



DIGITAL:
NEW DEAL
FOUNDATION

Avril 2018

L'ÂGE DU WEB DÉCENTRALISÉ

par Clément Jeanneau

CLÉMENT JEANNEAU

Cofondateur de Blockchain Partner, leader français de la transformation blockchain, Clément Jeanneau accompagne avec son équipe les grandes entreprises et institutions publiques dans l'exploration et l'adoption de ces technologies (Banque de France, Groupe Aéroports de Paris, Etat de Genève, SNCF...).

Auparavant, durant son cursus à l'ESCP il avait **cofondé Blockchain France**, organisme pionnier en France dans la démocratisation du sujet, avec lequel il a notamment lancé dès 2015 un appel intitulé «**La France ne doit pas rater la révolution blockchain**».

Il est également **co-auteur de «La Blockchain Décryptée»** (Netexplo, juin 2016), premier ouvrage en français paru sur ces technologies, et **publie régulièrement des analyses sur les cryptoactifs dans les médias** (Les Echos, La Tribune, Le Point...) pour mettre en valeur leurs enjeux et des propositions d'actions concrètes pour les pouvoirs publics.



SOMMAIRE

Avant-propos

- I La dynamique enrayée de l'économie numérique actuelle
- II La blockchain comme réponse aux limites du web actuel
- III La blockchain et les tokens ouvrent la voie d'une nouvelle économie numérique
- IV Les implications de la « token économie » au-delà du web
- V Les cryptomonnaies face au même scepticisme qu'Internet à ses débuts
- VI Une opportunité à saisir rapidement

Conclusion

AVANT-PROPOS

Malgré toute l'attention dont elle fait l'objet depuis de nombreux mois, les centaines d'articles parus à son sujet, les points de vue tranchés exprimés avec conviction par nombre d'experts en expertise, la blockchain reste une technologie mal comprise.

Une fois son énergie placée dans la (tentative de) compréhension de son fonctionnement, la patience vient parfois à manquer pour aborder en profondeur son utilité réelle, au-delà des sempiternels mêmes exemples, et ses multiples enjeux.

La blockchain répond pourtant bel et bien à un besoin, contrairement à sa réputation de solution encore à la recherche d'un problème à résoudre.

Dans cette perspective, la logique doit d'abord conduire, avant de présenter directement la solution dont il s'agit, à étudier les problèmes auxquels celle-ci s'attaque. C'est l'objet de la première partie de cette note. L'angle choisi, les limites de l'économie numérique actuelle, est volontairement restrictif. L'objectif ici n'est pas d'aborder l'ensemble des problématiques de la blockchain, qui nécessiteraient bien plus d'un rapport¹, mais de pointer du doigt ce qui est encore insuffisamment considéré et qui constitue pourtant une opportunité inédite pour la France et l'Europe : l'émergence d'une nouvelle économie numérique.

De la même façon qu'Internet suscite aujourd'hui des débats qui dépassent très largement ses mécanismes sous-jacents (TCP/IP, etc.), la blockchain doit être considérée au-delà de ses seules caractéristiques techniques, aussi révolutionnaire soient-elles. Comprendre son potentiel implique de comprendre les acteurs qui l'entourent, les nouvelles stratégies qu'elle rend possible, les logiques économiques qui lui sont propres, à commencer par les mécanismes d'incitation qui meuvent ses acteurs et le nouveau domaine d'étude qu'elle ouvre, la cryptoéconomie. C'est l'objet des parties deux à quatre de cette note.

A cet égard, un lecteur soucieux de saisir les enjeux de cette technologie ne pourra faire l'économie de se pencher sur la question des cryptomonnaies, dont on verra dans la cinquième partie pourquoi il est indispensable d'aller au-delà des idées reçues.

De façon générale, la blockchain demande à chacun, jeune ou moins jeune, encore sur les bancs de l'école ou spécialiste de son domaine d'activité, de se placer dans une posture d'apprenant. En d'autres termes, elle requiert une certaine humilité. Personne ne peut prétendre être un expert complet de ce sujet aussi transdisciplinaire, qui touche aux sciences mathématiques, économiques, sociales, de la cryptographie à la géopolitique, en passant par l'histoire de la monnaie, le droit, la finance, la sociologie, l'étude des organisations et de leur gouvernance...

En ce sens, la blockchain est un terrain d'étude infini pour tout esprit curieux intellectuellement. Gare à la tentation, vaine, de chercher à maîtriser cette technologie, et ce d'autant plus au vu de sa vitesse de développement. A défaut de chercher à l'embrasser tout entier, il est plus réaliste de chercher, plus modestement, à être explorateur de ce nouveau web extrêmement mouvant.

Ce chemin permet alors de comprendre en quoi la blockchain ouvre des possibilités inédites pour la France et l'Europe. Parvenu à ce stade, il sera l'heure, dans la dernière partie, de soumettre un certain nombre de propositions pour que nous puissions effectivement nous saisir pleinement de cette opportunité...

1 Ses enjeux monétaires ont déjà été traités notamment par la « Revue de la régulation » en 2015 dans un papier de recherche intitulé « L'alternative monétaire Bitcoin : une perspective institutionnaliste » <http://journals.openedition.org/regulation/11489> et plus récemment par l'Institut Sapiens dans son rapport « Bitcoin : totem et tabou » <https://www.institutsapiens.fr/bitcoin-totem-et-tabou/>

I. LA DYNAMIQUE ENRAYÉE DE L'ÉCONOMIE NUMÉRIQUE ACTUELLE

Internet, lieu bouillonnant d'innovations, symbole de l'accélération de l'innovation, de la « disruption » permanente : cette idée a aujourd'hui du plomb dans l'aile. Phénomène inédit depuis la création du web : la décennie 2010, qui se termine dans moins de deux ans, n'a vu émerger aucun nouveau géant du numérique (à l'exception peut-être de Snapchat, loin toutefois de menacer réellement les leaders technologiques actuels). La décennie précédente avait pourtant vu l'ascension éclair de Facebook et Twitter, puis, dans un second temps, l'émergence d'Uber, Airbnb ou encore Blablacar. C'était l'ère du web 2.0, de l'économie collaborative, qui apportait un vent de fraîcheur sur l'économie numérique.

Aujourd'hui, la dynamique de l'économie numérique semble bloquée, accaparée par les GAFAs dont la surpuissance croissante constitue un danger pour l'innovation elle-même.

1/ Jamais la centralisation du web n'a été aussi forte, au profit d'acteurs non-européens

« Le web a commencé à mourir en 2014 ». C'est ce qu'affirme le développeur André Staltz dans un article paru fin 2017, où il analyse, statistiques à l'appui, la domination progressive des GAFAs sur le web occidental. Une poignée de services, détenus par quatre entreprises (Google, Apple, Amazon, Facebook), contrôlent désormais en effet la majeure partie de l'usage du web.

L'ampleur de ce phénomène déjà bien connu a pris une nouvelle dimension depuis quelques années. Deux exemples parmi d'autres témoignent de cette prise de pouvoir : Google et Facebook ont accaparé 92% de la croissance du marché de la publicité en ligne en 2017, et constituent aujourd'hui l'ultra majorité (plus de 70%) des sources de trafic vers les éditeurs de médias.

Si la domination de Google n'a rien de nouvelle, celle de Facebook est, elle, plus récente. Au-delà du seul réseau social, qui a doublé en cinq ans son nombre d'utilisateurs actifs dans le monde (2 milliards désormais)², la société Facebook n'a fait que renforcer sa position dominante sur les réseaux sociaux, puisqu'elle contrôle aujourd'hui trois autres applications maîtresses du web : Messenger, qui a progressivement pris une certaine autonomie par rapport au réseau social, Instagram depuis 2012, et Whatsapp depuis 2014.

« En France, les 10 applications les plus consultées sur les magasins d'applications appartiennent toutes aux GAFAs »

Les deux autres GAFAs, Amazon et Apple, accentuent eux aussi leur avance sur leur marché respectif : le premier se rapproche à grande vitesse la barre symbolique des 50% de part de marché du e-commerce aux Etats-Unis³, tandis que le second a déjà dépassé fin 2017 cette barre des 50% sur son marché phare, la vente de smartphones⁴. Les systèmes d'exploitation de Google et Apple équipent du reste aujourd'hui 99% des smartphones du monde⁵.

2 <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>

3 <https://www.retaildive.com/news/report-amazon-to-control-nearly-45-of-e-commerce-in-2017/508113/>

4 Etude Statista, 2018

5 <https://www.lesechos.fr/tech-medias/hightech/0301289389014-le-spectre-de-la-standard-oil-plane-sur-la-silicon-valley-2156606.php>

In fine, la domination de ces quatre géants sur le web occidental apparaît aujourd'hui comme totale : en France, les 10 applications les plus consultées sur les magasins d'applications appartiennent toutes aux GAFAs⁶.

