N° XXX

___

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le xx xxx 2018.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA MISSION D'INFORMATION COMMUNE

sur les **chaînes de blocs (blockchains)** (1)

ET PRÉSENTÉ

PAR MME LAURE DE LA RAUDIÈRE ET M. JEAN-MICHEL MIS,

Députés.

___

(1) *La composition de cette mission figure au verso de la présente page.*

La mission d'information commune sur les chaînes de blocs (blockchains) est composée de : M. Julien Aubert, *président,* Mme Laure de La Raudière et M. Jean-Michel Mis, *rapporteurs* ; M. Ugo Bernalicis, Mme Barbara Bessot Ballot, MM. Éric Bothorel, Moetai Brotherson, Jean-René Cazeneuve, Mmes Typhanie Degois, Coralie Dubost, Paula Forteza, Christine Hennion, MM. Philippe Latombe, Michel Lauzzana, Jérôme Nury, Pierre Person, Raphaël Schellenberger, *membres*.

SOMMAIRE

___

Pages

INTRODUCTION

C’est une curiosité renouvelée [(1)] envers les innovations de notre époque, autant que la crainte de voir notre pays manquer le virage d’une nouvelle rupture technologique, qui ont conduit à la création, le 14 février 2018, d’une mission d’information commune sur les usages des bloc-chaînes (*blockchains*) et autres technologies de certification de registre. Présidée par M. Julien Aubert, député de Vaucluse, et ayant pour co-rapporteurs Mme Laure de La Raudière, députée de l’Eure-et-Loir, et M. Jean-Michel Mis, député de la Loire, la mission réunit 17 députés issus de trois commissions permanentes (affaires économiques, finances et lois).

Il faut dire que beaucoup de spéculations et de controverses – voire de mystères ou de fantasmes – entourent aujourd’hui ce procédé. Il en va ainsi des circonstances et de la paternité de sa conception, certain attribuant à un dénommé Satoshi Nakamoto, auteur d’un article remarqué publié en 2008, la fondation du Bitcoin et de la première *blockchain* ou « chaîne de blocs » [(2)]. Plus fondamentalement, d’aucun s’interroge sur l’exacte portée d’une technologie que les uns présentent comme « *la machine de confiance qui, au-delà du Bitcoin, pourrait changer le monde* » [(3)] et qui, pour d’autres, relève au mieux de l’effet de mode, au pire du « *grand mensonge* » [(4)].

D’après la définition de l’Office parlementaire d’évaluation des choix scientifiques et technologiques (OPECST) [(5)], 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

---

(1) Cf. le colloque « Blockchain : Disruption et Opportunités *» organisé le 24 mars 2016 par la Commission supérieure du service public des postes et des communications électroniques à l’Assemblée nationale.*

(2) Selon plusieurs experts rencontrés par les rapporteurs de l’Office parlementaire d'évaluation des choix scientifiques et technologiques, Satoshi Nakamoto ne serait pas un individu mais une équipe pluridisciplinaire, composée notamment de cryptographes de haut niveau, dont plusieurs membres seraient américains. Cet article décrit le fonctionnement d’un protocole permettant la production d’un registre infalsifiable, utilisant un réseau informatique pair à pair – la blockchain – comme couche technologique d’une nouvelle cryptomonnaie – le bitcoin. Il apporte une réponse aux difficultés que constituent les risques de double dépense et de pannes.

(3) The Economist, “The Trust Machine, How the technology behind bitcoin could change the world”, *31 octobre, 6 novembre 2015, n° 44.*

(4) Nouriel Nouribi, « Le grand mensonge de la *blockchain* », *Project Syndicate, 15 octobre 2018 (https://www.project-syndicate.org/commentary/blockchain-big-lie-by-nouriel-roubini-2018-10/french).*

(5) Rapport n° 1092 - Rapport de Mme Valéria Faure-Muntian, MM. Claude de Ganay et Ronan Le Gleut établi au nom de l’Office parlementaire d'évaluation des choix scientifiques et technologiques, sur les enjeux technologiques des blockchains *(chaînes de blocs), juin 2018.*

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.

Certes, il y a loin de la coupe aux lèvres et du concept à la preuve. Toutefois, chacun comprend les effets potentiellement disruptifs d'une technologie qui se donne pour objectif de rendre possible l'établissement d'un consensus au sein d'un groupe dans un cadre désintermédié.

Consciente des enjeux que recèle le développement de protocoles informatiques susceptibles de profondément renouveler les missions et la place des tiers de confiance et de la puissance publique, la mission s'est donné trois principaux objectifs : d'abord, faire œuvre de pédagogie, en présentant l'état de la technique et de ses possibles utilisations – sans s'apesantir toutefois sur la question des « cryptoactifs » ou « cryptomonnaies » qui relève du champ de la mission d'information de la commission des finances consacrée aux monnaies virtuelles ; ensuite, mesurer son impact sur les activités économiques et l'organisation de la vie sociale, y compris pour la vitalité de nos institutions et le bon fonctionnement des services publics ; enfin, permettre à notre pays d'aborder en pleine conscience ce qui pourrait constituer, au même titre qu'internet, l'intelligence artificielle ou l'émergence d'une société de la connaissance, une nouvelle rupture technologique et sociétale dont il importe que l'Europe saisisse cette fois toutes les virtualités afin d'affirmer un modèle et, à tout le moins, de préserver sa souveraineté.

Dans cette optique, au fil des auditions réalisées à l'Assemblée nationale, comme au cours de ses déplacements en France et en Suisse, la mission s'est d'abord attachée à prendre le pouls d'un écosystème en pleine affirmation. À cet effet, elle a recueilli l'expertise et pris note des initiatives de start-ups du secteur, d'entreprises, de développeurs et porteurs de projets, ainsi que de chercheurs. Elle a souhaité également prendre la mesure des enjeux juridiques, économiques, sociaux voire philosophiques qui s'attachent au développement de la *blockchain* et que peuvent appréhender des acteurs plus institutionnels. C'est la raison pour laquelle elle a jugé utile d'entendre, au-delà des rapports et travaux publiés, les représentants de France Stratégie, de la Banque de France, de la Caisse des dépôts et consignations, de la Fédération bancaire française (FBF), de l'Autorité des marchés financiers (AMF), de la Commission nationale de l'Informatique et des Libertés (CNIL), ou encore des ministères de la justice, de l'éducation nationale et des services du Premier ministre. En outre, la mission a pu très largement fonder ses analyses sur les éclairages apportés au plan technique par l'OPECST, d'abord dans le cadre d'une note scientifique, puis dans celui d'un rapport d'information ayant accordé une large place à des préoccupations communes.

Il en ressort que si les protocoles fondés sur des *blockchains* présentent une maturité très inégale, leur relative nouveauté ne saurait remettre en cause leur potentiel fondamentalement disruptif. Du point de vue la mission, la technologie

représente – et mérite – un investissement sur l'avenir qui suppose la mobilisation de ressources nationales dans un cadre juridique pertinent.

Voici près de 25 ans, le rapport Théry [(1)] contribuait à détourner la France de la révolution internet en fournissant des arguments à ceux qui sous-estimaient les capacités d'évolution d'une technologie alors balbutiante. Nous formons ici le vœu qu'au-delà des aléas de toute prédiction quant au devenir des innovations technologiques, les travaux de la mission contribuent à un débat nécessaire sur les moyens pour que la France tienne son rang dans les transformations numériques de l'économie.

(1) Gérard Théry, Alain Bonnafé et Michel Guieysse, Les autoroutes de l'information*, Rapport au Premier ministre, 1994.*

I. DES TECHNOLOGIES DONT LA RELATIVE NOUVEAUTÉ NE SAURAIT REMETTRE EN CAUSE LEUR POTENTIEL FONDAMENTALEMENT DISRUPTIF

A. UNE ASSOCIATION DE PROCÉDÉS RÉVOLUTIONNAIRES, REFONDANT LA CONFIANCE AU SEIN DE SYSTÈMES COMPLEXES

Il y a une promesse économique importante avec les *blockchains*, qui seraient la prochaine grande « disruption » technologique de l'ère internet. Lors de son audition par la mission, M. Gilles Babinet, « digital champion » de la France auprès de la Commission européenne, présentait les *blockchains* comme faisant partir d'un cycle d'innovations inédit : alors qu'internet, jusque-là, avait permis de démocratiser les informations et les échanges (réseaux sociaux, échanges de données en pair-à-pair, commerce en ligne), ce nouvel âge permet de démocratiser la valeur économique et même son principal support, la monnaie.

Toutefois, avant d'explorer cette promesse économique, et d'analyser les différentes applications et les potentiels des *blockchains* au service de l'innovation en France, cette première sous-partie a pour objet de présenter cette technologie. Il s'agira moins de s'attarder sur des développements techniques que de mettre en avant les éléments fondamentalement innovants des *blockchains* : la décentralisation de la confiance, la gouvernance par le grand nombre et la sécurité cryptographique, le recours à de nouveaux instruments de valeur pour aligner les intérêts.

1. Les *blockchains*, un ensemble de technologies

Si certains principes de fonctionnement contiennent un dénominateur commun à l'ensemble des *blockchains*, il faudra distinguer les différents niveaux que sont les *blockchains* ouvertes, les *blockchains* et les *blockchains* privatives.

a. Des dispositifs d'échange de données et de certification d'informations fondés sur la sécurité de la cryptographie et sur le recours au pair-à-pair

Les *blockchains* sont des « technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, 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 » [(1)].

On parle de **registre distribué** parce que la *blockchain* est en premier lieu une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont

(1) Définition proposée par l'OPECST.

également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique.

On parle de **blocs** parce que l'une des particularités de ce registre est d'enregistrer les données sur des blocs qui contiennent une quantité limitée d'informations et qui ne sont « construits » que lorsqu'ils sont validés par la communauté des utilisateurs. L'autre particularité de cette inscription sur bloc est le recours à la cryptographie : par une technique de hachage (*hash*) des données, il n'y a aucune équivalence entre les données brutes (l'historique d'une transaction, un échange, un script, etc.) et les données hachées inscrites effectivement sur le bloc après passage au tamis cryptographique. Chaque utilisateur détient une clé publique, qui lui sert d'identifiant sur le réseau, et une clé privée, intrinsèquement liée à sa clé publique (1) et qui permet de réaliser les opérations qui lui sont propres (acheter, vendre, conclure un contrat). Dans le cas d'une transaction de bitcoins validée par la communauté, le bloc contient la clé publique de l'émetteur de la transaction, le montant de la transaction et la clé publique du récepteur de la transaction. Ces informations sont visibles par l'ensemble du réseau. La clé privée de l'émetteur lui permet de payer effectivement ; celle du récepteur lui permet de recevoir le paiement (d'où la nécessité absolue de garder cette clé privée).

On parle de ***blockchains*** car les transactions ou les informations échangées entre les utilisateurs du réseau sont regroupées par blocs horodatés et irréversiblement liés les uns aux autres. Autrement dit, les blocs s'enchaînent les uns après les autres au terme d'un processus de validation (voir ci-après). Une fois un bloc validé, son contenu devient visible et figé pour l'ensemble des détenteurs du registre. Il est très important de relever que les écritures enregistrées sur ce bloc et sur tous les précédents sont inaltérables et infalsifiables. C'est une des principales plus-values de la *blockchain* : ce grand registre ne peut pas être modifié. Ce qui y est inscrit demeure visible par tous et pour toujours. Il faut, en réalité, un très rare consensus des acteurs de la *blockchain* pour effectuer un « retour en arrière » sur des blocs validés, et toujours pour des cas de force majeure.

Qui sont ces acteurs ? La *blockchain* est construite par certains utilisateurs du réseau davantage engagés que les utilisateurs « lambda ». Les blocs sont créés par certaines personnes, qui, dans la *blockchain* historique Bitcoin, sont appelées « mineurs » (*miners*). Ils mettent à contribution de la puissance de calcul informatique pour « miner » les blocs et sont rémunérés pour cela. Un bloc « miné » est transmis à tous les autres « nœuds » (*nodes*) du réseau, qui détiennent le registre distribué qu'est la *blockchain* et l'actualisent en permanence. Un bloc ne peut être validé et donc s'ajouter à la chaîne que si un consensus des nœuds le permet : les centaines, les milliers voire les dizaines de milliers de copies du registre sont alors mises à jour simultanément et régulièrement, à mesure que les blocs sont minés puis validés.

---

(1) Cette caractéristique fait d'une blockchain classique un système où l'on évolue sous pseudonyme mais non anonymement, contrairement à une idée répandue.

LECTURE : 9990 NŒUDS DE RÉSEAU SUR LA *BLOCKCHAIN* BITCOIN LE 15 NOVEMBRE 2018 ET LEUR EMPLACEMENT

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Nov 15 2018 17:27:38 GMT+0100 (Europe centrale).

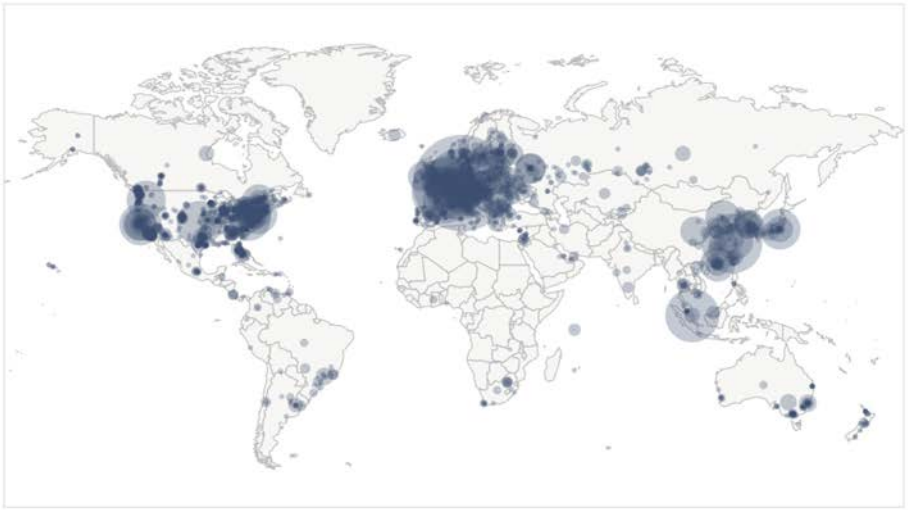
9990 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

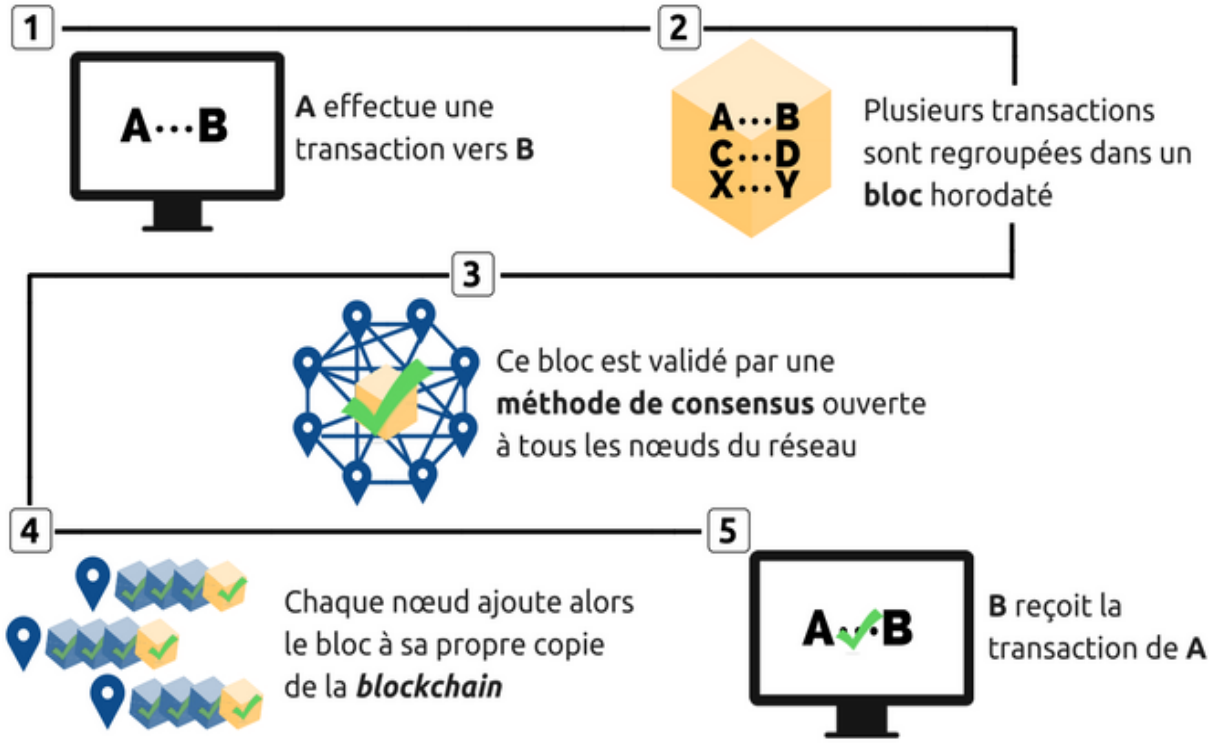
RANK	COUNTRY	NODES
1	United States	2361 (23.63%)
2	Germany	1934 (19.36%)
3	France	674 (6.75%)
4	China	654 (6.55%)
5	Netherlands	510 (5.11%)
6	n/a	461 (4.61%)
7	Canada	369 (3.69%)
8	United Kingdom	293 (2.93%)
9	Russian Federation	268 (2.68%)
10	Singapore	247 (2.47%)

More (100) »



Source : bitnodes.earn.com

Dans d'autres *blockchains*, la création de nouveaux blocs fonctionne sur des méthodes de consensus différentes que celle du minage, qui permet la création d'un bloc en contrepartie d'une preuve de travail (*proof of work*) [(1)]. Le présent rapport y reviendra en détail.



Source : OPECST

(1) Le minage est en réalité le processus de résolution d'une énigme cryptographique qui met en compétition tous les nœuds du réseau. Résoudre l'énigme permet d'être rémunéré pour cette preuve de travail. Cette résolution utilise des ressources de calcul informatique parfois importantes : le présent rapport y reviendra.

À quoi cela sert-il ? Les *blockchains* se sont historiquement développées pour soutenir des transactions réalisées sous une nouvelle forme de moyens de paiement, appelées cryptomonnaies et qui ont comme caractéristique principale de n'être gérées par aucun organisme centralisateur (comme une banque centrale), mais uniquement par l'action conjointe d'un programme informatique et des utilisateurs de ces cryptomonnaies. En fonction de la forme des *blockchains*, des caractéristiques différentes peuvent être mises en avant pour répondre à des besoins bien plus diversifiés que la gestion d'un système international de paiements. Ainsi, l'immuabilité et la publicité des *blockchains* autorisent des développements intéressants en matière de traçabilité des produits ou en matière de certification des échanges. C'est également un très bon moyen de garantir la fiabilité de certaines informations, comme la détention d'un diplôme qu'on déclare avoir obtenu telle année dans tel établissement. C'est enfin une technologie qui est particulièrement prometteuse pour faciliter l'exécution de contrats, appelés *smart contracts*. En réalité, les cas d'usage sont très nombreux et font l'objet d'expérimentations lancées à forte cadence depuis quelques années, y compris en France, où un écosystème spécifique (représenté par des associations comme la ChainTech, auditionnée par la mission, ou FranceBlocktech), par exemple, se développe.

En quoi est-ce si novateur ? À plusieurs titres :

- la *rapidité* : la validation d'un bloc selon l'infographie ci-dessus ne prend, pour les transactions en bitcoins, que quelques minutes – bien que la saturation de la *blockchain* historique tende à démentir progressivement ce constat. Pour d'autres cryptomonnaies comme les ethers, cela peut n'être que quelques secondes. *A contrario*, un virement entre banques prend aujourd'hui dans de nombreux cas, plusieurs jours ;

- la *sécurité* : la contrainte de validation par un ensemble de nœuds permet de se prémunir du risque de malveillance ou de détournement, puisque les nœuds surveillent le système et se contrôlent mutuellement. Ce contrôle par les pairs permet également d'éliminer le recours à une autorité centralisée qui exerce habituellement ce rôle de validation (pour les transactions bancaires, par exemple) ; en outre, la sécurité est renforcée par l'auditabilité des informations présentes sur les *blockchains*, qui sont ouvertes ou facilement rendues ouvertes à des tiers ;

- les *gains de productivité et d'efficacité* : les *blockchains*, en confiant l'organisation d'échanges à un protocole informatique, réduisent mécaniquement tout coût de transaction ou de centralisation [(1)] existant dans les systèmes traditionnels : frais financiers, frais de contrôle ou de certification, recours à des intermédiaires qui se rémunèrent pour leur service ; automatisation de certaines prestations, etc.

---

(1) Dans la dichotomie classique entre le marché et l'autorité, proposée par l'économiste R. Coase, une blockchain glisse vers l'autorité mais conserve beaucoup des caractéristiques du marché, notamment le caractère décentralisé et l'alignement des intérêts par une « main invisible ».

Est-ce vraiment nouveau ? Une critique récurrente de certains projets lancés sous la bannière des *blockchains* est qu'en réalité, ces projets n'utilisent des *blockchains* que le nom, et recourent en réalité à des techniques ou technologies déjà bien connues. Par exemple, les technologies de registre distribué – à savoir des bases de données accessibles depuis plusieurs terminaux de façon indépendante et simultanée – existent depuis vingt ans, et sont utilisées par le grand public (avec des logiciels ou des applications comme *Sharepoint* ou *Google documents*). De même, selon Emmanuelle Anceaume, chercheuse auditionnée par la mission, le mécanisme d'horodatage des *blockchains* est connu depuis 1992.

En réalité, les *blockchains* portent le principe de leur décentralisation complète : non seulement les usages sont décentralisés, mais la « propriété » et la gouvernance des *blockchains* appartiennent à l'ensemble du réseau. Seul le protocole initial, qui contient notamment une méthode de consensus et des règles de validation des opérations, permet d'apporter l'ordre parmi l'ensemble des utilisateurs du réseau qui vont désormais partager ces règles, partager les données contenues sur la *blockchain* et participer à sa construction. Partant, l'esprit de communauté et de partage du pouvoir sont des valeurs fortes des premiers « écosystèmes *blockchain* ».

Les fondements idéologiques des premières communautés *blockchain*

La première *blockchain*, Bitcoin, serait née d'un mouvement idéologique qui considère avec circonspection, sinon méfiance, les institutions publiques comme privées et la centralisation et l'autorité qu'elles représentent. La création du bitcoin comme « monnaie » concurrence frontalement une prérogative souveraine, « battre monnaie », et s'inscrit dans un rejet des institutions financières au sens large – États comme banques.

Les premières communautés *blockchain*, pour autant qu'on puisse les définir ou encore les caractériser de façon générale, valorisent le respect de la vie privée et la confidentialité des échanges (contre la surveillance étatique), corollaires de la liberté individuelle, principe qui ne doit, selon elles, être peu ou pas « entravé » par l'intervention publique.

Les premières technologies de *blockchains* véhiculent donc, par ses mécanismes et par les extensions d'usage qui sont parfois imaginées au-delà de la création de « monnaie », une vision de la société qui s'approche de celle portée par le libertarisme ou par l'anarchisme, qui partagent au moins la conception d'un État minimal et le rejet d'une autorité centralisée qui nuit à la liberté des individus.

Mais comme pour Internet, il n'y a pas véritablement de contenu idéologique d'une technologie. Agnostique, elle dépend des usages qui en sont faits et de son appropriation par le plus grand nombre. Si les pionniers d'Internet mettaient en avant l'anonymat et l'horizontalité des échanges ou encore le développement du pair-à-pair, la massification des usages a conduit à une réalité tout autre.

Inversement, il est possible de reprendre toutes les caractéristiques d'une *blockchain* (notamment la protection cryptographique ou l'immuabilité des données) tout en conservant le pouvoir sur celle-ci. On quitte alors le principe de

la *blockchain* « chimiquement pure » pour obtenir des technologies plus maniables, plus opérationnelles, plus compatibles avec les réglementations en vigueur mais également moins disruptives.

Il faut attacher une grande importance à la distinction entre ces deux catégories de *blockchains* – les *blockchains* ouvertes et les *blockchains* privatives car cette distinction est capitale dans la compréhension des principaux enjeux à venir pour les *blockchains*.

b. Une distinction capitale : les blockchains ouvertes et les blockchains privatives

Il existe plusieurs façons de distinguer les *blockchains* ouvertes, qui comportent l'ensemble des caractéristiques techniques présentées ci-dessus, et les *blockchains* privatives, qui ne sont utilisées que par certains acteurs en nombre limité et non par une multitude de personnes.

Le tableau ci-dessous, produit par un groupe de travail de France Stratégie (1), auditionné par la mission, illustre clairement le nuancier des *blockchains*.

Type de blockchain	Lecture du registre	Réalisation d'une transaction	Validation	Exemple
Ouverte	Ouverte à tous	N'importe qui	N'importe qui, à condition de réaliser un investissement significatif en puissance de calcul (*proof of work*) ou dans la détention de cryptomonnaie (*proof of stake*)	Bitcoin, Ethereum
	Ouverte à tous	Participants autorisés	Tout ou partie des participants autorisés	Sovrin
Fermée	Restreinte aux participants autorisés	Participants autorisés	Tout ou partie des participants autorisés	Banques opérant un registre partagé
	Totalement privée ou limitée à un ensemble de nœuds autorisés	Limitée à l'opérateur du réseau	Limitée à l'opérateur du réseau	Registre interne à une banque partagé entre des filiales

Source : Global Blockchain Benchmarking study, Dr Garrick Hileman et Michel Rauchs, 2017

Les *blockchains* ouvertes (*permissionless*) sont peu nombreuses aujourd'hui. Elles sont essentiellement le support de cryptomonnaies et sont utilisées à des fins de transaction : Bitcoin (qui produit des bitcoins) ou Ethereum (qui produit des ethers) sont les plus développées. Ethereum est également le support de *smart contracts*, avec un potentiel et des limites qui sont exposés dans des développements ultérieurs.

Dans les ***blockchains* ouvertes**, tout le monde peut être à la fois à l'origine de transactions, d'échanges et être un nœud du réseau. La décentralisation est

(1) France Stratégie (groupe de travail présidé par Mme Joëlle Toledano), « Les enjeux des blockchains », juin 2018.

complète. L'existence d'une cryptomonnaie est requise pour créer les incitations financières suffisantes pour organiser de façon vertueuse les relations entre utilisateurs.

Dans les ***blockchains* semi-ouvertes, parfois qualifiées par l'anglicisme « permissionnées »**, les *blockchains* sont visibles par tous (mode lecture activé) mais pas modifiables, au sens de la validation de blocs, par tous (mode écriture désactivé). Ces *blockchains* remettent un cran de centralisation puisque seuls les nœuds autorisés (donc connus) peuvent modifier la *blockchain*.

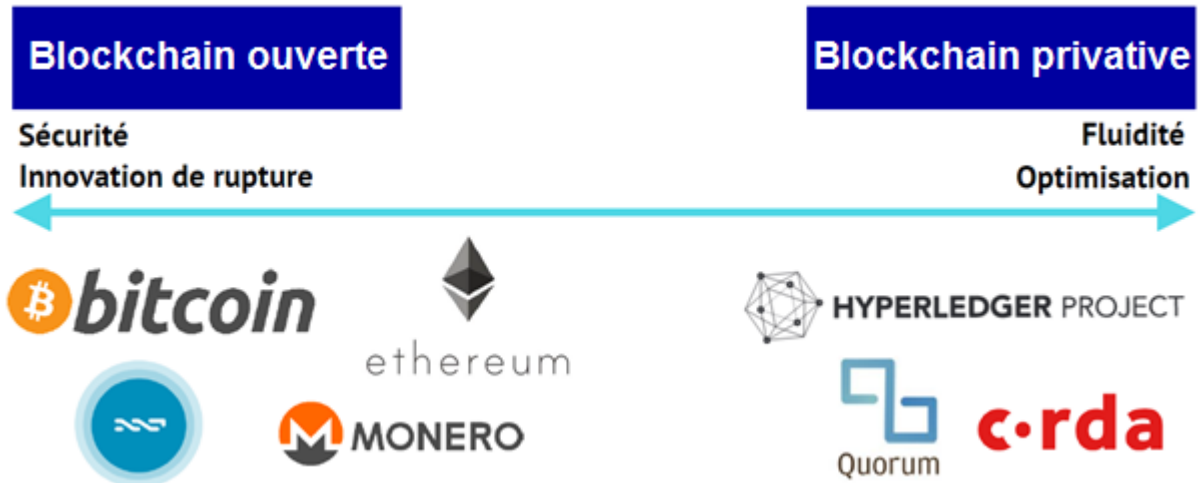
Les *blockchains* privatives vont plus loin.

La ***blockchain* « de consortium »** permet de réunir plusieurs acteurs en nombre limité et de faciliter la gouvernance de leurs intérêts mutuels, pour résoudre des situations de « dilemme du prisonnier » [(1)]. C'est le même principe qu'une *blockchain* ouverte mais avec une logique de club : il s'agit de partager les informations, de faciliter les échanges, de résoudre les litiges et d'instaurer la confiance entre plusieurs personnes – souvent morales, comme des entreprises – de façon peu coûteuse, plus fluide et en mettant de côté leurs intérêts divergents. Chaque participant est un nœud du réseau ; il n'y a ni minage des blocs, ni besoin d'établir des solutions de consensus. Les acteurs s'entendent autrement que par la technologie, qui devient donc principalement utilitariste. L'exemple le plus connu d'une telle forme de *blockchain* est Corda, développée par le consortium R3 qui réunit des établissements financiers (plus de 80) pour accélérer l'enregistrement de leurs flux de transactions. Mais d'autres initiatives sectorielles connaissent un certain succès, comme la *blockchain* en faveur du négoce international de matières premières, avec un cas d'usage porté par *Komgo SA*, qui fera l'objet d'un développement ultérieur.

Enfin, les ***blockchains* purement privatives** s'apparentent davantage à une application intranet qui permet d'apporter du service ou des gains de productivité au sein d'une même organisation. Il s'agit de reprendre certaines caractéristiques innovantes des *blockchains* en matière de gestion de l'information ou d'archivage (horodatage, données non modifiables et facilement rendues ouvertes, etc.). La centralisation est complète : un seul acteur (l'entreprise, le ministère, le service informatique) gère le développement de la *blockchain* en fonction de l'usage qui en est attendu.

---

(1) Ce dilemme bien connu de la théorie des jeux montre que des acteurs aux intérêts divergents (par exemple, des entreprises en concurrence), ne parviennent pas spontanément à partager les informations ou à trouver une solution qui leur serait mutuellement bénéfique. Le dilemme du prisonnier conduit naturellement à un équilibre de Nash, ou équilibre de second rang : les acteurs en présence ne parviennent qu'à une solution sous-optimale.



Source : Blockchain Partners

Les développements à venir seront l'occasion de présenter plusieurs cas d'usage. Il est cependant important de préciser, à ce stade, pourquoi la distinction entre *blockchain* ouverte et *blockchain* privative est si importante [(1)].

La *blockchain* ouverte est celle dont le contenu en innovation est le plus important mais dont les différentes filières économiques ne se sont pas encore appropriées suffisamment le potentiel technologique. Parvenue à maturité, elle pourra avoir des conséquences significatives sur l'organisation de nos modèles économiques, notamment sur leur gouvernance. C'est une **innovation radicale**.

La *blockchain* privative est celle qui met à profit les caractéristiques les plus immédiatement utiles de cette technologie, et écarte celles qui posent aujourd'hui des problèmes non résolus : la décentralisation, la gouvernance à grande échelle, le contrôle par les pairs, la sécurité face aux attaques, etc. En somme, une *blockchain* mais contrôlée, qui a comme principal bénéfice de proposer des solutions utiles à court terme, et qui sont celles qui se développent le plus rapidement aujourd'hui. C'est une **innovation incrémentale**.

Par exemple, en France, la Banque de France développe une *blockchain* expérimentale, MADRE, pour faciliter les virements SEPA entre acteurs bancaires. Elle permet d'assurer la confidentialité des échanges et d'instaurer un cadre de gouvernance partagé entre six acteurs bancaires. L'avantage sera de gagner du temps (quelques minutes *versus* quelques jours) pour les virements. Cette *blockchain* est en réalité un dérivé de consortium de la *blockchain* ouverte Ethereum, modulée afin de s'inscrire sans ambiguïté dans le cadre juridique du

---

(1) Le présent rapport n'ira cependant pas sur le terrain du jugement de valeur. Pour certains acteurs très engagés dans les communautés des blockchains ou pour certains observateurs, les blockchains *privées, parfois qualifiées de « pseudo-*blockchains *» ou de « fausses* blockchains *» spolient le concept et dénaturent la philosophie à l'origine de cette innovation. Les paradoxes sont pourtant nombreux dans cet écosystème : par exemple, le bitcoin avait pour objet de libérer les personnes des institutions financières centralisées, mais elles se sont depuis largement appropriées les cryptoactifs, souvent à des fins spéculatives – quand les vrais puristes, les « hodlers », ont conservé leurs bitcoins même quand le cours atteignait des niveaux insoupçonnables à l'origine.*

Règlement général sur la protection des données (RGPD) et d'être facile d'accès pour les acteurs qui souhaiterait rejoindre le projet.

