur ce dernier point, le défi consiste à trouver un équilibre, durable, stable et flexible dans lequel les *Code of Law*, *Code is Law* et possiblement *Code as Law* coexistent et collaborent, sans présenter de risques inacceptables ou de préjudices pour les participants au réseau ou pour la communauté d'utilisateurs. Alors seulement, il sera pourra être considérée la proposition audacieuse de Nick Szabo, selon laquelle : « La décentralisation est ce qui permet à Bitcoin de substituer une armée informatique à une armée de comptables, d'enquêteurs et d'avocats ».

A. F.