Ce phénomène de centralisation se retrouve dans l'Internet chinois, de façon plus accentuée encore. L'application WeChat, détenue par le géant Tencent, constitue en effet un Internet dans l'Internet : à partir de cette seule application, les Chinois commandent leur taxi, règlent leurs factures, réservent leur billets de train et d'avions, leurs places de cinéma, paient dans les magasins et cafés, et bien sûr appellent et échangent avec leurs proches, puisque WeChat n'était initialement qu'un service de messagerie instantanée...L'application rassemble ainsi à la fois les fonctionnalités de Facebook, Whatsapp, Paypal, Instagram, Skype et bien d'autres. Aujourd'hui, WeChat compte plus de 900 millions d'utilisateurs, soit la moitié de la population chinoise et près du triple de la population américaine !

Cette centralisation, qui suscite des crispations, ne devrait pourtant aller qu'en s'accéléralant avec le développement de l'intelligence artificielle, ou IA. Loin de rebattre les cartes, l'IA risque de favoriser les géants technologiques déjà dominants : ces géants bénéficient en effet du meilleur accès qui soit aux données des internautes, qui constituent le carburant de l'IA.

Plus généralement, ces géants disposent d'une force de frappe financière inédite qui leur permet d'attirer les meilleurs talents mondiaux, de racheter les startups les plus prometteuses (ou dangereuses...) et d'exercer un lobbying surpuissant : en 2017, les GAFAs ont ainsi dépensé en lobbying près de 50 millions de dollars rien qu'aux Etats-Unis (24% de plus que l'année précédente⁷)

2/ Cette centralisation pose problème en particulier pour l'innovation elle-même

Pour acquérir puis renforcer leur position dominante actuelle, les GAFAs ont bénéficié d'un mécanisme bien connu dans le monde numérique : **l'effet de réseau**, théorisé par la loi de Metcalfe (selon laquelle l'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs). Cet effet a en particulier un corollaire : **il renforce les barrières à l'entrée pour les acteurs qui tenteraient de concurrencer les GAFAs**. A partir d'une certaine masse critique atteinte par une plateforme numérique, il devient en effet très difficile pour un concurrent de pouvoir la rattraper, ce qui conduit à un effet « winner-takes-it-all » où chaque vainqueur sur un marché ne fait, au fil du temps, que consolider plus fortement sa puissance.

Dans ces conditions, l'émergence de rivaux devient toujours plus difficile avec le temps. Les géants technologiques ont en effet à leur disposition plusieurs armes pour contrer de potentielles menaces, outre leur capacité à recruter les meilleurs talents et à financer les efforts d'innovation (notamment en intelligence artificielle) :

- comme énoncé par la loi de Metcalfe, leurs services en eux-mêmes ne font que s'améliorer grâce à l'arrivée de nouveaux utilisateurs, ce qui crée un effet boule de neige : cette amélioration de qualité de service attire en retour de nouveaux internautes. Ainsi, Facebook est d'autant plus attirant pour un internaute donné que le réseau compte comme utilisateurs plusieurs des proches de l'internaute, ce qui va l'inciter à s'inscrire sur ce réseau plutôt que sur un autre.

- lorsqu'un concurrent dangereux commence à émerger, les GAFAs tentent souvent de le racheter grâce à leurs moyens considérables. C'est ce qui a conduit Facebook à racheter Instagram en 2012 pour 1 milliard de dollars, et Whatsapp en 2014 pour 19 milliard de dollars (soit 11 fois le prix d'achat de YouTube par Google en 2006 !), de même que Microsoft avait racheté LinkedIn, que Google avait racheté YouTube, etc.

⁶ Etude Médiamétrie Février 2018 https://twitter.com/Mediametrie/status/966613328448622592/photo/1?ref_src=twsrc%5Etfw

⁷ <https://fr.statista.com/infographie/10396/les-gafa-rois-du-lobbying/>

-si l'entreprise refuse le rachat, les GAFAs n'hésitent pas à la copier et à incorporer ses atouts dans leurs propres services. Ainsi, après que Facebook a échoué à racheter Snapchat fin 2013 malgré une offre de 3 milliards de dollars⁸, Mark Zuckerberg a choisi de copier certaines fonctionnalités de Snapchat (les « stories », ces publications de photos ou vidéos éphémères) pour les inclure sur l'application Instagram rachetée précédemment. Outre une chute en Bourse momentanée de Snapchat, cette décision a permis à Facebook de limiter la croissance de son rival, au profit d'Instagram. Aujourd'hui, même si le réseau social Facebook voit son étoile pâlir, l'entreprise en elle-même reste le leader absolu des réseaux sociaux puisqu'elle possède Instagram. Il a fallu 7 ans à Snapchat pour construire une base de 150 millions d'utilisateurs grâce à des fonctionnalités inédites comme les « stories » ; il a fallu moins d'un an à Facebook pour surpasser cette base avec l'introduction des « stories » sur Instagram.

« Chaque GAFAs est en mesure de jouer de son pouvoir dominant sur son marché pour freiner l'arrivée de concurrents »

En outre, voire surtout, les caractéristiques propres aux plateformes numériques introduisent de barrières à l'entrée propres à l'économie numérique. Chaque acteur est en mesure de jouer de son pouvoir dominant sur son marché pour freiner l'arrivée de concurrents. Google est par exemple accusé depuis plusieurs années par Yelp (service de recommandations⁹ de sorties) de biaiser les résultats de son moteur de recherche, au profit de son propre service de recommandations. De la même façon, ProtonMail, qui propose un service d'emails chiffrés, a dénoncé en 2016 les agissements de Google (propriétaire de Gmail) qui aurait écarté volontairement ProtonMail de certains résultats de recherche pendant plus d'un an¹⁰. Sur certains mots-clés comme « email sécurisé » et « email chiffré », aucun lien n'était affiché sur Google vers ProtonMail, alors que les autres moteurs de recherche le plaçaient en première page.

Plus généralement, Google et Apple se retrouvent juges et parties sur certains choix qui sont de nature à bloquer l'entrée de concurrents sur leur marché. Comme l'explique Sébastien Soriano, président de l'ARCEP, « *aujourd'hui, une startup qui souhaite se lancer ne peut pas le faire aussi facilement qu'avant, notamment dans le mobile*¹¹ ». Les entrepreneurs qui se lancent dans une application sur smartphone font en effet face à une différence fondamentale vis-à-vis du web traditionnel : « *l'application doit être approuvée par le magasin d'applications. L'App Store ou Google Play va donc décider, en fonction d'un certain nombre de critères, si cette innovation est acceptable ou non. N'importe quelle startup qui veut se lancer aujourd'hui doit avoir une approbation soit d'Apple, soit de Google* ». Dès lors, Apple et Google peuvent refuser certains services de façon unilatérale. En 2016, Spotify affirmait ainsi qu'Apple refuserait probablement la nouvelle version de son application afin de ne pas concurrencer le service Apple Music.

Spotify affirmait ainsi qu'Apple refuserait probablement la nouvelle version de son application afin de ne pas concurrencer le service Apple Music.¹²

« Aujourd'hui, une startup qui souhaite se lancer ne peut pas le faire aussi facilement qu'avant »

⁸ <http://www.forbes.com/sites/jjcolao/2014/01/06/the-inside-story-of-snapchat-the-worlds-hottest-app-or-a-3-billion-disappearing-act/>

⁹ <https://techcrunch.com/2014/07/09/yelp-google-anti-trust/> et <https://www.wired.com/story/yelp-claims-google-broke-promise-to-anti-trust-regulators/>

¹⁰ <https://protonmail.com/blog/search-risk-google/>

¹¹ <https://www.april.org/la-neutralite-du-net-c-est-l-absence-de-censure-usbek-rica>

¹² <https://www.recode.net/2016/6/30/12067578/spotify-apple-app-store-rejection>

Comme l'exprime Sébastien Soriano, ce mécanisme « *pose une vraie question sur la capacité des startups d'aujourd'hui à devenir les Google de demain* », et ce d'autant plus qu'il ne concerne pas seulement les services qui entrent en concurrence directe avec les GAFA, mais aussi ceux que Google et Apple considère arbitrairement comme dangereux pour leurs utilisateurs : c'est par exemple le cas des services liés aux cryptomonnaies (et pourtant légaux), régulièrement voire systématiquement refusés de l'Apple Store. Pour tenter de contre-carrer cette surpuissance des GAFA qui menace la dynamique de l'économie numérique (le fondateur du web, Tim Berners-Lee, alerte lui-même : « *Il faut re-décentraliser le web* »), plusieurs pistes sont évoquées, dont l'idée d'un démantèlement - ce qu'avait réalisé le gouvernement américain avec la Standard Oil il y a plus de cent ans. Cette piste reste cependant controversée. In fine, même s'il est nécessaire d'étudier toutes les options pour rétablir une concurrence plus équilibrée, une approche plus offensive doit être adoptée, de façon complémentaire : puisqu'il sera difficile de battre les GAFA sur leur propre terrain, il est essentiel que la France et l'Europe investissent non seulement les terrains de demain, mais plus encore, ceux où ces géants ne seront pas à leur place.