Cet exemple illustre un autre aspect essentiel dans la dichotomie ouverte/privative. Les *blockchains* ouvertes ouvrent de nouvelles perspectives mais posent des problématiques que nos modèles de responsabilité juridique ou de gouvernance actuels ont des difficultés à gérer. En particulier, ce sont ces *blockchains* qui posent le plus grand défi au cadre normatif dont le législateur est en partie responsable. L'adaptation du cadre juridique aux enjeux de confidentialité, de sécurité, de gestion de risques ou des données personnelles est une question à approfondir plus amplement, ce qui sera l'objet de la deuxième partie du présent rapport.

Si on constate aujourd'hui que la plupart des expérimentations en cours ont lieu sur des *blockchains* privatives, plus pratiques, plus faciles à réguler, plus utiles à court terme, vos rapporteurs insistent sur le fait que **l'horizon d'innovation demeure celui de la *blockchain* ouverte**. Or, aujourd'hui, les acteurs français ou européens, notamment publics, n'ont guère d'autre choix que de recourir aux *blockchains* ouvertes déjà relativement bien développées, comme Ethereum ou Bitcoin, qui partagent le point commun d'échapper à notre souveraineté (1), à nos standards et à notre cadre juridique. Il devient donc urgent de déployer, au bon niveau de taille critique – le niveau européen est probablement le plus adapté – les germes d'une *blockchain* ouverte qui puisse rivaliser avec les meilleures *blockchains* aujourd'hui développées.

Proposition n° 1 : Favoriser la création d'un écosystème suffisamment mature pour que se développe une *blockchain* ouverte issue d'initiatives françaises ou européennes, alimentées par des financements publics de soutien à la recherche et au développement, sur le modèle de l'intelligence artificielle.

2. Un moyen technique d'assurer la confiance avec une gouvernance décentralisée, en organisant en théorie l'alignement des intérêts

Cette sous-partie a pour objet d'approfondir les fondamentaux des *blockchains* ouvertes, à savoir leur philosophie, leur fonctionnement et leur potentiel disruptif. Bien qu'il ne soit plus fait référence à la dichotomie entre *blockchains* ouvertes et privatives, il est facile de déduire quels développements sont communs aux deux catégories de *blockchains* et lesquels ne concernent que l'étude des *blockchains* ouvertes.

a. La décentralisation de la confiance

Dans sa philosophie initiale, la *blockchain* est la promesse d'éliminer la centralisation, l'intermédiation et la nécessité de recourir à des tiers de confiance

(1) On pourrait arguer qu'elles échappent à toute souveraineté nationale, par principe. La réalité est plus complexe : c'est une bataille de définition des normes, des standards, des précédents technologiques (l'effet de sentier) qui se joue aujourd'hui.

pour valider certaines opérations économiques. Comme cela a déjà été rappelé, la première *blockchain*, Bitcoin, a été créée spécifiquement pour éliminer le recours à des institutions financières comme les banques [(1)], mais le potentiel technologique des *blockchains* peut avoir des conséquences économiques et sociales beaucoup plus importantes.

En effet, les principales *blockchains* ouvertes, Bitcoin et Ethereum, sont parvenues à assumer une fonction qui était, jusqu'alors et dans nos économies contemporaines, exclusivement souveraine : créer de la monnaie. La fonction de la monnaie, en particulier de la monnaie sous forme fiduciaire (billets ou pièces), est de véhiculer de la confiance : en soi, un billet de banque n'a aucune valeur, puisque ce n'est qu'un bout de papier. Un billet de 10 euros a une valeur de 10 euros parce que l'ensemble des agents économiques a confiance dans le fait que ce billet permet de véhiculer cette valeur, confiance qui est garantie par l'État et par les banques centrales. L'indépendance des banques centrales, largement répandue de nos jours (à l'exception notable de certaines économies développées comme le Royaume-Uni ou le Japon), a d'ailleurs comme principal intérêt d'augmenter encore le capital de confiance des citoyens dans la monnaie : l'État ne peut plus jouer avec la planche à billets pour réduire sa dette.

L'exploit qu'est parvenu à accomplir l'écosystème des *blockchains* est celui de se substituer – à son échelle – au vaste système financier et à la confiance dans la monnaie qui a mis plus d'une centaine d'années à s'acquérir, en créant une « monnaie » [(2)] purement virtuelle, sans cours contrôlé par une autorité publique, et dont la masse monétaire n'évolue que par l'exécution d'un protocole informatique. Il s'agit donc d'**une grande opération de désintermédiation**, qui pourrait tout à fait se répliquer dans d'autres secteurs que le secteur financier.

En effet, la *blockchain* Bitcoin n'a que dix ans d'ancienneté et sa communauté est déjà parvenue à développer un système mondial de paiements avec beaucoup moins d'intermédiaires que le système traditionnel et les bitcoins s'échangent librement sans contrôle bancaire ou étatique particulier. Comme le présent rapport le montrera, ce système n'est pas exempt de failles. Toutefois, il démontre qu'**une technologie peut véhiculer de la confiance** sans qu'un tiers, généralement une autorité ou une institution (une banque, une poste, un État, une commune, etc.) ne soit impliqué.

Si la confiance n'est plus dans l'intermédiaire mais dans la technologie, qui est neutre et ne peut être manipulée, c'est parce que cette technologie a instauré les conditions de la confiance : un protocole qui garantit la sécurité des échanges, la transparence de l'information et la stabilité du système grâce à une

---

(1) La première phrase du white paper *de « Satoshi Nakamoto » introduisant Bitcoin en 2008 indique que « le commerce en ligne est arrivé au point de dépendre presque exclusivement d'institutions financières qui servent de tiers de confiance pour effectuer les paiements électroniques » (traduction libre).*

(2) L'usage des guillemets se justifie car la question de savoir si une cryptomonnaie comme le bitcoin possède tous les attributs économiques d'une monnaie est débattue. Par exemple, le bitcoin a bien une valeur d'échange mais est-ce un actif de réserve, comme l'or ? En outre, une grande majorité de biens et de services ne peut être acquise avec des cryptomonnaies, à ce jour.

complète décentralisation de la décision ; la *blockchain* n'appartient à personne et elle appartient à tous, selon des règles fixes et transparentes de fonctionnement – le protocole informatique – connues de tous**. La décentralisation de la confiance est donc, vraisemblablement, la caractéristique la plus disruptive des *blockchains***. Par exemple, théoriquement, les utilisateurs de la *blockchain* Bitcoin détiennent eux-mêmes leurs bitcoins – tandis que la monnaie traditionnelle est principalement détenue par le système bancaire (monnaie fiduciaire ou scripturale, présente sur les comptes courants).

La confiance ainsi créée tient cependant à peu : elle nécessite la robustesse et l'infaillibilité de la technologie sur laquelle elle repose. C'est pourquoi les communautés de développeurs des *blockchains* sont si préoccupées de la sécurité de leur système. D'une part, la sécurité est l'un des *credo* des *blockchains* ; d'autre part, si le code d'une *blockchain* est trop faillible ou a été piraté, la confiance s'évanouit, la cryptomonnaie qui lui est associée s'effondre et, avec elle, la *blockchain* et tous ses usages.

Bien au-delà de la monnaie, la *blockchain* contient donc le pouvoir théorique de supprimer les intermédiaires et les tiers de confiance, sur un édifice qui demeure fragile pour le moment. Des développements montreront que ce postulat est plus complexe qu'il n'y paraît, car il faut toujours distinguer ce qu'il se passe sur la *blockchain* et en dehors (le lien entre les deux pouvant être fait par un *oracle* – voir ci-après) : à l'usage, il est possible d'affirmer que les technologies de *blockchains* et les tiers de confiance trouvent davantage à se renforcer mutuellement qu'à se nuire.

Comment la décentralisation peut être mise à profit du renforcement d'une communauté d'utilisateurs : l'exemple du jeu vidéo

Le jeu vidéo est la première industrie culturelle en France en 2018. Ce secteur a connu d'importants bouleversements ces dernières années, notamment avec l'apparition de grandes communautés de joueurs évoluant ensemble sur internet. Un des principaux éditeurs de jeux actuels, Ubisoft, a lancé une opération de recherche et de développement autours des *blockchains* afin de tirer partie des potentialités de cet « internet décentralisé » pour ses joueurs.

Selon les représentants de cette entreprise, auditionnés par la mission, les avantages d'une décentralisation de certains aspects des jeux permettront un niveau d'implication plus fort du joueur et la possibilité d'imaginer une gouvernance partagée (entre joueurs, voire entre joueurs et éditeurs).

Par exemple, avec les incitations financières adaptées, à savoir des jetons qui pourront être dépensés dans le jeu ou faire l'objet de transactions sur des marchés secondaires (1) organisés, les éditeurs de jeux pourront récompenser les services rendus par la communauté des joueurs (*beta testing*, entraide entre joueurs, mise en avant de comportements respectueux).

De façon plus ambitieuse, la décentralisation de la *blockchain* pourra permettre de faire du joueur un co-créateur, notamment des règles de jeu (avec un consensus à trouver au sein de la communauté) ou de niveaux ou de modes de jeu nouveaux. Cela existe déjà (le *modding*) mais l'initiative serait partagée entre joueurs et récompensée par l'écosystème. Le salon Vivatech de 2017 a été l'occasion de montrer qu'un jeu d'exploration et de chasse au trésor pouvait même être continûment étendu par l'action des joueurs qui créent de nouvelles îles.

La question des joueurs âgés de moins de dix-huit ans se pose toutefois. De la même façon qu'ils peuvent être trop facilement exposés à des jeux violents ou à des contenus inappropriés, il est problématique qu'ils puissent avoir accès à des systèmes de jetons qui peuvent s'apparenter à des jeux d'argent. Mais parmi les promesses des *blockchains* pourrait figurer celle d'un meilleur contrôle de l'âge dans l'accès au contenu – avec des clés d'accès qui contiennent cette information de façon sûre.

b. La gouvernance et le consensus

La confiance n'est pas le seul ingrédient qui fait fonctionner une *blockchain*. La décentralisation qu'elle autorise doit conduire à une gouvernance de tous les utilisateurs impliqués sur le réseau de la *blockchain*.

Cette conception, qui ressort en quelque sorte d'un **pari de philosophie politique**, est au fondement de la construction d'une *blockchain* puisque, comme il a été indiqué précédemment, un bloc ne peut être créé que lorsqu'un consensus émerge pour le valider.

Il faut donc distinguer deux consensus : le consensus algorithmique, qui permet de répondre au protocole informatique et d'autoriser la validation d'un

(1) Un tel marché est déjà existant et bien développé : par exemple, le « Marché de la communauté Steam », qui est une plateforme de vente de jeux vidéos.

bloc – il est acquis selon des modalités propres à chaque *blockchain* – et le consensus politique, qui consiste, pour les utilisateurs, à **se mettre d'accord**. Les deux consensus se confondent généralement. Cependant, il arrive que les utilisateurs du réseau soient en désaccord sur le consensus algorithmique à trouver. Cette situation pose un problème de gouvernance qui peut donner lieu à l'apparition de « schismes » : dans la *blockchain* ouverte, il n'y a pas de Salomon pour trancher. On parle de bifurcation (*fork*), qui peut être douce (*soft fork*) ou radicale (*hard fork*). Les bifurcations douces renvoient à une modification du code qui permet aux blocs produits sous la nouvelle version d'être validés par des nœuds fonctionnant encore sous l'ancienne version de la *blockchain* ; les *hard forks* renvoient aux situations dans laquelle une telle rétrocompatibilité est impossible et où les nœuds doivent faire un choix.

Comment cela se déroule-t-il concrètement ? Une *blockchain* dont le code est modifié, par exemple pour une mise à jour bénigne donne, en réalité, naissance à une nouvelle *blockchain*. Celle-ci ne fonctionne que si une majorité suffisante de nœuds du réseau l'accepte et l'intègre dans son processus de validation. À la différence des logiciels classiques, dont l'éditeur propose à l'utilisateur de façon unilatérale une mise à jour, la *blockchain* fonctionne, sur un modèle décentralisé. Lorsque la mise à jour ne pose pas de problème, la nouvelle *blockchain* est acceptée à l'unanimité.

Cependant, lorsque les modifications radicales du code ne sont pas intégrées par l'ensemble du réseau, par exemple lorsqu'un ensemble de nœuds « puristes » refusent une modification du code originel malgré la présence d'une faille, **deux *blockchains* commencent à coexister**. En août 2017, les *blockchains* Bitcoin Cash et Bitcoin Gold sont ainsi nées de bifurcations de Bitcoin d'origine (*core*) : les trois cryptomonnaies se font désormais concurrence. En cela, un tel mouvement de bifurcation n'est guère différent d'un contentieux classique entre associés, sur l'avenir de leur entreprise par exemple, et qui conduit au départ de certains d'entre eux pour créer une entreprise concurrente [(1)]. De même, Bitcoin bénéficie toujours d'un effet réputationnel plus important et c'est à ses concurrents de « faire leurs preuves » pour attirer de nouveaux utilisateurs, tout comme une nouvelle entreprise doit forger son image de marque.

Outre une mise à jour du code, les modifications d'une *blockchain* peuvent avoir pour objet « d'effacer » des blocs, c'est-à-dire de revenir à un état antérieur de la *blockchain* lorsque celle-ci a été altérée.Par exemple ce fut le cas lorsque la *blockchain* Ethereum a subi l'attaque de son projet TheDAO [(2)]. Cela suppose aussi d'annuler les transactions légitimes mais ultérieures aux transactions malveillantes. L'impact majeur d'une telle décision sur l'ensemble du système, associé au nécessaire consensus qu'il faut dégager pour y parvenir, justifie que de

(1) À ceci près que le droit des affaires contrôle bien mieux ces situations, avec des exigences comme l'interdiction du démantèlement ou les clauses contractuelles de non-concurrence.

(2) Pour un résumé : https://www.ethereum-france.com/the-dao-post-mortem/

telles opérations soient rares et fassent systématiquement l'objet de débats passionnés et tendus au sein de la communauté concernée.

La gouvernance d'une *blockchain*, fonctionnant à coups de consensus, serait souvent dans l'impasse si, à l'instar d'une organisation décentralisée comme un marché, un mécanisme n'était pas mis en œuvre pour favoriser l'alignement des intérêts. Il s'agit des cryptoactifs qui sont nécessairement associés aux *blockchains* ouvertes.

c. L'incitation financière grâce à l'émission de jetons

La particularité des technologies des *blockchains* est leur lien très étroit avec un système d'échange de valeur se rapprochant fortement de monnaies (cryptomonnaies) ou d'actifs financiers (jetons). Les *blockchains* ne peuvent donc pas être étanches dans le monde des « cryptos ». Après tout, la première *blockchain* n'a été conçue que pour supporter le développement d'un nouvel outil monétaire.

La présence d'un système d'échange d'actifs au sein d'une *blockchain* ouvertes est fréquente pour au moins trois raisons :

- la *blockchain* est un outil particulièrement adapté aux transactions ;

- l'échange de valeur « économicise » la *blockchain* : elle permet d'y intégrer des logiques d'incitation financière et d'alignement des intérêts privés (la « main invisible » d'Adam Smith), bref, une logique de marché pour permettre de coordonner l'action de très nombreux utilisateurs sans force centralisatrice (de « commissaire-priseur », pour filer la comparaison avec l'économie classique) ;

- le potentiel disruptif des *blockchains* tient beaucoup à leur capacité à engendrer des flux financiers et à créer de la valeur grâce à des systèmes de jetons : dans la deuxième partie seront notamment exposés les mécanismes des offres publiques de jetons (ICO).

Inversement, dans le cas de *blockchains* privatives ou de consortium, où les acteurs sont peu nombreux, connus et où l'utilité de la *blockchain* réside davantage dans ses autres caractéristiques (rapidité des échanges, sécurité des données conservées, gouvernance optimisée, etc.), le recours à un cryptoactif ne se justifie pas obligatoirement.

L'exemple du projet Ark

Reçus par la mission, les représentants de la start-up Ark Ecosystem ont présenté leurs projets en cours. C'est une société coopérative qui a pour ambition de livrer des *blockchains* clé-en-main à leurs clients, et de tisser une toile (SmartBridge) de *blockchains* qui relient tous les usages pour lesquelles elles auront été conçues, à partir d'Ark, une *blockchain* matricielle.

Fonctionnant avec un jeton, l'ark, qui a fait l'objet d'une émission (ICO) en 2016, la *blockchain* Ark évolue donc en permanence, avec un système de consensus fonctionnant à partir d'une preuve d'enjeu déléguée (delegated proof of stake, DPoS) qui permet à des nœuds appelés délégués de valider les blocs en échange d'arks.

Pour ses représentants, il faudra encore de nombreuses années avant que la *blockchain* fasse l'objet d'une « compréhension sociale », accessible à tous et qui permette sa réelle généralisation. Les solutions proposées par l'entreprise sont, comme beaucoup dans cet écosystème, des solutions d'entreprises (*B-to-B*).

Source : Mission d'information commune sur les usages des bloc-chaînes (blockchains) et autres technologies de certification de registres.

Pour vos rapporteurs, une des principales disruptions des *blockchains* est là : elles créent la capacité de rémunérer, d'intéresser les utilisateurs d'un réseau selon les tâches qu'ils fournissent pour le réseau ou pour l'écosystème ou pour adopter un comportement vertueux, le tout de façon décentralisée. Des expérimentations ont par exemple actuellement cours pour encourager des patients, contre rémunération en jetons, à fournir leurs données de santé à une *blockchain* créée à des fins de recherche, afin de récolter des données récentes et fiables et ainsi faire progresser la recherche médicale. Rappelons qu'une autre disruption d'importance est la révolution de la gouvernance, notamment entre acteurs ayant des intérêts non seulement distincts, mais parfois concurrents, comme au sein d'une filière : la *blockchain* permet d'échanger des informations pertinentes pour tous, tout en protégeant les secrets d'affaires de chacun.

Les *blockchains* autorisent donc d'imaginer l'avènement d'un internet de la valeur, qui serait plus efficace et mieux maîtrisé. Les applications sont importantes : le lien entre un échange de biens ou une prestation de services et le paiement associé peut être automatisé grâce à un *smart contract* simple et géré sur une *blockchain*, sans passer par l'intermédiaire financier (une banque, un système de paiement comme Paypal ou Lydia, de l'argent liquide). En quelque sorte, la gestion de la valeur redescend au niveau des utilisateurs de la *blockchain*, qui est en mesure de la redistribuer de façon parfaitement neutre, en appliquant son code, et la captation de la valeur, la présence de marges, pourrait être beaucoup plus lisible et transparente, puisque la *blockchain* a vocation à être ouverte.

Toutefois, comme des développements à venir le montreront, la création d'un jeton (et son émission au public) comporte le risque d'être dévoyé comme de la création de la valeur. Un jeton a une valeur d'échange, parfois une valeur d'usage (comme posséder des droits politiques sur l'entreprise qui émet le jeton),

mais rarement une valeur intrinsèque qui justifie qu'on puisse le posséder comme une fin en soi ou pour des motifs de spéculation.

B. UN DÉVELOPPEMENT DE LA TECHNIQUE ENCORE EXPÉRIMENTAL MAIS SUSCEPTIBLE DE DÉVELOPPEMENTS OPÉRATIONNELS RAPIDES

Beaucoup des auditions menées par la mission ont abouti aux mêmes conclusions : bien que particulièrement prometteuses, les technologies de *blockchains* pâtissent encore aujourd'hui d'un certain manque de maturité qui les expose à plusieurs limites techniques et économiques et à des critiques.

Cependant, un rapide panorama du potentiel de recherche et des expérimentations menées autour des *blockchains* permet un réel optimisme sur la résolution de la plupart de ces limites, au moins à moyen terme.

1. Des questions restent ouvertes quant aux capacités des *blockchains* à fonctionner à grande échelle

La principale limite aujourd'hui identifiée des *blockchains* est le « changement d'échelle » (*scalability*) ou l'industrialisation, c'est-à-dire la perspective de généraliser une *blockchain* à destination du grand public et non d'un public avisé ou de quelques acteurs réunis en consortium.

Le passage à grande échelle d'une *blockchain*, à savoir son utilisation par une grande masse de personnes, pose aujourd'hui des problèmes de trois ordres principaux : la capacité technique et la sécurité, la consommation énergétique et la capacité à déployer des *smart contracts* formalisant des relations économiques complexes.

a. Les capacités techniques et la sécurité

– la capacité technique

La *blockchain* Bitcoin « pèse » aujourd'hui plus de 200 gigaoctets (Go) de données de transactions enregistrées. Pourtant, techniquement, une *blockchain* ne contient pas toutes les informations qu'elle véhicule, mais seulement une empreinte (le *hash*). Ces 200 Go sont l'équivalent du poids d'une soixantaine de longs métrages en très haute définition. L'objet, qui doit être constamment mis à jour, commence donc à être **peu malléable**, et sa taille ne peut que s'accroître.

Il ne sera donc pas possible pour n'importe qui, demain, d'être un nœud de réseau s'il faut la puissance de calcul suffisante pour valider des milliers de transactions ou pour stocker une *blockchain* qui pourra atteindre plusieurs téraoctets de données dans un avenir proche. Le problème n'est pas la taille en elle-même, mais la pérennité d'un réel modèle distribué et décentralisé de gouvernance et de prise de décision au bénéfice de quelques-uns, professionnalisés, qui pourraient être en situation de « **capturer » la *blockchain***.

À ce propos, le mode de validation reposant sur la preuve de travail connaît aussi des limites qui, si la *blockchain* continue de grossir, remettent en cause son modèle historique. En matière de minage, par exemple, la montée des cours du bitcoin a favorisé l'apparition de « pools » de mineurs qui ont mutualisé de la puissance de calcul pour valider davantage de blocs et donc pour améliorer leur rendement. Ce **mouvement de concentration** se poursuit, au bénéfice de « grands acteurs » majoritairement chinois et américains. Cela pose d'ores et déjà une vraie question sur le pouvoir que de telles structures peuvent obtenir sur la gouvernance de la *blockchain*, qui apparaît moins décentralisée qu'à ses prémisses.

Pourtant, la décentralisation de la *blockchain* est un problème à part entière. Il est, par exemple, avéré que certaines évolutions du protocole de la *blockchain* Bitcoin – qui demeure la principale référence du présent rapport en raison de son caractère historique et précurseur – seraient vertueuses, pour permettre des gains d'efficacité ou de temps. Pourtant, **atteindre un consensus est une opération particulièrement complexe**, et chaque tentative donne lieu à des débats d'une rare intensité dans la communauté concernée et, la plupart du temps, à des bifurcations brutales (*hard forks*) qui divisent cette communauté, comme entre Bitcoin Core et Bitcoin Cash, en août 2017.

Enfin, Bitcoin connaît un **problème d'engorgement**. Beaucoup de transactions sont réalisées au même moment mais le nombre de transactions inscrites sur chaque bloc et la durée de validation d'un bloc (*blocktime*) sont limités. Cela signifie que les transactions sont mises en file d'attente le temps de leur validation : d'une promesse de validation expresse des transactions (quelques secondes, quelques minutes), la réalité peut conduire à une validation mesurée en heures, à cause de cet engorgement. En outre, cela donne lieu à d'autres altérations de la « promesse » de la *blockchain* : la réduction des frais de transaction, élevés dans le monde financier traditionnel pour les virements internationaux. En effet, des pratiques de frais de transaction se développent sur chaque transaction en bitcoins, selon une logique imparable : plus les utilisateurs sont prêts à payer des frais de transaction importants, plus la transaction sera « remontée » en bonne position dans la file d'attente de validation.

– L'exposition des blockchains aux fraudes et aux piratages

Le sujet est d'importance. Si les *blockchains* doivent connaître un essor économique important, c'est en garantissant que leur plus-value technique, à savoir la preuve de l'authenticité et de l'inviolabilité des informations inscrites sur les blocs sans passer par un tiers de confiance, est irréfutable. L'intérêt des *blockchains* réside donc essentiellement dans leur sécurité intrinsèque. Si elles sont exposées à des risques informatiques, humains ou à des failles, leur potentiel de développement serait donc mécaniquement entravé.

Le rapport de l'OPECST, précité, présente les différentes modalités techniques d'attaques informatiques ou de fraudes qui posent la question de la

sécurité des *blockchains*. Vos rapporteurs y renvoient pour des explicitations techniques. Ces développements montrent notamment que **les principales failles de l'écosystème des *blockchains* ne se situent pas dans ces dernières mais dans les « couches » qui s'appuient dessus** pour développer leur activité : plateformes d'échanges de cryptoactifs ou de stockage de clés privées mal sécurisées, applications de *smart contracts* mal codées et puis, de façon plus classique, toutes les failles humaines qui sont susceptibles de manœuvres d'ingénierie sociale.

Le principal risque d'exposition des *blockchains* ouvertes aux fraudes et aux piratages ne réside donc pas dans les protocoles informatiques eux-mêmes : la cryptographie et le recours à des fonctions de hachage, associés à des preuves de travail coûteuses pour « miner » la *blockchain*, garantissent un niveau de sécurité hors pair. Le contre-exemple souvent cité est « l'attaque des 51 % », qui permet, en simplifiant, de contrôler la majorité des nœuds permettant d'écrire la *blockchain* à un certain moment, afin de pouvoir y inscrire des transactions frauduleuses (doubles dépenses, dépenses effacées, etc.). Pour une *blockchain* aussi développée que Bitcoin, pour laquelle réunir une puissance de calcul équivalente à la moitié de la puissance cumulée de tous les autres mineurs réclamerait des investissements d'un coût complètement démesuré, l'attaque des 51 % est jugée théorique par les acteurs rencontrés par la mission. Une telle attaque a cependant eu lieu sur une *blockchain* plus « jeune », Bitcoin Gold.

En outre, vos rapporteurs, étant soucieux des **enjeux de souveraineté liés aux *blockchains***, se demandent s'il est absolument inimaginable qu'un acteur qui n'agisse pas uniquement en termes de rationalité économique (postulat de la réfutation de la possibilité de l'attaque des 51 % sur une *blockchain* mature) mais, par exemple, pour le compte d'une organisation ou d'un État mal intentionnés parvienne à réunir les moyens suffisants pour réussir une telle attaque à la seule fin de déstabiliser tout l'écosystème ? Cette question ne doit pas être écartée : la *blockchain* repose sur la confiance dans le protocole informatique. Sans elle, elle n'a plus d'utilité et les cryptomonnaies qui s'appuient dessus ont de fortes chances de ne plus rien valoir.

En outre, est-ce que les évolutions technologiques à venir seraient susceptibles de remettre en cause, par d'autres moyens, le haut niveau de sécurité des *blockchains* ? Les auditions ont permis d'avoir des débats nourris autour de l'arrivée prochaine de l'informatique quantique.

Sans présumer pouvoir expliquer exactement comment l'informatique quantique pourrait menacer le fonctionnement des *blockchains*, il est cependant possible d'en imaginer les principaux éléments. Le fonctionnement cryptographique des *blockchains*, qui permet de ne pas pouvoir modifier des données inscrites sur des blocs déjà validés ou de pouvoir maintenir sa clé privée complètement distincte de sa clé publique, s'appuie sur des terminaux dont la puissance de calcul est physiquement limitée et qui ne sont pas en mesure de casser ce chiffrement. Ainsi, il est mathématiquement impossible, sur un ordinateur traditionnel, de retrouver une clé privée à partir de la clé publique

lisible par tous en « renversant » l'opération cryptographique qui a eu lieu. Cela garantit l'intégrité de l'ensemble du système.

Cependant, **dans l'univers quantique, cette barrière mathématique serait levée**. La puissance de calcul des ordinateurs quantiques n'augmenterait pas *stricto sensu*, mais ces ordinateurs calculeraient autrement, en utilisant des paradoxes de la mécanique quantique, pour étudier des énormes quantités de scénarios possibles (donc de solutions cryptographiques). Toutefois, selon les experts en cryptographie rencontrés par la mission, notamment M. Daniel Augot (X-Inria), pour effectivement réaliser un calcul mathématique, il faut bien à un moment, « sortir » du champ quantique (voir si le chat est vivant ou non), ce qui limite largement l'impact de l'informatique quantique pour « résoudre » ou « casser » des problèmes cryptographiques. Par ailleurs, si l'arrivée de l'informatique quantique est souvent annoncée, et ce depuis vingt ans : la maturité de cette technologie n'a pas encore d'échéance bien maîtrisée.

b. La consommation énergétique

*– Des besoins de calcul coûteux dès l'origine (*by design)

Les *blockchains* qui se construisent à partir d'un consensus fondé sur la preuve de travail (*proof of work*) ont la caractéristique commune d'être énergivores.

Pourquoi ? Le protocole informatique sur lequel repose la *blockchain* Bitcoin, par exemple, contient un mécanisme d'**augmentation progressive de la difficulté des problèmes cryptographiques à résoudre** en fonction du nombre de bitcoins en circulation, afin de lisser ce nombre (par ailleurs plafonné) dans le temps et de contrôler la masse monétaire en circulation. Plus le nombre de blocs créés est important, plus chaque nouveau bloc sera difficile à miner, et requerra donc une puissance informatique importante (pour simuler l'ensemble des solutions mathématiques possibles au problème cryptographique posé par le protocole).

Dans les premières années, un simple processeur suffisait à « miner du bitcoin » (miner de nouveaux blocs en échange de bitcoins si le bloc miné est validé par les autres nœuds). La hausse des cours de cette cryptomonnaie associée à la montée de la difficulté de minage a progressivement conduit les mineurs à recourir à des cartes graphiques de plus en plus puissantes, puis à des équipements surpuissants construits uniquement à des fins de minage. Des « fermes de minage » se sont ainsi développées, tournant 24 heures sur 24, et mobilisant une puissance de calcul de plus en plus importante pour miner de nouveaux blocs, et ainsi être récompensées en bitcoins. L'opération, économiquement, est rentable. D'un point de vue énergétique, cependant, des critiques se sont élevées à juste titre contre la consommation électrique de tels équipements qui produisent une cryptomonnaie n'ayant pas de valeur légale. À cette consommation énergétique s'ajoute aussi la consommation d'équipement informatique spécialisé, rapidement

obsolète en raison d'une course à la performance entre mineurs, et donc rapidement gaspillé, puisqu'il ne sert qu'à « miner ».Le rapport de nos collègues de l'OPECST, précité, s'attarde longuement sur la mesure de cette consommation énergétique au niveau mondial : il est particulièrement délicat d'en avoir une connaissance précise et plusieurs méthodes sont présentées. Toutefois, plusieurs estimations sont plus largement reprises : la consommation électrique utilisée pour la seule *blockchain* Bitcoin serait d'au moins 24 TWh/an, et pourrait atteindre les 40 TWh/an. Pour donner un ordre d'idée, le Danemark, dans son ensemble, a consommé environ 25 TWh d'électricité pendant l'année 2017.

– Une vision moins inquiétante mérite toutefois d'être avancée

Premièrement, la plupart des *blockchains* qui se développent aujourd'hui sont privatives, et ne demandent donc pas de validation par preuve de travail qui réclamerait une consommation énergétique disproportionnée. En outre, les *blockchains* ouvertes auront probablement vocation à se concurrencer, parfois à se regrouper mais peu devraient parvenir à la fois à la maturité et au passage à l'échelle qui pourrait faire redouter l'explosion insoutenable de leurs besoins énergétiques. Ces *blockchains* pourront, par ailleurs, rendre de réels services (voire se substituer à des services existants) qui rendront leur consommation énergétique plus acceptable, car davantage proportionnée à leur utilité.

En second lieu, il faut également rappeler que le coût énergétique d'une *blockchain* ouverte est aujourd'hui le « coût de la sécurité ». C'est grâce au fonctionnement de la preuve de travail que, dans un cadre complètement décentralisé, la technologie garantit que personne n'est en mesure de prendre le pouvoir pour altérer la *blockchain* à son avantage.

Enfin, déjà aujourd'hui, le souci de rentabilité économique qui anime les mineurs demeure un frein aux excès. Les principales fermes de minage se développent dans des pays au climat tempéré (car les équipements informatiques chauffent, et le refroidissement a un coût) et près des sources de production d'énergie (centrales hydroélectriques, par exemple) pour éviter les frais de transport de l'électricité. Pendant les auditions, il a pu être rappelé qu'en Chine, les partenariats développés avec les gestionnaires d'infrastructures énergétiques permettaient de faire en sorte que ce soit la surproduction énergétique qui soit principalement consommée par ces « nouveaux fermiers ».

Proposition n° 2 : Reconnaître le crypto-minage comme une activité électro-intensive bénéficiant des tarifs préférentiels de l'électricité, afin de maintenir cette activité en France.

c. Le déploiement des smart contracts

Les *blockchains* ouvertes ont montré leur efficacité, à une échelle maîtrisée, pour organiser un système de transactions entre utilisateurs tiers. Les *blockchains* privatives qui sont expérimentées montrent que le potentiel des *blockchains* est très large : certification de diplômes, partage de données de santé,

organisation d'incitations financières dans des communautés, alignement des intérêts de personnes concurrentes, etc.

Cependant, est-il possible d'avoir les deux ? Une *blockchain* ouverte, qui accueillerait un grand nombre d'utilisateurs tout en permettant des relations économiques complexes entre eux, par la voie contractuelle ? Est-ce que les *blockchains* peuvent supporter la mise en place de « contrats intelligents » (*smart contracts*) qui permettent d'assurer, sans intermédiaire (place de marché, notaire, plateforme commerciale, institution financière, etc.) un échange de biens ou de services entre deux personnes physiques ou morales ?

La principale promesse économique des technologies de *blockchains* repose sur cette capacité-là.