Un grand domaine technologique répond aujourd'hui à ce critère : celui des technologies blockchain. Celles-ci sont en effet, dans leur nature et leur mode de fonctionnement, à l'opposé même des logiques des GAFA, qui n'ont absolument pas les codes de ce nouveau terrain d'innovation. Ce simple fait doit inciter les entrepreneurs, les acteurs économiques, les pouvoirs publics et les citoyens à s'intéresser de très près à ces technologies, et plus encore, à se saisir au plus vite des opportunités qu'elles ouvrent.

II. LA BLOCKCHAIN COMME RÉPONSE AUX LIMITES DU WEB ACTUEL

1/ La décentralisation permise par la blockchain permet de revenir aux principes originels d'Internet

Par nature, la blockchain s'oppose aux logiques du web actuel. Au cœur de cette technologie figure en effet une notion centrale : la décentralisation. Cette dernière se manifeste à plusieurs égards :

- La technologie blockchain permet de réaliser des échanges de valeur en pair-à-pair, c'est-à-dire directement d'un utilisateur A à un utilisateur B, sans passer par un quelconque intermédiaire ni nécessiter l'accord d'un tiers. Les transactions réalisées dans ce cadre sont validées et ajoutées au registre blockchain par des acteurs appelés mineurs, répartis partout dans le monde, et tous mis en compétition. Ceux-ci effectuent de puissants calculs pour tenter de résoudre un problème mathématique, dont la résolution leur permet de gagner des fractions de cryptomonnaies. Chacun peut devenir mineur en mettant à la disposition du réseau la puissance de calcul de son ordinateur. (Nb : le mécanisme présenté ici est celui de la blockchain historique, celle de Bitcoin, créée en 2009 et choisie dans ce paragraphe et le suivant par souci de simplicité¹³)

- Une blockchain est littéralement une chaîne de blocs, un registre, qui contient l'ensemble des transactions réalisées par ses utilisateurs. Ce registre, sécurisé par des mécanismes cryptographiques et économiques, est décentralisé : aucune entité centralisée n'en possède le contrôle. Aucun individu ni entité ne peut par exemple décider à lui seul de modifier ou supprimer une inscription. Le registre est partagé partout dans le monde sur des milliers d'ordinateurs, et ainsi détenu par l'ensemble de ses utilisateurs. La mise à jour du registre (ajouts de nouveaux blocs de transactions les uns à la suite des autres) est assurée par les mineurs, via le mécanisme cité ci-dessus.

- A partir de cette technologie, il est possible de construire des applications décentralisées (qui fonctionnent sur un réseau décentralisé, par opposition aux applications classiques qui dépendent de serveurs centralisés), dont il en existe déjà plusieurs centaines¹⁴, ainsi que des organisations décentralisées, appelées DAO (Decentralized Autonomous Organization), qui poussent la logique encore plus loin en décentralisant leur gouvernance elle-même ; ces dernières restent cependant encore avant tout expérimentales à ce jour.

Cette décentralisation permise par la blockchain explique pourquoi cette technologie est qualifiée de « *permissionless* » : ses utilisateurs n'ont en effet aucune autorisation à demander pour effectuer des échanges de valeur en pair-à-pair, inscrire une donnée dans le registre, valider les transactions, créer ou utiliser une application décentralisée, etc.

13 Par souci de simplicité est présentée ici uniquement la méthode de la « preuve de travail », aujourd'hui la plus répandue sur les blockchains publiques (Bitcoin en particulier). Il existe néanmoins d'autres algorithmes pour atteindre le consensus sur un réseau blockchain, qui fonctionnent de façon différente et ne nécessitent pas tous une mise en compétition par la puissance de calcul. La blockchain Ethereum vise le passage à un algorithme moins énergivore, la « preuve d'enjeu ».

14 Voir sur <https://www.stateofthedapps.com>

En ce sens, la blockchain constitue un retour à l'esprit originel d'Internet. Comme le rappelle Sébastien Soriano, *"Internet veut dire inter-networks, c'est-à-dire c'est un réseau de réseaux sur lequel tout le monde peut arriver avec son petit bout de réseau (son ordinateur personnel, l'ordinateur d'une entreprise...) et se connecter au grand réseau sans avoir à demander l'autorisation de quiconque. Là est vraiment la nature même d'Internet : cette interconnexion libre dans laquelle chacun peut consulter, regarder et poster librement"*.

Progressivement, cette décentralisation a été mise à mal avec le développement des GAFAs. Pour surfer sur le web, les internautes ont en effet commencé à passer de plus en plus par la médiation des services privés captifs, construits par-dessus les protocoles web publics. Ces services ont en effet développé une expérience utilisateur très travaillée, les rendant très attractifs pour les internautes. Ainsi, en théorie, tout internaute peut encore envoyer des emails via le protocole public SMTP créé pour ce faire dès les années 1970 ; néanmoins en pratique il préférera presque toujours utiliser un service simple d'utilisation et efficace comme Gmail.

L'autre point fort de ces services réside dans un aspect plus technique : leur capacité à conserver les multiples informations issues de leurs centaines de millions d'utilisateurs (likes, photos, commentaires, connections les uns aux autres, dans le cas de Facebook) dans de gigantesques bases de données, dont le stockage dans de grands centres de serveurs, très coûteux et particulièrement complexe, est financé et géré par les GAFAs. La création d'une base de données capable de tracer les interactions de l'ensemble de ces utilisateurs est une prouesse d'ingénierie que Facebook a été capable de réaliser grâce au recrutement de nombreux talents. Notons d'ailleurs que cette base de données est distribuée, puisqu'elle repose sur de multiples serveurs répartis partout dans le monde, et non décentralisée, puisque ces serveurs sont tous contrôlés par une même entité.

Cette nouvelle donne a impacté aussi bien les particuliers que les entreprises.

« En 2015, la France était le pays du monde où Facebook a supprimé le plus de pages, devançant l'Inde et la Turquie »

Pour les internautes, entre autres conséquences, l'utilisation des services des GAFAs leur imposent de laisser à ces derniers la gestion de leurs données personnelles. Les internautes doivent donc accepter de perdre le contrôle sur leurs données. En outre, chacun peut se voir interdire la publication de son contenu sur certaines plateformes numériques, de façon unilatérale. Les exemples de censure sur Facebook ne manquent pas (citons, entre autres, le cas en 2011 d'une image reproduisant la peinture « L'Origine du monde » de Gustave Courbet, dont la suppression s'était accompagnée de la fermeture du compte de l'internaute ; en 2012, d'une image d'un tableau de Gerhard Richter postée par la page du Centre Pompidou ; en 2016, de la célèbre photo "La fillette brûlée au napalm" prise en 1972 durant la guerre du Vietnam ; en mars 2018, d'une publicité représentant le tableau « La Liberté guidant le peuple » d'Eugène Delacroix avec Marianne seins nus ; etc.).

Pour les entreprises, le problème va au-delà de la liberté d'expression puisqu'il touche à des enjeux économiques. Facebook a en effet la capacité de désactiver et fermer des pages quand bon lui semble, sans en avertir en amont les administrateurs concernés. En France, outre des pages culturelles comme celle du musée du jeu de Paume en 2016, des journaux comme Le Monde ont déjà été confrontés à une désactivation temporaire de leur page Facebook, pour cause de publications jugées « non-conformes¹⁵ ». A l'heure où une partie importante du trafic dirigé vers les éditeurs provient des réseaux sociaux, on mesure à quel point une telle décision peut fragiliser le modèle économique d'un média ; et ce

15 <http://rezonances.blog.lemonde.fr/2012/12/14/quand-facebook-censure-le-monde-pour-une-photo-dactualite/>

d'autant plus que Facebook va parfois plus loin que la désactivation temporaire, en supprimant purement et simplement certaines pages, selon les critères qu'il s'est soi-même fixés. La France est d'ailleurs le pays du monde où Facebook a supprimé le plus de pages en 2015 (près de 38 000), devançant l'Inde et la Turquie¹⁶.

« Début 2018, un mois après la mise en place du nouvel algorithme de Facebook, un premier média mettait déjà la clef sous la porte, en licenciant ses cent salariés »

Au-delà de la seule question de la censure de contenus, et outre les enjeux cités plus haut concernant la difficulté des startups d'aujourd'hui à devenir les champions de demain, la domination des GAFAs a conduit à un autre problème : leur capacité à changer les règles du jeu avec leurs « partenaires » de façon unilatérale, quasiment du jour au lendemain. C'est ainsi que les médias ont appris soudainement début 2018 que Facebook s'apprêtait à modifier son algorithme de telle façon que les utilisateurs verraient moins de contenus issus de « pages », et plus de contenus venant de leurs proches. Un mois après la mise en place de ce nouvel algorithme, un premier média, le site féminin LittleThings dont 75% du trafic venait de Facebook, mettait déjà la clef sous la porte, en licenciant ses cent salariés¹⁷.

Loin d'affecter seulement les médias, le problème concerne de façon plus générale les entreprises et les entrepreneurs. Durant la phase initiale de leur croissance, les grandes plateformes ont en effet incité les entrepreneurs et les développeurs à utiliser leurs interfaces de programmation d'applications (API), qu'elles ont ouvertes à dessein. Une API peut être vue comme une porte d'entrée laissée ouverte par une plateforme pour que des tiers y développent des nouveaux services. Nous utilisons au quotidien de nombreuses API sans même le savoir : une des plus répandues au monde est ainsi l'API de Google Maps, qui permet aux développeurs d'intégrer une carte Google Maps sur leur site web.