Les *smart contracts* peuvent se définir comme des **programmes informatiques inscrits dans la *blockchain***. Cette dernière contient alors non l'historique d'une transaction, mais des lignes de code qui permettent l'exécution de plusieurs commandes (« si la condition X est remplie, alors effectuer l'opération Y ») de façon automatique. Le terme de contrat est un peu galvaudé : ce programme informatique ne partage que peu de caractéristiques communes avec l'objet juridique du contrat au sens du code civil. Au mieux, le programme auto-exécutable s'adosse à un contrat électronique sous forme de conditions générales d'utilisation ou de vente (CGU et CGV) que les utilisateurs seraient appelés à accepter. Quel est l'intérêt de recourir à une *blockchain* pour automatiser une relation économique ? Une fois inscrit dans la *blockchain*, le *smart contract* est automatique, indélébile et transparent : son exécution aura lieu exactement comme prévu, puisque le code ne peut pas être modifié et qu'il peut être librement lu et vérifié par les parties en présence.

Les *smart contracts* qui sont utilisés dans les *blockchains*, et en particulier sur Ethereum, précurseur en la matière, sont des contrats plutôt simples. Par exemple, si un service aisément vérifiable est rendu (par exemple, la mise à disposition d'un appartement, observable informatiquement par le déverrouillage d'une serrure numérique), il est procédé à un paiement (le client qui a déverrouillé l'appartement mis à disposition). De même, dans le milieu assurantiel, la réalisation d'un événement (comme un retard de train) peut donner lieu à une indemnisation automatique des assurés, en fonction de critères définis dans le code (raisons techniques du retard, durée, conditions de remboursement applicables, etc.). Avec un bon code, donc un bon *smart contract*, un tel recours à la *blockchain* permet d'économiser des démarches à l'assuré et du temps de travail à l'assureur.

Toutefois, ce qui marque la différence entre un véritable contrat juridique, qui lie deux parties, et un « contrat intelligent » (*smart contract*) codé sur *blockchain* relève de deux ordres : **la complexité du réel**, d'une part, qui justifie que des professionnels soient à l'origine de la rédaction des clauses ; **l'existence d'un organe de contrôle**, le juge, qui puisse arbitrer les différends.

Les *smart contracts* progressent sur ces deux tableaux. En particulier, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), auditionné par la mission et qui détient la mission d'assurer la compétitivité de l'industrie française, mobilise des ressources pour rechercher les applications industrielles des *blockchains*, ce qui passe par la gestion des relations contractuelles. Il faut donc des équipes de recherche pour développer des *smart contracts* complexes (qui deviennent des logiciels, en réalité), puis assurer un traitement informatique performant de ces contrats (notamment sur le raisonnement et les déductions des programmes : font-ils ce qu'ils sont supposés faire ?). Enfin, il faut déployer des solutions d'auditabilité et de certification des logiciels et des programmes qui contiennent les contrats, afin d'assurer leur bon fonctionnement et leur équilibre. Selon les propos des chercheurs du CEA, corroborés par d'autres chercheurs auditionnés (notamment de l'équipe Specfun d'Inria), l'enjeu d'un fonctionnement parfait des *smart contracts* est d'autant plus important que, sur les *blockchains*, il est prévisible que la plupart de ces contrats seront conclus et exécutés par des intelligences artificielles, mises en relation *machine-to-machine*, M2M [(1)], sans interaction humaine.

Par exemple, le CEA participe au développement de la start-up *Connected Food* (hébergée chez Station F), qui crée des *smart contracts* types pour maîtriser l'origine de denrées alimentaires sur une chaîne de production agroalimentaire. Le CEA développe des surcouches logicielles au-dessus des *blockchains* utilisées par les acteurs agroalimentaires concernés, notamment l'écriture de contrats (leur codage), leur certification (la preuve de cohérence du contrat) et l'audit des contrats passés.

Sur le second tableau, qui est celui du règlement des différends, les *blockchains* font face à un problème structurel : **si l'information inscrite sur la *blockchain* est immuable, rien ne garantit qu'elle soit vraie**. Une *blockchain* est un registre : son contenu strict est déclaratoire. C'est pourquoi, sur la *blockchain* Ethereum, un tiers de confiance, qualifié d'oracle, est défini pour faire le lien entre la *blockchain* et le réel.

(1) Pour des précisions sur ce concept, vos rapporteurs renvoient à un rapport parlementaire de la précédente législature n° 4362 de Mmes Corinne Erhel et Laure de La Raudière sur les objets connectés, janvier 2017.

Qu'est-ce qu'un oracle ?

La *blockchain* est un réseau fermé dont les seules informations sûres sont celles inscrites sur le registre. Dès qu'il faut y intégrer des données exogènes, rien ne permet de garantir que ces données soient vraies. Or, l'exécution de *smart contracts* requiert, la plupart du temps, d'enregistrer de telles données exogènes, qui, par exemple, vont conditionner l'exécution d'un contrat (pour un pari inscrit sur la *blockchain*, l'issue du match).

Afin de permettre le développement des *smart contracts*, Ethereum a introduit l'oracle. Il s'agit d'un prestataire de services, neutre, qui fournit sur la *blockchain* des données certifiées auxquelles les autres utilisateurs pourront faire confiance. En somme, c'est un tiers de confiance.

Cette nouvelle forme de « certification de l'information » qu'est un oracle pose des questions sur la philosophie initiale des *blockchains* mais représente plutôt une véritable chance pour les acteurs traditionnels qui souhaitent s'engager dans l'écosystème des *blockchains*. Les acteurs publics qui accomplissent des missions de tiers de confiance, comme La Poste, pourraient constituer des oracles efficaces et réputés.

Source : Mission d'information commune sur les usages des bloc-chaînes (blockchains) et autres technologies de certification de registres.

Le développement des *smart contracts* au-delà de l'exécution de contrats simples suscite, pour le moment et chez la plupart des acteurs auditionnés par la mission, de la circonspection. Il est toutefois fort bienvenu que nos chercheurs s'attachent à approfondir le potentiel de ce sujet, tant il pourrait être structurant pour l'avenir des *blockchains*.

Proposition n° 3 : Accentuer les efforts de recherche interdisciplinaire (informatique, économie, droit) sur le potentiel applicatif des *smart contracts*, qui représentent l'avenir des *blockchains*, par exemple par le biais d'une équipe Inria-Sorbonne-Paris School of Economics.

2. Des obstacles et limites techniques pas insurmontables au regard des recherches en cours

Face aux réserves qui viennent d'être exprimées, des progrès peuvent déjà être enregistrés dans plusieurs domaines. La recherche et la technique sont particulièrement évolutives en la matière, et beaucoup d'énergie, souvent mutualisée dans de grandes communautés de codeurs ou de chercheurs, est consacrée à la résolution des principaux problèmes des *blockchains*. La présentation ci-après ne pourra donc pas s'assimiler à un état de la technique qui serait rapidement obsolète. Il s'agit davantage de présenter les champs de progression les plus prometteurs.

– Une certaine plasticité des blockchains

Comme il a été vu, le passage à l'échelle des *blockchains* peut être freiné par leur taille, leur manque de maniabilité et leur lenteur, qui augmentent à mesure

que la chaîne grossit. Toutefois, il existe déjà un ensemble d'approches complémentaires pour améliorer la souplesse, donc le déploiement et le passage à l'échelle des *blockchains*.

La première approche la plus évidente est l'**approche concurrentielle**. En raison d'une méthode de consensus difficilement atteignable en raison de sa décentralisation maximaliste, la *blockchain* Bitcoin est difficilement réformable. De nombreuses *blockchains*, proposant des cryptomonnaies nouvelles, sont apparues en « corrigeant » certaines caractéristiques contraignantes de Bitcoin, comme le temps de validation des transactions ou le poids de la chaîne. C'est par exemple le cas de Litecoin, qui, comme son nom l'indique, est une *blockchain* Bitcoin allégée, avec sa propre cryptomonnaie ; ou de Monero, qui vise la confidentialité complète des transactions, grâce à une *blockchain* non transparente (les clés publiques ne sont pas visibles).

En second lieu, c'est l'écosystème autour d'une *blockchain* qui peut permettre de lui faire gagner en efficacité, dans une **logique de symbiose**. Par exemple, si la *blockchain* Bitcoin n'est pas suffisamment souple, les utilisateurs peuvent recourir à d'autres cryptomonnaies [(1)] pour leurs transactions mineures mais conserver leurs bitcoins comme actifs de référence (voire de réserve – un peu comme le dollar dans le système monétaire international classique), ce qui allège d'autant le recours à la *blockchain* principale. Il y aurait une ou plusieurs *blockchains* « mères » et une multitude de *blockchains* plus accessoires ou plus spécialisées, afin que l'équilibre de l'ensemble de l'écosystème soit préservé.

Les autres solutions ne sont pas économiques, mais technologiques. Elles ne sont, pour la plupart, pas encore parfaitement stabilisées.

En premier lieu, une *blockchain* peut admettre des **réseaux de second rang** : des chaînes latérales (*sidechains* sur Bitcoin) ou des fragments (*sharding* sur Ethereum) qui enregistrent des échanges temporaires ou des informations secondaires ; le fruit de ces échanges, par exemple le paiement final, est lui bien inscrit sur la *blockchain* principale. Les informations présentes sur une chaîne latérale peuvent être facilement supprimées, ce qui permet aussi d'organiser un droit à l'oubli que ne permet pas la logique initiale de la *blockchain*. Dans une *blockchain* fragmentée, les nœuds interviennent à des échelles différentes, selon le fragment qu'ils doivent valider (nœuds de fragments, nœuds de plus haut niveau), et des « nœuds complets » ou « super-complets » assurent la cohésion de l'ensemble.

En deuxième lieu, il existe des **algorithmes de compression et de stockage** qui permettent de limiter les besoins de stockage. Les fonctions non utilisées de certaines chaînes latérales ou fragmentées peuvent ainsi être désactivées de façon algorithmique. De même, les développeurs de la *blockchain* Bitcoin sont parvenus à mettre en place un protocole de vérification simplifiée

(1) On parle d'altcoins pour désigner toutes les cryptomonnaies – dénombrables en milliers – alternatives au bitcoin.

(*simplified payment verification* – SPV) permettant à un utilisateur de scanner rapidement l'ensemble des données de la *blockchain* et de n'exploiter que les informations concernant les transactions le concernant afin de gagner en maniabilité.

En troisième lieu, des **solutions logicielles**, des « surcouches » applicatives, peuvent être développées sur la *blockchain* pour faciliter certaines opérations – la *blockchain* étant donc moins mise à contribution. Pour Bitcoin, par exemple, c'est le réseau Lightning qui est actuellement en cours d'expérimentation : il s'agit d'ouvrir des canaux de paiement sur la *blockchain*, qui autorisera, de façon beaucoup plus souple et rapide les paiements en bitcoins entre utilisateurs qui partagent le même canal de paiement. Les transactions ne seront plus inscrites sur la *blockchain*, mais uniquement le canal de paiement, ce qui devrait garantir la sécurité des transactions. Les canaux de paiement fonctionnent en réseau : plus le nombre d'utilisateurs recourant à un canal de paiement est important, plus le nombre de transactions qui peuvent avoir lieu « en dehors » de la *blockchain* augmente. Cet effet de réseau permettrait à Bitcoin de réussir son passage à l'échelle, puisqu'il lui serait plus facile de gérer des milliers de transactions simultanées.

– La détermination d'autres modalités de consensus

Un des freins significatifs à la montée en charge des *blockchains* en termes de nombres d'utilisateurs ou d'applications est son coût énergétique. À titre de comparaison, le réseau Visa, qui organise les paiements à une échelle bien supérieure à celle de la *blockchain* Bitcoin, est également beaucoup moins consommateur d'énergie.

Dans les *blockchains* de consortium ou privatives, la question ne se pose pas, dans la mesure où le consensus est obtenu autrement (autorité centralisatrice, nœuds peu nombreux et connus, etc.). C'est par exemple le cas de la *blockchain* proposée par LO3 pour l'échange d'énergie solaire produite localement dans un quartier de Brooklyn, où un seul nœud gère la validation de la chaîne. Plus généralement, tout consensus trouvé grâce à un ou plusieurs nœuds « maîtres » du réseau (on parle parfois de « preuve d'autorité ») permet d'obtenir une *blockchain* parfaitement fonctionnelle… tout en renonçant, par là-même, à l'un des principes philosophiques à la racine de cette technologie, à savoir la décentralisation et le fonctionnement en pair-à-pair. La *blockchain* Ripple et la cryptomonnaie associée sont, pour cette raison, particulièrement décriées par les différentes communautés concurrentes.

Dans les *blockchains* ouvertes, d'autres méthodes de consensus que la **preuve de travail** (*proof of work*) présentée ci-avant existent. La principale alternative est la **preuve d'enjeu** (*proof of stake* – PoS), appelée aussi preuve de participation. La preuve d'enjeu est fournie par un utilisateur aléatoire du réseau, ce qui convient bien à la philosophie décentralisée de la technologie. Afin d'éviter les dérives et le non-respect du protocole de validation (multiplication

d'utilisateurs fantômes pour prendre la main sur le réseau – attaque Sybil), la détermination du nœud peut être pondérée relativement à la possession de cryptomonnaies par l'utilisateur [(1)] puis, dans certaines configurations, mises en gage pour faire son travail de validation (ce qui permet d'appliquer des sanctions – la destruction de ces jetons – en cas de comportement non vertueux). Le fonctionnement est, en apparence, simple : les nœuds « misent » une somme prédéfinie, et tous ceux qui ont misé contre le consensus de validation vertueux, qu'on suppose nécessairement majoritaire, perdent leurs jetons.

Le rapport de l'OPECST précité fournit une présentation avancée de cette preuve d'enjeu. Des dérivés peuvent ainsi être cités : la preuve de possession (*proof of hold*), fondée sur la durée de possession, la preuve d'utilisation (*proof of use*), en fonction du volume de transactions effectuées par l'utilisateur, la preuve d'importance (*proof of importance*), reposant sur la « réputation », ou encore la preuve de destruction (*proof of burn*) qui revient à détruire des cryptomonnaies pour obtenir la confiance du réseau.

L'avantage de cette méthode de consensus, et de ses dérivés, est de ne pas nécessiter de puissance de calcul particulière, donc d'éviter des dépenses énergétiques exponentielles. Le principal inconvénient de cette méthode est de rendre la *blockchain* aujourd'hui, en l'état de la technologie, plus exposée aux risques d'attaques, de failles, d'accident de parcours – rappelons que la confiance dans la *blockchain* est absolument nécessaire à son bon fonctionnement, ne serait-ce que pour éviter les chutes brutales de cours des cryptomonnaies qui y sont associées. La preuve d'enjeu n'est toujours pas utilisée par une « grande » *blockchain* ouverte : la communauté Ethereum y réfléchit depuis longtemps mais n'a pas encore trouvé la solution pour la mettre en place à grande échelle sans faire prendre un trop grand risque à cette *blockchain*.

Le tableau ci-après, réalisé par l'OPECST à partir de travaux de chercheurs coréens recensant l'ensemble des méthodes de consensus existantes, résume les points faibles et forts de trois grandes catégories de modes de preuve.

(1) Avec, dans ce cas, un risque oligarchique, sinon ploutocratique à ne pas sous-estimer. Par exemple, la cryptomonnaie peercoin fonctionne sur une blockchain qui mélange la preuve de travail et la preuve d'enjeu, en adaptant la difficulté du travail de minage en fonction de la part relative de cryptomonnaies possédée par le mineur correspondant.

AVANTAGES ET INCONVÉNIENTS DE LA PREUVE DE TRAVAIL (POW), DE LA PREUVE D'ENJEU (POS) ET D'UNE FORME HYBRIDE DES DEUX MODES DE PREUVE

Critères	Preuve de travail	Preuve d'enjeu	Forme hybride entre preuve de travail et preuve d'enjeu
Consommation énergétique	Très importante	Faible	Très importante
Besoin de matériel informatique spécialisé	Très important	Pas nécessaire	Important
Risque de séparation du réseau (*forking*)	Possible, lorsque deux nœuds trouvent le bon hash au même moment	Très improbable	Probable
Vulnérabilité aux attaques des 51%	Existante	Faible	Existante, mais moins que pour la preuve de travail simple
Vitesse de création des blocs	Lente, dépend de plusieurs variables	Rapide	Lente, dépend de plusieurs variables
Risque de regroupement en *pools*	Oui, mais peut être prévenu	Oui, mais difficile à prévenir	Oui
Exemples	Bitcoin	Nextcoin	PPcoin, Blackcoin

Source : OPECST, d'après Giang-Truong Nguyen and Kyungbaek Kim (1)

La détermination du consensus est le parfait exemple d'une technologie qui est encore en phase de maturation. Des solutions plus résistantes sont en cours de développement dans la communauté scientifique. Le mathématicien spécialiste de la cryptographie, Silvio Micali, a ainsi proposé un protocole de *blockchain*, Algorand, qui est une des principales solutions de gouvernance à la fois prouvée mathématiquement et particulièrement souple : elle « tourne » même avec l'hypothèse de présence d'un tiers de nœuds malveillants dans l'ensemble du réseau.

De même, il est possible de relever l'initiative française de recherche BART (Inria, Télécom ParisSud, Télécom ParisTech et SystemX) qui développe aujourd'hui un mécanisme de validation de *blockchain* par des méthodes de consensus robustes du point de vue cryptographique mais peu énergivores. En parallèle, l'architecture qu'ils essaient de construire vise également la conciliation entre fiabilité et passage à l'échelle.

C. UNE INNOVATION PORTEUSE DE RENOUVELLEMENTS POUR LES FONDEMENTS DE L'ORGANISATION ÉCONOMIQUE ET SOCIALE

Pour le grand public, le terme de *blockchains* évoque assez naturellement le phénomène contemporain que représente le développement de *Bitcoin* et *d'Ethereum*. Toutefois, les cryptomonnaies ou les « cryptoactifs » ne sauraient à elles seules résumer la technologie dans toute sa complexité et, surtout, rendre compte de ses possibles usages. Suivant l'image utilisée par Mme Sally Davies, journaliste spécialiste de la rubrique technologie du Financial Times, « *le bitcoin est à la chaîne de bloc, ce que le courriel est à Internet. Un vaste système*

(1) Giang-Truong Nguyen et Kyungbaek Kim, «A survey about consensus algorithms used in blockchain », Journal of Information processing systems, février 2018.

électronique, à la surface de laquelle vous pouvez développer des applications. La monnaie constitue juste l'une d'entre elle. »[(1)]

Ainsi que le montrent les travaux de la mission, le concept de *blockchains* ou « de registres distribués » recouvre aujourd'hui une assez grande diversité de standards et de configurations techniques. Certains intègrent l'émission de jetons ou donnent lieu à l'usage de cryptomonnaies. D'autres semblent à la recherche de procédés susceptibles de s'affranchir de ce trait caractéristique initial.

Voici déjà trois ans, *The Economist* s'interrogeait en une sur « *la manière dont la technologie derrière le bitcoin pouvait changer le monde* » [(2)]. De fait, au-delà des spécifications techniques, le concept de *blockchains* inspire aujourd'hui un foisonnement d'initiatives et de projets innovants qui donnent à penser que, demain, la technologie pourrait s'appliquer à de très nombreux domaines de la vie économique et sociale et, à terme, permettre le dépassement de modèles établis.

1. Le *token*, fondement d'un nouveau modèle économique à conforter

Au plan technique, le terme « *token* » ou « jeton » désigne un actif numérique pouvant être transféré (et non copié) entre deux parties sur internet, de pair à pair. Ils sont fongibles et divisibles si nécessaire.

Dans la rédaction issue des travaux de l'Assemblée nationale en première lecture, le projet de loi relatif à la croissance et à la transformation des entreprises (dit « projet de loi PACTE ») propose d'appliquer cette qualification à « *tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement le propriétaire dudit bien* » [(3)].

S'il n'existe à ce jour aucune définition communément admise, les « tokens » ou jetons peuvent être classés en **trois catégories du point de vue de leur fonction économique**. On distingue alors :

– **les jetons de paiement** : il s'agit des jetons acceptés comme des moyens de paiement pour l'achat de marchandises ou de services (en pratique ou selon l'intention de leur émetteur), ou qui permettent la transmission de fonds ou de valeurs ; cette catégorie correspond pour l'essentiel aux cryptomonnaies [(4)]; les jetons ne confèrent aucun droit à l'égard de leur émetteur ;

---

(1) Citée par M. Bernard Marr, "A Very Brief History Of Blockchain Technology Everyone Should Read"*, Forbes.com, 16 février 2018.*

(2) The Economist, "The Trust Machine, How the technology behind bitcoin could change the world"*, 31 octobre -6 novembre 2015, n° 44.*

(3) Cf. article 26 du Projet de loi, adopté, par l'Assemblée nationale, relatif à la croissance et la transformation des entreprises, déposé le 9 octobre 2018 (TA n 179). Le projet de loi complète les dispositions du code monétaire et financier.

(4) Dans une certaine mesure, le bitcoin se présente comme le premier token*.*

– **les jetons d'utilité** : ces jetons donnent accès à un droit usage ou d'accès à un service ou à un produit ; ils peuvent conférer un droit de vote, constituer un moyen de paiement ou plus globalement une unité de valeur d'échange au sein d'une application ou d'un écosystème donné ; ils sont émis par des *start-up* qui développent des applications fondées sur la technologie des *blockchains* et acquis par des internautes qui les achètent en cryptomonnaies ;

– **les jetons d'investissement** : ces jetons représentent des valeurs patrimoniales, le cas échéant une créance au sens des droits des sociétés ; ils peuvent être assimilés à des actions, des obligations ou un instrument dérivé suivant l'analyse des régulateurs nationaux. La catégorie peut également comprendre des jetons censés rendre négociables sur les *blockchains* des objets de valeur physiques.

Outre la place occupée dans le fonctionnement des « *blockchains* », les « tokens » constituent aujourd'hui l'instrument d'une nouvelle méthode de financement des projets destinés au développement de cette technologie. Popularisée sous **le vocable d'*Initial Coin Offering* (ICO), cette forme de financement participatif consiste à proposer l'acquisition d'actifs numériques destinés à l'élaboration d'un produit ou d'un service fondé sur l'application de la technologie des *blockchains* en contrepartie de l'apport de fonds** (sous forme de monnaie banque centrale ou de cryptomonnaies) (1).

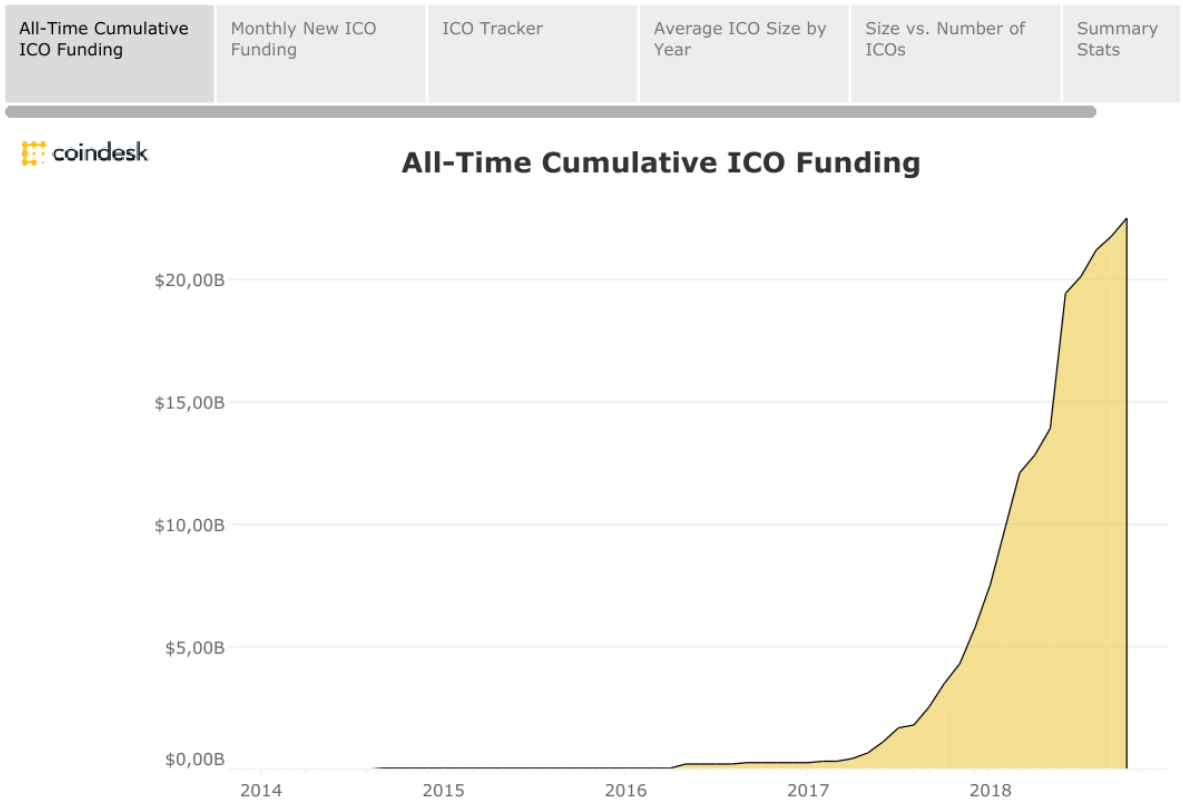
D'après les derniers chiffres disponibles, la valeur totale des fonds levés dans le cadre des ICO réalisés depuis 2014 s'élèverait à 22,50 milliards de dollars au 31 octobre 2018 (contre 3,40 milliards de dollars au 30 octobre 2017) (2). Les levées réalisées reposeraient davantage sur Ethereum que sur Bitcoin, dès lors que les ethers permettent le reversement automatique de la contrepartie grâce aux *smart contracts*. Ainsi que le montre le graphique ci-après, ce montant connaît une progression spectaculaire qui illustre l'intérêt croissant pour ce type de mode de financement.

---

(1) Cf. Cf. article 26 du Projet de loi, adopté, par l'Assemblée nationale, relatif à la croissance et la transformation des entreprises, déposé le 9 octobre 2018 (TA n 179). Le texte crée dans le code monétaire et financier un article L. 552-3 définissant ces levées de fonds de la manière suivante : « Une offre publique de jetons consiste à proposer au public, sous quelque forme que ce soit, de souscrire à ces jetons ».

(2) D'Après l'étude EY citée par France Stratégie, le montant des fonds levés dans le cadre des ICO par des entreprises établies en France s'élevait, en décembre 2017, à 12 millions de dollars (cf. EY Research : initial coin offerings (ICO), *décembre 2017).*

ÉVOLUTION DU MONTANT CUMULÉ DES ICO RÉALISÉS DEPUIS 2014



Source/ Coindesk

Du point de vue des rapporteurs, l'essor des ICO **participe potentiellement d'un modèle innovant fondé sur une nouvelle classe d'actifs** susceptibles, dans une économie accordant une place croissante au numérique, de renouveler trois déterminants essentiels de la vie des entreprises : le financement de l'innovation ; les conditions de la création des entreprises et de l'investissement ; les modalités d'échanges de biens et de services, ainsi que la création de valeur. Afin d'assurer les garanties nécessaires à la protection des investisseurs, un cadre réglementaire a été adopté en première lecture du projet de loi « PACTE » à l'Assemblée nationale.

a. De nouvelles modalités de financement de l'innovation

L'intérêt le plus évident du développement des *tokens* réside dans les capacités nouvelles de financement procurées par les ICO. Au-delà des arbitrages de gestion de portefeuille rendus dans une certaine mesure possibles par l'émergence d'une nouvelle catégorie d'actifs**, les tokens peuvent permettre d'affranchir les start-up de contraintes bancaires aujourd'hui persistantes en France**.

Suivant un constat établi par de nombreux observateurs et que corroborent les signalements reçus par vos rapporteurs, **nombre d'entreprises du secteur ont rencontré ou rencontrent encore des difficultés dans l'accès à des services**

bancaires et/ou de paiement. À l'exemple de la *Maison du Bitcoin* (1), certaines d'entre elles se sont ainsi vues signifier la fermeture de leurs comptes – parfois avec un préavis assez restreint. D'autres ont même été contraintes de solliciter des établissements bancaires européens.

Cela étant, il s'avère que ces réticences pouvaient aussi exister au-delà des frontières. La plupart des acteurs de l'écosystème suisse que les rapporteurs ont pu rencontrer ont ainsi fait part de problèmes analogues à ceux évoqués par les entreprises françaises s'agissant du financement de leurs projets, ainsi que de l'usage de comptes et de moyens de paiement. Toutefois, les témoignages recueillis par vos rapporteurs donnent à penser que l'attitude de l'Association des banquiers suisses et des établissements qu'elle représente tend à évoluer. En effet, des établissements bancaires publics tels que la Banque du canton de Neuchâtel offrent la possibilité de disposer d'un compte bancaire (2). On soulignera également l'engagement – semble-t-il décisif – de la Confédération et des cantons, avec notamment la création auprès du ministre suisse des Finances d'une *task force* et la volonté d'affirmer le statut de « *crypto nation* ».

Dans ce contexte, **les levées de fonds réalisées par le biais des ICO paraissent de nature à procurer des ressources dans des conditions plus adaptées à l'enjeu majeur du financement des entreprises du secteur des *blockchains***.

En atteste à l'évidence l'exemple d'Ethereum. Le développement des activités de cet acteur majeur du secteur des *blockchains* procède du lancement, en 2014, d'un ICO à Zoug (Suisse) lui ayant permis de collecter plus de 18 millions de dollars. Compte tenu de la hausse spectaculaire du cours de l'éther (passé de 0,145 euro en 2014 à près de 155,97 euros au 15 novembre 2018), la société possède aujourd'hui des ressources financières importantes susceptibles de lui donner la capacité d'approfondir son projet.

Les ICO permettent ainsi, d'une part, de s'affranchir de la taille du marché et de recourir – sous certaines réserves réglementaires – au financement international. Ce faisant, ainsi que l'ont relevé devant les membres de la mission les représentants de *Blockchain Partner*, ces levées de fonds tendent à procurer aux start-up les moyens d'une certaine indépendance, par l'appel direct à un plus large public de potentiels investisseurs.

De surcroît, les ICO présentent l'avantage – mis en exergue par les travaux de l'Office parlementaire d'évaluation des choix scientifiques et technologiques

---

(1) Rebaptisée Coinhouse *depuis juin 2018.*

(2) Sous l'autorité du canton de Neuchâtel, la Banque cantonale mène une politique de soutien aux entreprises développant des projets fondés sur l'utilisation de la technologie des « blockchains ». D'après les éléments recueillis auprès de M. Stéphane Leuba, sous-directeur et responsable compliance, elle met cependant deux conditions à l'établissement d'un lien d'affaire : d'une part, le respect des obligations légales à laquelle le projet est assujetti ; d'autre part, la valeur ajoutée du projet pour l'économie du canton et la présence physique de l'entreprise sur son territoire.

(OPECST) [1] – de **satisfaire des besoins spécifiques tels que la rapidité du financement des innovations, la souplesse, le pari sur le long terme et l'adhésion à un projet présentant une certaine technicité pour les investisseurs**. La levée de fonds réalisée par *Tezos* en fournit une illustration : cette fondation de droit suisse aura recueilli, dans un délai de deux semaines en juillet 2017, l'équivalent de 232 millions de dollars en cryptomonnaies, somme destinée au financement d'un protocole susceptible de permettre l'automatisation de transactions complexes.

Certes, l'exemple même de *Tezos* montre que la collecte de ressources exceptionnelles n'implique pas nécessairement la concrétisation de projets innovants à brève échéance. Ainsi que le relève le rapport de France Stratégie, dans un article publié en 2017, *Bloomberg* concluait après analyse de 226 ICO qu'au moment de l'enquête, seules vingt entreprises utilisaient effectivement les fonds collectés. Néanmoins, **ce constat remet moins en cause l'intérêt même de ce type de levée de fonds que le cadre juridique et les garanties dans lequel celles-ci peuvent être organisées.**

b. Un procédé renouvelant les conditions de création des entreprises et de l'investissement

Dans l'économie actuelle, la création d'une entreprise procède de la constitution d'un capital (par versement de fonds propres ou souscription d'un emprunt) remboursé par le *cash flow* tiré des résultats de l'activité de l'entreprise. La rémunération des premiers investisseurs donne lieu à la perception d'un dividende ou tient au remboursement de l'emprunt consenti, voire en la cession des parts acquises dans l'entreprise.

Les ICO modifient les conditions de ce financement initial car les jetons émis ne confèrent pas nécessairement une créance ou un droit de sociétariat à l'égard de leur émetteur. En fonction des modalités de la levée de fonds, les investisseurs peuvent, par ailleurs, recevoir les jetons dès le lancement de l'ICO (dans le cas d'une *blockchain* déjà développée) ou dans un avenir déterminé, après le développement de la technologie sous-jacente et des services associés. On parle alors de « préfinancement ».

Au-delà de l'apport des ressources nécessaires à la réalisation d'un projet faisant appel aux *blockchains***, l'usage des *tokens* peut contribuer à l'évolution des conditions de l'intéressement à la création de l'entreprise et à la réalisation des projets innovants.** Dès lors que les actifs gagnent de la valeur avec le succès de la start-up émettrice, les investisseurs se voient inciter à acquérir des jetons le plus tôt possible, alors que ceux-ci présentent une valeur encore relativement faible. Il s'agit de miser sur le développement à venir du produit ou

(1) Rapport n° 1092 - Rapport de Mme Valéria Faure-Muntian, MM. Claude de Ganay et Ronan Le Gleut établi au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, sur les enjeux technologiques des *blockchains* (chaînes *de blocs*), *p. 80.*

du service proposé qui, suivant la valorisation ultérieure de l'actif, rendra envisageable une revente.

c. Un nouveau mode d'échanges de biens et de services et de création de valeur dans l'économie numérique ?