L'intérêt des géants technologiques, en ouvrant leurs API durant leurs premières années, était clair : accroître la valeur ou l'usage de leurs plateformes, en profitant du travail et du talent d'entrepreneurs prêts à construire des services spécifiques. Ces entrepreneurs, en échange, profitaient de la qualité de service de ces plateformes, ainsi que, selon les types d'API, d'un accès inédit à de multiples utilisateurs potentiels.

La suite peut cependant s'avérer bien moins profitable aux entrepreneurs, puisque ceux-ci dépendent entièrement du bon vouloir des plateformes dans ce système. Comme l'écrit l'investisseur Chris Dixon dans un billet intitulé « Pourquoi la décentralisation importe¹⁸ », « plus une plateforme grandit, plus son pouvoir sur ses utilisateurs et les tierces parties s'accroît, jusqu'à atteindre un point critique où ses relations avec les participants du réseau passent d'un jeu à somme positive à un jeu à somme nulle. La façon la plus facile de continuer à croître réside alors dans l'extraction de données des utilisateurs et dans la concurrence avec les tierces parties sur les audiences et les profits ». C'est ainsi que Twitter a décidé en 2012 de limiter fortement la possibilité de développer des applications tierces sur sa plateforme¹⁹ ; cette décision fût très contestée²⁰, car certains entrepreneurs avaient construit des modèles d'affaires grâce aux API de Twitter, et ont donc dû fermer leurs activités. LinkedIn a pris la même décision en 2015, après avoir ouvert ses API durant plusieurs années²¹. Plus récemment, Google a annoncé fin 2017 la fermeture à venir de son API de référencement de vol, ce qui risque de mettre en péril de nombreux sites de référencement et réservation de vols. Google souhaite en effet développer ses propres services en la matière - et donc, là encore, centraliser l'innovation.

16 <https://www.journaldunet.com/ebusiness/le-net/1178058-la-france-grande-championne-de-la-censure-de-contenus-facebook-en-2015-statista/>

17 <http://www.businessinsider.fr/us/littlethings-online-publisher-shuts-down-and-blames-facebook-algorithm-2018-2?op=1>

18 <https://medium.com/@cdixon/why-decentralization-matters-5e3f79f7638e>

19 <https://www.theverge.com/2012/8/23/3263481/twitter-api-third-party-developers>

20 <http://lifehacker.com/5937648/whys-everybody-so-pissed-about-twitter-and-should-i-care>

21 <https://www.lemondeinformatique.fr/actualites/lire-linkedin-restreint-l-utilisation-de-ses-api-60236.html>

2/ Ce que permet la décentralisation de la blockchain

Par nature, la blockchain s'oppose aux logiques du web actuel. Au cœur de cette technologie figure en effet une notion centrale : la décentralisation. Cette dernière se manifeste à plusieurs égards :

Il apparaît dès lors plus clairement pourquoi l'émergence de technologies décentralisées peut être souhaitable. **Une plateforme décentralisée, fondée sur une blockchain, n'aurait en effet pas la possibilité de censurer un contenu, d'interdire un échange entre deux utilisateurs, de désactiver ou fermer une page s'il s'agit d'un réseau social, ou encore de changer son algorithme, ses fonctionnalités ou ses conditions d'utilisation, de façon unilatérale. Avec la blockchain, le créateur d'une plateforme décentralisée n'en est plus le maître absolu : il n'en est que le concepteur et l'initiateur.**

Ces principes ont conduit à la création de premières applications qui utilisent la blockchain pour décentraliser des usages existants. Citons ainsi OpenBazaar, sorte d'Ebay décentralisé ; Storj, qui propose de décentraliser les plateformes cloud comme celle d'Amazon ; DTube, variante décentralisée de YouTube ; etc. Sur chacune de ces plateformes, aucun administrateur central ne peut exercer de censure sur les contenus postés, bannir un utilisateur donné, changer unilatéralement les règles de fonctionnement, ou plus globalement s'immiscer dans les échanges entre utilisateurs.

Ces applications, qui consistent avant tout à décentraliser certains usages du web 2.0, sont cependant loin de résumer à elles seules les atouts de la blockchain pour l'économie numérique. La décentralisation de cette dernière, couplée à ses autres caractéristiques, apporte **plusieurs autres avantages majeurs** :

A/ L'échange de rareté numérique en pair-à-pair

Elle permet d'abord de surmonter un problème encore non-résolu jusqu'à présent : échanger, sur Internet, de la valeur fondée sur de la rareté en pair à pair, c'est-à-dire d'un individu à un autre, sans passer par une autorité centrale.

Illustration concrète : aujourd'hui, lorsqu'un internaute A envoie un fichier à un internaute B sur Internet (document écrit, vidéo, chanson...), l'internaute B ne reçoit en réalité pas le fichier en lui-même, mais une copie. L'internaute A, de son côté, conserve son fichier. Ce système, qui fonctionne bien pour les fichiers échangés sur Internet, n'est pas viable pour les actifs de valeur fondés sur de la rareté : si l'internaute A envoie 1 euro à l'internaute B et conserve en même temps cet euro, celui-ci perd de sa valeur. Internet tel qu'il est conçu empêche donc de pouvoir s'envoyer de la rareté numérique de pair à pair, sans passer par une autorité centrale comme une banque.

Ce problème fondamental est résolu par la blockchain. Son exemple d'application le plus connu à ce jour est la possibilité de transférer un bitcoin d'une personne A à une personne B, sans devoir passer par un quelconque tiers, et sans avoir besoin de compte bancaire (rappelons que 2 milliards d'adultes sur Terre n'ont pas de compte bancaire). Lorsque A envoie un bitcoin à B, aucune copie du bitcoin n'est créée, et A ne le possède plus.

« Internet empêche de pouvoir s'envoyer de la rareté numérique de pair à pair, sans passer par une autorité centrale. Ce problème fondamental est résolu par la blockchain »

Ce qui est valable pour le bitcoin l'est également pour de multiples autres actifs numériques échangeables via la blockchain. Ces actifs, pouvant être créés par tout internaute, sont appelés tokens, ou « jetons » en français (présentés dans la troisième partie).

In fine, la blockchain est à la valeur ce qu'Internet a été à l'information.

Internet a permis de décentraliser l'information. Avec Internet, tout individu a pu s'emparer d'un pouvoir inédit : publier et échanger l'information qu'il veut, instantanément, auprès du monde entier, sans devoir en demander la permission.

La blockchain permet de décentraliser la valeur. Avec la blockchain, tout individu s'empare d'un nouveau pouvoir : créer et échanger de la valeur, avec l'internaute qu'il veut, instantanément, sans nécessiter la permission d'un quelconque tiers.

B/ La (re)prise de contrôle pour l'internaute de ses données personnelles, et, au-delà, de son identité numérique

a/ Les problèmes actuels du web en matière d'identité

La question de l'identité numérique est un des grands manques des protocoles publics développés par les fondateurs d'Internet. Ces derniers n'ont pas créé de standard sécurisé et ouvert qui aurait permis d'établir une identité numérique sur le réseau. Dans le monde réel, l'identité des individus ne constitue pas un marché, puisque les numéros de cartes d'identité, de passeports, de sécurité sociale, sont émis par des autorités centralisées, liées aux Etats le plus souvent. Dans le monde numérique, les acteurs privés, et en particulier Facebook, se sont engouffrés dans la brèche laissée ouverte par l'absence de règles et de protocoles standardisant l'identité. Facebook, dont la majorité des droits de vote est détenue par une seule personne (Mark Zuckerberg), contrôle les données qui définissent l'identité numérique de deux milliards d'individus aujourd'hui dans le monde.

Comme l'explique Sajida Zouarhi, Architecte Blockchain au sein de la société Consensys, « *le web 2.0, composé des plateformes comme Facebook, YouTube, LinkedIn, est un « ami toxique » pour ses utilisateurs. Certes, il apporte des services exceptionnels, mais l'utilisateur ne contrôle pas ses données et doit signer des conditions d'utilisation déséquilibrées. Celles d'Instagram par exemple sont terrifiantes : ils peuvent faire tout ce qu'ils veulent de vos photos. L'internaute est contraint de faire confiance aux plateformes pour gérer convenablement ses données* ».