Cette perspective découle des caractéristiques mêmes de la technologie des *blockchains* et des actifs sur l'émission desquels repose son fonctionnement.

En premier lieu, **le droit d'usage d'un produit ou d'un service conféré par un jeton émis dans le cadre d'une ICO tend à renouveler les rapports (de transaction et de consommation) dans l'économie marchande classique**. Ainsi que l'ont relevé plusieurs des personnes interrogées par la mission, la motivation des personnes acquérant des jetons dans le cadre d'une ICO se révèle très diverse. Elle peut aller de la simple philanthropie à la recherche de valeurs rémunératrices, en passant par la volonté de contribuer par l'investissement au développement de solutions innovantes. Dès lors qu'ils sont échangeables sans intermédiaires, **les *tokens* pourraient contribuer à renouveler l'objet et les conditions de l'échange au sein de l'économie numérique des biens et des services auxquels ils donnent accès**, notamment en rendant possible de nouvelles transactions et en modifiant les rapports entre d'un côté, producteurs de biens et fournisseurs de services, et de l'autre, les consommateurs et usagers.

L**a technologie des *blockchains* pourrait puissamment contribuer à l'émergence de l'internet des objets (*Internet of Things – IoT*), dans un contexte marqué par le développement de l'intelligence artificielle.**

Le concept « d'internet des objets » désigne tout autant des objets physiques capables d'émettre de la donnée grâce à des capteurs, que le réseau par lequel ces données transitent, ainsi que les plateformes capables de les recueillir et de les analyser. Suivant l'exemple recueilli dans le cadre des travaux de la mission, on pourrait envisager qu'un particulier, grâce à un système équipant sa voiture, puisse vendre des informations à Météo France dans un secteur où l'établissement possède peu de stations de mesure des conditions climatiques.

En second lieu, par la désintermédiation et l'absence d'autorité centralisatrice qu'elles favorisent, **les *blockchains* concourent à une certaine réorganisation de la chaine de la valeur créée**. D'après les analyses convergentes des personnes entendues par la mission, la technologie conduit, d'une part, à réexaminer l'utilité du rôle des acteurs d'un certain nombre de secteurs économiques, notamment par la transparence quant à leur apport respectif à la création de valeur ajoutée.

D'autre part, du fait des échanges directs qu'il autorise de pair à pair, de l'absence de propriété en principe du code source, **le fonctionnement des *blockchains* parait de nature à empêcher qu'un acteur tire une rémunération ou une « rente » de sa position d'intermédiaire entre consommateurs et fournisseurs**. Ce modèle pourrait remettre en cause l'économie des plateformes

numériques, dont la valeur procède de la capacité d'un acteur pivot à proposer un dispositif de mise en relation et à en assurer l'attractivité (avec une interface utilisateurs, des applications, des outils spécifiques). **La véritable valeur réside dans les protocoles sur la base desquels sont développées des applications**. Seule une partie de la valeur se distribue tout au long de la chaine des applications.

Les *blockchains* offrent la possibilité de se passer de la médiation d'une plateforme, notamment par l'usage des *smart contracts*. Certains voient ainsi dans *Slock.it* [(1)] ou *Arcade City* [(2)] une remise en cause potentielle du modèle d'affaires *d'Airbnb* et d'*Uber*.

Cela étant, **au regard des logiques constatées dans le développement de l'économie numérique**, on ne peut exclure que les protocoles fondés sur le concept de *blockchain* perdent de leur importance au plan économique face aux applications, à mesure que l'usage de cette technologie se sera démocratisé. Dans cette hypothèse – et compte tenu de l'intérêt croissant des principaux acteurs des nouvelles technologies de l'information et de la communication – **on pourrait assister à l'émergence de nouveaux géants disposant de positions monopolistiques. Pour la France – comme pour l'Union européenne – cette perspective ne rend que plus vitale la maîtrise des infrastructures.**

Pour certains observateurs entendus par la mission, **les tokens permettraient en effet d'envisager le passage d'un internet de l'information à un internet de la valeur.** De fait, par la diversité de l'objet des transactions inscrites dans les *blockchains* et des droits qui s'attachent aux jetons, la technologie renforce encore l'importance de la donnée et permet à ses détenteurs de lui conférer une valeur marchande. Dans cette perspective, on citera le projet présenté à vos rapporteurs par M. Daniel Gasteiger, directeur général de *Procivis SA*. Établie à Zurich et fournissant des solutions digitales destinées à permettre aux particuliers de disposer pleinement d'une identité numérique, cette société entend permettre aux individus, à partir d'une application installée sur smartphone, de vendre ou de monétiser des données personnelles. Pour la réalisation de ce projet, *Procivis* indique avoir recours à des ICO.

Il peut paraître sans doute prématuré d'envisager une « tokenisation » de l'économie, dans la mesure où les protocoles de *blockchain* présentent encore une certaine immaturité au plan technique et peuvent inspirer encore des réticences. Toutefois, ainsi que le souligne le rapport de France Stratégie [(3)], **la technologie a vocation à s'étendre à de nombreux secteurs**. De fait, l'usage des levées de fonds réalisées dans le cadre d'ICO se diversifie depuis 2017, après avoir essentiellement porté jusque-là sur

---

(1) Le concept repose sur la « création » de portes d'appartement connectées à une blockchain *pour enregistrer la location et effectuer le paiement.*

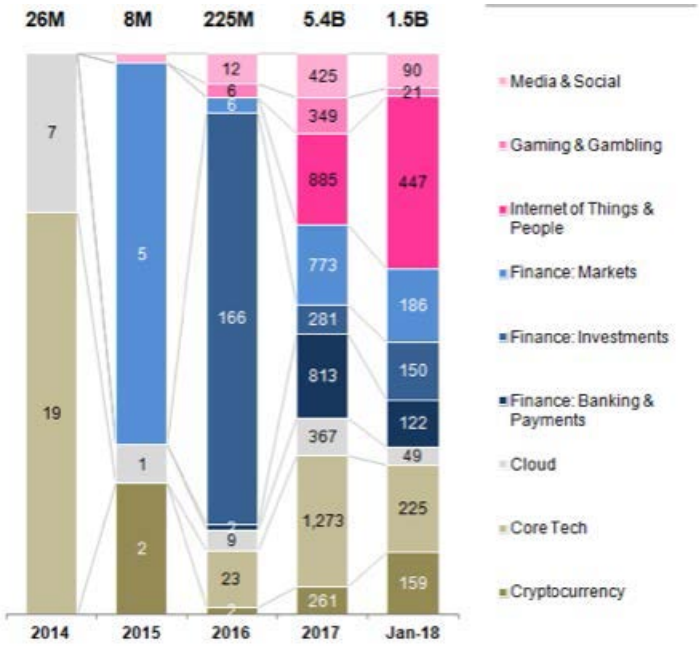
(2) Arcade City *se présente comme une sorte de « coopérative » de chauffeurs de VTC qui obtiennent des courses par l'intermédiaire d'une* blockchain*, de pair à pair.*

(3) France Stratégie, Les enjeux des *blockchains,* Rapport du groupe de travail présidé par Mme Joëlle Toledano*, juin 2048, p. 49.*

l'amélioration des infrastructures des *blockchains* et le développement des cryptomonnaies.

Ainsi, l'extension du champ du financement apporté par les ICO paraît de nature à favoriser l'émergence de nouveaux cas d'usage rendant déjà concevables quelques évolutions dans les rapports de production, de travail et de consommation.

LES FONDS LEVÉS PAR LES ICO : UNE DIVERSIFICATION DES SECTEURS



Source : France Stratégie

2. Des cas d'usage rendant déjà concevables quelques évolutions significatives dans les rapports de production, de travail et de consommation

Ainsi que l'ont souligné nombre des personnes auditionnées par la mission, l'usage de protocoles fondés sur la technologie des *blockchains* ne représente pas nécessairement une solution innovante pour l'ensemble des secteurs d'activité. Il s'avère en effet que l'usage de bases de données et d'internet peut, en l'état, permettre de dégager des gains d'efficience comparables pour certains d'entre eux. Dès lors, les *blockchains* apportent – au mieux – une optimisation des processus existants.

Du point de vue des rapporteurs, la véritable valeur ajoutée de cette technologie réside dans sa capacité à établir un lien de confiance, à favoriser le partage d'informations et à résoudre des problèmes de gouvernance parfois aigus dans le cadre des relations établies entre acteurs concurrents.

Les travaux de la mission fournissent plusieurs exemples qui montrent qu'au-delà d'effets de mode propres aux écosystèmes entrepreneuriaux,

caractérisés par l'OPECST dans son rapport, les protocoles de *blockchains* répondent à de véritables besoins et soulèvent de nouveaux enjeux.

a. Dans le domaine des banques et assurances

● **Outre l'impact potentiel sur les coûts de transaction, l'usage des technologies de *blockchains* intéresse nécessairement le secteur bancaire en ce qu'il affecte son statut d'intermédiaire dans le financement de l'économie**.

Les ICO offrent une première illustration évidente du caractère disruptif de la technologie puisqu'elles favorisent l'échange de valeurs et procurent des ressources hors des circuits classiques du crédit et du financement des entreprises.

Pour leur part, **le phénomène des cryptomonnaies ou cryptoactifs invite à s'interroger sur l'apparition de moyens de paiement nouveaux, potentiellement concurrents ou complémentaires de la monnaie émise par les banques centrales et distribuée par les banques commerciales** même si les cryptoactifcs remplissent aujourd'hui très imparfaitement les fonctions dévolues à une monnaie.

Certes, d'après les chiffres cités par l'OPECST, la valorisation des 1 600 cryptoactifs, se limitait en juin 2018, à 250 milliards de dollars [(1)]. Du reste, ainsi que le montrent les chiffres cités par le rapport Landau [(2)], le volume des transactions se révèle très faible, les cryptoactifs demeurant peu utilisés en tant que moyens de paiement : le Bitcoin représente, en effet, 0,2 % du volume des transactions au sein de la zone euro ; en montant, les paiements mondiaux en Bitcoin (soit 100 millions de dollars par jour) s'élèvent à moins de 1 % des seuls paiements réalisés par Visa et Mastercard aux États-Unis (respectivement 16,5 et 9,8 milliards de dollars par jour).

Cela étant, même si les masses en jeu ne mettent pas aujourd'hui en cause la stabilité financière, ainsi que la conduite de la politique monétaire, **il ressort de l'analyse développée par les représentants de la Banque de France que l'offre de certaines cryptomonnaies peut se révéler problématique du point de vue de l'information des investisseurs, compte tenu de la volatilité des cours.**

Du point de vue des rapporteurs, ce constat ne rend que plus nécessaire une adaptation du cadre prudentiel et de la régulation dont le projet de loi PACTE a jeté les bases.

Par ailleurs, **il donne tout son intérêt à une réflexion sur la mise en place de « monnaies » digitales émises par banques centrales**, ainsi qu'y invite

---

(1) Rapport n° 1092 - Rapport de Mme Valéria Faure-Muntian, MM. Claude de Ganay et Ronan Le Gleut établi au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, sur les enjeux technologiques des blockchains (chaînes), *pp. 73-74.*

(2) Les crypto-monnaies, Rapport au Ministre de l'Économie et des Finances remis par Jean-Pierre Landau, avec la collaboration d'Alban Genais, 4 juillet 2018, pp. 10 et 11.

le rapport Landau [1] en considération des risques inhérents à une dématérialisation totale de la monnaie fiduciaire. Ainsi que le relève France Stratégie, des monnaies digitales banque centrale pourraient également répondre aux besoins inhérents au plein développement de l'internet de la valeur, à savoir un actif pouvant supporter des transactions de bout en bout entre les *blockchains* et la monnaie quotidienne [2]. Du point de vue des rapporteurs, il ne s'agirait pas de conférer à cette « monnaie » la fonction d'un étalon (à l'exemple d'une sorte d'étalon or) mais d'en faire un instrument d'échange de nature à soutenir le développement d'une économie autour de l'usage des *blockchains*. Il conviendrait évidemment de déterminer qui de la Banque centrale européenne (BCE) ou des banques centrales nationales assurerait le pilotage de l'émission de ce nouveau compartiment de la masse monétaire, étant observé que pour la stabilité de la « monnaie » digitale, l'établissement d'un cours stable avec l'euro pourrait être utile.

Proposition n° 4 : Envisager la création d'une « monnaie » numérique émise par la banque centrale.

Mais les *blockchains* affectent également les conditions d'exercice de l'activité des établissements bancaires et des établissements de crédit.

Par la désintermédiation qui la caractérise, la technologie ouvre, en premier lieu, la possibilité de valider des transactions sans l'intermédiaire d'une chambre de compensation, ce qui devrait permettre – sous réserve de leur volume – de certifier des opérations dans des délais beaucoup plus courts (de l'ordre de quelques secondes à quelques minutes).

En second lieu, **elle peut favoriser le partage d'informations entre acteurs concurrents d'une place financière dans le respect du secret de leurs données commerciales et, ce faisant, faciliter la gestion de structures ou d'instruments communs en réduisant les coûts de contact et les frais d'administration.**

On trouvera une illustration de l'intérêt des *blockchains* pour les acteurs du secteur financier dans le projet MADRE. Il s'agit en l'occurrence d'un registre partagé entre la Banque de France et des banques commerciales partenaires, enregistré sur une *blockchain* privative (fondée sur le protocole Ethereum) et permettant l'attribution des identifiants créanciers SEPA (ICS). D'après l'état des lieux établi par les représentants de la Banque de France, le dispositif confère une certaine efficacité à la tenue de ce fichier (en améliorant la détection des identifiants frauduleux). Sa mise en œuvre dégagerait des gains de productivité

(1) Les crypto-monnaies, *Rapport au ministre de l'Économie et des Finances remis par Jean-Pierre Landau, avec la collaboration d'Alban Genais, 4 juillet 2018, pp. 64-67.Cf. également l'étude de la Banque des règlements internationaux (BRI) publiée en septembre 2017 et relative aux formes possibles de cryptomonnaies émises par une banque centrale : Morten Bech et Rodney Garratt,* « Central bank cryptocurrencies », *BIS Quaterly review*, septembre 2017.

(2) France Stratégie, Les enjeux des *blockchains,* Rapport du groupe de travail présidé par Mme Joëlle Toledano*, juin 2048, p. 53.*

permettant d'affecter des personnels à des tâches présentant une plus haute valeur ajoutée.

On citera également un projet évoqué par les représentants de Paris Europlace et mené en collaboration avec la Caisse des dépôts et consignations autour de la gestion des « obligations vertes » (*green bonds*). Faisant appel à la technologie des *blockchains*, il vise à assurer la transparence des titres financiers sous-jacents au financement de projets écologiques.

Rappelons enfin que l'ordonnance du 28 avril 2016 (1) autorise l'enregistrement de la détention et du transfert des minibons grâce à « des dispositifs d'enregistrement électronique partagé », c'est-à-dire des *blockchains*.

Cela étant, il apparaît que les *blockchains* privatives offrent aujourd'hui davantage de perspectives que les *blockchains* ouvertes pour les acteurs du secteur financier et l'essor des *Fintech*.

En effet, en l'état de la technique, le fonctionnement de ces dernières soulève encore des problèmes n'ayant pas reçu de réponses satisfaisantes (par exemple du point de vue de la préservation de la confidentialité des données inscrites sur les *blockchains*). D'après l'analyse développée devant les rapporteurs par les représentants de la Banque de France, de manière générale, l'usage de la technologie ne serait aujourd'hui pertinent que dans le cas d'activités financières peu sophistiquées.

Son potentiel apparaît aujourd'hui également encore restreint en ce qui concerne les systèmes de paiement et le traitement des transactions par les délais nécessaires à la validation des blocs (de l'ordre de 10 minutes pour Bitcoin). Ainsi, d'après les statistiques disponibles, le protocole devrait permettre la validation de vingt transactions à la seconde (contre 4 en 2017), chiffre à comparer avec la capacité de traitement de la société VISA (soit 20 000 transactions par seconde). Ce constat vaut également pour Ethereum dont la capacité de traitement était évaluée à 15 transactions par seconde au premier semestre 2018.

● **En ce qui concerne les assurances, l'apport des *blockchains* semble tenir davantage à l'automatisation des procédures et à l'allégement de certaines formalités à la charge des sociétés comme de leurs clients**. Ces améliorations paraissent de nature à accélérer le versement des indemnités, notamment grâce au recours à des *smart contracts*, sous réserve que les hypothèses dans lesquelles l'assurance est appelée à assurer l'indemnisation d'un préjudice soient clairement établies.

Ainsi, dans le cadre de son offre « *Fizzy* », AXA propose à ses assurés des contrats garantissant un remboursement en cas de retards d'avion. Le recours à un *smart contract* permet de vérifier l'heure d'arrivée du vol, de mesurer le retard éventuel, et surtout d'appliquer des conditions de remboursement préétablies.

(1) Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.

L'indemnisation découle d'une procédure automatisée ne donnant pas lieu à l'intervention de l'assureur ou à des démarches de l'assuré.

b. Dans le champ de la grande distribution, de l'agroalimentaire et de la logistique

Dans ces deux domaines, la technologie des *blockchains* présente à l'évidence **deux intérêts : d'une part, assurer une traçabilité des produits, ainsi que la mémoire des interventions des différents intervenants d'une chaine de production et de distribution ; d'autre part, alléger des formalités et créer les conditions d'une coopération entre les acteurs d'une filière**, notamment du point de vue de l'échange d'informations.

● On trouvera une première illustration de l'apport de la technologie en **matière de traçabilité dans le développement de nouvelles filières qualité dans la grande distribution.**

L'usage des blockchains dans la grande distribution :

l'exemple des filières qualité

Devant la mission, les représentants du groupe *Carrefour* ont ainsi indiqué avoir développé une *blockchain* (fondée sur Ethereum) en ce qui concerne la filière du poulet d'Auvergne – produit qui faisait déjà l'objet d'une démarche qualité – et vouloir étendre le recours à ce procédé à cinq ou huit autres produits alimentaires.

L'enseigne se donne pour objectif de répondre au besoin de transparence exprimé par les consommateurs à la suite de certains scandales sanitaires en leur donnant accès à des informations allant au-delà des prescriptions réglementaires.

Dans le cas du poulet d'Auvergne, les consommateurs pourraient ainsi obtenir des éléments sur la durée de l'élevage, l'alimentation reçue ou les soins vétérinaires. À cet effet, une plateforme en ligne a été développée qui permet une consultation des informations sur les produits référencés et renvoie les informations sur les smartphones des clients.

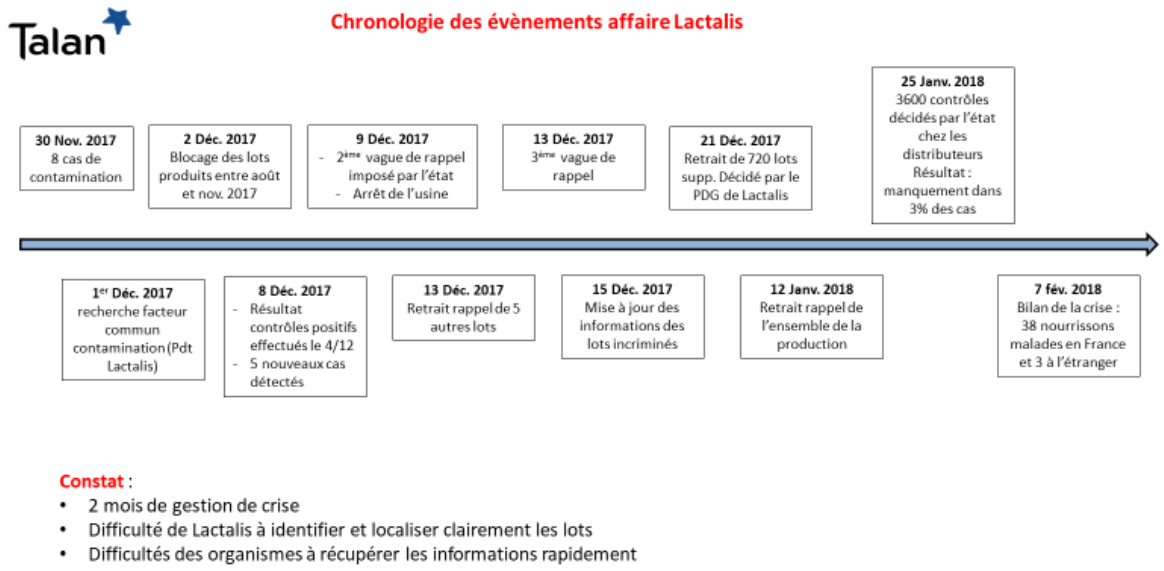
L'enseigne a équipé les producteurs afin qu'ils puissent renseigner dans la *blockchain* des éléments d'information faisant l'objet de documents qu'il doit remplir par ailleurs, notamment dans le cadre des relations contractuelles établies avec le groupe *Carrefour*.

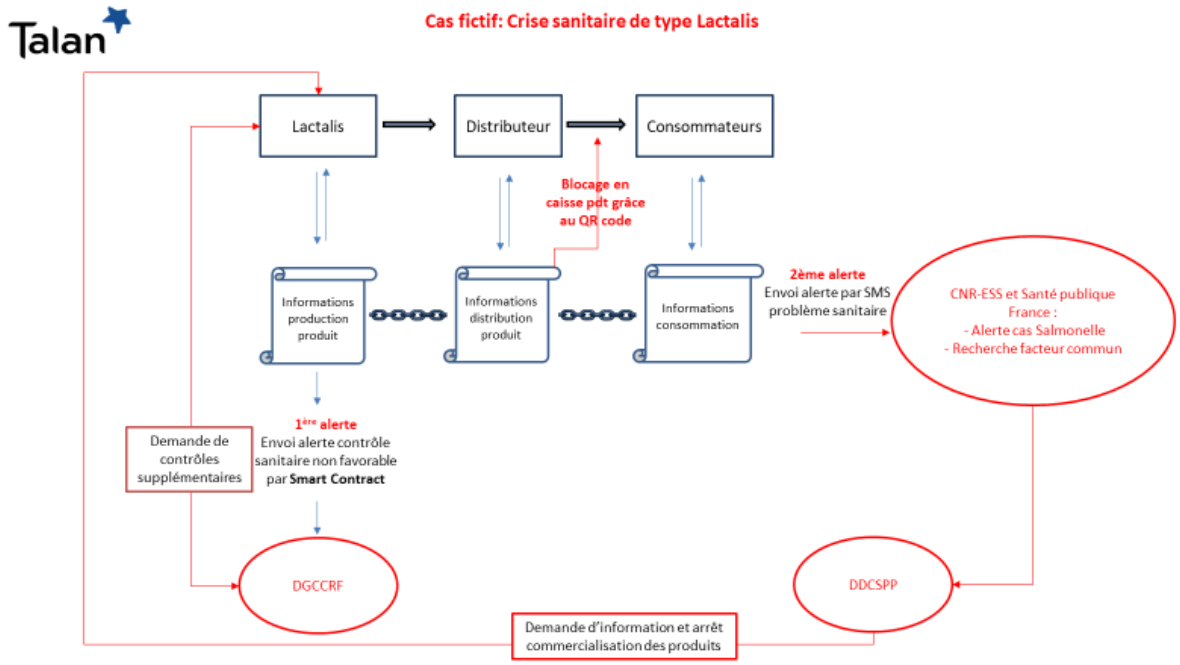
Dès lors, l'intérêt de la technologie réside dans la mise à disposition et la préservation de données figurant sur des documents papier souvent inaccessibles aux consommateurs. Il a été en outre avancé par les représentants de *Carrefour* que les *blockchains* utilisées dans le cadre des filières qualité peuvent en outre créer les conditions d'une relation plus directe avec les producteurs. On notera toutefois que cet objectif suppose que la pleine participation des consommateurs au sein de la gouvernance de la filière.

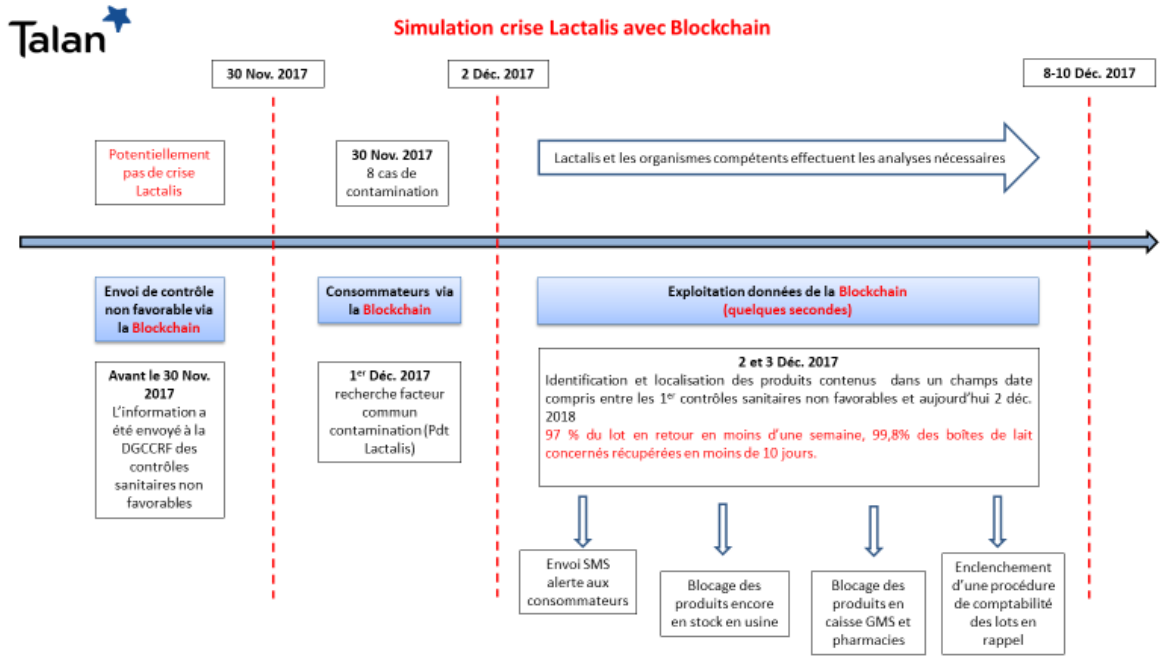
● De manière plus globale, **la filière agroalimentaire** fournit un second exemple d'un usage possible des *blockchains* dans le suivi du parcours de produits et de gestion des relations contractuelles au sein d'un secteur économique intégré.

L'Etat pourrait aussi inviter au développement l'usage de la technologie blockchain dans le secteur agro-alimentaire pour mieux gérer les crises sanitaires. Mathieu Lesueur, chercheur doctorant à l'université de Rennes, en contrat CIFRE avec le groupe TALAN, a présenté une synthèse de la problématique que la blockchain pourrait résoudre de façon beaucoup plus performante qu'aujourd'hui, permettant ainsi de rassurer plus rapidement les populations (et à l'Etat de faire appliquer la réglementation de façon plus certaine).

Voici une synoptique pour expliquer cette potentielle application des blockchains, en prenant comme exemple l'affaire Lactalis de décembre 2017 – février 2018.







● **Le négoce des matières premières** montre quant à lui l'intérêt de ces protocoles dans l'échange d'informations et la simplification des démarches entre acteurs concurrents.

Cette activité consiste en l'occurrence à trouver de la matière première et à en assurer l'acheminement des producteurs vers les clients finaux. Elle fait ainsi intervenir de nombreux acteurs ou intermédiaires ; elle donne lieu à un certain nombre de transactions et de documents destinés à sceller les engagements respectifs (notamment la livraison d'un produit déterminé dans des quantités

données, à une échéance et à un prix prédéfinis). Le négoce des matières premières repose sur la logistique mais implique également l'intervention d'intermédiaires, dont les banques qui assurent le financement de chaque étape de la transaction. D'où l'existence de nombreux documents (notamment relatifs au financement de l'export), source de nombreuses formalités, d'une succession de signatures, les procédures faisant du reste l'objet de contrôles manuels.

C'est afin de remédier à ces lourdeurs qu'a été créée en août 2018, la société *Komgo SA*. Installée à Genève, elle associe une quinzaine d'entreprises (dont un pool bancaire représentant 80 % de l'activité de financement du négoce « pétrole » et des entreprises comptant parmi les dix premiers investisseurs du secteur, ainsi que Shell). Elle propose une plateforme digitalisée de négoce des matières premières reposant sur la technologie des « *blockchains* » (en l'occurrence, le protocole *Ethereum*). Il s'agit d'offrir un service de vérification de l'identité des clients, par un échange de documents de manière cryptée, sans base de données centrale, ainsi qu'une « lettre de crédit digitale », en remplacement des lettres de crédits documentaire.

D'après les explications fournies aux rapporteurs dans le cadre de leur entretien avec les représentants du *Crédit agricole SA Indosuez* à Genève, les protocoles de *blockchains* proposent des réponses à des questions que d'autres technologies ne sauraient résoudre.

Le premier avantage de la technologie réside dans la capacité à partager des informations sans y donner accès. Chaque acteur peut inscrire une donnée de manière confidentielle qui peut être réutilisée, ce qui tend à favoriser l'établissement d'une certaine confiance entre des professionnels veillant scrupuleusement à la protection de leurs informations à raison de l'immuabilité des données inscrites.

Le second intérêt des protocoles tient aux échanges rapides et sécurisés de documents aussi cruciaux que des titres de propriété alors qu'aujourd'hui, leur acheminement repose sur l'envoi de courriers.

En dernier lieu, la *blockchain* dispense les acteurs de formalités inutiles (notamment de contrôle des signatures, de ressaisie et de retransmission de document) ; elle permet des échanges et des contrôles dans des délais correspondant à ceux du négoce, étant observé qu'un chargement de matières premières peut changer de propriétaires à plusieurs reprises avant même sa livraison effective.

c. Dans le secteur de l'énergie électrique

Par les propriétés de leur fonctionnement, les *blockchains* paraissent en effet susceptible d'accentuer la transformation d'un secteur qui, avec le développement des énergies renouvelables et de l'autoconsommation, se trouve confrontée à la perspective d'une décentralisation de ses modes de production et de distribution. De fait, **en autorisant l'échange de services et de valeurs en**

dehors d'une instance de gestion centrale, la technologie crée potentiellement les conditions de la mise en place – à une plus ou moins grande échelle suivant les capacités techniques des protocoles – de réseaux locaux de production, d'échange et de revente d'énergie verte.

D'une part, elle constitue en soi un instrument de partage des informations sur les flux d'énergie (production et besoins) et certifie les échanges (qui n'ont pas à être monétisés ni transportés sur de longues distances). D'autre part, elle donne la possibilité, par l'usage des *tokens*, de rémunérer la fourniture d'énergie entre les membres du réseau et, au-delà, d'échanger directement des crédits d'énergie par la mise en œuvre de *smart contracts*. Dès lors, ainsi que le relevaient les représentants de Réseau de transport d'électricité (RTE), on peut considérer que le développement des « *blockchains* » dans le domaine de l'énergie comporte la promesse d'une gestion décentralisée, ainsi que de l'apport de nouvelles solutions techniques en ce qui concerne la distribution d'énergie, voire l'équilibre entre l'offre et la demande.

De fait, la technologie semble d'ores et déjà offrir le support d'un certain nombre d'initiatives innovantes.

L'usage des blockchain dans la production et la distribution d'électricité :

une expérience new yorkaise

On citera évidemment l'expérimentation conduite à New York depuis avril 2016, dans le quartier de Brooklyn. Elle a donné lieu à la mise en place, à l'initiative de la coopérative *TransActive Grid* (1), d'un micro-réseau d'électricité locale fondé sur l'usage des énergies renouvelables et le recours à un protocole Ethereum. Celui-ci constitue le support technique d'un compteur spécialement développé afin de remplir trois fonctions : fournir des capacités non encore disponibles sur le marché de l'énergie ; indiquer aux propriétaires de panneaux solaires la quantité d'énergie qu'ils produisent ; vendre directement des crédits d'énergie. D'après les informations publiées sur des sites spécialisés (2), le réseau porterait aujourd'hui sur « dix pâtés de maison » dans Brooklyn et *TransActive Grid* se donnerait pour objectif d'atteindre le seuil de 1000 participants en 2018 (dont des immeubles d'habitation, des immeubles industriels, des écoles).

Source : Mission d'information commune sur les usages des bloc-chaînes (blockchains) et autres technologies de certification de registres.

D'après les éléments recueillis auprès du Commissariat à l'énergie atomique et aux énergies alternatives (CEA), cet usage des potentialités des « *blockchains* » ne revêt pas un caractère isolé.

(1) TransActive Grid se présente comme une joint-venture *composée de deux entreprises : Lo3Energy, qui développe des réseaux d'énergie solaire ; ConsenSys, un incubateur d'applications fondées sur la technologie des blockchains.*

(2) https://www.siliconrepublic.com/machines/brooklyn-microgrid-blockchain-energy-networks.

On observe ainsi en Angleterre l'existence de groupes de producteurs d'énergie particuliers utilisant la technologie afin de réguler leurs relations avec le réseau. Un distributeur d'électricité du Texas utilise également un protocole afin de certifier l'énergie produite et reçue par ses clients et fournisseurs.

En France, on signalera l'exemple des contrats de performance énergétique dans le cadre desquels *Véolia* met en œuvre un algorithme qui autorise la réalisation de transaction par le biais de *smart contract*, fournis par le CEA. On relèvera également que le laboratoire CEIDO (commun à Telecom ParisTech et EDF) développe une place de *trading* d'énergie, basée sur des *smart contracts* et le protocole Ethereum. D'après l'OPECST, ce projet a vocation à s'étoffer avec le support de Mines ParisTech qui va introduire de nouveaux algorithmes en théorie des jeux.

Cela étant, ainsi que l'ont souligné plusieurs personnes auditionnées par la mission, **dans le domaine de l'énergie comme dans d'autres secteurs, le recours à la technologie des *blockchains* soulève une question fondamentale : celle des preuves formelles de l'intégrité du contenu des *smart contracts* et des données inscrites.**

Dès lors, il ne parait pas hors de propos de concevoir la nécessité de confier à un opérateur (par exemple, EDF) une fonction de tiers de confiance ou un rôle assurantiel afin de garantir la continuité de l'approvisionnement des réseaux.

3. Une technologie dont la généralisation n'apparaît pas sans incidence pour toutes les institutions faisant office de tiers de confiance

En droit français, la notion de « tiers de confiance » renvoie moins au statut d'une profession déterminée qu'à un ensemble de missions et de prestations [(1)]. Celles-ci visent dans l'ensemble à remplir au moins trois fonctions : s'assurer de l'identité et de la capacité des parties prenantes à l'accomplissement d'un acte ; garantir l'authenticité et la régularité des actes conclus, ce qui pose la question du consentement ; organiser la publicité, la conservation et l'archivage.

Bien que la législation accorde une place croissante aux outils numériques et procédures dématérialisées, le développement des *blockchains* ouvre de nouvelles perspectives s'agissant de l'usage de la signature électronique, de

---

(1) À proprement parler, la qualification de « tiers de confiance » s'applique en droit fiscal. Aux termes de l'article 170 du code général des impôts, il s'agit d'une personne choisie parmi les membres des professions réglementées d'avocat, de notaire ou de l'expertise comptable et ayant signé avec l'administration fiscale une convention individuelle, habilitée à recevoir d'un contribuable assujetti à l'obligation de dépôt d'une déclaration annuelle des revenus déclarer ses revenus, les pièces justificatives des charges ouvrant droit au bénéfice de déductions, de réductions ou de crédits d'impôts.

Dans le cadre juridique créé par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, la notion de « tiers de confiance » désigne également un organisme habilité à mettre en œuvre des signatures électroniques reposant sur des architectures d'infrastructure à clés publiques ou PKI *(*Public Key Infrastructure*). Il peut aussi s'agir d'un tiers auquel est confiée une copie de la partie secrète d'une clé de chiffrement publique.*

l'archivage électronique et de l'identité numérique. Dès lors, se pose nécessairement la question du rôle et des modalités d'intervention des professions juridiques réglementées, voire de la puissance publique elle-même.

a. Un impact certain sur les professions juridiques réglementées et les avocats

Aux termes de la directive européenne sur les qualifications professionnelles [(1)], constitue une profession juridique réglementée « *une activité ou un ensemble d'activités professionnelles dont l'accès, l'exercice ou une des modalités d'exercice est subordonné directement ou indirectement, en vertu de dispositions législatives, réglementaires ou administratives, à la possession de qualifications professionnelles déterminées ; l'utilisation d'un titre professionnel limitée par des dispositions législatives, réglementaires ou administratives aux détenteurs d'une qualification professionnelle donnée constitue notamment une modalité d'exercice* ». En droit français, cette qualification s'applique ordinairement aux huissiers et aux notaires. Avec les greffiers des tribunaux de commerce, ces deux professions jouissent du statut d'officiers publics et ministériels, dans la mesure où leurs membres – outre leur nomination par le garde des Sceaux – possèdent la prérogative d'établir des actes authentiques faisant foi jusqu'à inscription de faux en écriture publique.

● **De prime abord, l'usage des *blockchains* apporte une remise en cause de ce monopole légal** dès lors que la technologie parait en mesure de remplir des fonctions similaires à celles dévolues aux professions juridiques réglementées. En effet, les protocoles garantissent en principe l'authenticité des actes inscrits grâce à la certification, l'horodatage et **l'immutabilité des blocs. En outre, ils procurent les moyens d'un archivage et d'une certaine publicité** qui peut conduire à considérer que les *blockchains* – sous réserve de certaines limites techniques et des choix du législateur – pourraient remplir un office comparable à celui des notaires.

Cela étant, les éléments recueillis par la mission donnent à penser qu'en l'état, **la technologie ouvre moins la perspective d'un remplacement des professions juridiques réglementées que d'une évolution parfois assez profonde des conditions d'exercice de leurs missions.** Ce constat vaut en particulier s'agissant des notaires.

D'une part, la profession semble déjà en mesure de s'approprier les outils nouveaux que procure la technologie des *blockchains*. D'après l'analyse développée devant la mission par les représentants du Conseil supérieur du notariat (CSN), son usage contribuerait à la poursuite de la dématérialisation des actes notariés. Au-delà de l'automatisation de l'établissement des actes et de leur numérisation, la technologie rendrait notamment possible la délivrance de copies exécutoires présentant toutes les garanties grâce à la certification et à la traçabilité

(1) Cf. article 3 de la d*irective 2005/36/CE du Parlement européen et du Conseil du 7 septembre 2005 relative à la reconnaissance des qualifications professionnelles.*

assurées par les protocoles. Dans cette optique, la profession travaillerait à la création d'une *blockchain* sur laquelle pourrait être déposé un *hasch* attestant de la correspondance entre la copie délivrée et l'acte (par exemple, un acte de propriété établi par un notaire). D'après le CSN, pour la pleine efficacité de ce dispositif, il ne paraîtrait pas hors de propos d'y associer à terme les huissiers et les banques. Par ailleurs, la technologie pourrait faciliter à la consultation de certains fichiers légaux, à l'exemple du fichier immobilier (1), le cadastre faisant par ailleurs déjà l'objet de traitements automatisés par la direction générale des Finances publiques (2).

D'autre part, il s'avère que dans l'état actuel de la technique**, le seul recours à un protocole automatisé tel que celui des *blockchains* ne semble pas permettre de satisfaire tous les besoins** auxquels sont censées répondre les professions juridiques réglementées en général et, en particulier, les notaires.

Certes, ainsi que l'ont admis les représentants du Conseil supérieur du Notariat, la technologie offre potentiellement la capacité d'automatiser la collecte des informations requises et utilisées dans l'établissement des actes notariés.

En revanche, **elle ne paraît pas en mesure d'assurer aujourd'hui la nécessaire vérification des droits des différentes parties prenantes** (par exemple, le droit de collatéraux ou de tiers comme les communes dans la vente d'un bien immobilier). De surcroît, on ne saurait occulter l'importance décisive des diligences requises afin de vérifier le caractère libre et éclairé du consentement d'une partie à un acte (par exemple, un acquéreur ou un vendeur). Or, d'après l'analyse du CSN, ce contrôle ne va pas de soi dans l'univers numérique, avec notamment la question de l'identité numérique d'une personne habilitée à représenter une personne morale.

Au-delà, comme indiqué précédemment (3), **le problème posé reste celle de la correspondance entre les données inscrites dans les *blockchains* et le monde réel, ainsi que la véracité des informations inscrites dans les protocoles**. Dans cette optique, plusieurs des personnes auditionnées par la mission ont évoqué la nécessaire intervention d'une instance tierce qui assumerait une fonction d' « oracle ». Son rôle consisterait à vérifier les événements survenus dans le « monde réel » et à présenter cette information aux acteurs d'une *blockchain*.

Ainsi que l'ont relevé plusieurs observateurs, l'intervention d'un « oracle » soulève des questions à la fois de principe – au regard de la philosophie

---

(1) Le Fichier immobilier recense les propriétaires et les immeubles, et archive les actes soumis à publication, les mutations, les ventes, les donations, ainsi que les inscriptions de privilèges, comme les hypothèques, les charges et les servitudes qui grèvent le terrain ou l'immeuble (servitude de passage, de tout-à-l'égout, de mitoyenneté, etc.).

(2) Cf. arrêté du 10 décembre 2010 relatif à la mise en service par la direction générale des finances publiques d'un traitement automatisé de données à caractère personnel dénommé « VIsualisation de la DOcumentation Cadastrale (VIDOC).

(3) Cf. supra *pp. 27-28.*

des *blockchains* – mais aussi pratique. Qui peut assumer la fonction d'« oracle » ? Quelle confiance lui accorder ? Que faire si l'information n'est pas ajoutée par l'oracle, ou si elle est fausse ?

À bien des égards, **le statut d'une profession juridique réglementée comme celle des notaires peut être considéré comme apportant certaines garanties de nature à répondre à ces interrogations, dans le cadre renouvelé des missions assignées par le législateur.**

● **À un moindre degré, la technologie des blockchains crée également les conditions de nouveaux développements pour les avocats**. Même si un certain nombre de projets demeure au stade de la preuve de concept, les éléments recueillis auprès de représentants et de membres de la profession laissent entrevoir la possibilité de nouveaux cas d'usage susceptibles de renouveler les conditions d'exercice du métier.

De manière plus générique, **la technologie semble pouvoir contribuer à une certaine automatisation de tâches présentant une faible valeur ajoutée**, à l'instar d'outils informatiques permettant d'ores et déjà de répliquer des clauses ou moyens utilisés fréquemment. De l'avis des professionnels auditionnés, cette évolution – qui donnerait aux avocats les moyens de se recentrer sur le cœur de leurs savoir-faire – pourrait ne pas rester sans conséquences sur les attentes des clients – peu désireux désormais de rétribuer des taches à faible valeur ajoutée – mais aussi sur le déroulement des carrières – les jeunes avocats pouvant trouver un intérêt à un premier recrutement au sein des entreprises en tant que juristes avant de rejoindre éventuellement des cabinets.

En outre, **l'usage des *blockchains* pourrait étoffer les outils déjà mis en place pour les échanges entre professionnels, qui exigent le recours à la signature électronique et à l'identité numérique, la certification et la confidentialité des documents et pièces**.

Devant la mission, **certains professionnels ont également évoqué la perspective d'une gestion de la rétribution des prestations accomplies au titre de l'aide juridictionnelle** au moyen de cette technologie. Dans le cadre institué par la loi du 10 juillet 1991 [(1)], le paiement des missions accomplies (assistance au cours des gardes à vue et des procédures devant les juridictions) comporte de fait des délais administratifs : il suppose de multiples diligences de la part des professionnels comme des caisses autonomes des règlements pécuniaires des avocats (CARPA). Afin de remédier à cette situation parfois préjudiciable, l'usage de *smart contracts* serait envisagé.

En dehors de l'amélioration des procédures existantes, **les *blockchains* semblent surtout ouvrir de nouveaux champs d'expertise et de responsabilité.**

(1) Loi n° 91-647 du 10 juillet 1991 relative à l'aide juridique.

Outre des questions nouvelles posées en droit, le développement possible des *smart contracts* peut ainsi conforter les avocats dans leur fonction de conseil. Comme indiqué précédemment (1), les *smart contracts* désignent en réalité des programmes informatiques inscrits dans une *blockchain*, contenant les termes d'un accord préalablement conclu entre des parties et fixant les conditions de son exécution (par exemple, le paiement d'un prix en échange d'un service). En principe, le caractère inviolable des protocoles doit garantir que les termes d'un contrat ne puissent être modifiés et s'exécutent suivant les stipulations convenues, sans intermédiaire.

Dès lors, il importe que les parties puissent définir de manière très précise leurs droits et obligations, préalablement à l'établissement du programme informatique. **Cette nécessité peut justifier le recours aux conseils d'un avocat, dont l'office consistera à la fois à examiner et proposer des stipulations conventionnelles inscrites dans une *blockchain* mais aussi – le cas échéant – à auditer le dispositif technique sur lequel devra reposer leur exécution**.

Ainsi que l'ont relevé l'ensemble des professionnels auditionnés, **cette nouvelle prestation impliquera nécessairement une évolution des formations.** À l'école du Barreau de Paris et de Lille, les avocats recevraient ainsi une formation au codage informatique. Du point de vue la mission, il s'agit là d'une orientation opportune dès lors qu'il existe des projets tendant à concevoir des protocoles susceptibles de traduire en plusieurs langues du code informatique et, en conséquence, de rédiger des contrats de manière informatique.

L'usage croissant des *smart contracts* pourrait également rendre nécessaire d'attribuer expressément aux avocats la fonction de tiers de confiance numérique. Du point de vue des rapporteurs, ce rôle ne paraît pas incohérent avec le conseil que pourrait apporter la profession dans le recours au *smart contracts*. Du reste, dans la mesure où l'exécution de ces programmes repose sur des instructions conditionnelles (2), il importe de s'assurer de la véracité des informations extérieures introduites dans une « *blockchain* ».

Dans l'optique de la mission, rien n'interdit d'envisager qu'une mission de certification des informations introduites dans des *blockchains* puisse incomber aussi bien aux professions juridiques réglementées, un panel beaucoup plus large d'acteurs (tels que les avocats) et ne pas être exercée en vertu d'un monopole légal. Cette dernière orientation supposerait bien entendu, dans l'esprit de la loi sur la confiance numérique – qui a créé dans une autre finalité le statut de « prestataires de services de certification électronique » (3), d'actualiser le cadre légal en vigueur.

Dans cette optique, **la mission estime qu'il conviendrait d'examiner l'intérêt de formaliser dans la loi le statut de « tiers de confiance**

(1) Cf. supra pp. 27-28.

(2) Si telle condition est vérifiée, alors telle conséquence s'exécute.

(3) Cf. article 33 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

numérique ». Sur la base de la définition proposée par la Fédération nationale des tiers de confiance (FNTC), cet acteur – de droit public ou privé – pourrait recevoir la mission d'intervenir dans la protection de l'identité, des documents, des transactions et de la mémoire numérique. Il engagerait sa responsabilité juridique dans les opérations qu'il effectue pour le compte de ses clients.

La loi devrait lui faire obligation de garantir son interopérabilité avec les autres tiers de confiance numérique. Il devrait démontrer sa capacité de continuité de service au-delà de sa propre existence en garantissant la réversibilité de ses services.

Enfin, le « tiers de confiance numérique » devrait être membre d'un ordre, d'une association ou d'une fédération disposant d'une charte et d'un comité d'éthique. Il serait tenu à des obligations d'intégrité, de transparence et de stricte confidentialité. Il s'engagerait à respecter la règlementation, les normes ou labels en vigueur et se soumettrait à des audits externes réguliers.

Cela pourrait permettre de renforcer la confiance dans les services offerts par les *blockchains*, nécessitant l'intervention d'un « oracle » à un moment de l'exécution des services.

Proposition n° 5 : Évaluer l'intérêt de consacrer dans la loi le statut de tiers de confiance numérique chargé d'assurer la protection de l'identité, des documents, des transactions et en mesure d'auditer et de certifier les protocoles blockchains.

b. Un État lui-même questionné sinon dans son rôle, du moins dans l'exercice de ses missions

L'essor des *blockchains* expose les personnes publiques à une remise en cause de même nature que celles auxquelles se trouvent confrontées les professions juridiques réglementées et, plus largement, les acteurs assumant la fonction de tiers de confiance. **Par les « prestations » et les garanties qu'elle ambitionne d'apporter, la technologie tend en effet à délégitimer le monopole dont elle dispose pour l'accomplissement de missions et qui les placent en position de médiateur dans les relations sociales.** Ainsi que le souligne le Conseil d'État dans sa réflexion sur l'impact des plateformes numériques sur l'action publique (1), cette remise en cause touche plus particulièrement la fonction de certification, c'est-à-dire celle visant à garantir la qualité ou la conformité d'un état par rapport à un référentiel donné.

● Ainsi que l'ont souligné la plupart des personnes auditionnées, **la perspective d'un dépassement de l'État ou d'échanges sociaux sans intermédiaires participe de l'essence même d'une technologie non dénuée de fondements idéologiques.**

(1) Conseil d'État, Puissance publique et plateformes numériques : accompagner l'«ubérisation», *Étude annuelle 2017, septembre 2017, pp. 94-95.*

Parmi les sources d'inspiration de ses promoteurs, on trouve naturellement le mouvement pour le logiciel libre, initié dans les années 1980 par Richard Stallman autour de la Fondation pour le logiciel libre [(1)] et du système d'exploitation libre GNU. Il convient également de mentionner le rôle de la communauté Cypherpunk [(2)] : depuis une trentaine d'années, celle-ci milite en faveur d'une utilisation des technologies de chiffrement en vue de créer une monnaie électronique et de garantir des transactions anonymes, échappant au contrôle ou à la surveillance des autorités publiques.

Ces influences ont pu inspirer un certain nombre de tentatives de créer des monnaies numériques [(3)]. La création du *bitcoin* manifeste aussi vraisemblablement une défiance vis-à-vis de la politique des banques centrales et des banques commerciales, dans le contexte de la crise de 2008. Elle vise en tous cas à donner aux individus les moyens d'opérer directement des transactions sans intermédiaire, de manière décentralisée.

À défaut d'en être directement inspirée, la technologie des *blockchains* répond à tout le moins aux aspirations du mouvement libertarien qui postule un retrait de l'État et l'abandon de son privilège de battre monnaie.

Ainsi que le remarquait M. Éric Salobir, président d'Optic [(4)], **cette philosophie prône une société fondée sur les relations contractuelles entre individus, en rupture avec une organisation fondée sur un contrat social particulier**. Même si tous les usages envisagés ne traduisent pas cette ambition, les *blockchains*invitent à transférer la confiance des institutions publiques (telles que l'État, les banques centrales) vers le protocole, suivant le principe : « *code is law* ».

Dès lors, nonobstant l'innovation technique, **le concept revêt également une dimension politique en ce qu'il s'efforce de proposer une réponse à une crise de confiance frappant la société et porte en lui une redéfinition des relations sociales et des rapports d'autorité.**

À certains égards, la dimension de groupe organisé en dehors des formes sociales classiques transparaît dans les projets DAO (*Decentralized Autonomous Organization*). Ainsi, le projet « TheDAO » créé en 2016 à l'initiative de la start-up *Slock.it*, poursuivait trois objectifs : évaluer des projets qui lui sont soumis ; décider collectivement avec les détenteurs de jetons de la DAO de financer ou non ces projets ; distribuer les risques et récompenses qui y sont relatifs.

---

(1) Free Software Foundation (ou FSF)

(2) Terme inventé par Jude Milhon à Berkeley en 1992, à partir de l'anglais cipher (ou chiffrement) et « cyberpunk » lui-même issu des mots « cybernétiques » et « punk » et renvoyant à des œuvres de fiction dystopiques basées sur les technologies.

(3) Rapport n° 1092 - Rapport de Mme Valéria Faure-Muntian, MM. Claude de Ganay et Ronan Le Gleut établi au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, sur les enjeux technologiques des blockchains (*chaînes de blocs*)*, pp.14-15.*

(4) Ordre des prêcheurs pour les technologies, l'information et la communication (Optic).

● De fait, **il existe aujourd'hui un certain nombre de projets dont la réalisation peut – sous réserve d'une technologie mature – rendre concevable le recours aux *blockchains* dans l'exercice de certaines prérogatives publiques.**

Parmi les exemples évoqués devant la mission, on citera **la possibilité de remédier à l'absence ou à la déficience d'un cadastre**. Ainsi d'après les indications des représentants du Conseil supérieur du notariat, en Géorgie, le recours à un protocole de *blockchains* a permis de certifier des propriétés immobilières dans des circonstances historiques troublées. De même, la tenue du registre des terres appartenant à l'État du Honduras repose aujourd'hui sur cette technologie. On signalera enfin l'initiative d'une organisation non gouvernementale au Ghana, pays dans lequel près de 90 % des terres rurales ne sont pas enregistrées sur des bases de données officielles, et où de nombreux citadins n'ont pas encore d'adresse officielle, qui a abouti à la mise en place un cadastre enregistré au moyen de ce procédé.

Les *blockchains* semblent par ailleurs de nature à pallier l'absence d'adresse géographique dans certains pays et, dans une certaine mesure, de répondre aux exigences de connaissance de la clientèle. (1)

Dans l'usage de l'identité numérique, l'Estonie montre **l'apport des *blockchains* à la simplification des relations entre les usagers (particuliers et entreprises) et les services publics**.

L'apport des *blockchains* dans le développement de l'administration numérique : l'exemple estonien

Cette ex-république soviétique a en effet engagé, dès le début des années 2000, une politique fondée sur l'émission d'une carte d'identité électronique et l'interconnexion progressive de l'ensemble des bases de données numériques des services de l'État.

Elle offre aujourd'hui, par l'interconnexion de 170 bases de données publiques, plus de 2 000 services à plus de 900 organisations (institutions, ministères et entreprises privées).

Depuis 2008, ces services procèdent d'une infrastructure cryptographique de type *blockchains* dénommée KSY (2), qui permet de vérifier, de manière indépendante la consultation ou le changement éventuel d'une donnée.

S'agissant de la traçabilité des aides publiques, les représentants de la Caisse des dépôts et consignations ont signalé à la mission l'existence d'un atelier de travail avec le Secrétariat général pour les affaires régionales (SGAR) de Bretagne portant sur la contractualisation, les subventions et les allocations.

(1) « Know touryour customer » (KYC).

(2) Pour Keyless Signature infrastructure.

Pour ce qui est du vote électronique, les informations recueillies par la mission donnent à penser que **les caractéristiques de la technologie soulèvent des questions auxquelles il paraît difficile d'apporter aujourd'hui des réponses totalement satisfaisantes, en tous cas pour l'organisation de scrutins nationaux et locaux.**

Telle est la conclusion que l'on peut tirer de l'état de la réflexion des autorités de Genève (1) dressé par M. Vincent Pignon, conseiller en innovation et en technologie de l'information auprès du canton. Il ressort en effet de son analyse qu'au plan technique, le recours aux *blockchains* rend possible la création d'une urne électronique qui permet d'établir le nombre de votants, sans que l'on sache vers qui se sont portés leurs suffrages.

Toutefois, le dispositif ne résout pas nécessairement **le problème de la conservation des données relatives aux votes émis** : la connaissance des pseudonymes utilisés par les électeurs permet en effet de retracer l'expression de leurs suffrages. En outre, **la détention des clés pour les participants du réseau demeure une source de fragilité (sauf à concevoir la possibilité d'une clé aléatoire pour un vote électronique donné) et pose la question de la vérification certaine de l'identité de l'électeur**. D'après les réponses apportées par M. Pignon, la réflexion menée par le Canton de Genève depuis plus de six mois n'aurait pas à ce jour permis de trouver de solutions adéquates.

● Du point de vue des rapporteurs, **les contraintes et limites auxquelles se heurtent encore aujourd'hui les *blockchains* ne sauraient conduire à en exclure l'usage car la technologie procure un indiscutable levier de modernisation**.

Ils partagent les conclusions du Conseil d'État qui, dans une étude publiée en 2017 (2), a qualifié la technologie des *blockchains* d'« *enjeu crucial* » et a estimé que celle-ci pourrait permettre des « *usages particulièrement intéressants dans des perspectives d'intérêt public* ». D'après son analyse, certains domaines de l'action publique, tels que celui de la commande publique (3), apparaissent ainsi particulièrement propices à sa mise en œuvre. En cela, le Conseil d'État adopte une approche comparable à celle du *Government office for Science* du Royaume-Uni qui, dans un rapport publié dès janvier 2016, affirmait que la technologie pouvait répondre à un certain nombre d'exigences de l'action publique (4).

Dans le cadre de ses propres travaux, la mission a également recueilli des signalements relatifs à **des projets innovants qui, de prime abord, paraissent**

---

(1) Genève a envisagé d'utiliser la technologie des blockchains *pour l'organisation des « votations ». Le canton autorise le vote électronique pour ce type de scrutins.*

(2) Conseil d'État, Puissance publique et plateformes numériques : accompagner l'«upérisation», *Étude annuelle 2017, septembre 2017.*

(3) Dans cette matière, un objectif de dématérialisation totale avait été fixé pour le 1er octobre 2018.

(4) Government office for Science, Distributed ledger technology: beyond block chain, A report by the UK Government Chief Scientific Adviser, *janvier 2019 (https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain).*

susceptibles de renouveler les modalités d'intervention de la puissance publique.

– **Dans le domaine de l'enseignement supérieur**, il en va ainsi du projet d'établir une grande *blockchain* distribuée au sein de laquelle seraient inscrits les diplômes universitaires. Selon les explications fournies par Mme Perrine de Coëtlogon, expert numérique et animatrice à l'université de Lille d'un groupe de travail *#Blockchain4EDU*, il s'agirait de permettre à tout étudiant de produire ses titres – voire de justifier de compétences spécifiques évaluées par les universités (1) – à partir des informations contenues dans un espace de confiance. De fait, dans le cadre de leur visite à la Station F, vos rapporteurs ont pu rencontrer les représentants de start-ups qui, à l'instar de BCDiploma, développent des protocoles poursuivant cet objectif.

Un tel usage paraît de nature à conforter le mouvement de dématérialisation et de simplification des procédures et pourrait – sous réserve de progrès techniques – participer à la réalisation de projets aussi ambitieux qu' « *Erasmus without paper* », avec notamment pour perspectives : l'établissement d'une carte d'étudiant européen, qui éviterait de renouveler certaines démarches dans le cadre d'une inscription ; la création d'un dépôt de logiciels et de ressources universitaires accessibles à l'ensemble des membres d'un réseau d'établissements de l'enseignement supérieur à l'échelle de l'Europe.

– **Dans le domaine des administrations**, il convient à l'évidence de faire état des perspectives ouvertes par les projets actuellement conduits en Suisse et, en particulier à Genève.

D'après l'état des lieux dressés par M. Vincent Pignon, après avoir examiné en 2016 les cas d'usage possibles, le canton a recours depuis 2017 à une *blockchain* afin d'assurer la certification des données contenues dans le registre du commerce et la délivrance d'actes (2) certifiés de façon automatique. On notera que d'après la description établie par M. Pignon, le protocole Ethereum utilisé par le canton de Genève permet la délivrance d'un nombre illimité d'actes administratifs pour un coût de « production » annuel très modique, estimé à l'équivalent de 17,54 euros.

Sur la base de résultats très satisfaisants, il est désormais envisagé d'employer la technologie afin d' « industrialiser » la délivrance de nombreux actes administratifs (actes de naissance, de décès, etc.).

Le canton entend par ailleurs – avec l'accord de la Confédération – développer l'usage de la signature électronique et de permettre l'obtention d'une identité numérique afin de rendre possible des échanges entre les résidents et ses services. Dans le cadre d'une autre *blockchain*, il envisage enfin de donner aux détenteurs de droits à bâtir sur des terrains constructibles en zones industrielles la

(1) Par le biais de petits supports dématérialisés appelés open badges*.*

(2) Pour autant, pour des motifs de confidentialité, la tenue du registre ne repose pas sur le protocole.

capacité de les échanger directement. Dans une première version du dispositif censée être mise en service en décembre 2018, il reviendrait aux notaires de s'assurer de l'identité du cédant et de l'acquéreur mais de gérer la transaction. La puissance publique prélèverait automatiquement les droits à ce stade. Dans une seconde version, les promoteurs pourraient vendre des droits à bâtir sans intermédiaire ; les droits seraient enregistrés dans le registre foncier, ce qui réduirait les coûts et les délais des procédures et assurerait une plus grande transparence.

En soi, cet exemple invite à considérer l'apport possible de la technologie des *blockchains* à l'organisation, ainsi qu'au fonctionnement des services publics et des administrations en France en termes de coût, d'efficacité des ressources allouées et de simplification des démarches de l'usager. Or, les échanges avec des représentants de services ministériels – comme avec des professionnels et opérateurs du secteur – accréditent l'idée qu'au sein des administrations, il n'existe pas à ce jour de réflexion globale sur les potentiels gains d'efficience à tirer de cette technologie. Les initiatives et études auxquelles celles-ci peuvent donner lieu semblent ne revêtir qu'un caractère très sectoriel et limité car reposant avant tout sur des curiosités individuelles.

Aussi, **la mission appelle le Gouvernement à se saisir pleinement des enjeux inhérents à l'essor des *blockchains* en se dotant d'une instance capable d'établir une stratégie nationale et de coordonner les efforts des services de l'État nécessaires à la pleine exploitation de cette technologie.**

Dans l'esprit des rapporteurs, cette fonction d'expertise et de pilotage ne saurait être assumée par la seule direction interministérielle des systèmes d'information et de communication de l'État (DINSIC). En effet, les questions soulevées excèdent assez largement la seule dimension technique de ce procédé. C'est la raison pour laquelle **les rapporteurs souscrivent volontiers à la recommandation formulée par France Stratégie de s'appuyer sur « *un groupe à compétences transversales à l'intérieur de l'État* »** [(1)]. De leur point de vue, ce dispositif parait en effet le plus adapté à une démarche interministérielle indispensable afin de permettre à la France de s'approprier pleinement une technologie prometteuse. La direction interministérielle des systèmes d'information et de communication de l'État (DINSIC) semble aux rapporteurs la plus indiquée pour réaliser cette tâche.

Proposition n° 6 : Créer au sein de la DINSIC un groupe de travail transversal chargé d'une mission d'évaluation des conditions du développement de la technologie des *blockchains* dans la vie économique et sociale et de son usage par les collectivités publiques.

(1) France Stratégie, Les enjeux des blockchains, Rapport du groupe de travail présidé par Mme Joëlle Toledano, *juin 2048, pp. 65-66.*

II. UN INVESTISSEMENT SUR L'AVENIR SUPPOSANT LA MOBILISATION DE RESSOURCES NATIONALES DANS UN CADRE JURIDIQUE PERTINENT

Les technologies de *blockchains* sont-elles de la poudre aux yeux ? Vos rapporteurs estiment que, **sans sombrer dans le « solutionnisme » technologique** qui verrait dans les *blockchains* le remède de nombreux maux, il convient de prendre en considération ce nouveau vecteur de croissance et de développement dont le **potentiel disruptif est, effectivement, immense**. Le travail de fond mené par vos rapporteurs permet même de faire ce pari : ce potentiel disruptif est sans doute aussi important que celui d'internet depuis vingt-cinq ans.

Aujourd'hui, les technologies liées aux *blockchains* connaissent une situation paradoxale : d'une part, un effet de mode et un engouement médiatique important lié notamment au grand éventail des applications imaginables pour les *blockchains* dans le monde de demain ; d'autre part, de nombreux amalgames entre ce qui relève de véritables *blockchains*, telles que la première partie du rapport les a présentées, et des technologies de registre très conventionnelles qui s'en approprient le nom et l'usage, souvent à des fins marketing. Il faut souvent être initié, sinon expert, pour déceler l'innovation réelle ou débusquer le faux-nez [(1)].

Et pourtant, l'innovation liée aux technologies des *blockchains* peut devenir rapidement, vos rapporteurs en sont persuadés, **un enjeu de souveraineté pour la France et de stratégie pour l'Union européenne**. Il faut faire en sorte de ne pas dépendre des choix technologiques et politiques d'autres pays qui auraient su, avant nous, développer les *blockchains* et imposer leurs standards. Il faut donc assurer que les conditions réglementaires, financières et fiscales soient réunies pour qu'un écosystème de la *blockchain* puisse efficacement prospérer et être de taille dans la révolution technologique qui s'annonce. La France et l'Europe doivent disposer de champions qui puissent faire prévaloir en priorité nos intérêts.

Le pari de ce rapport est qu'avec les technologies des *blockchains*, **l'ensemble des filières économiques va être transformé**. Il s'agit d'une nouvelle économie : nous ne devons donc pas refaire les mêmes erreurs que celles que la France et l'Europe ont commises au début d'internet – comme le fait de croire que les faiblesses d'internet, au début, –ne permettraient pas d'en faire un réseau susceptible de supporter des échanges commerciaux, ni laisser des pays qui montreraient davantage d'audace ou de réactivité prendre la place qui doit être celle de la France en raison de la qualité et du talent de nos entrepreneurs comme de nos chercheurs dans ce domaine.

---

(1) Un constat partagé par nos collègues de l'OPECST, qui, dans leur rapport précité, constataient : « Un regard distancié paraît nécessaire, en raison des effets de mode propres aux écosystèmes entrepreneuriaux. Ces effets de mode, visibles dans le recours à certains concepts, tels que les technologies disruptives, l'intelligence artificielle, les données massives (big data), le cloud, l'internet des objets (IoT pour internet of things) ou, encore, la blockchain*, sont parfois le reflet de stratégies marketing séduisantes, mais sans toujours s'accompagner d'innovations aussi majeures que celles annoncées. »*

A. SOUTENIR UN ÉCOSYSTEME NAISSANT ET PROMETTEUR

Notre pays a **tous les atouts pour réussir** : une recherche scientifique de haute qualité, de bonnes formations et des entrepreneurs talentueux. Un premier développement permettra d'établir que les conditions économiques du déploiement d'un écosystème performant des *blockchains* sont bien présentes en France.

Cela n'est cependant pas suffisant. Pour donner un cadre à la fois souple et sécurisant à la transformation de l'économie qui débute grâce à cette nouvelle technologie, il faut poser les jalons d'une nouvelle régulation. Celle-ci doit encourager l'innovation plutôt que d'être considérée comme un « irritant » par les entrepreneurs ou par les institutions (bancaires en particulier) ; celle-ci doit aussi sortir cette nouvelle économie du « far west », de l'insécurité juridique dans lequel elle ne peut que s'enliser. La réputation sulfureuse des « cryptos » tient beaucoup à l'opacité du contexte financier, fiscal et réglementaire dans lequel ces innovations s'inscrivent aujourd'hui.