L'appel du fondateur du web à reprendre le contrôle sur nos données

A la suite du scandale Cambridge Analytica impliquant Facebook, le fondateur du web lui-même, Tim Berners-Lee, a écrit ces mots sur Twitter en mars 2018 : « *C'est un moment sérieux pour le futur du web. Mais je veux que nous restions optimistes. Les problèmes que nous voyons aujourd'hui sont des bugs dans le système. Les bugs peuvent créer des dégâts, mais ils sont créés par les gens, et peuvent être fixés par les gens. Règles générales pour nous tous : toute donnée à mon propos, où qu'elle soit, est mienne et doit être sous mon contrôle. Mon message à tous les utilisateurs du web aujourd'hui est le suivant : j'ai beau avoir inventé le web, mais c'est vous qui en faites ce qu'il est. Cela tient à nous tous de construire un web qui reflète nos espoirs et réalise nos rêves plus qu'ils renforcent nos peurs et agrandit nos divisions. Continuez de vous battre pour le web que vous voulez. Le web ne réalisera pas son potentiel sans vous²² ».*

En outre, notre identité numérique est aujourd'hui fragmentée entre de multiples services captifs : Facebook, mais aussi Google (via par exemple nos contacts sur Gmail), Amazon (via nos historique d'achats, pages consultées et donc produits susceptibles d'être achetés à l'avenir), etc. La portabilité de ces différentes identités fait aujourd'hui défaut. Ainsi, les utilisateurs qui souhaiteraient quitter Facebook pour rejoindre un autre réseau social (plus respectueux de leur vie privée, ou mettant l'accent sur d'autres fonctionnalités) ne peuvent pas transférer leur identité construite sur Facebook : ils doivent la reconstruire depuis le départ sur la nouvelle plateforme.

²² https://twitter.com/timberners_lee/status/976623317808484352

Enfin, les systèmes d'identification en silo du web actuel posent des problèmes de sécurité. Les internautes utilisent fréquemment les mêmes mots de passe pour leurs multiples comptes, ce qui est très risqué. En outre, les piratages de plateformes pouvant conduire à des vols de mots de passe surviennent régulièrement. Yahoo, LinkedIn, Dropbox ont notamment déjà été touchés par des piratages de données.²³

b/ En quoi la blockchain constitue-t-elle une solution ?

La blockchain peut permettre à l'internaute de se réappropriier son identité numérique et ses données personnelles (de son historique d'achat jusqu'à son réseau d'amis, en passant par ses informations personnelles). Plutôt qu'une approche en silo, où l'identité numérique est contrôlée par chaque plateforme, c'est une approche holistique qui est privilégiée, avec un seul maître de chaque identité : l'utilisateur lui-même. Cette approche permet en outre de fortement limiter les risques de sécurité cités ci-dessus.

Le grand concept sous-jacent est celui d'identité auto-souveraine (« self-sovereign identity »), dont découle celui de données auto-gérées (« self-managed data »). « *Il est impossible de construire des self-managed data sans self-sovereign identity : vos données sont liées à vous* » explique Sajida Zouarhi. Plusieurs projets blockchain travaillent sur ces questions, parmi lesquels uPort.

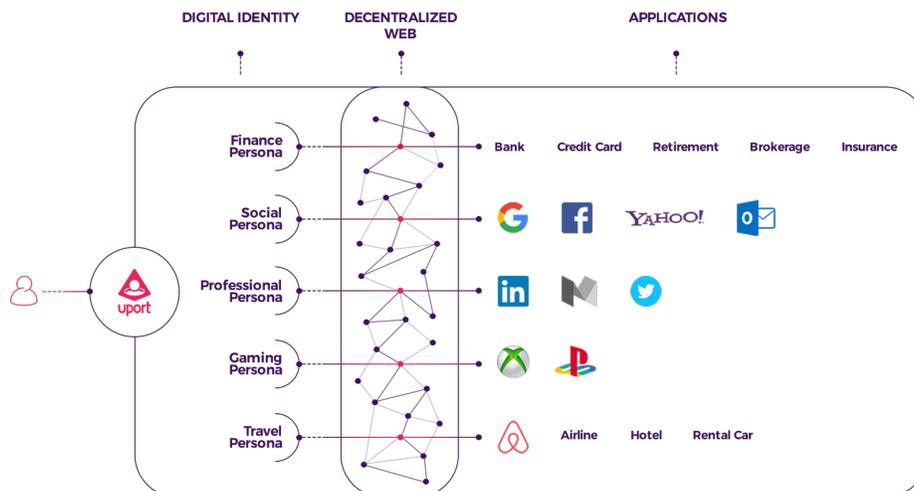
Le projet uPort veut permettre à ses utilisateurs de choisir les services qui accéderont à leurs données : ils auront ainsi le pouvoir d'autoriser et de révoquer les accès²⁴, tout en conservant l'historique des requêtes. L'utilisateur pourra également rendre certaines requêtes payantes, de façon à monnayer ses données.

Pour ce faire, l'utilisateur se connectera à une application mobile, elle-même reliée à un contrat numérique qui représentera son identité. Ce contrat fera le lien entre la blockchain (utilisée alors comme autorité de certification d'identité) et les services qui voudront accéder à l'identité numérique de l'utilisateur.

Les pirates informatiques auront bien moins d'incitation économique à attaquer ce système car ils pourraient seulement s'en prendre à un utilisateur à la fois, au lieu d'attaquer un serveur sur lequel sont stockés des millions de mots de passe.

c/ Une identité à plusieurs facettes

Un principe clef sous-tend le mécanisme présenté ci-dessus : l'idée selon laquelle chaque utilisateur a une identité unique mais contextuelle. Autrement dit, l'individu pourra présenter une certaine facette de son identité selon le contexte (financier, social, professionnel...), sans avoir à présenter toute son identité.



23 Liste des grands sites ayant été victimes de piratages de données : <https://haveibeenpwned.com/PwnedWebsites>

24 Voir la présentation de uPort <https://www.ethereum-france.com/uport-ou-la-gestion-de-lidentite-par-la-blockchain/>

« Ce principe de facettes se traduit au niveau de l'architecture technique par plusieurs verticales qui se rejoignent toutes au niveau d'une même base, constituée de l'identité de l'utilisateur », explique ainsi Sajida Zouarhi, qui développe au sein de l'équipe Ethcompute (chez Consensus) un protocole de partage de données et de calcul décentralisé visant à être interopérable avec uPort.

Les silos du web actuel sont alors déverrouillés, ce qui rend possible, par nature, une interopérabilité des données. « Pour les applications, et les startups qui les développent, n'importe quelle verticale sera un point d'entrée. L'utilisateur pourra autoriser une nouvelle application à accéder à ses données déjà existantes : l'application nouvellement installée pourra par exemple accéder à des informations sur les données des 3 derniers mois de l'utilisateur. Ce principe change complètement la façon dont seront construites les applications ».

Les applications pourront ainsi profiter des données longitudinales, c'est-à-dire le fait qu'un même individu crée des données, sources de valeur, toute sa vie durant. « La blockchain est utilisée dans ce cadre pour stocker et gérer l'accès à ces données. Cette gestion sera effectuée avec des règles définies par l'utilisateur et exécutée par la blockchain, qui ne fera que respecter les directives données » explique Sajida Zouarhi.

Ce mécanisme ouvre la voie à des croisements de données au sein d'un écosystème où toutes les parties prenantes – utilisateurs, entreprises existantes, entrepreneurs – peuvent être gagnantes. « L'idée n'est pas d'exclure qui que ce soit, mais de remettre l'individu au centre. Si tout le monde coopère, chaque acteur peut bénéficier de ce système ». Confidentialité et sécurité des données sont alors compatibles avec performances économiques : en effet, un tel système permettrait d'aboutir à des résultats qui ne peuvent pas être atteints aujourd'hui (en l'absence de base commune permettant une interopérabilité entre les données des applications). Comme le présente Sajida Zouarhi, « les accès seront contrôlés par l'utilisateur en passant par une autorité décentralisée grâce à la blockchain, en lieu et place d'une autorité centralisée comme Facebook par exemple. Tout sera interopérable par défaut ».

Ces possibilités ne signifient pas pour autant qu'un bousculement des règles du jeu se produira en quelques mois. Un grand travail reste encore à réaliser pour atteindre ces promesses, qui seront sans doute amenées à s'affiner. Comme l'explique Michael Casey, conseiller principal de la Digital Currency Initiative du MIT Media Lab, « nous ne sommes pas en train de dire que demain vous pourrez actionner un interrupteur et qu'une blockchain règlera tous les problèmes [liées aux données]. Ce qui importe est le fait qu'elle ouvre la voie à une nouvelle manière de considérer ces problèmes auxquels nous faisons face ».

C/ Une sécurité inédite

La décentralisation de la blockchain apporte un niveau de sécurité inédit au niveau de sa couche protocolaire (rappelons que certains sous-jacents techniques d'Internet sont bien plus fragiles qu'ils ne le semblent²⁵). Cette sécurité tient au moins à deux aspects, comme l'écrit Vitalik Buterin, fondateur de la blockchain Ethereum²⁶ :

-le risque de pannes : « les systèmes décentralisés ont moins de chances de tomber en panne accidentellement, car ils reposent de multiples éléments distincts » ;

-la résistance aux attaques : « les systèmes décentralisés coûtent plus chers à attaquer et détruire ou manipuler, car ils n'ont pas de points centraux sensibles qui, eux, peuvent être attaqués à un coût bien plus faible que la taille économique du système qui les entoure ».

25 Voir par exemple le discours de Danny Hillis intitulé « Internet pourrait planter. Il nous faut un plan B » (TED, 2013) https://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b

26 <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>

La blockchain de Bitcoin, malgré son caractère sulfureux, constitue ainsi l'une des blockchains les plus sécurisées au monde si ce n'est la plus sécurisée, en raison non seulement de la décentralisation de son registre (il n'existe aucune entité centrale à pirater, et pirater un ordinateur parmi les milliers d'autres ne changerait rien à la sécurité du réseau), mais également pour des raisons d'incitations économiques. Certains considèrent même que la résistance de Bitcoin constitue une prouesse inégalée à ce jour en termes de sécurité informatique.

Pour le comprendre, il faut d'abord rappeler qu'un système informatique est sûr non pas quand il est inattaquable – ce qui est théoriquement impossible –, mais quand il coûte trop cher à attaquer. Bitcoin rend justement l'attaque informatique trop chère et non-intéressante économiquement : un acteur ayant une très grande puissance de calcul a en effet plus intérêt à participer au bon fonctionnement du réseau (en validant les transactions, ce qui lui fera gagner de la cryptomonnaie) qu'à essayer de l'attaquer. Ce mécanisme constitue une force inédite du réseau Bitcoin, qui permet d'ailleurs de comprendre pourquoi les critiques sur le coût énergétique de Bitcoin sont elles-mêmes très contestées : elles omettent le fait que cette dépense énergétique est la condition d'une sécurité inédite au monde.

En ce sens, la blockchain de Bitcoin, dont la valeur de marché dépasse début avril 2018 les 110 milliards de dollars, constitue l'un des Graal de la sécurité informatique que des milliers de hackers et chercheurs tentent de pirater sans succès depuis de nombreuses années. Qui-plus-est, même si un (groupe de) surdoué(s) y parvient un jour, son butin s'effriterait rapidement sous ses yeux : le cours de la cryptomonnaie associée à cette blockchain s'effondrerait probablement, rendant le piratage bien moins profitable économiquement, et l'ensemble des utilisateurs basculeraient sur une autre chaîne, créée à partir de la chaîne initiale. Ce mécanisme, appelé fork, est clef dans la gouvernance des blockchains. Il sera explicité plus en détails dans la troisième partie.

D/ Une nouvelle dynamique d'innovation

Enfin, et c'est tout l'objet de cette note, ces technologies rendent possible une dynamique d'innovation plus saine car plus équilibrée. Avec la blockchain, le pouvoir ne réside plus dans la main unique de géants comme les GAFAs. Certes, plusieurs champions émergeront très certainement grâce à ces technologies, et pourront être amenés, eux aussi, à concentrer un grand nombre d'utilisateurs, cependant :

- Ces ascensions seront le fait de tout nouveaux acteurs, ce qui doit inciter la France et l'Europe à produire les efforts nécessaires pour, cette fois-ci, ne pas rater le coche.

- Ces acteurs devraient être moins captifs que les GAFAs pour deux raisons : d'une part, le code des applications décentralisées sera par nature open source (chacun pourra y accéder et le copier-coller pour créer des dérivés, à condition de respecter une licence donnée) à la différence de celui des GAFAs ; d'autre part, les plateformes décentralisées introduiront des logiques qui ne seront plus « maître-esclave », à l'opposé de celles des GAFAs qui disposent d'un pouvoir unilatéral, mais pair-à-pair.

- Enfin, la blockchain permettra par nature à de nouveaux acteurs, grâce à des mécanismes d'incitations économiques regroupés sous le terme de cryptoéconomie et présentés dans la troisième partie, de concurrencer bien plus facilement les futurs grands acteurs du secteur, ce qui pêche justement dans l'économie numérique actuelle.

In fine, la décentralisation de la blockchain permet bel et bien de contrecarrer les déséquilibres du web actuel. **Après des années de centralisation où les GAFAs se sont emparés du contrôle d'Internet, la blockchain ouvre la voie à un retour de balancier.**

Cependant, plus encore qu'un retour à une situation originelle, elle permet surtout l'émergence d'une nouvelle économie numérique, avec de nouveaux acteurs, de nouvelles règles, de nouvelles stratégies.

III. LA BLOCKCHAIN ET LES TOKENS OUVRENT LA VOIE D'UNE NOUVELLE ÉCONOMIE NUMÉRIQUE

La blockchain rebat les cartes du monde numérique : si l'intelligence artificielle constitue une nouvelle étape de l'économie numérique, la blockchain ouvre la voie à une nouvelle économie numérique à elle seule.

Pour la découvrir et la comprendre, il convient au préalable de lever certains malentendus sur les technologies blockchains et les cryptomonnaies.

1/ Blockchain et cryptomonnaies : déconstruire deux malentendus

La technologie blockchain et les cryptomonnaies sont parfois, si ce n'est souvent, considérées sous le mauvais angle. Deux grands malentendus se sont installés.

a/ Le premier est de considérer que la blockchain seule comme la véritable révolution, et les cryptomonnaies comme une anecdote de l'histoire.

Ce point de vue, répandu, est adopté par nombre de grands acteurs institutionnels, économiques et financiers, en particulier parce qu'il permet de passer outre les problématiques épineuses des cryptomonnaies, à la réputation sulfureuse. Lister les avis exprimés en ce sens serait infini, tant ceux-ci sont ceux défendus par nombre de grandes figures, jusqu'à Jean Tirole, prix Nobel d'économie, très critique des cryptomonnaies mais qui tient à préciser que son « scepticisme » ne concerne pas la blockchain, une « innovation bienvenue » à ses yeux.²⁷

Il est effectivement possible de construire et utiliser une blockchain sans cryptomonnaie : c'est le principe des blockchains privées. Celles, souvent développées au sein d'entreprises et d'institutions publiques, peuvent faire entièrement sens. L'intérêt d'une blockchain -registre transparent, incorruptible et distribué entre toutes ses parties prenantes - est alors triple :

- responsabiliser chaque acteur sur ce qu'il y est inscrit, afin de maximiser les chances d'avoir une base de données « propre » et de pouvoir détecter plus rapidement, en cas de problème, quel acteur a commis une erreur ou une fraude ;
- répartir le coût de gestion du fichier sur l'ensemble des acteurs de cette blockchain privée ;
- régler le problème politique de la propriété du registre, puisque la propriété devient techniquement répartie entre tous les acteurs.

Entre autres applications, la mise en place de blockchains privées peut améliorer la traçabilité en logistique, dans l'agroalimentaire, le luxe, les transports, le commerce international, l'aéronautique et l'automobile pour les pièces détachées, etc. Ce type de blockchains est par ailleurs testé depuis plusieurs années par les acteurs bancaires, qui y voient la perspective d'économies importantes grâce, notamment, à une réduction des coûts d'infrastructure.

²⁷ Tribune de Jean Tirole dans le Financial Times en novembre 2017 <https://www.ft.com/content/1c034898-d50f-11e7-a303-9060cb1e5f44>

Cependant, aussi intéressantes soient-elles pour les organisations en termes de réduction de coûts et de sécurisation, les applications de blockchain privées, intra-entreprises ou entre plusieurs entreprises, relèvent d'une logique d'optimisation, et non d'innovation radicale. La blockchain en elle-même n'est qu'un registre.

Pour dresser le parallèle avec Internet, les blockchains privées constituent l'équivalent des intranets, c'est-à-dire des réseaux restreints à certains utilisateurs spécifiques, loin de l'innovation radicale qu'a été Internet.

Comme l'écrit Laurent Bénichou, directeur de l'innovation d'Axa et fin connaisseur du sujet, pour en exploiter tout son potentiel « *il faut penser la blockchain en termes d'innovation, et non en termes d'IT²⁸* ». « *Arrêtez de transformer la fièvre blockchain en projets IT ennuyeux* » appelle-t-il, en critiquant le remplacement du terme blockchain par l'expression « distributed ledger technology » qui désignent les blockchains privées, décorrélées de l'innovation apportée par les cryptoactifs.

Soyons donc clairs : l'innovation de rupture viendra uniquement des cryptomonnaies et des protocoles publics, et non des blockchains privées. Ce point de vue commence du reste à être partagé par plusieurs acteurs de l'économie « traditionnelle », comme le cabinet de conseil EY²⁹ ou des entreprises comme Carrefour, dont le PDG, Alexandre Bompard, a déclaré récemment que « *la crypto n'est pas un phénomène de mode qui passera : c'est quelque chose de puissant et l'on ne pourra pas passer à côté de cette transformation-là³⁰* » - signe que ces enjeux commencent à être compris au-delà des sphères « tech ».

b/ Le deuxième malentendu concerne les cryptomonnaies elles-mêmes. Leur appellation pose problème pour appréhender la nouvelle économie numérique, car elle est trop restrictive.

Le terme de cryptomonnaies enferme le débat autour de la notion de monnaie. Ce débat conduit à une guerre des tranchées entre

-ceux qui affirment que les cryptomonnaies ne peuvent en aucun cas être considérées comme des monnaies (le plus souvent, des économistes), parce qu'elles ne « reposeraient sur rien » ou parce qu'elles ne coheraient pas les trois critères de la définition habituelle d'une monnaie (unité de compte, moyen de paiement, réserve de valeur) ;

-et ceux qui considèrent le contraire, arguant notamment du fait que l'euro et le dollar ne reposent pas plus sur un quelconque actif tangible depuis la fin de l'étalon-or, et soulignant l'idée selon laquelle les cryptomonnaies permettent d'empêcher l'usage de la méthode controversée de la « planche à billets » abondamment utilisée par les banques centrales depuis la crise de 2008.