Un deuxième développement présentera donc les avancées les plus récentes du cadre réglementaire français, sur les volets économiques (création d'un marché organisé des émissions de jetons), financiers (droit et accès aux institutions bancaires) et fiscaux (fiscalité des transactions réalisées en cryptoactifs). Plus largement, ce cadre réglementaire doit reposer sur une meilleure définition, une normalisation (administrative, fiscale et comptable) des objets innovants qu'il faut réguler : le jeton, le registre distribué, le livre blanc, le portefeuille de cryptoactifs, etc.

Enfin, afin de garantir la place de la France comme puissance inspiratrice et modèle de cette nouvelle économie, il ne faut pas seulement **organiser l'attelage de souplesse et de sécurité juridique** souhaité par vos rapporteurs. Il faut encore que ce cadre soit approprié par les innovateurs et les entrepreneurs, que des ressources financières suffisantes puissent être accessibles, et que le secteur public soit également mis en chantier et s'ouvre aux perspectives de ces innovations. En somme, **les pouvoirs publics ont un rôle d'impulsion** qu'il conviendra de préciser.

1. Identifier les besoins et développer les compétences

La *blockchain* Bitcoin a dix ans cette année. Comme toute nouvelle technologie ou grappe de technologies dont le contenu innovant est radical, et non incrémental, le vrai potentiel économique et social des *blockchains* est à peine perceptible, et il reste beaucoup à imaginer et à inventer. Les nombreuses auditions menées par la mission rappellent que la technologie des *blockchains* n'est pas suffisamment mature : cela ne signifie pas qu'elle n'est pas déjà utile, mais que les gains à en tirer à moyen et à long termes doivent encore être explorés.

C’est pourquoi, si la France veut se doter d’un écosystème propice à la montée en charge des technologies de *blockchains* et de leurs usages, il faut mobiliser l’ensemble des atouts dont notre pays dispose en amont du processus d’innovation (recherche fondamentale, sciences de l’ingénieur) comme en aval (stimulation de l’entrepreneuriat, connexions entre les univers de la recherche et de l’entreprise, appropriation commerciale des intuitions techniques).

Il convient, d’abord, de rappeler les réels atouts dont notre pays dispose, mais qu’il faut encore mobiliser et valoriser sur ce secteur d’avenir qu’est la *blockchain*. Il faut ensuite faire l’état des lieux des manques ou des retards observés à l’heure actuelle et auxquels il faut remédier rapidement.

a. Les atouts français à valoriser

Contrairement à la plupart des innovations technologiques majeures récentes, les *blockchains* ne sont pas apparues dans des laboratoires de recherche fondamentale. Bitcoin, la première *blockchain*, a été créée, développée, diffusée sur internet – ses auteurs sont inconnus. Cet épisode atypique (1) dans l’histoire de l’innovation ne doit pas laisser penser que l’essor théorique et pratique des *blockchains* ne sera pas réalisé d’abord dans les centres d’innovation qui y auront, les premiers, consacrés une énergie et des ressources suffisantes.

Dans cette course, la France dispose d’atouts certains. En premier lieu, **sa recherche fondamentale demeure l’une des meilleures du monde** en sciences exactes, notamment en mathématiques. La cryptographie et les probabilités sont au cœur des *blockchains*. Si le monde académique éprouvait parfois des difficultés à traduire ses résultats en applications économiques innovantes, industrielles ou commerciales, le transfert et la valorisation vers les entreprises des résultats de la recherche publique se sont considérablement améliorés. Les sociétés d’accélération du transfert de technologie (SATT), créées en 2010, les incubateurs et accélérateurs créés au sein même de certains laboratoires et centres de recherche ainsi que les instruments financiers comme les programmes d’investissement d’avenir (PIA), qui permettent à des chercheurs de monter des projets et d’obtenir des fonds pour investir dans leur activité, sont autant de bons signaux qui améliorent le potentiel d’innovation français. Des structures, comme les pôles de compétitivité ou les instituts de recherche technologiques (IRT), sont spécifiquement bâties autour de la nécessité de rapprocher les différents acteurs de l’innovation, publics et privés.

La mission a ainsi pu rencontrer des représentants de l’IRT SystemX. Financé par le PIA pour rapprocher monde académique et entreprises en matière de recherche appliquée, SystemX a mobilisé vingt personnes sur les sujets relatifs aux *blockchains* (doctorants, ingénieurs de recherche, chercheurs habilités) sur

---

(1) Un autre exemple récent pourrait être trouvé dans la résolution d’un problème mathématique important apportée par un contributeur anonyme sur un site consacré à un anime japonais, ce que relatait le site Numerama en octobre dernier : https://www.numerama.com/sciences/435102-un-anonyme-de-4chan-a-une-solution-a-un-probleme-de-math-et-la-science-ne-sait-pas-comment-lutiliser.html

trois thèmes prioritaires : les transports, l'énergie et la finance. À ce stade, leur principale mission est de caractériser l'intérêt économique des *blockchains*, d'effectuer des études de faisabilité, d'opérer des choix technologiques puis d'être en mesure de conseiller des voies de déploiement aux entreprises. En 2017, SystemX a lancé un appel relayé par plusieurs grands médias pour attirer des startups de l'écosystème des *blockchains* afin de dynamiser les ressources mobilisées sur le sujet et profiter mutuellement d'un effet de réseau sur cette technologie.

Par exemple, dans le secteur énergétique et en partenariat avec EDF, le principal enjeu de l'équipe de l'IRT a été la définition d'un *smart contract* et de ses conditions techniques et économiques pour permettre le déploiement et le fonctionnement d'un réseau local de production et de distribution d'électricité. Une *blockchain* relie les consommateurs et les producteurs et organise les échanges de flux entre eux à partir des données de leurs compteurs Linky.

En outre, et plus spécifiquement sur le sujet des *blockchains*, la France dispose d'un atout supplémentaire : **sa capacité à travailler de façon interdisciplinaire** et sa souplesse pour monter des équipes de chercheurs *ad hoc* sur certains projets de long terme correspondent parfaitement au caractère hybride des *blockchains*, qui nécessitent des compétences en cryptographie, en algèbre, en sciences de l'ingénieur, en informatique, en économie ou encore en gestion de données.

Par exemple, Inria, dont plusieurs chercheurs ont également été auditionnés, a cité les *blockchains* parmi les défis scientifiques de son Plan stratégique scientifique 2018-2022. Inria, Institut national de recherche en sciences du numérique, a développé plusieurs partenariats avec des écoles, des laboratoires ou des centres de recherche comme Polytechnique, Centrale Supélec, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA) ou le Centre national de la recherche scientifique (CNRS). Des équipes pluridisciplinaires, comme l'équipe-projet CIDRE, ont concentré leur action récente sur les sujets de *blockchains*. Enfin, l'action d'Inria dans l'écosystème de l'innovation est plus générale : l'institut a accompagné la création de 130 start-ups, par amorçage ou par prise de participations, ainsi qu'en encourageant les transferts technologiques.

Proposition n° 7 : Favoriser l'émergence d'équipes interdisciplinaires et autonomes en fléchant les crédits du PIA ou de l'Agence nationale de la recherche (ANR) vers le financement pérenne de telles structures de recherche agiles et conditionner ce financement à la recherche d'une issue commerciale ou industrielle.

b. Les faiblesses françaises auxquelles remédier

Le meilleur moyen de dépasser le stade de l'effet de mode ou du marketing *blockchains* est encore de proposer des formations, des cursus, des certifications qui permettent de créer une filière sérieuse, reconnue et compétente.

Cela permettrait en outre de compenser une faiblesse qui n'aura de cesse de s'amplifier si rien n'est fait : le **manque de main-d'œuvre formée** par rapport aux besoins des entreprises qui proposent des solutions de *blockchains* ou souhaitent franchir le pas.

Si les atouts français sont importants dans les différents champs abordés par les *blockchains* (de la cryptographie au développement web), encore faut-il structurer l'offre de formation et les voies d'apprentissage, créer des métiers des *blockchains*, organiser des cursus attractifs et diplômants pour les jeunes.

Les auditions menées par la mission ont confirmé que la France risquait de ne pas parvenir à rattraper son retard si l'offre de formation n'était pas suffisamment évolutive pour s'adapter aux besoins – dont certains ne sont sans doute pas encore connus – des entreprises en main-d'œuvre qualifiée : les futurs architectes des données et des *blockchains* doivent être formés dès aujourd'hui.

Ce constat a également été dressé par le groupe de travail de France Stratégie, présidé par Mme Joëlle Toledano, auditionnée par la mission. Dans leur rapport de juin 2018, « Les enjeux des *blockchains* », les membres du groupe de travail formulent deux propositions en lien avec les développements précédents : « promouvoir des travaux de recherche et développement en misant sur l'interdisciplinarité » et « inciter au développement de formations approfondies et favoriser l'appropriation du sujet ». Ce rapport rappelle que seul le pôle universitaire Léonard de Vinci a su, très tôt (en 2015), proposer un cours sur les *blockchains*, tandis que la plupart des grandes universités américaines ont déjà structuré une offre de formation autour de ce sujet. Des masters spécialisés, des modules de formation obligatoires en école de commerce ou d'ingénieur, des interventions ponctuelles d'experts du sujet devraient rapidement éclore dans notre système d'enseignement supérieur.

En outre, au-delà de la formation initiale, il convient de mobiliser l'ensemble des branches professionnelles autour d'une même recherche prospective des emplois et des compétences dont cet écosystème a besoin, d'une part, puis d'adapter les emplois et les compétences existantes aux bouleversements qui pourraient découler de la généralisation des technologies de *blockchains*.

Le *think tank* #Leplusimportant propose ainsi aux branches professionnelles de recourir à leurs observatoires prospectifs des métiers et des qualifications (OPMQ) et d'engager ce travail prospectif au plus vite.

Vos rapporteurs s'associent à cette recommandation ainsi qu'à celles de France Stratégie : **l'adaptabilité de notre système de formation et de notre système professionnel est souvent prise en défaut face à l'innovation**.

Proposition n° 8 : Établir une « vision prospective partagée des emplois et des compétences » en vue de structurer une sous-filière *blockchains* au sein de la filière numérique.

2. Donner aux entreprises les moyens de leur développement

Cette sous-partie vise à présenter le cadre réglementaire, financier et fiscal, qui permettrait aux entreprises innovantes et recourant aux technologies des *blockchains* qui se développent en France d'être compétitives et de prendre des parts de marché à l'international, mais aussi à la France d'être attractive pour que des activités économiques liées aux *blockchains* choisissent de s'y installer.

La régulation d'un « secteur », d'une « technologie » ou d'un « écosystème » est d'autant plus délicate que, précisément**, l'innovation autour des *blockchains* est fortement évolutive, fugace et peu maîtrisable**. Une régulation trop forte tuerait l'innovation en France, qui se réfugierait donc dans des pays limitrophes ; une régulation trop faible serait inutile – dans le cas des cryptoactifs, qui sera exposé ci-après, il en va pourtant de la protection des investisseurs et de la lutte contre les activités criminelles – ; dans tous les cas, **la régulation est souvent rapidement dépassée** alors même qu'elle est souvent réclamée par les acteurs économiques concernés, qui sont **à la recherche de sécurité juridique** pour développer leurs activités.

Comme cela sera développé dans une partie ultérieure, une façon de sortir de ces dilemmes de l'intervention publique est de produire une régulation d' « avance de phase » : construire un cadre réglementaire expérimental, au périmètre borné mais permettant de créer librement pour accélérer le développement de l'écosystème. Cette **logique de « bac à sable »** se couple avec un recours de plus en plus systématique, de la part de l'État ou des autorités régulatrices, à des consultations auprès de l'ensemble des acteurs concernés. Cela a été fait préalablement à l'écriture des ordonnances relatives aux titres non cotés [(1)], ainsi que du projet de loi dit « PACTE » [(2)] à propos de la régulation des émissions de jetons. Cette démarche est essentielle à la bonne compréhension des enjeux et des solutions à traiter par l'ensemble des parties prenantes.

Toutefois, les éléments suivants visent à **préconiser un cadre plus général que celui de l'expérimentation**, qui ne doit pas être abandonné mais qui doit être complété par un cadre stable et pérenne qui permettra d'apporter la sécurité juridique suffisante aux entreprises déjà installées et qui souhaitent se développer rapidement tout en demeurant en France. Ce cadre repose sur trois piliers : la sécurisation des émissions de jetons ; l'adaptation de la réglementation bancaire et fiscale ; la mise à disposition de moyens financiers et techniques

(1) Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.

(2) Projet de loi relatif à la croissance et à la transformation des entreprises, déposé le 19 juin 2018 sur le bureau de l'Assemblée nationale et adopté en première lecture le 9 octobre 2018.

publics suffisants et durables pour soutenir l'émergence et le renforcement de l'écosystème français des *blockchains*.

a. Sécuriser les offres publiques de jetons (ICO)

Comme la première partie du rapport a permis de le préciser, le développement des technologies de *blockchains* est fortement lié au recours aux cryptoactifs dont elles sont souvent le support. Un point doit d'ailleurs être de nouveau rappelé : il est erroné d'opposer ce qui serait une « bonne » technologie, la *blockchain*, et ce qui serait une dérive, les cryptoactifs. En effet, la transformation de l'économie qui pourrait découler de la généralisation des *blockchains* est étroitement liée à la manière dont sont émis, enregistrés et utilisés les cryptoactifs.

Les cryptoactifs font donc intégralement partie de cette nouvelle économie, ce que matérialise parfaitement le concept d'offre publique de jetons, mieux connu sous son acronyme anglo-saxon d'ICO, pour *Initial Coin Offering* [(1)]. L'ICO est une technique de levée de fonds qui s'appuie sur l'émission de jetons (*tokens*), acquis en échange de cryptomonnaies ou de monnaies classiques (*fiat*), et qui peuvent être conservés, par exemple en vue de détenir certains droits politiques dans la société ou de recevoir des dividendes, ou échangés sur des plateformes numériques [(2)].

Il s'agit d'un mode de financement de l'innovation en pleine expansion : depuis début de 2018, en France, les principales ICO ont permis de lever 500 millions d'euros, soit 20 opérations d'un montant de 25 millions environ. Généralement, les ICO visent à développer des activités ou des applications en lien avec les *blockchains* : l'appétit nourri pour les ICO, en particulier en 2017, se justifie autant par des motifs spéculatifs que par une volonté affirmée d'une partie de l'écosystème « crypto » de soutenir les projets de développement des *blockchains*.

(1) Par analogie aux Initial Public Offerings *(IPO), qui sont les introductions en bourse.*

(2) Cf. supra *I C du présent rapport.*

Une ICO réussie en France : le projet iEx.ec

Reçue par la mission en audition, l'entreprise iEx.ec, issue d'Inria, développe un projet de création d'une place de marché décentralisée de ressources informatiques (*cloud computing*) pour des besoins applicatifs, donc sans intermédiaire de confiance et grâce aux cryptomonnaies. Les représentants de l'entreprise ont expliqué comment ils sont parvenus à lever l'équivalent de 12,5 millions de dollars en cryptomonnaies (bitcoins et ethers) en moins de trois heures en avril 2017. Ils ont notamment mis en avant l'efficacité de cette levée de fonds, là où un tour de table classique leur aurait probablement permis de lever moins de fonds, auprès d'investisseurs institutionnels, et au terme d'un processus d'au moins un an.

En revanche, le montant de la levée de fonds varie au gré des cours de ces cryptomonnaies, très volatils. Si l'ICO a d'abord pris beaucoup de valeur (jusqu'à 30 millions de dollars), elle en a également beaucoup perdu à la suite de la brutale baisse des cours de début 2018.

La puissance des ICO explique qu'elles fassent l'objet d'une compétition européenne et mondiale, et, à cette heure, la France est largement dépassée par la Suisse, très en avance dans ce domaine : deux cents ICO ont été conduites en Suisse, contre une vingtaine en France. Or une ICO menée en Suisse encourage les porteurs de projet, les entrepreneurs, les innovateurs, à localiser l'ensemble de leur activité dans ce pays-là, au détriment de la France.

Vos deux co-rapporteurs ont pu se rendre en Suisse. Ils ont pu constater que l'Autorité fédérale de surveillance des marchés financiers (FINMA), l'homologue de l'Autorité des marchés financiers (AMF) et de l'Autorité de contrôle prudentiel et de résolution (ACPR) en France, a su y bâtir rapidement un cadre souple permettant aux entreprises de lever des fonds en toute sécurité. Le cadre juridique favorable, notamment le droit des fondations qui font l'objet d'une imposition faible, explique également le succès suisse.

Il faut donc rapidement reprendre la main, sans verser dans l'excès inverse d'un cadre de régulation beaucoup trop lâche. Aujourd'hui, selon les estimations des experts auditionnés par la mission, entre un tiers et la moitié des ICO lancées dans le monde (essentiellement aux États-Unis, en volume) relèvent en réalité d'escroqueries pour aspirer les cryptomonnaies d'investisseurs crédules ou attirés par des rendements élevés. La France doit, dans la continuité de son droit et de la doctrine de l'AMF, assurer un niveau suffisant de protection des investisseurs. En outre, l'opacité de certains projets pour lesquels les ICO sont lancées est porteuse de réels risques en matière de blanchiment d'argent ou de financement d'activités criminelles.

Proposition n° 9 : Garantir un cadre de régulation des cryptoactifs qui réponde à l'exigence de protection des investisseurs français.

En effet, les cryptoactifs fonctionnent sur des *blockchains* qui, par définition et par philosophie, rejettent le contrôle d'autorités publiques centralisées

(comme une banque centrale) sur les transactions effectuées et peuvent, donc, plus aisément contourner les exigences normatives nationales, européennes ou internationales (1) que les monnaies « fiat » (comme l'euro ou le dollar) et leurs circuits bancaires traditionnels. Ainsi, la Chine a choisi, purement et simplement, d'interdire les levées de fonds en cryptomonnaies.

Pour des développements plus précis sur le fonctionnement des cryptomonnaies et des ICO, vos rapporteurs renvoient au rapport au ministre de l'économie et des finances rendu par M. Jean-Pierre Landau, en juillet 2018 (2), qui comprend notamment, en son annexe n° 3, une liste des principales ICO réalisées en France à la date de mai 2018. En outre, la commission des finances de l'Assemblée nationale a créé une mission sur les cryptomonnaies, dont le président est M. Éric Woerth et le rapporteur M. Pierre Person.

Le projet de loi dit « PACTE », précité, est aujourd'hui le principal véhicule juridique permettant d'établir ce cadre de régulation innovant. Actuellement en cours de discussion, l'adoption définitive de la loi devrait intervenir au printemps 2019. Les dispositions adoptées par l'Assemblée nationale en première lecture sont susceptibles d'évoluer dans le cours de la navette ; les développements à venir, qui présentent donc les dispositions du projet de loi à date, sont susceptibles de devenir caducs en fonction des débats parlementaires à venir.

Actuellement, et jusqu'à l'adoption de ce projet de loi, les offres de jetons au public ne font l'objet d'aucun régime juridique et, plus généralement, le sens juridique du jeton doit être explicité.

---

(1) Vos rapporteurs rappellent cependant que l'utilisation de cryptomonnaies comme les bitcoins ou les ethers ne sont nullement une garantie d'anonymat et de confidentialité, et que certaines cryptomonnaies comme les ripples reposent sur des blockchains *au fonctionnement bien moins décentralisé que la* blockchain *Bitcoin.*

(2) https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/184000433.pdf.

Le déroulement d'une ICO

L'opération se déroule généralement en trois étapes :

– l'annonce de l'ICO sur internet ;

– la publication de l'offre, à travers un document d'information ou *white paper*, décrivant notamment la nature du projet, les fonds nécessaires, le type de jetons et les droits associés. Ce *white paper* peut être considéré comme l'équivalent du prospectus ou document d'information synthétique prévus pour les levées de fonds « classiques » sur les marchés financiers ;

– la vente de jetons, en contrepartie d'un virement par l'investisseur de la monnaie demandée. Elle peut être précédée d'une phase de « vente privée » (vente restreinte) et de « prévente » (première vente à un prix avantageux).

La levée de fonds par cette voie permet donc de financer le développement d'un projet dès ses premiers stades auprès d'un public averti. Ce mode de financement est par nature international, rapide et sans intermédiaire financier. Ces caractères constituent à la fois l'intérêt des ICO mais sont aussi à la source de risques importants : arnaques, disparition des fonds récoltés ou de la personne à l'origine de l'opération, abus de marché ou encore financement du terrorisme.

Source : rapport parlementaire n° 1237 sur le projet de loi relatif à la croissance et à la transformation des entreprises (n° 1088), septembre 2018

Afin de compenser cette lacune normative, l'Autorité des marchés financiers a lancé en octobre 2017 une consultation publique de trois mois sur les ICO. 82 réponses de professionnels de la finance, de cabinets d'avocats, d'entrepreneurs « crypto » et de personnels académiques ont permis de conduire aux trois constats suivants :

– la grande diversité qualitative des documents d'information (*white papers*) distribués aux potentiels investisseurs et leur absence de contrôle ;

– la qualification juridique qui pourrait être appliquée aux jetons doit être précisée (titre financier, intermédiaire en bien divers, statut *sui generis*), notamment selon l'objet du jeton (jeton d'usage, jeton offrant de vrais droits politiques et de propriété, etc.) ;

– la nature de la régulation qui serait optimale à ce stade, entre un droit souple (charte de bonnes pratiques) et l'application aux ICO de la (lourde) réglementation applicable aux offres de titres au public.

En ce qui concerne ce dernier constat, qui intéresse plus particulièrement le présent développement, l'option d'un régime législatif propre aux ICO, nouveau et spécifique, de nature facultative, a été retenue par le Gouvernement à l'issue de la consultation. Les deux co-rapporteurs soutiennent aussi cette solution pragmatique tant les offres de jetons ne rentrent pas dans un cadre classique de régulation. Ce régime consisterait donc notamment en un **visa optionnel délivré par l'AMF sur les offres de jetons** s'adressant au public français. Les offres

n’ayant pas obtenu le visa ne seraient pas pour autant illicites et les offres ayant obtenu le visa demeureraient très risquées financièrement.

Le caractère optionnel du visa, que les émetteurs de jetons peuvent donc choisir de solliciter ou non, a comme principal intérêt de récompenser les offres « vertueuses », qui ne sont ni des escroqueries ni des arnaques manifestes, dans une logique de labellisation. Au contraire, un visa obligatoire aurait porté le risque d’entraver le développement des ICO en France en instaurant une régulation trop contraignante.

Le projet de loi « PACTE », à l’article 26, organise donc les modalités de ce visa facultatif, en précisant notamment qu’il portera sur le document d’information (*white paper*) établi par l’émetteur et destiné à donner les informations utiles au public sur l’émetteur, sur le projet et sur l’offre. Ce document devra présenter un « contenu exact, clair et non trompeur » et permettre « de comprendre les risques afférents à l’offre ». Le visa sera également conditionné à la constitution, par l’émetteur, d’une personne morale de droit français, établie ou immatriculée en France, ainsi qu’à la mise en place de « tout moyen permettant le suivi et la sauvegarde des actifs recueillis dans le cadre de l’offre », c’est-à-dire d’un mécanisme de séquestre des fonds récoltés, éventuellement sur une *blockchain*.

En outre, cet article permet plusieurs définitions juridiques : – celle de jeton con_u comme « tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits, pouvant être émis, inscrits, conservés ou transférés au moyen d’un dispositif d’enregistrement électronique partagé (1) permettant d’identifier, directement ou indirectement, le propriétaire dudit bien. » ; d’autre part, celle d’offre au public de jetons, qui « consiste à proposer au public, sous quelque forme que ce soit, de souscrire à ces jetons ».

Les débats parlementaires à l’Assemblée nationale ont permis d’aller beaucoup plus loin. En particulier, en séance publique, à l’initiative de plusieurs députés, un **régime relatif aux prestataires de services sur actifs numériques a été créé**. Parmi les nouveaux services et « métiers » encadrés par ce régime, figure notamment l’échange d’actifs numériques sur une place de marché, afin de favoriser l’essor d’un marché secondaire des jetons (2) et des cryptoactifs en général. La création d’un marché secondaire régulé permettra des échanges de cryptoactifs entre investisseurs de façon beaucoup plus sûre qu’aujourd’hui. Rappelons que de nombreux vols, escroqueries ou « piratages » de cryptoactifs ne s’appuyaient pas sur des failles des *blockchains* mais bien sûr les plateformes, pas toujours assez scrupuleuses ou sécurisées, qui permettent de négocier des cryptomonnaies. Pour cela, le projet de loi « PACTE » issu de l’Assemblée nationale instaure un environnement législatif robuste permettant le

(1) Ce qui est, aujourd’hui, la définition légale de la blockchain *en France.*

(2) En effet, les ICO forment un marché primaire : on ne peut obtenir de jetons que lors de leur première émission.

développement de nouveaux services financiers gravitant autour des marchés de jetons, transparents et protégés – notamment par la transposition de certaines dispositions de la quatrième directive révisée sur l'antiblanchiment et le financement du terrorisme [(1)] de mai 2018.

Les prestataires de ces services établis en France pourront solliciter un agrément optionnel. Dans la même logique vertueuse que le visa optionnel des ICO, il s'agit **d'attirer l'activité économique en France en proposant de la sécurité juridique** mais un degré limité de contrainte. La délivrance de l'agrément serait effectuée par l'AMF, en lien étroit avec l'Autorité de contrôle prudentiel et de résolution (ACPR), qui aura notamment la capacité d'émettre un avis conforme sur l'enregistrement auprès de l'AMF de certains de ces prestataires. Il s'agit, selon les dispositions actuelles du projet de loi, des :

– « prestataires de services de conservation pour le compte de tiers d'actifs numériques ou de clés cryptographiques privées, en vue de détenir, stocker et transférer des actifs numériques » (les plateformes de stockage d'actifs numériques mais aussi les entreprises de conservation de clés privées) ;

– « prestataires de services d'achat ou de vente d'actifs numériques en monnaie ayant cours légal » (les plateformes de conversion des cryptomonnaies en monnaie fiat).

Cet équilibre, selon vos rapporteurs, pourrait toutefois être revu. En effet, les services de vente de supports de clés privées ou les services de conservation de clés cryptographiques privées ne peuvent être assimilés à des services de dépôt d'actifs numériques. Si ces derniers peuvent légitimement entrer dans le giron de l'ACPR, le lien « bancaire » est beaucoup moins évident pour une entreprise comme Ledger, implantée en France, qui fabrique des clés permettant le stockage, non des cryptoactifs eux-mêmes, mais de la trace permettant de les lier avec le « porte-monnaie » de l'utilisateur.

Proposition n° 10 : Faire évoluer les équilibres du projet de loi « PACTE » pour que la régulation des services financiers et bancaires soit clairement distincte des services tiers en matière de cryptoactifs.

Enfin, la mise en place d'un cadre de régulation des ICO et des cryptoactifs ne relève pas uniquement de la compétence du législateur. Les dispositions législatives qui seront adoptées dans la future loi « PACTE » seront précisées et appliquées dans le cadre du Règlement général de l'AMF. En outre, le Gouvernement a annoncé avoir lancé des travaux, avec l'Autorité des normes comptables notamment, afin de définir d'ici fin 2018 un cadre comptable clair pour les émetteurs et les investisseurs.

(1) Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE.

b. Poser un cadre fiscal et bancaire ne dissuadant pas l'investissement

La régulation des activités économiques liées aux *blockchains* doit également intervenir sur les volets fiscaux et bancaires.

Dans le cadre du projet de loi « PACTE », précité, plusieurs amendements parlementaires ont été adoptés afin de mieux garantir aux émetteurs de jetons et plus généralement aux professionnels des *blockchains* qui manipulent des cryptoactifs, l'accès à un compte bancaire en France. Il s'agit de compléter toutes les mesures qui visent à favoriser une activité économique pérenne en France autour des *blockchains*. Vos rapporteurs insistent sur ce point : **sans droit au compte, donc sans ancrage bancaire et financier stable, il n'y a pas de sécurité suffisante pour prospérer** et ce sera nécessairement un pays étranger qui sera privilégié.

Le témoignage d'une start-up française confrontée au refus d'ouverture de compte bancaire : BCDiploma

« Je me permets de vous écrire pour vous présenter la situation de notre start-up Edtech & Blockchain BCDiploma (Blockchain Certified Data SAS) et lancer une proposition constructive d'action commune.

« BCDiploma propose aux établissements d'enseignement supérieur une nouvelle technologie pour sécuriser et partager des diplômes et des données sur la blockchain Ethereum. Les fonds pour développer et déployer l'application ont été récoltés au cours d'une offre de jetons (« ICO »). L'opération s'est déroulée dans la plus grande transparence vis-à-vis de l'AMF, de Tracfin et des investisseurs, et a permis de récolter 1800 ETH (soit l'équivalent d'environ 1,50 M€) au 19 janvier 2018. C'est la 4e ICO française réussie à ce jour.

« Notre objectif est d'inscrire nos activités dans l'économie française et nous y travaillons activement. Nous sommes actuellement incubés à Station F-Chain Accelerator et nos premiers clients sont l'IAE de Nantes et Bärchen. Nous sommes membres de Systematic, et Bpifrance nous soutient à travers son programme Émergence.

« Après quatre mois de démarches intensives, force est de constater :

• qu'il nous est impossible d'ouvrir un compte bancaire dans un établissement bancaire de l'Espace économique européen ;

• que le remboursement de la TVA par le SIE est bloqué depuis la création de l'entreprise, ce blocage provenant de la présence de factures ayant donné lieu à un règlement en cryptoactifs ;

• l'absence de vision claire du point de vue des schémas comptables et fiscaux est source d'insécurité pré- et post-ICO, au regard du risque que les règles encore attendues à ce jour remettent en cause les choix effectués en amont.

« Nous affirmons des convictions fortes : il doit être possible, en France, par l'expérimentation et l'action commune de l'administration, des acteurs bancaires et des entrepreneurs de construire des nouveaux schémas économiques. La France doit montrer la voie pour être une terre d'accueil des projets entrepreneuriaux en cryptoactifs, au risque de voir les ICOs et activités associées se délocaliser durablement dans d'autres pays notamment limitrophes. »

Aujourd'hui, les entrepreneurs français éprouvent donc des difficultés à développer leur activité sereinement parce qu'ils ont besoin d'un cadre juridique suffisamment stable. Si le Gouvernement et les différentes autorités publiques concernées ont montré leur ouverture d'esprit pour encourager cet écosystème, force est de constater que **les institutions bancaires demeurent circonspectes, sinon frileuses, pour accompagner les acteurs de ce nouvel écosystème** – ne serait-ce que pour ouvrir un compte de dépôt.

Cela s'explique par le droit de l'Union européenne, très contraignant en matière de lutte contre le blanchiment et le financement d'activités criminelles, et au regard duquel les banques ne souhaitent pas prendre de risque d'exposition trop important. Cela s'explique également par l'opacité trop fréquemment associée aux cryptoactifs, à leur durabilité, leur volatilité et donc la valeur réelle qu'ils véhiculent. Enfin, il faut également mentionner l'extraterritorialité de la loi américaine, applicable dès que des transactions ont un lien avec le dollar, qui peut avoir des conséquences importantes pour les établissements de crédit. Une des raisons pour laquelle la Suisse a pu prendre de l'avance en matière de développement bancaire de l'écosystème des *blockchains* tient au fait qu'une banque publique suisse, la Banque cantonale neuchâteloise (BCN), non tenue par les mêmes engagements internationaux que les grandes banques françaises vis-à-vis des États-Unis, accepte plus volontiers l'ouverture de comptes bancaires aux acteurs de cet écosystème.

Les dispositions adoptées en première lecture à l'Assemblée nationale dans le cadre du projet de loi « PACTE » permettent un grand pas en avant en la matière :

– un **droit au compte** a été explicitement ouvert pour les émetteurs de jetons ayant bénéficié du visa de l'AMF (voir ci-dessus) ainsi que pour les start-ups souhaitant développer des services de *blockchains*, dans la mesure où ils respectent et mettent en place des diligences en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ;

– l'**accès aux services bancaires** a également été acquis pour les plateformes d'échanges et pour les prestataires permettant l'investissement en actifs numériques, agréés par l'AMF et par l'ACPR (voir également ci-dessus) ;

– un **principe d'ouverture de compte en dernier ressort**, qui confie à la Caisse des dépôts et consignations – la navette parlementaire pourrait également

conduire à privilégier la Banque de France ou la Banque postale – la mission de garantir le droit au compte bancaire aux acteurs (ayant bénéficié du visa de l'AMF) manipulant des cryptoactifs qui n'auraient pas vu aboutir leurs démarches auprès d'autres banques.

Proposition n° 11 : Garantir un droit au compte en dernier ressort, assuré par la Caisse des dépôts et consignations, par la Banque de France ou par la Banque postale, pour les acteurs ayant bénéficié du visa de l'AMF.

Vos rapporteurs estiment que ce cadre bancaire, adossé au cadre financier des ICO présenté auparavant, permettra d'améliorer sensiblement l'attractivité de la France parmi les entrepreneurs des *blockchains*. Il convient cependant de compléter le tableau par une évolution du cadre fiscal.

Ainsi, dans le cadre de l'examen en séance publique de la seconde partie du projet de loi de finances pour 2019, l'Assemblée nationale a adopté un amendement du Gouvernement, modifié par les parlementaires, qui définit un **régime fiscal applicable aux cryptoactifs**.

Sans régime spécifique prévu jusqu'alors, trois régimes ont pu être appliqués par l'administration fiscale pour les produits tirés de la cession de cryptomonnaies par des particuliers. Ainsi, en 2014, le bulletin officiel des finances publiques (BOFiP) a créé une doctrine selon laquelle le profit tiré des plus-values de cession de cryptomonnaies (le bitcoin seulement, à l'époque) devait être considéré comme un bénéfice non commercial (BNC), alors soumis au barème progressif de l'impôt sur le revenu, lorsque la cession est occasionnelle, ou comme un bénéfice industriel et commercial (BIC) lorsque les cessions sont le produit d'une activité habituelle.

Saisi par plusieurs requérants, qui estimaient que ces plus-values devraient être imposées dans la catégorie des biens meubles, le Conseil d'État, dans une décision du 26 avril 2018, a prononcé l'annulation partielle de cette instruction fiscale. Les bitcoins ont alors bien le caractère de biens meubles incorporels, sauf exceptions qui maintiennent l'application de la doctrine fiscale originelle.

Pour clarifier ce cadre fiscal peu lisible, le projet de loi de finances pour 2019, issu de l'Assemblée nationale en première lecture, crée un régime fiscal adapté à l'imposition, à l'impôt sur le revenu et aux prélèvements sociaux, des gains réalisés à titre occasionnel par les particuliers lors de la cession de cryptoactifs. Pour tenir compte des nombreuses microtransactions réalisées en cryptoactifs, l'imposition ne porterait que sur la plus-value « globale », nette de tous les échanges opérés au cours de l'année, **du moment que cette plus-value s'obtient par la cession de cryptoactifs en échange de monnaies ayant cours légal** (*fiat*).

L'assiette de l'imposition sera une part de la plus-value latente globale sur l'ensemble des cryptoactifs détenus (c'est-à-dire celle qu'il réaliserait s'il vendait tout son portefeuille). Le **taux sera celui de 30 %,** pour 12,8 % au titre de l'impôt

sur le revenu et pour 17,2 % au titre des prélèvements sociaux. Ce taux a l'avantage de se situer au niveau de l'imposition classique de la fiscalité du capital : le prélèvement forfaitaire unique (PFU).

En outre, afin d'assurer la diligence nécessaire à la lutte contre le financement d'activités criminelles, l'administration fiscale aura la faculté d'obtenir une **déclaration des détenteurs de comptes de cryptoactifs**, même lorsque ces comptes sont détenus sur des plateformes de droit étranger. Une amende pourra être appliquée en cas de non-respect de cette obligation déclarative.

L'entrée en vigueur de ce nouveau régime fiscal est prévue au 1er janvier 2019 et celle de l'obligation déclarative au premier janvier 2020.

Enfin, trois sous-amendements d'origine parlementaire ont complété ce dispositif :

– un amendement de M. Éric Woerth, président de la commission des finances, reprend la définition des actifs numériques, retenue dans le projet de loi PACTE, afin qu'elle puisse entrer en vigueur début 2019 (PACTE ne sera promulguée que plus tard) (1) ;

– un amendement de M. Éric Bothorel, qui crée un abattement annuel de 305 euros sur le montant des cessions afin, d'une part, d'exempter d'imposition cette somme mineure et, d'autre part, d'éviter aux contribuables de les soumettre à l'obligation déclarative (2) ;

– enfin, un sous-amendement de votre rapporteure, Mme Laure de La Raudière, qui intègre au calcul du prix total d'acquisition du portefeuille de cryptoactifs, la valeur des services fournis en contrepartie de ces cryptoactifs. Il faut en effet tenir compte du fait que **la rémunération de services en cryptoactifs a vocation à se développer** grâce aux nouveaux cas d'usage des *blockchains* décrits dans le présent rapport (3).

---

(1) Cf. amendement n° II-2548 portant article additionnel après l'article 51 du projet de loi de finances pour 2019.

(2) Cf. sous-amendement n° II-2565 présenté par M. Bothorel, Mme Faure-Muntian et Mme Hennion à l'amendement n° 2523 du Gouvernement portant article additionnel après l'article 51du projet de loi de finances pour 2019.

(3) Cf. sous-amendement n° II-2557 présenté par Mme Laure de La Raudière à l'amendement n° 2523 du Gouvernement portant article additionnel après l'article 51du projet de loi de finances pour 2019.

Proposition n° 12 : Améliorer encore le dispositif fiscal proposé dans le PLF pour 2019, notamment en ne fiscalisant les plus-values liées aux crypto-échanges qu'au moment où celles-ci sont encaissées sur un compte bancaire traditionnel.

c. Organiser des investissements publics pérennes dans les blockchains

Afin de donner à l'écosystème des *blockchains* en France toutes les chances de prendre les devants, **les pouvoirs publics ont une responsabilité** qui n'est pas uniquement celle de proposer un cadre juridique, bancaire et fiscal attractif. Les soutiens budgétaires publics doivent également pouvoir cibler cet écosystème en particulier.

Dans un développement à venir, vos rapporteurs présenteront dans quelle mesure les administrations publiques peuvent, dans le cadre de la modernisation des services publics, investir dans les *blockchains*.

Ici, il faut rappeler que des outils particulièrement efficaces, comme les programmes des investissements d'avenir (PIA) ainsi que le Grand plan d'investissement (GPI) permettent aux opérateurs que sont Bpifrance ou encore la Caisse des dépôts et consignations d'investir durablement dans les entreprises des *blockchains*. Encore faut-il les identifier et que ce secteur soit jugé suffisamment stratégique.

La Caisse des dépôts et consignations se mobilise sur les *blockchains*

Trois modalités d'interventions ont été déployées par la Caisse sur le thème des *blockchains* dans les derniers mois :

– la BChain, un laboratoire d'innovation consacré aux usages dans les secteurs bancaire, de la finance et de l'assurance, regroupant 31 partenaires (grands groupes et start-ups) et les régulateurs publics concernés autour de cas d'usages tels que l'identité numérique et les procédures de connaissance du client (*know your customer* – KYC), l'assurance-décès ou encore la gestion d'un fonds d'investissement en cryptomonnaies.

– BloCDChain, un programme d'actions au sein même du groupe CDC, développant des expérimentations sur les obligations vertes (*green bonds*), sur les pactes d'actionnaires ou sur le développement d'un pass multiservices avec la filiale Transdev ;

– des partenariats *ad hoc* au service de nos métiers et du développement de l'écosystème, notamment en recherche et développement, par le financement de chaires ou de thèses : SystemX, institut Louis Bachelier et Toulouse School of Economics (TSE).

De même, plus en amont, les financements des équipes de recherche qui se créent autour des *blockchains* doivent être stimulés, par exemple par les crédits des pôles de compétitivité ou ceux de l'Agence nationale de la recherche (ANR).

La création du Fonds pour l'innovation et pour l'industrie, dans le cadre du projet de loi « PACTE », précité, pourrait aussi être utilement mis à

contribution pour prendre des participations dans des start-ups prometteuses des *blockchains*. Cela serait d'ailleurs compatible avec la politique d'investissement de l'État dans les principaux secteurs d'innovation stratégique : les solutions liées aux *blockchains* ont des convergences réelles avec l'économie de la donnée (notamment le *big data*), l'internet des objets ou l'intelligence artificielle.

B. FIXER UN CADRE CONCILIANT LE DÉVELOPPEMENT DES *BLOCKCHAINS* ET LA PRÉSERVATION D'INTÉRÊTS PUBLICS IDENTIFIÉS

L'objectif découle très naturellement du constat – partagé par l'ensemble des personnes auditionnées – que **l'incertitude peut freiner les initiatives s'agissant d'une technologie aussi potentiellement disruptive que celles des « *blockchains* ».** Pour développer des usages allant au-delà de l'optimisation de processus existants et inscrire leurs investissements dans la durée, les porteurs de projets doivent pouvoir disposer de ressources humaines et matérielles sur le territoire national. Mais il leur importe également de pouvoir jouir d'une certaine sécurité juridique.

Du point de vue de la mission, **il appartient dès lors au Parlement de dire le droit, sans attendre que la justice soit saisie de litiges la conduisant à forger une jurisprudence. Il s'agit autant de donner une visibilité aux opérateurs économiques – en distinguant le licite de l'illicite – que de protéger les usagers (particuliers, entreprises, secteurs bancaires et financiers) des aléas d'un procédé innovant**.

Dans cette optique, fixer un cadre conciliant le développement des *blockchains* et préservation d'intérêts publics identifiés comporte deux exigences : d'une part, adapter le droit national, soit – le cas échéant – par l'expérimentation, soit par des mesures ponctuelles ; d'autre part, engager l'Union européenne dans une action résolue et indispensable à la préservation de notre souveraineté.

1. Laisser une place à l'expérimentation et procéder à des adaptations ponctuelles au plan national ?

Ainsi que le montrent les exemples étrangers, il existe en effet deux manières d'assurer le développement d'une innovation telle que celle des « *blockchains* » dans un État de droit.

La première consiste à laisser aux acteurs de l'écosystème – ainsi qu'aux usagers – une certaine latitude dans l'offre et l'utilisation de produits et de services tirés de l'utilisation des protocoles. L'expérimentation donne lieu à la réalisation de tests dans un environnement réglementaire favorable et peut même conduire à suspendre l'application de certaines normes. C'est l'approche dite du « bac à sable », dont le terme reprend l'idée mise en œuvre au Royaume-Uni dans le domaine des *Fintech*.

Les pouvoirs publics peuvent également vouloir établir un cadre juridique global, avec pour ambition d'appréhender l'ensemble des problématiques et usages d'une nouvelle technologie. C'est le choix opéré aujourd'hui par certains États à l'exemple de Malte.

La mission n'entend pas ici trancher de manière définitive et catégorique entre les avantages supposés de ces deux modes de régulation. Toutefois, **les inconvénients d'un environnement juridiquement incertain l'inclinent plutôt à juger nécessaire un encadrement du développement des *blockchains* par l'application de normes de droit positif.**

Cette position la conduit à dresser un état des lieux plutôt nuancé – voire optimiste – sur la capacité du droit national à appréhender pleinement les enjeux qui entourent les usages possibles de cette technologie.

a. Un droit déjà favorable à l'usage des blockchains ?

La question peut se poser dès lors que **tout en évoquant des difficultés dans l'application de certaines diligences ou de certaines catégories du droit, nombre des personnes auditionnées ont appelé à ne pas brider l'innovation et à tirer les enseignements de l'usage des « *blockchains* » avant de légiférer.** En soi, ce message présente sur le fond des similitudes avec les recommandations de France Stratégie. Ses travaux se concluent en effet par la recommandation d'« établir des régulations de base pour contrôler les usages frauduleux des cryptomonnaies » et « de mettre en place des règles minimales efficaces tout en conservant les caractéristiques de simplicité des dispositif actuels ».

● D'une part, le droit en vigueur comporte déjà certaines notions susceptibles d'autoriser l'utilisation des protocoles.

L**a loi en fournit une définition – et donc une reconnaissance juridique – depuis l'ordonnance du 28 avril 2016** [(1)]. L'article L. 223-12 du code monétaire et financier vise ainsi « un dispositif d'enregistrement électronique partagé permettant l'authentification [des] opérations d'émission et de cession de minibons ». **L'ordonnance n° 2017-1674 du 8 décembre 2017** [(2)] **consacre la possibilité légale d'inscrire des titres financiers sur ce type de dispositif**. À ce jour, il reste toutefois à publier le décret en Conseil d'État prévu à l'article L. 211-3 du code monétaire et financier, ce texte étant censé définir les conditions dans lesquelles des titres financiers pouvaient être échangés par ce moyen.

● D'autre part, il ressort de l'analyse convergente des représentants du ministère de la justice et du Conseil d'État que le droit français semble en mesure d'appréhender un certain nombre de situation créées par l'usage des « *blockchains* ». La loi ne paraît pas devoir faire obstacle pour l'essentiel au

(1) Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.

(2) Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.

recours à cette technologie et, à l'inverse, ses grands principes directeurs paraissent applicables à son usage.

– il en va ainsi en ce qui concerne l'application des normes relatives au traitement de données, au moins d'un point de vue juridique. D'après les éléments communiqués par le Bureau du droit des obligations, en tant que dispositifs d'enregistrement et de transmission électronique partagés, les protocoles doivent respecter les mêmes conditions de licéité que tout traitement de données [(1)].

Lorsque ce traitement porte sur des données se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement (cas où un pseudonyme est utilisé) [(2)], il devra notamment respecter les limites fixées par ces textes, ainsi que par l'article 8 de la Charte des droits fondamentaux de l'Union européenne. L'un des enjeux sera donc de préserver les droits fondamentaux qui s'appliquent par essence de façon neutre technologiquement.

– **S'agissant des *smart contracts***, les premières analyses du ministère de la Justice donnent à penser que **l'essentiel des principes du droit des contrats pourrait régir les obligations contractées dans le cadre de la mise en œuvre d'un protocole fondé sur la technologie des *blockchains*.**

Rappelons que les *smart contracts* constituent avant tout des programmes informatiques censés assurer l'exécution immuable d'engagements conventionnels préalables [(3)].

En cas de litige, **le juge devra examiner les éventuels manquements à ce contrat en application des règles du droit commun de la responsabilité contractuelle**. Il convient de rappeler ici que la preuve des obligations reste libre entre commerçants et pour les actes sous signatures privées – ce qui exclut toutes les matières pour lesquelles un acte authentique est requis, notamment les ventes immobilières – dont le montant est inférieur à 1 500 euros. Pour les contrats dont l'enjeu excède ce montant, la production d'un écrit est certes nécessaire mais suivant les principes du code civil, l'écrit électronique revêt une même valeur qu'un écrit sur support papier.

À défaut de convention définissant en amont la responsabilité et les obligations de chacun, il appartiendra au juge, après observations des parties, de trancher leur éventuel désaccord sur la qualification de l'opération en cause (vente, prestation de services, prêt, gage, etc.).

---

(1) D'après l'analyse du ministère de la justice, l'« enregistrement », quelle que soit la technologie utilisée, est un « traitement » de données au sens de l'article 4(2) du règlement (UE) n° 2016/679 et de l'article 3(2) de la directive (UE) 2016/680 du 27 avril 2016.

(2) Au sens de l'article 4(1) du règlement (UE) n° 2016/679 ou 3(1) de la directive (UE) n° 2016/680.

(3) Il peut cependant leur être adossé un contrat électronique, en particulier des conditions générales d'utilisation que les utilisateurs seraient appelés à accepter avant de pouvoir intervenir sur une blockchain *mais ce cas de figure correspond à l'hypothèse d'une* blockchain *privée.*

D’après l’analyse du ministère de la justice, **les clauses du contrat trouveraient à s’appliquer de la même manière que s’il s’agissait d’une transaction passée physiquement entre ces intervenants.** En particulier, la portée des clauses limitatives de responsabilité ou attributives de juridiction, ainsi que le régime juridique de l’article 1171 du code civil applicable aux contrats d’adhésion, s’agissant de la portée des clauses qui créent un déséquilibre significatif entre les droits et obligations des parties au contrat, seraient appréciées comme en droit commun.

S’agissant en dernier lieu de **la désignation conventionnelle du droit applicable,** le ministère de la justice estime que sa portée dépendrait de la matière concernée. À titre d’exemple, l’application du droit français ne pourrait être éludée dans les conventions portant sur des biens immobiliers ou sur l’état ou la capacité des personnes [(1)].**Les règles de conflit des conventions bilatérales ou multilatérales de droit international privé auraient également vocation à s’appliquer.**

L’ensemble de ces considérations portent le ministère de la Justice à estimer qu’il n’existe pas de vide juridique dans l’application du droit des contrats, l’enjeu résidant davantage dans la qualification juridique des opérations (vente, prestation de service, prêt, etc.).

Ce raisonnement par analogie vaut-il pour l’ensemble des usages permis par les protocoles « chanes de bloc » ? De fait, la pseudonymisation des acteurs du réseau dans le cadre d’une *blockchain* ouverte laisse entier le problème de l’identification des détenteurs de droits et d’obligations.

Dès lors, le fonctionnement des protocoles exige-t-il un encadrement spécifique et l’édiction de nouvelles règles de droit ? Faut-il réguler ? Sur cette question, il existe à l’évidence un clivage au sein de la doctrine.

Certains juristes, à l’instar de M. Guy Canivet, ancien Premier président de la Cour de cassation, estiment que la question n’est pas de réguler les *blockchains* en tant que technologie mais de savoir s’il est nécessaire et utile de réguler leur application à une activité quelconque. Dans cette optique, la nécessité de réguler ou non les activités s’appuyant sur ce procédé dépendrait ainsi d’un certain nombre de critères à examiner tels que l’application d’une réglementation, l’intervention d’une profession juridique réglementée ou l’impact sur d’autres acteurs du secteur concerné.

D’autres considèrent néanmoins que la technologie elle-même peut comporter des failles en termes de sécurité – du point de vue de la protection des données personnelles, du recours au pseudonymat ou de la localisation des mineurs contribuant au fonctionnement des protocoles. Ils soulignent que la *blockchain* crée certes de **nouvelles opportunités mais aussi** de **nouveaux**

(1) En application de l’article 3 du code civil.

risques – par exemple, au regard de la détermination du droit applicable et de la juridiction compétente ou de la charge de la preuve.

Dans le cadre de ses travaux, la mission n'a pas recueilli d'éléments lui permettant d'identifier de manière formelle des dispositions normatives empêchant l'usage de la technologie. **En revanche, certaines des personnes auditionnées ont attiré son attention sur l'existence de lacunes ou d'incertitudes en l'état du droit.** Celles-ci portent notamment sur les conditions d'échanges des titres financiers prévues par l'ordonnance précitée du 8 décembre 2017, le traitement fiscal de certains usages de la technologie tels que les ICO ou encore, sur l'inscription en comptabilité des cryptoactifs et sur les conditions d'utilisation de l'identité numérique.

Ainsi que l'a montré la consultation publique organisée par la direction générale du Trésor à propos des réformes législatives et réglementaires relatives à l'usage des *blockchains***, la logique qui sous-tend aujourd'hui l'intervention de l'État consiste à accompagner l'émergence des acteurs du secteur et de déterminer les éventuels « hiatus » entre de nouveaux usages et le cadre en vigueur.**

La mission considère que cette méthode serait de nature à concilier liberté des acteurs, maintien de la capacité d'innovation et protection des intérêts publics et privés. Dans le cadre de l'examen du projet de loi PACTE et du projet de loi de finances pour 2019, les pouvoirs publics travaillent actuellement à l'édification d'un régime fiscal susceptible de répondre aux enjeux spécifiques de la fiscalité sur les cryptoactifs, des investissements ou des cessions de titres dans le secteur des *blockchains* [(1)]. **Il importe de poursuivre cette démarche par une revue générale des normes susceptibles de conditionner l'essor des protocoles afin de permettre au législateur de poursuivre l'adaptation de notre droit et de garantir sa stricte neutralité au plan technologique.**

Proposition n° 13 : Mener une revue générale des normes susceptibles de conditionner l'essor de la technologie des *blockchains*.

b. Des éclaircissements à apporter pour conforter la valeur probatoire des blockchains et le régime de responsabilité

À l'évidence, ces enjeux ne présentent une réelle acuité que dans le cas des *blockchains* ouvertes. De fait, les *blockchains* privatives ou de consortium associent un nombre restreint de membres qui, en conséquence, sont plus aisément identifiables ; elles comportent, en pratique, une entité centrale susceptible de contrôler les accès et l'application des règles en vigueur sur le réseau.

● Fréquemment évoquée par les personnes auditionnées par la mission**, la valeur probatoire des éléments inscrits dans *blockchains* soulève la question**

(1) Cf. supra pp. 74-78.

des conditions d'application des règles en matière de preuve électronique et de signature numérique.

En l'occurrence, dans le cadre fixé par le règlement européen n 910/2014 du 23 juillet 2014 (dit « règlement eIDAS ») [(1)], le droit français repose sur un système centralisé de confiance présumée et la non-discrimination de l'écrit électronique. Cela signifie en pratique que la signature électronique ne peut être refusée en tant que moyen de preuve en justice au motif qu'elle ne se présente pas sous format papier ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée définie par le règlement européen. En revanche, seule la « signature électronique qualifiée » produit, de manière irréfragable, des effets équivalents à ceux qui s'attachent à une signature manuscrite.

Ainsi, suivant le principe réaffirmé à l'article 1er du décret n° 2017-1416 du 28 septembre 2017 [(2)], « la fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée ». De surcroît, l'article 1366 du code civil conditionne la force probante d'un écrit électronique à l'identification de la personne dont il émane, ainsi qu'à conservation « dans des conditions de nature à en assurer l'intégrité ». Pour sa part, l'article 1367 du même code exige « un procédé fiable d'identification » garantissant un lien entre l'acte et son auteur. Il établit une présomption simple, qui plus est sous réserve que « l'identité du signataire [soit] assurée et l'intégrité de l'acte garantie ».

Les différentes signatures reconnues par le « règlement eIDAS »

– La signature électronique simple : la notion désigne des données sous forme électronique jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer ;

– La signature électronique avancée (SEA) : elle a pour caractéristiques : d'être liée au signataire de manière univoque ; de permettre son identification ; d'avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; enfin, cette signature est liée aux données qui lui sont associées, de telle sorte que toute modification ultérieure de ces données soit détectable (article 26) ;

– La signature électronique qualifiée (SEQ) : elle doit satisfaire les critères précités de la SEA et doit en outre avoir été créée à l'aide d'un dispositif de création de signature électronique qualifié (art. 29) et reposer sur un certificat qualifié de signature électronique (art. 28).

Par la traçabilité garantie par la fonction d'horodatage et l'immuabilité des transactions, les protocoles *blockchains* pourraient répondre en partie à ces spécifications. Toutefois, en l'état du droit, **aucun texte ne détermine la portée**

(1) Règlement européen n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

(2) Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique.

juridique des éléments inscrits sur un protocole technique. **Dès lors qu'il ne fait pas partie des moyens de preuve actuellement reconnus au plan juridique, il appartient au juge de déterminer leur valeur probatoire, au vu des circonstances de l'espèce** [(1)]**.**

En outre, **le fonctionnement des protocoles contrevient à plusieurs exigences fixées par le droit découlant du « règlement eIDAS »** :

– un dispositif permettant la **mise en œuvre de processus de vérification contraignants** ;

– **l'identification du signataire** – condition qui ne peut être remplie par les *blockchains* ouvertes dont les membres utilisent un pseudonyme ;

– **le recours obligatoire à un « *prestataire de services de confiance qualifié* »**, tant pour générer ou gérer les données de création de signature électronique pour le compte d'un signataire, que pour l'horodatage des données [(2)] : suivant les observations du ministère de la Justice, les dispositifs de signature électronique à distance (*server signing*) ou signature électronique embarquée ne répondent pas à la définition des services de confiance qualifiés au sens du règlement eIDAS, faute de tiers de confiance.

Dès lors que la loi nationale transpose les principes fixés par le droit européen, **conférer une valeur probante certaine aux informations inscrites au sein des *blockchains* suppose une modification du « règlement eIDAS ».** Du point de vue des rapporteurs, cette reconnaissance constitue une nécessité pour l'essor de la technologie.

Toutefois, ainsi que le remarque le ministère de la justice dans ses réponses au questionnaire adressé par la mission, **la certification des protocoles pourrait sans doute permettre d'atteindre un objectif comparable** en ce qu'elle pourrait renforcer les garanties autour de l'intangibilité des données inscrites. Même si elle revient à introduire l'intervention d'un tiers de confiance, elle n'en parait pas moins de nature à conforter la confiance dans ce procédé innovant.

Proposition n° 14 : Envisager une adaptation du régime applicable en matière de preuve électronique et de signature numérique par une révision du règlement du règlement européen n° 910/2014 du 23 juillet 2014 (dit « règlement eIDAS »).

Appuyer les initiatives tendant à favoriser l'établissement de standards européens ou internationaux pour le fonctionnement des *blockchains*.

---

(1) Dans le cadre de l'application du « règlement eIDAS », le niveau de fiabilité de la signature électronique reste sans incidence directe sur la preuve et la validité de la signature, qui peuvent être démontrées par tous moyens.

(2) En application de l'article 41 du « règlement eIDAS », les « horodatages électroniques qualifiés » bénéficient « d'une présomption d'exactitude de la date et de l'heure qu'ils indiquent et de l'intégrité des données auxquelles se rapportent cette date et cette heure ».

● Au regard de ce dernier objectif, **l'établissement d'un régime de responsabilité paraît soulever des questions autrement plus complexes, notamment dans le cas des *blockchains* ouvertes**. Dans le cadre d'un protocole fondé sur la distribution du consensus, la décentralisation des échanges et sur un code *open source*, **quel(s) acteur(s) devrai(en)t effectivement assumer la réparation d'un préjudice ? Pourrait-on s'en remettre à la théorie du cas de force majeure ?**

Pour le ministère de la justice, les problématiques susceptibles d'apparaitre à raison de l'usage croissant des *blockchains* pourraient vraisemblablement être appréhendées de manière assez satisfaisante par l'application du droit commun de la responsabilité, en particulier contractuelle.

Dans cette optique, il appartiendrait aux parties ou au juge d'examiner, dans chaque cas d'espèce, la constitution, l'organisation et la gouvernance du protocole en cause. Il s'agirait d'analyser la nature des relations contractuelles entre les différents acteurs et le rôle de chacun, afin d'identifier le fait générateur de responsabilité et de déterminer son imputabilité à une ou plusieurs personnes déterminées.

Toutefois, ainsi que le relève le ministère de la justice lui-même dans ses réponses à sa mission, **le recours au pseudonyme et la décentralisation d'une *blockchain* ouverte constituent autant d'obstacles à l'identification éventuelle du ou des auteurs d'un dommage.**

Les éléments d'analyse recueillis par les rapporteurs ne permettent pas de dégager une solution satisfaisante. Faut-il mettre en cause le créateur du protocole, le concepteur de l'application utilisée ou l'ensemble de la communauté des membres – ce qui apparaît en pratique impossible, ainsi que le rappelle l'OPECST ? Sur ce point, les avis divergent, certaines personnes auditionnées renvoyant aux conditions générales d'utilisation que les utilisateurs seraient appelés à souscrire dans le cadre d'un contrat électronique avant de pouvoir devenir membre d'un réseau.

Dès lors, **la mission juge indispensable que les pouvoirs publics engagent une réflexion sur l'établissement d'un régime de responsabilité adapté aux différents usages des *blockchains*. Dans l'esprit de ses membres, cette proposition ne préjuge pas de la nécessité d'édicter des règles spécifiques mettant en cause l'unicité du droit en vigueur**. Elle suppose seulement un travail d'évaluation des principes et normes applicables, travail qui pourrait être mené par exemple dans le cadre du « groupe à compétences transversales à l'intérieur de l'État » qu'elle appelle de ses vœux.

Proposition n° 15 : Engager une réflexion au niveau européen et français permettant l'établissement d'un régime de responsabilité permettant d'appréhender les usages des protocoles fondés sur la technologie des *blockchains*.

Du point de vue de la mission, créer un cadre propice à l'essor de cette technologie suppose également de garantir autant que possible la parfaite information du consommateur.

Les articles L. 112-1 à L. 112-8 du code de la consommation consacrent aujourd'hui, à la charge de tout vendeur de produit ou de tout prestataire de services, des obligations générales en ce qui concerne l'information sur les prix et les conditions de vente. La « directive sur le commerce électronique » fixe quant à elle des prescriptions plus spécifiques quant aux informations requises pour l'usage des services de la « société de l'information » – concept dont le droit européen donne une définition relativement large [(1)].

Dans le cadre de ses travaux, la mission n'a recueilli aucun indice d'une quelconque incompatibilité entre les exigences du cadre juridique en vigueur et les usages permis par la blockchain. Mais à l'inverse, rien ne garantit la possibilité d'une application des normes par analogie. Dans une situation de flou juridique quant aux garanties sur les produits ou services fournis et aux recours possibles au juge, quelle pourrait être la réaction des consommateurs ?

Devant cette question essentielle, il apparaît à tout le moins nécessaire de préciser les notions du droit de la consommation et du commerce électronique aux spécificités des relations nouées dans l'usage des services et produits fournis par cette technologie.

Proposition n° 16 : Examiner la nécessité d'une adaptation des normes européennes et nationales du droit de la consommation au regard des usages permis par les protocoles fondés sur la technologie des *blockchains*.

c. Une question particulière à ne pas négliger : la protection des données personnelles

Le régime de protection des données personnelles procède aujourd'hui du règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 [(2)] (dit « règlement RGPD), ainsi que de la loi n° 2018-493 du

(1) Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»).

(2) Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Le RGPD est complété par la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

20 juin 2018 relative à la protection des données personnelles. Entré en vigueur le 25 mai 2018, le RGPD consacre un certain nombre de principes et d'exigences essentielles :

– la détermination du responsable de traitement et de son sous-traitant ;

– l'exercice du droit à la rectification et du droit à l'effacement des données personnelles ;

– l'encadrement des échanges transfrontaliers de données : l'article 44 du RGPD dispose en l'occurrence que « les données personnelles ne peuvent être envoyées vers des pays tiers que s'ils garantissent un niveau adéquat de protection des données des individus ou si des outils spécifiques sont en place et que la personne a expressément consenti à ce transfert » ;

– l'exercice du droit à la notification de violation des données ;

– le respect de l'obligation d'apporter la preuve du consentement ;

– le respect du principe de « *privacy by design* » : en application de l'article 25 du RGPD, le responsable de traitement devra se conformer au principe de protection des données tant dans la détermination des moyens du traitement que dans la mise en œuvre du traitement lui-même.

Au sens du règlement, constituent des données personnelles relevant de son champ d'application toute donnée traitée susceptible de permettre l'identification directe ou indirecte d'une personne physique. On notera en outre que le règlement modifie la nature du contrôle exercé par les autorités nationales (1) afin de garantir le respect par les entreprises de la protection des données personnelles : en effet, il établit un système de contrôle *a posteriori*, fondé sur l'appréciation par le responsable de traitement des risques causés par la mise en œuvre de ce dernier (2).

Les éléments d'analyse développés devant la mission par les représentants de la Commission nationale de l'informatique et des libertés (CNIL) (3) donnent à penser qu**'il n'existe pas d'incompatibilité irrémédiable entre les principes du**

---

(1) Au-delà des pouvoirs de contrôle a posteriori, *la loi n° 2018-493 du 20 juin 2018 confie ainsi à la Commission nationale de l'Informatique et des Libertés – désignée autorité de contrôle nationale au sens et pour l'application du RGPD –, la mission de favoriser un environnement juridique sécurisé par l'utilisation d'instruments « de droit souple », tels que l'établissement de lignes directrices, la publication de recommandations et de référentiels.*

(2) Dans ce cadre, la contrepartie de la disparition des démarches administratives préalables au traitement de données à caractère personnel réside dans la pleine responsabilité des personnes et des sous-traitants chargés du traitement de données personnelles. Ainsi, en application des articles 37 à 39 du RGPD, il incombe au délégué à la protection des données désigné au sein d'une entreprise de tenir un registre des traitements, à la disposition de la CNIL.

(3) Cf. CNIL, « Blockchain *– Premiers éléments d'analyse de la CNIL », septembre 2018 (https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles).*

RGPD – qui présenterait une certaine « plasticité » – et la technologie des *blockchains*.

D'une part, **les catégories sur lesquelles repose le régime de protection des données personnelles trouveraient à s'appliquer**.

Il en va ainsi de la notion même de données personnelles. Même si tous les projets reposant sur l'usage des *blockchains* n'impliquent pas nécessairement un traitement, la CNIL constate qu'en pratique, de nombreuses utilisations de cette technologie nécessitent la manipulation de ces données, tant au regard du contenu que des informations liées aux participants.

Dans cette optique, la CNIL estime qu'un dispositif fondé sur ces protocoles peut contenir **deux catégories de données à caractère personnel** :

– **l'identifiant des participants et des « mineurs »** : chaque participant/ « mineur » dispose d'une clé ouverte, ce qui permet d'assurer l'identification de l'émetteur et du destinataire d'une transaction ;

– **des données complémentaires, inscrites « dans » une transaction** (telles qu'un diplôme ou titre de propriété) : si ces données sont relatives à des personnes physiques, éventuellement autres que les participants, directement ou indirectement identifiables, il s'agit de données à caractère personnel.

D'après l'analyse de la CNIL, **dès lors que les informations contenues dans une *blockchain* relèveraient de l'une de ces deux catégories, les exigences fixées par le RGPD (identification du responsable de traitement, mise en œuvre des droits, mise en place de garanties appropriées, obligation de sécurité, etc.) s'imposeraient.**

De même, **le fonctionnement des protocoles rendrait concevable l'application du statut de « responsable de traitement »**. D'après l'analyse de la CNIL, le participant à une *blockchain* peut être considéré comme tel dès lors :

– qu'il est une personne physique et que le traitement de données personnelles est en lien avec une activité professionnelle ou commerciale – c'est-à-dire une activité qui n'est pas exclusivement personnelle ;

– qu'il est une personne morale et qu'il inscrit une donnée à caractère personnelle dans un protocole.

En revanche, la CNIL estime que le statut ne s'applique pas aux « mineurs » dans la mesure où leur rôle se cantonne à la validation des transactions et qu'ils n'interviennent pas sur l'objet de ces dernières. Dans ces conditions, au sens du RGPD, ils ne déterminent pas les finalités et les moyens à mettre en œuvre.