Ce débat, qui n'en est du reste pas un puisque les points de vue sont très rarement confrontés en direct (à quand la tenue d'un face-à-face entre un économiste critique des cryptomonnaies, comme Jean-Marc Daniel, et un spécialiste reconnu du sujet, comme Jacques Favier ou Alexandre Stachtchenko ?), occulte un aspect essentiel. Les cryptomonnaies ne constituent désormais qu'un pan du sujet. Il est nécessaire de considérer également les tokens (jeton numérique), car ceux-ci constituent un des outils majeurs de la nouvelle économie numérique qui s'ouvre³¹.

28 <https://medium.com/@laurentbenichou/counter-chemists-please-stop-transforming-blockchain-fever-into-it-boredom-58f39f1c24f4>

29 Lire l'analyse du Global Innovation Leader for blockchain du cabinet EY : <https://www.coindesk.com/public-blockchains-lure-will-become-irresistible-enterprises-2018/>

30 <https://twitter.com/ArnaudLeRoux/status/978695148845617154>

31 Sur les tokens, lire l'article visionnaire de Balaji S. Srinivasan : <https://news.earn.com/thoughts-on-tokens-436109aabcb>

Qu'est-ce qu'un token ?

Un token est un actif numérique émis et échangeable sur une blockchain, et qui présente plusieurs atouts clefs :

- Comme une cryptomonnaie, il peut être transféré (sans duplication) entre deux parties en pair-à-pair, c'est-à-dire sans nécessiter l'intervention ou l'accord d'un tiers. Il possède également les autres caractéristiques d'une cryptomonnaie : infalsifiabilité, unicité, enregistrement des échanges dans un registre immuable, sécurité des échanges, etc.
- Il peut être créé par tout internaute.
- Il est personnalisé par son créateur, afin de pouvoir être utilisé (le plus souvent) dans une application décentralisée. A ce titre, il peut représenter, par exemple, un droit d'usage d'un produit ou service blockchain ; un droit de vote ; un droit d'auteur ; un moyen de paiement ; une réputation ; ou encore, plus globalement une unité de valeur d'échange au sein d'une application décentralisée ou d'un écosystème donné.
- Il peut être vendable et achetable à tout moment, en particulier sur des plateformes d'échange à un prix fixé en temps réel par l'offre et la demande. Il est donc très liquide.

Exemples :

▪ **Storj est un service de stockage cloud décentralisé** qui n'est utilisable qu'en faisant usage d'un token appelé Storjcoin. Tout utilisateur peut louer l'espace libre de son ordinateur sur le réseau en échange de Storjcoin, et inversement peut acheter de l'espace de stockage sur le réseau Storj contre des Storjcoin. En résumé, lorsqu'un utilisateur achète ou reçoit des Storjcoin, il peut ensuite soit acheter de l'espace sur le réseau (à un coût censé être moindre qu'avec les services existants, et sans devoir placer ses fichiers chez un tiers de confiance), soit les garder dans une perspective de spéculation, soit les convertir dans sa monnaie traditionnelle (euro, dollar...).

▪ **iExec est un projet franco-chinois qui vise à développer une place de marché décentralisée de la ressource de calcul** (un « Airbnb du serveur » pour reprendre l'expression de son fondateur Gilles Fedak) : tout utilisateur, particulier comme professionnel, pourra louer la puissance de calcul inutilisée de son ordinateur ou de ses data centers sur le réseau, en échange de tokens iExec. Inversement, tout utilisateur pourra acheter de la puissance de calcul avec des tokens sans devoir payer pour l'infrastructure, celle-ci étant décentralisée.

De multiples applications sont envisageables, notamment en intelligence artificielle, en recherche médicale, en cybersécurité, etc. Des entreprises, par exemple du secteur industriel, pourraient utiliser ce service lorsqu'elles ont besoin de plus de puissance de calcul lors de certains pics d'activité, sans devoir posséder le matériel le plus puissant qui soit.

La notion de tokens montre que les technologies blockchain n'ont pas toutes vocation, loin de là, à disrupter les systèmes monétaires existants. Chris Dixon, investisseur réputé du monde du capital-risque aux Etats-Unis, dit ainsi « aimer ce terme de token parce qu'il souligne clairement la similarité avec un jeu d'arcade : vous vous y rendez, et au sein de ce jeu d'arcade, vous pouvez utiliser ces tokens. Ils ne visent pas le remplacement des monnaies traditionnelles, mais à être utilisé au sein de ce monde³² ». Dan Finlay, créateur de l'application blockchain Metamask, abonde en ce sens : « Ce qui est intéressant avec les tokens est le fait que nous programmons de nouveaux systèmes de valeur, qui n'ont pas à rassembler de la monnaie ».

Plutôt que de cryptomonnaies, il est préférable de parler de cryptoactifs afin de rendre compte de la variété des actifs numériques sur la blockchain. Le terme de cryptoactif permet en effet de couvrir l'ensemble des actifs échangeables sur une blockchain :

- les cryptomonnaies, comme le bitcoin, qui permettent de faire fonctionner une blockchain publique ;
- les tokens, qui fonctionnent le plus souvent par-dessus une blockchain publique.

Une part croissante des acteurs du secteur et des régulateurs emploient désormais le terme de cryptoactifs. La Banque de France prône par exemple depuis début 2018 ce terme en lieu et place de cryptomonnaies³³.

Les cryptoactifs doivent être considérés comme une nouvelle classe d'actifs à part entière³⁴, qui diffère radicalement des autres. Ainsi, comme le montre le spécialiste Chris Burniske dans son ouvrage « Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond » paru fin 2017, le bitcoin est extrêmement peu corrélé aux autres actifs (actions du S&P 500, pétrole, or, bonds américains, immobilier). L'étude des mouvements du bitcoin de 2011 à 2017 montre qu'il est indifférent aux mouvements des classes d'actifs traditionnelles.

Les cryptoactifs ont un rôle majeur : permettre l'émergence et l'utilisation d'applications décentralisées. De ce fait, ils ouvrent la voie à un nouveau web, le web décentralisé, mené par de nouveaux acteurs, qui suivent de nouvelles logiques économiques.

2/ De nouveaux acteurs

Les acteurs du web décentralisé sont différents de ceux du web actuel, du moins aujourd'hui. Les règles de ce nouveau web étant fondamentalement distinctes de celles du web 2.0 (voire plus bas), les acteurs à l'aise dans l'économie numérique actuelle, à commencer par les fonds de capital-risque, doivent explorer et comprendre les nouvelles logiques à l'œuvre s'ils veulent pouvoir jouer un rôle dans ce nouveau domaine.

Aujourd'hui la Silicon Valley n'est pas le point central dans ce nouveau monde ; les codes et les mentalités des GAFA et des startups « classiques » sont sensiblement différents de ceux du web décentralisé. Aux Etats-Unis le centre de gravité de la blockchain est au moins autant sur la côte Est (New York) que sur la côte Ouest (San Francisco).

Plus globalement, il faut noter que les Etats-Unis ne disposent pas d'une hégémonie particulière en matière de cryptoactifs. Les montants des Initial Coin Offerings ou ICO, ces levées de fonds en cryptoactifs (présentées plus bas), se répartissent ainsi assez équitablement entre Amérique du Nord, Europe et Asie³⁵. L'Europe est même citée dans une étude d'octobre 2017 comme le premier continent en montants levés en ICO (46% des montants) et en nombre de levées (40% des ICO).³⁶

32 <https://mobile.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html>

33 <https://www.banque-france.fr/sites/default/files/medias/documents/adp-07032018.pdf>

34 Lire l'analyse du fondateur de la startup Chain, Adam Ludwin <https://blog.chain.com/a-letter-to-jamie-dimon-de89d417cb80>

35 Voir visuellement la répartition géographique des montants levés en ICO : <https://elementus.io/blog/token-sales-visualization/>

36 <https://www.coindesk.com/report-european-startups-take-in-half-of-all-ico-funding/>

Il est vrai qu'un pays en particulier tire fortement ces chiffres : la Suisse. Selon une étude de Pwc, un quart des d'ICO dans le monde ont été réalisées en Suisse, et en particulier dans le Canton de Zoug, surnommé la « Crypto Valley » par sa position unique de « hub » de référence dans le monde sur les cryptoactifs. Au-delà de sa fiscalité incitative pour les startups (14,6% d'impôts sur les sociétés), la Crypto Valley s'est construite sur une politique d'accueil volontariste vis-à-vis des organisations blockchain, avec de nombreux signes de bienveillance et de bonne volonté sur ces technologies témoignés par les pouvoirs publics (qui ont par exemple lancé un projet pilote pour pouvoir payer ses impôts en bitcoin). Le Canton de Zoug, et plus particulièrement la ville éponyme, attire ainsi un grand nombre de projets blockchain. Plusieurs projets de pointe se sont ainsi basés à Zoug pour leur levée en ICO (Ethereum, Tezos, Bancor, Cosmos et bien d'autres).