Dans le cas de la mise en œuvre conjointe d'un traitement de données fondé sur l'usage d'une *blockchain*, on pourrait considérer que l'ensemble des

participants portent une responsabilité conjointe, conformément à l'article 26 du RGPD. En conséquence, il leur incomberait de définir, de manière transparente, les obligations de chacun aux fins d'assurer le respect des règles relatives à la protection des données personnelles.

D'autre part, les caractéristiques du fonctionnement des protocoles paraissent correspondre à certaines exigences du RGPD.

Ainsi, on peut estimer que par l'intangibilité des données inscrites et la fonction d'horodatage, les *blockchains* permettent d'assurer une certaine traçabilité du traitement des données personnelles, correspondant aux finalités – à défaut de respecter les prescriptions relatives aux informations requises – du registre des activités de traitement prévu à l'article 30 du RGPD.

Par ailleurs, dans la mesure où les participants à une *blockchain* conservent la propriété de leurs données et disposent d'un accès au registre partagé par l'ensemble des membres du réseau, l'utilisation des protocoles apparaît compatible avec le principe de droit d'accès consacré par l'article 15 du RGPD.

Cela étant, ainsi que l'observent la CNIL et certaines personnes auditionnées par la mission, **l'application des catégories et des procédures du régime de protection des données personnelles ne va pas de soi selon que le traitement est réalisé dans le cadre d'une** *blockchain* privative **ou dans celui d'une *blockchain* ouverte. Les caractéristiques de ces protocoles soulèvent en effet plusieurs difficultés qui touchent** :

– à la détermination du responsable de traitement et de son sous-traitant, démarche nécessairement complexe dans le cadre d'une architecture dépourvue d'instance centrale de contrôle et organisant un consensus décentralisé ;

– à l'exercice du droit de rectification et du droit d'effacement des données personnelles (affirmés par les articles 16 et 17 du RGPD), dès lors qu'il n'existe pas de responsable de traitement, que les informations inscrites dans les *blockchains* sont censées être intangibles – ce qui du reste parait peu conciliable avec le principe d'une durée du traitement des données personnelles – et que le registre est distribué entre de multiples nœuds.

– aux restrictions apportées au transfert de données personnelles vers des pays tiers, le RGPD exigeant que ces États garantissent un niveau adéquat de protection des données des individus, la mise en place d'outils spécifiques, ainsi que le consentement expresse au transfert par l'individu objet de ces données ;

– à la protection même des données personnelles, le recours aux pseudonymes n'assurant pas nécessairement l'impossibilité de tracer les actions d'un membre du réseau ; en outre, les mineurs se répartissent tout autour du globe et ne sont pas connus.

Dans son appréciation de la compatibilité de la technologie des *blockchains* avec les prescriptions du RGPD, la CNIL raisonne du point de vue des risques que chaque usage peut éventuellement comporter pour la protection des données personnelles.

La mission considère cette approche pragmatique comme pertinente.

Certes, au vu des conclusions travaux de l'OPECST, on peut éprouver un doute quant à la crédibilité des différentes solutions techniques actuellement envisagées afin de garantir la protection des données personnelles. Les hypothèses examinées portent en l'occurrence sur l'intégration directe de la réglementation dans le code des protocoles, sur la délivrance d'une nouvelle adresse publique à chaque transaction ou encore sur des procédés d'offuscation (1) des données inscrites rendant en théorie impossible leur consultation ou accès par d'autres membres d'un réseau (2).

Cela étant, il ne parait pas hors de propos d'envisager des évolutions techniques susceptibles de satisfaire les exigences de la protection des données personnelles, notamment dans le cas des *blockchains* ouvertes. Dans cette perspective, **la mission appelle les collectivités publiques à soutenir la réalisation des projets de recherche et développement de nature à répondre à cet objectif, notamment en renforçant les capacités de chiffrement des protocoles.**

Il importe sans doute également de préciser les conditions d'application du RGPD au secteur des *blockchains*. Il ne s'agit pas ici de méconnaître l'effort fourni par la CNIL afin de diffuser une culture de la protection des données personnelles et permettre à chacun de mesurer la pertinence du recours aux *blockchains* pour la mise en œuvre d'un traitement. Mais, ainsi que le montrent les éléments recueillis dans le cadre des travaux de la mission, rien ne garantit que les catégories et notions en vigueur permettent d'appréhender parfaitement l'ensemble des usages rendus possibles par une technologie au potentiel disruptif.

Aussi, il paraît utile que les institutions de l'Union européenne et ses États membres entreprennent un travail d'évaluation et, le cas échéant, d'actualisation du RGPD à la lumière des enjeux inhérents à l'essor des *blockchains*. Du point de vue de la mission, cette tache participerait utilement à l'action résolue et indispensable à la préservation des intérêts fondamentaux du pays dans laquelle il importe d'engager l'Union européenne.

---

(1) L'offuscation consiste à rendre illisible une information inscrite dans une blockchain ou à en empêcher l'accès.

(2) Rapport n° 1092 - Rapport de Mme Valéria Faure-Muntian, MM. Claude de Ganay et Ronan Le Gleut établi au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, sur les enjeux technologiques des blockchains (chaînes de blocs), pp. 97-99.

Proposition n° 17 : Évaluer les conditions d'application du règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (dit « règlement RGPD).

Soutenir la réalisation des projets de recherche et développement de nature à renforcer les capacités de chiffrement des protocoles fondés sur la technologie des *blockchains*.

2. Engager l'Union européenne dans une action résolue et indispensable à la préservation de notre souveraineté

Il importe en effet de garantir la maîtrise d'infrastructures, de procédés techniques et de compétences qui, très probablement, pourraient constituer les ressorts de l'économie de demain. À l'évidence, la France ne saurait relever le défi par une politique se bornant à soutenir un écosystème et à établir un cadre juridique adapté à l'échelle nationale.

S'il possède des avantages comparatifs indéniables, notre pays doit également affronter une âpre concurrence.

De fait, nombre de ses partenaires – et concurrents – économiques tendent à développer des stratégies nationales destinées à valoriser leur propre potentiel et à s'arroger des ressources essentielles pour la maîtrise de la technologie. Comme observé précédemment (1), la compétition porte sur la localisation des mineurs, des États comme la Chine ou la Russie disposant d'atouts énergétiques ou s'efforçant d'obtenir leur implantation. Mais elle prend également la forme d'une concurrence au plan juridique, certains États à l'instar de la Suisse ou de Malte se donnant pour objectif d'établir un cadre normatif propice à leur attractivité, notamment dans l'usage des cryptomonnaies et le développement de services financiers.

Ainsi que l'a souligné l'OPECST (2), l'investissement des États pour les *blockchains* – souvent plus précoce que celui fourni par notre pays – se mesure aussi aux ressources disponibles dans l'enseignement et la recherche.

(1) Cf. supra p. 25.

(2) Rapport n° 1092 - Rapport de Mme Valéria Faure-Muntian, MM. Claude de Ganay et Ronan Le Gleut établi au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, sur les enjeux technologiques des blockchains (chaînes de blocs), p. 102.

Aperçu de stratégies nationales

en faveur du développement des *blockchains*

– Royaume-Uni : Le rapport du *Government Office for Science* publié en janvier 2016 s'inscrit dans la démarche engagée par le Gouvernement britannique et le *Government Digital Services* (GDS) afin de réaliser un examen systématique des emplois possibles de la technologie des *blockchains.* Le GDS semble acquis à l'idée d'utiliser ce type de protocole afin d'assurer l'intégrité des registres gouvernementaux dans des domaines tels que la tenue du cadastre ou le recensement des données d'entreprise. Le rapport du Government Office for Science prône également le recours aux *blockchains* dans tout un ensemble de services gouvernementaux afin de réduire la fraude, améliorer la communication avec les usagers et renforcer la capacité d'innovation des administrations et services publics.

– États-Unis : Le Gouvernement fédéral a accordé 3 millions de dollars aux chercheurs afin d'examiner les utilisations de crypto-monnaies, y compris leur application aux *smart contracts*.

– Singapour : Le Gouvernement de Singapour, ainsi que l'Autorité monétaire de Singapour (MAS), ont investi environ 225 millions de dollars dans le secteur des « *Fintech* » (technologies financières) et en innovation, dont une partie concerne l'utilisation de la technologie des blockchains.

– Malte : Aspirant à devenir « *l'île des* blockchains », l'État maltais a promulgué au début du mois de juillet 2018 trois lois destinées à établir un cadre juridique global pour la régulation et le développement des usages fondés sur cette technologie.

Le *Malta Digital Innovation Authority Act* (MDA) prévoit la création d'une nouvelle autorité de régulation chargée de promouvoir et d'assurer le développement du secteur des technologies innovantes à Malte. Elle sera compétente pour la réglementation de l'usage des *blockchains* et des cryptomonnaies, notamment par le biais d'une certification des plateformes de registres distribués destinée à protéger les utilisateurs

L'*Innovative Technology Arrangements and Services Act (« ITAS Act »)* fonde le régime applicable pour l'enregistrement des prestataires de services de technologie et la certification des accords dans le cadre de la mise en œuvre d'une technologie. Au sens de la loi, relèvent de cette dernière catégorie les logiciels et les « architectures » utilisés pour concevoir et mettre en œuvre un registre distribué, des *smarts contracts* et les applications qui leur sont liées (DAO, et tout autre accord dans le cadre de la mise en œuvre d'une technologie qui pourrait être désigné par l'autorité ministérielle).

Le *Virtual Financial Assets Act* (« VFAA » Act) vise à établir un cadre approprié à la levée de fonds au moyen des ICO, ainsi qu'aux échanges de cryptoactifs. Il comporte ainsi des prescriptions relatives aux documents d'informations (*white paper*) publiés dans le cadre des ICO et fixe le régime réglementaire applicable aux plateformes d'échange de monnaies virtuelles. Le législateur maltais a en outre créé un « test » (*Financial Intruments Test)* qui détermine la catégorie dont relève un actif émis par un protocole de type « registre distribué ». Cette qualification s'applique à toutes les cryptomonnaies et tous les *tokens*. Le « test » les classe dans trois catégories : *token* virtuel, instruments financiers et actifs financiers virtuels.

De surcroît, le développement de cette technologie semble devoir obéir à une logique à l'œuvre dans l'économie numérique et qui favorise la création de monopoles ou d'oligopoles. Il soulève à l'évidence des enjeux transnationaux qui se jouent des frontières, à l'exemple de la régulation des cryptomonnaies dont s'est saisi le G20 en mars 2018 sur la base d'une initiative franco-allemande.

Dès lors, **il importe que l'action des pouvoirs publics trouve des relais à l'échelle européenne. Dans cette optique, on ne peut que se féliciter de ce que les institutions de l'Union européenne prennent la mesure des enjeux entourant l'usage des *blockchains*** [(1)] et affirment la volonté de donner au « Vieux continent » les moyens de tirer pleinement parti de ces innovations au plan économique.

À la suite du rapport de M. Jakob von Weizsäcker sur les monnaies virtuelles [(2)], la Commission européenne a installé, en février 2017, **l'Observatoire-forum des *blockchains* de l'Union européenne,** avec le soutien du Parlement européen. La création de cette instance poursuit plusieurs objectifs : en premier lieu, collecter des informations, suivre et analyser les tendances et examiner le potentiel socio-économique des *blockchains* ; en second lieu, offrir un forum de débat aux spécialistes de la technologie, aux innovateurs, aux citoyens et aux parties prenantes du développement du secteur (pouvoirs publics, autorités de régulation) ; enfin, favoriser la coopération transfrontalière sur des cas concrets.

Par ailleurs, dans la continuité du Septième programme-cadre de recherche et du programme Horizon 2020, **la Commission a indiqué vouloir consacrer 340 millions d'euros au financement de projets susceptibles de faire appel aux technologies *blockchains* d'ici à 2020**.

Du point de vue des rapporteurs, l'enjeu réside autant dans la capacité de l'Union européenne à dégager les ressources nécessaires au financement de projets innovants que dans l'établissement d'un cadre juridique propice au développement des écosystèmes nationaux.

---

(1) https://ec.europa.eu/luxembourg/news/la-commission-europ%C3%A9enne-lance-lobservatoire-forum-des-cha%C3%AEnes-de-blocs-de-lue_fr.

(2) Parlement européen, Rapport sur les monnaies virtuelles (2016/2007(INI)), présenté à la Commission des affaires économiques et monétaires par M. Jakob von Weizsâcker, rapporteur pour avis, mai 2016.

Favoriser la capacité d'entreprendre et créer les conditions de l'émergence de champions européens dans le secteur requiert, d'une part, la définition de normes techniques communes, susceptibles de garantir l'interopérabilité des *blockchains*. Mais au-delà d'une harmonisation ou d'une convergence des législations au sein du Marché unique, cet objectif implique aussi que l'Union européenne (ou ses principaux États membres) prenne toute sa part aux travaux visant à l'établissement de standards internationaux, tels que ceux menés dans le cadre du mandat donné à l'*Australia's national standards Authority* par l'Organisation internationale de normalisation (ISO) (1).

Cette démarche revêt un caractère indispensable dans la mesure où elle conditionne la capacité des États européens à garder la maîtrise d'infrastructures économiques essentielles. Il en va sans doute également de la protection de leurs valeurs ou de modèles propres, dans des domaines aussi sensibles que la protection des données personnelles ou la défense du droit de propriété intellectuelle.

D'autre part, le développement des modèles d'affaires ou de capacités de production dans le secteur des *blockchains* exige un environnement juridique stable, compréhensible et assurant la rentabilité des investissements réalisés. Comme à l'échelle nationale, **cette démarche implique d'abord de fixer, dans le droit de l'Union européenne, une définition permettant de caractériser les protocoles fondés sur la technologie des *blockchains*, ainsi que ses principaux usages** (par exemple dans le domaine des cryptoactifs).

Du point de vue des rapporteurs, sans nécessairement conduire à la création d'un cadre dérogatoire, **il convient ensuite d'évaluer l'impact des normes européennes en vigueur susceptibles d'affecter le développement des *blockchains***. De fait, le droit de l'Union comporte des textes généraux qui conditionnent certains usages de la technologie. Il en va ainsi naturellement de la « directive sur le commerce électronique » (2) mais on peut également penser à des textes de portée plus générale régissant le marché des capitaux, la supervision financière, l'union monétaire ou la lutte contre le blanchiment (3).

Dès lors, il apparaît nécessaire d'évaluer la pertinence de certains critères d'application de règles prudentielles applicables aux secteurs bancaires et financiers. Il pourrait s'agir également d'envisager des « accommodements

---

(1) Pour International Organization for Standardization*. En l'occurrence, l'Organisation internationale de normalisation a chargé l'Autorité australienne d'établir une feuille de route afin d'assurer le développement de standards internationaux pour la technologie des « chaines de blocs ». L'Autorité australienne dirige en conséquence un comité technique comprenant 16 membres, parmi lesquels sont entre autres représentés la France, la Malaisie, l'Allemagne, les États-Unis, la Chine, la Corée et le Japon.*

(2) Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»).

(3) Directives (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.

raisonnables » dans la mise en œuvre du droit de la concurrence, voire de travailler à un rapprochement des fiscalités sur les cryptoactifs.

Le propos de la mission n'est pas de créer pour la technologie des *blockchains* un statut dérogatoire l'affranchissant de toutes règles**. Il s'agit de favoriser l'émergence d'un secteur économique prometteur en établissant des obligations proportionnées en droit.**

Proposition n° 18 : Inscrire dans le droit de l'Union européenne une définition permettant de caractériser les protocoles fondés sur la technologie des *blockchains*, ainsi que ses principaux usages.

Évaluer les normes susceptibles d'affecter le développement de la technologie et envisager les ajustements nécessaires, notamment dans le domaine du droit de la concurrence et du commerce électronique.

Au-delà – pour autant que les États s'accordent sur les fins et les moyens **– rien n'interdit d'envisager la mise en place des instruments d'une politique plus intégrée (ou de coopérations renforcées) ayant pour objectifs :** l'établissement d'une stratégie européenne ; la mise en place d'un financement communautaire ; le développement de projets d'infrastructures et de standards communs dans la sphère publique, de mutualisation des ressources académiques et de coopérations transfrontalières. **Une telle démarche contribuerait à donner toute sa portée à la déclaration adoptée par les États membres le 10 avril 2017 en vue de l'établissement d'une coopération sur un partenariat européen pour les *blockchains* [(1)].**

Proposition n° 19 : Favoriser l'engagement d'une politique européenne intégrée sur la base des objectifs fixés par la déclaration adoptée par les États membres le 10 avril 2017 en vue de l'établissement d'une coopération sur un partenariat européen pour les *blockchains*.

(1) https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership.

CONCLUSION

Au terme du présent rapport, un constat s'impose : alors que nos économies connaissent une transformation accélérée grâce à la dématérialisation croissante des échanges, ainsi qu'à une nouvelle offre de produits et de services numériques, la France ne saurait demeurer à l'écart de l'étonnant foisonnement d'initiatives et d'innovation que suscite aujourd'hui l'affirmation du secteur des *blockchains*.

Certes, dans certains domaines, les protocoles présentent encore les signes d'une relative immaturité et bien des questionnements peuvent subsister face à un certain nombre de projets qui peinent à franchir le stade du concept. La mission n'entend éluder ici aucun de ces questionnements qui invitent à faire la part de l'optimisation des process existants et des effets de mode.

Cela étant, ainsi que le montre le présent rapport, la technologie permet d'ores et déjà des usages nouveaux, qui ouvrent la perspective d'un possible renouvellement des organisations, des relations économiques et de travail, ainsi que des habitudes de consommation. En outre, les solutions qu'elle peut proposer sont le fait d'un écosystème aujourd'hui en pleine affirmation et qui se structure autour d'organismes de recherche et de start-up prometteuses.

Dans ce secteur, la France dispose d'un certain nombre d'atouts. Dès lors, pour que notre pays valorise ces ressources et acquiert la maîtrise de savoir-faire et d'infrastructures indispensables au développement de cette technologie, il importe de lever des freins à l'innovation. Dans le cadre du projet de loi « Pacte » et du projet de loi de finances pour 2019, les pouvoirs publics se sont engagés dans l'élaboration d'un cadre juridique susceptible de rassurer les investisseurs dans le secteur des cryptoactifs et, ce faisant, de créer les conditions d'un essor des usages permis par les *blockchains*. Alors que nos principaux partenaires – et non moins concurrents – mènent des stratégies nationales destinées à conforter leur attractivité, il s'agit d'une démarche essentielle. En effet, au-delà des financements publics que peut nécessiter la réalisation de certains projets, l'innovation est affaire de confiance et de prévisibilité.

Mais au-delà, il appartient sans doute à l'État – en quelque sorte – de donner l'exemple en se saisissant pleinement d'un levier possible de modernisation des administrations et des services publics. L'État peut, en outre, soutenir le recours aux *blockchains* au titre de sa politique industrielle. Favoriser le développement et la prise en main de telles technologies au sein des filières économiques qui ont besoin d'être mieux structurées pourrait être un levier important de gains de productivité et de compétitivité à moyen terme.

Proposition n° 20 : Poursuivre la réflexion sur les chantiers de transformation qui pourrait être conduite grâce à la *blockchain* dans :

– l'amélioration des services publics grâce au potentiel de certification, de reconnaissance de l'identité numérique et d'archivage des *blockchains*, par exemple pour favoriser la participation citoyenne (organisation de consultations locales dématérialisées et sécurisées), pour délivrer plus rapidement des titres administratifs (carte grise, dossier médical partagé, carte Vitale, K Bis, numéro Sirene, etc.) ou pour archiver en confiance des diplômes universitaires ;

– la structuration et de l'animation des filières économiques (agroalimentaire, télécommunications, énergie, automobile), grâce à l'impulsion, au départ au moins, d'acteurs de confiance et reconnus tout au long de ces filières (interprofessions, régulateurs, entités publiques).

PROPOSITIONS DE LA MISSION

L'impulsion de l'État

Proposition n° 1 : Favoriser la création d'un écosystème suffisamment mature pour que se développe une *blockchain* ouverte issue d'initiatives françaises ou européennes, alimentées par des financements publics de soutien à la recherche et au développement, sur le modèle de l'intelligence artificielle.

Proposition n° 3 : Accentuer les efforts de recherche interdisciplinaire (informatique, économie, droit) sur le potentiel applicatif des *smart contracts*, qui représentent l'avenir des *blockchains*, par exemple par le biais d'une équipe Inria-Sorbonne-Paris *School of Economics*.

Proposition n° 6 : Créer au sein de la DINSIC un groupe de travail transversal chargé d'une mission d'évaluation des conditions du développement de la technologie des *blockchains* dans la vie économique et sociale et de son usage par les collectivités publiques.

Proposition n° 19 : Favoriser l'engagement d'une politique européenne intégrée sur la base des objectifs fixés par la déclaration adoptée par les États membres le 10 avril 2017 en vue de l'établissement d'une coopération sur un partenariat européen pour les *blockchains*.

Proposition n° 20 : Poursuivre la réflexion sur les chantiers de transformation qui pourrait être conduite grâce à la blockchain dans :

– l'amélioration des services publics grâce au potentiel de certification, de reconnaissance de l'identité numérique et d'archivage des blockchains, par exemple pour favoriser la participation citoyenne (organisation de consultations locales dématérialisées et sécurisées), pour délivrer plus rapidement des titres administratifs (carte grise, dossier médical partagé, carte Vitale, K Bis, numéro Sirene, etc.) ou pour archiver en confiance des diplômes universitaires ;

– la structuration et de l'animation des filières économiques (agroalimentaire, télécommunications, énergie, automobile), grâce à l'impulsion, au départ au moins, d'acteurs de confiance et reconnus tout au long de ces filières (interprofessions, régulateurs, entités publiques).

Le soutien de l'écosystème

Proposition n°2 : Reconnaître le crypto-minage comme une activité électro-intensive bénéficiant des tarifs préférentiels de l'électricité, afin de maintenir cette activité en France.

Proposition n° 9 : Garantir un cadre de régulation des cryptoactifs qui réponde à l'exigence de protection des investisseurs français.

Proposition n° 10 : Faire évoluer les équilibres du projet de loi « PACTE » pour que la régulation des services financiers et bancaires soit clairement distincte des services tiers en matière de cryptoactifs.

Proposition n° 11 : Garantir un droit au compte en dernier ressort, assuré par la Caisse des dépôts et consignations, par la Banque de France ou par la Banque postale, pour les acteurs ayant bénéficié du visa de l'AMF.

Proposition n° 12 : Améliorer encore le dispositif fiscal proposé dans le PLF pour 2019, notamment en ne fiscalisant les plus-values liées aux crypto-échanges qu'au moment où celles-ci sont encaissées sur un compte bancaire traditionnel.

Proposition n° 13 : Mener une revue générale des normes susceptibles de conditionner l'essor de la technologie des *blockchains*.

Proposition n° 14 : Envisager une adaptation du régime applicable en matière de preuve électronique et de signature numérique par une révision du règlement du règlement européen 910/2014 du 23 juillet 2014 (dit « règlement eIDAS »).

Appuyer les initiatives tendant à favoriser l'établissement de standards européens ou internationaux pour le fonctionnement des *blockchains*.

Proposition n° 18 : Inscrire dans le droit de l'Union européenne une définition permettant de caractériser les protocoles fondés sur la technologie des *blockchains*, ainsi que ses principaux usages.

Évaluer les normes susceptibles d'affecter le développement de la technologie et envisager les ajustements nécessaires, notamment dans le domaine du droit de la concurrence et du commerce électronique.

La prospective

Proposition n° 4 : Envisager la création d'une « monnaie » numérique émise par la banque centrale.

Proposition n° 5 : Évaluer l'intérêt de consacrer dans la loi le statut de tiers de confiance numérique chargé d'assurer la protection de l'identité ; des documents, des transactions et en mesure d'auditer et de certifier les protocoles *blockchains*.

Proposition n° 7 : Favoriser l'émergence d'équipes interdisciplinaires et autonomes en fléchant les crédits du PIA ou de l'ANR vers le financement pérenne de telles structures de recherche agiles et conditionner ce financement à la recherche d'une issue commerciale ou industrielle.

Proposition n° 8 : Établir une « vision prospective partagée des emplois et des compétences » en vue de structurer une sous-filière blockchains au sein de la filière numérique.

Proposition n° 15 : Engager une réflexion au niveau européen et français permettant l'établissement d'un régime de responsabilité permettant d'appréhender les usages des protocoles fondés sur la technologie des *blockchains*.

Proposition n° 16 : Examiner la nécessité d'une adaptation des normes européennes et nationales du droit de la consommation au regard des usages permis par les protocoles fondés sur la technologie des *blockchains*.

Proposition n° 17 : Évaluer les conditions d'application du règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (dit « règlement RGPD). Soutenir la réalisation des projets de recherche et développement de nature à renforcer les capacités de chiffrement des protocoles fondés sur la technologie des blockchains.

LISTE DES PERSONNES AUDITIONNÉES

France Stratégie

Mme Joëlle Toledano, professeure des universités en économie, président du groupe de travail « Les enjeux des *blockchains* »

Mme Liliane Dedryver, cheffe de projet numérique

Blockchain Partner

M. William O'Rorke, directeur juridique

Chaintech (association des acteurs professionnels de la blockchain en France)

M. Alexandre Stachtchenko, président

Table ronde « recherche » (1/2)

M. Daniel Augot, INRIA

M. Julien Prat, ENSAE

M. Georges Gonthier, équipe Specfun

Mme Emmanuelle Anceaume, Équipe Cidre, Rennes

M. Gilles Fedak, créateur de la start-up iEx.ec

Table ronde « recherche » 2/2

M. Éric Salobir, président du Réseau Optic

M. Thibault Douville, professeur

M. Guillaume Buffet, président de UChange

M. Kariappa Bheemaiah

Personnalités qualifiées

Mme Primavera de Filippi, chercheuse rattachée au CERSA (unité mixte du CNRS et de l'Université Paris-II)

M. Gilles Babinet, représentant du numérique pour la France auprès de la Commission européenne

M. Mathieu Davy, avocat associé chez Oramedia

M. Xavier Lavayssière, expert en régulation de bloc-chaîne, président des Bricodeurs

M. Jérôme Deroulez, avocat

Mme Mélanie Cras, juriste

Caisse des dépôts et consignations

Mme Nadia Filali, directrice des programmes blockchains et pilote de *La BChain*

M. Philippe Blanchot, directeur des relations institutionnelles

Banque de France

M. Michel Spiri, adjoint au Secrétaire général de la Banque de France

Mme Véronique Bensaid-Cohen, conseillère parlementaire

Conseil d'État

M. Timothée Paris, rapporteur général adjoint de la section du rapport et des études

Syntec Numérique

M. Laurent Baudart, délégué général

Mme Philippine Lefèvre, déléguée aux relations institutionnelles

M. Vidal Chriqui, directeur général chez 808 Labs

Microsoft

M. Marc Gardette, directeur de la stratégie cloud

M. Quang-Minh Lepescheux, responsable des affaires publiques

Accenture

M. Emmanuel Viale directeur exécutif Accenture France

M. Michaël Gaborit, adjoint au directeur Accenture Labs

Table ronde « instruments financiers »

M. Arnaud de Bresson, délégué général de Paris Europlace

M. Alain Pithon

Mme Carine Delfrayssi

Mme Valentine Baudouin, avocate au barreau de Paris

M. Alexis Roussel, secrétaire du Cercle du Coin

Table ronde « énergie »

RTE

M. Emanuele Colombo, direction de l'économie du système électrique

M. Philippe Pillevesse, directeur

Sales et Marketing KeeeX

M. Cyprien Veyrat, vice-président

IRT System X

M. Charles Kremer, directeur « territoires intelligents »

Ministère de la Transition Ecologique et Solidaire,

Dr. Marc Solinhac, chargé des études et de la prospective, projet d'immatriculation avec la blockchain

Chainhero

M. Nicolas Hersog

WOOBE

M. Philippe Morel, fondateur

M. Olivier Bougé, Business Development Manager

GS1 France

M. François Deprez, Président

M. Xavier Barras, directeur des Opérations

M. Cédric Lecolley, directeur Marketing

M. Ons Sassi, Innovation Project manager

Mme Sophie La Pallec, directrice des Affaires publiques

Groupe La Poste

M. Alain Roset, direction numérique

Ministère de la Justice

Mme Anne-Sophie Hutin, rédactrice au bureau du droit des obligations

Mme Marie-Charlotte Dreux, chef du bureau du droit des obligations

Ministère de l'Économie et des Finances - Direction générale des entreprises

M. Loïc Duflot, sous-directeur réseaux et usages numériques au sein de la direction générale des entreprises

Mme Aurore Tual, adjointe à la cheffe du bureau des usages du numérique de la direction générale des entreprises

Mme Laura Hiel, chargée de mission au sein du bureau des usages du numérique de la direction générale des entreprises

IBM

M. Vincent Fournier, Senior Managing Consultant Blockchain

Mme Diane Dufoix-Garnier, Directrice affaires publiques

Table ronde financement de l'économie

M. Jon Matonis, économiste spécialisé sur les questions monétaires

M. Stéphane Vincent, consultant externe auprès de la commission

UTOCAT

M. Clément Francomme, président

M. Alexis Mévellec, VP Business Development

M. Martin Kruczkowski, juriste

Fédération bancaire française (FBF)

M. Benoit de la Chapelle Bizot

M. Nicolas Bodilis-Reguer

Mme Frédérique Fagès, chargée de mission Numérique et moyens de paiement

Groupe Carrefour

M. Hervé Gomichon - Directeur Qualité (en charge de la Blockchain)

M. Éric Adam, responsable des affaires publiques

Stratum

M. Jérôme Lefebvre, Directeur général

Mme Séraphie de Tracy, Directrice Assurances

Commissariat à l'énergie atomique

M. François Terrier, chef du département Ingénierie Logiciels et Systèmes du CEA

M. Julien Chiaroni, adjoint du directeur de l'institut CEA/List

M. Jean-Pierre Vigouroux, Chef du Service des Affaires publiques - Chargé des Relations avec le Parlement

Table ronde sur l'usage de la blockchain dans les administrations et les services publics

Mme Perrine de Coëtlogon, expert numérique participant (anime le groupe de travail #Blockchain4EDU au sein de ministère de l'Éducation sur la blockchain)

Mme Nina Fabrizi-Racine, juriste spécialisée en droit numérique, membre de la Direction interministérielle du numérique (DINSIC)

Table ronde sur l'usage des blocs-chaînes dans les industries culturelles

Ubisoft

Mme Anne Puck, Directrice juridique adjointe

M. Nicolas Pouard, Analyste, Laboratoire d'innovation stratégique

M. Romain Poirot-Lellig, conseiller du PDG pour les affaires publiques

Mme Marie Sophie de Waubert, vice-présidente relations institutionnelles Europe

Sacem

M. Xavier Costaz, directeur de projet,

M. Blaise Mistler, directeur des relations institutionnelles

Soonvibes

Mme Natacha Ordas, Présidente

Commission nationale de l'informatique et des libertés (CNIL)

M. Gwendal Le Grand, Directeur des technologies et de l'innovation

Mme Amandine Jambert, Ingénieur expert en technologie de l'information, service de l'expertise technologique

M.Thomas Dautieu, directeur-adjoint à la Direction de la conformité

Mme Nacéra Bekhat, juriste au service santé

Mme Tiphaine Havel, Conseillère pour les questions institutionnelles et parlementaires

Table ronde « Potentiel des bloc-chaînes publiques par rapport aux bloc-chaînes fermées »

M. Simon de Charentenay, Maître de conférence et CEO d'OpenFlow,

Ark.io

M. François-Xavier Thoorens, CTO et fondateur de ARK Ecosystem

M. Arnaud Deborne

Table ronde « Bloc-chaîne et droit »

M. Barthélémy Lemiale, avocat, co-fondateur de IPO©AMP, service de protection de la propriété intellectuelle en Blockchain

Mme Juliette Sénéchal, Maître de conférences à l'Université de Lille-2 et membre de TransEuroExperts, réseau européen d'experts en droit

Conseil national des barreaux (CNB)

M. Louis Degos, président de la commission « Prospective »

M. Jean-Laurent Bourel, membre de la commission « Numérique »

Avotech, association d'acteurs du droit sur les sujets technologiques

M. Henri de La Motte Rouge, avocat

Conseil Supérieur du Notariat

Me Jean François Humbert, 1er Vice-président

M. Nicolas Tissot Directeur de la Direction du Numérique et des Systèmes d'Information

Mme Christine Mandelli, chargée des relations avec les institutions

Autorité des marchés financiers (AMF)

M. Benoît de Juvigny, secrétaire général

Mme Domitille Dessertine, directrice de division, division Fintech, Innovation, Compétitivité à la direction de la Régulation et des Affaires Internationales

Madame Anne Maréchal, directrice de la direction des affaires juridiques

Mme Laure Tertrais, conseillère parlementaire et législation, direction des affaires juridiques

Table ronde « Protection des données personnelles »

Mme Nathalie Chiche, présidente de Data Expert, déléguée à la protection des données externes

M. Olivier Dion, P-DG de Onecub

Compagnie régionale des commissaires aux comptes d'Aix Bastia

M. Farouk Boulbahri, commissaire aux comptes, président de la Compagnie régionale des commissaires aux comptes d'Aix Bastia

Mme Nathalie Malicet, vice-présidente de la commission numérique et innovation

Fondation IOTA

M. Pierre Hoffmann, *Business development* – France Lead