De son côté, l'Asie est bien positionnée dans le monde des cryptoactifs grâce à plusieurs pays leaders que sont la Corée du Sud (où un sondage récent, effectué par la Banque de Corée, montre que 40% des jeunes adultes sont désireux de détenir des cryptoactifs³⁷), Singapour, le Japon, la Chine et Hong Kong³⁸. Pour plusieurs spécialistes, il est même probable que l'usage grand public des cryptoactifs commencera en Asie, que ce soit en Corée du Sud (qualifiée de « patient zéro » par l'observateur Sizhao Yang qui parle de « viralité du virus crypto³⁹ ») ou au Japon (qui reconnaît officiellement le bitcoin comme moyen de paiement depuis 2017).

De façon générale, à la différence du web actuel, les grands acteurs du web décentralisé ne sont pas spécialement américains. La blockchain phare du web décentralisé, Ethereum, qui par nature n'est pas liée à un pays particulier, a ainsi été créé en 2015 par un développeur russo-canadien, Vitalik Buterin. Sa valeur de marché est aujourd'hui supérieure à 35 milliards de dollars soit, à titre de comparaison, pratiquement la valeur de marché combinée de Twitter et Snapchat.

Vitalik Buterin, 23 ans, est aujourd'hui la personnalité phare du monde blockchain (l'inventeur de la blockchain Bitcoin restant inconnu). Le magazine Fortune l'a du reste placé dans sa liste des personnalités de moins de 40 ans les plus influentes du monde business, aussi bien en 2016 (31e) qu'en 2017 (10e), aux côtés de personnalités comme Emmanuel Macron et Mark Zuckerberg.

Ethereum est à la fois un protocole blockchain et une plateforme sur laquelle sont développées des applications, et vise un objectif : non pas créer un système de cash électronique pair-à-pair comme Bitcoin, mais ouvrir la voie à un nouveau web, constitué de multiples applications décentralisées, appelées DApps dans l'univers Ethereum. Il en existe aujourd'hui plus de mille, qui sont la plupart à leurs premiers stades de développement et qui sont construites par des développeurs partout dans le monde.

D'autres protocoles plus jeunes, comme EOS (tout juste naissant, mais qui a déjà levé plus de 800 millions de dollars) ou NEO (porté par une équipe chinoise qui vise un développement en conformité avec les réglementations étatiques), ambitionnent eux aussi de s'imposer comme des infrastructures de référence de ce nouveau web. Ils accusent aujourd'hui un retard important sur Ethereum ; néanmoins, les technologies blockchain et le monde des cryptoactifs n'étant encore qu'à leurs débuts, il serait prématuré, si ce n'est impossible, d'affirmer avec certitude quels protocoles sortiront gagnants à terme.

Autour de chaque protocole blockchain (pouvant être porté, notamment techniquement, par une fondation à but non-lucratif, comme la fondation Ethereum), se développent des écosystèmes composés de multiples acteurs. Au cœur de ces écosystèmes se situent les entrepreneurs et plus encore les ingénieurs et développeurs spécialisés en blockchain (perles rares très convoités), qui créent des applications décentralisées ou des outils connexes - par exemple pour accéder aux applications, pour suivre les transactions sur le réseau, etc.

37 <https://www.coindesk.com/report-european-startups-take-in-half-of-all-ico-funding/>

38 Voir <https://www.smithandcrown.com/observations-geography-token-sales/>

39 <https://threadreaderapp.com/thread/966214870327799809.html>

D'autres acteurs gravitent autour de ce noyau : citons ainsi des fonds de capital-risque focalisés uniquement sur les cryptoactifs, comme Polychain ; des « agences de notation » des projets d'ICO, comme ICOBench ou ICORating ; des sites spécialisés dans les statistiques relatives à la « token économie » comme TokenData ; etc.

« Les blockchains qui attirent les développeurs en quantité et en qualité ont toutes les chances d'être celles qui s'imposeront à l'avenir »

Aujourd'hui, les multiples possibilités ouvertes par les tokens (qui sont créés avant tout sur Ethereum à l'heure actuelle⁴⁰) et notamment les ICO (Initial Coin Offering), présentées plus bas, expliquent en grande partie le dynamisme de l'écosystème Ethereum. La force d'Ethereum réside dans sa communauté de développeurs qui est une des plus importantes, si ce n'est la plus importante, du monde blockchain. Or les blockchains qui attirent le plus de développeurs (talentueux) ont toutes les chances d'être celles qui s'imposeront à l'avenir - c'est-à-dire d'être utilisées « naturellement » par les entrepreneurs et les utilisateurs, de façon massive, à terme. Néanmoins, répétons-le encore : toutes les options restent ouvertes à ce stade de la « course ». Il y a bel et bien une bataille des protocoles, et donc de leurs écosystèmes associés, qui est engagée et loin d'être terminée.

Segmentation du marché du web décentralisé

Les investisseurs Joel Monegro et Chris Burniske présentent ainsi la façon dont ils se représentent schématiquement les acteurs du web décentralisé :

« Nous segmentons le marché en trois couches : la couche protocolaire, la couche applicative et la couche composée des interfaces utilisateurs.

La couche protocolaire est composée des protocoles d'infrastructures, sur lesquels travaillent les développeurs. Les tokens associés à ces protocoles offrent l'accès à des composants essentielles du web décentralisé comme l'identité, la puissance de calcul, de stockage, etc.

La couche applicative est composée des applications décentralisées, ou « DApps », qui reposent sur les protocoles d'infrastructure et sont destinées aux utilisateurs finaux. L'étendue des applications potentielles est infinie : tout ce qui constitue un réseau d'informations peut être transformé en application décentralisée (or il s'avère que la plupart de l'économie est un réseau d'informations d'une certaine façon).

Enfin, les utilisateurs finaux interagissent avec ces réseaux à travers une variété d'interfaces utilisateurs indépendantes. Certaines interfaces offrent des fonctionnalités additionnelles, mais fonctionnent sans tokens. Les plateformes d'échange de cryptoactifs font par exemple partie de cette catégorie, de même que les applications mobiles permettant d'accéder aux DApps [comme par exemple Metamask, une application qui fait le pont entre le web actuel et le web décentralisé, en permettant d'accéder à ce dernier à partir d'un navigateur web classique]. Ces interfaces reposent le plus souvent sur des business models traditionnels comme la publicité, les commissions ou l'abonnement⁴¹. »

40 A noter que le principe des tokens pré-existait à Ethereum : le protocole Bitcoin a rendu possible en premier la possibilité de personnaliser des « coins » pour représenter des actifs réels, via la notion de « colored coins ».

41 <https://ipfs.io/ipfs/QmZL4eT1gxnE168Pmw3KyejW6fUfMNzMgeKMgcWJUfYGRj/Placeholder%20Thesis%20Summary.pdf>

3/ De nouvelles logiques économiques

Les caractéristiques des cryptoactifs, et en particulier des tokens, en font le pilier d'une nouvelle économie numérique, dans laquelle émergent de nouvelles stratégies et règles.

a/ Un nouveau partage de la valeur

Les tokens permettent de mieux partager la valeur créée par une organisation et ses parties prenantes. Comme l'explique Philippe Honigman⁴², fin connaisseur des enjeux de gouvernance et des technologies blockchain, une part importante « *des organisations modernes sont passées d'un mode autarcique où toute la valeur était créée en interne, à un mode plus ouvert sur leur écosystème* », via les notions de plateforme et d'open innovation notamment. Cependant, cette valeur créée à plusieurs est le plus souvent « *capturée dans la "trappe à rente" de l'organisation centrale. Les tokens permettront à tous les acteurs, internes et externes, d'accéder à une juste part de la valeur future créée par la conjonction de leurs efforts* ».

Avec l'économie des tokens, la valeur économique est en effet distribuée au travers d'une communauté bien plus large que la seule entité (commerciale ou non) qui cherche à grandir. Ce mécanisme permet ainsi :

-de rémunérer financièrement les contributeurs d'un service. Aujourd'hui, les plateformes numériques traditionnelles permettent déjà de rémunérer les contributeurs en les « rétribuant » en notes de réputation (« quatre étoiles sur cinq » par exemple, pour un utilisateur qui serait particulièrement compétent ou actif, tel qu'un chauffeur Uber). Les tokens changent cependant la donne : ce travail pourra être rémunéré de façon financière directement, ce qui constitue sans doute une incitation bien plus forte à devenir (bon) contributeur.

-d'aligner toutes les parties prenantes (les fondateurs du projet, les développeurs, les utilisateurs, les investisseurs et tierces parties) sur un objectif commun⁴³ : maximiser la croissance du service, et ainsi la valeur du token. Ce token, quel que soit le statut ou la fonction de son détenteur, pourra en effet être revendu ensuite plus cher que son coût d'achat (permettant une plus-value à son détenteur) ou utilisé dans le service en question avec un meilleur « pouvoir d'achat ».

Cet alignement des parties prenantes grâce au token constitue un bouleversement vis-à-vis des modèles existants, dans lesquels les parties prenantes extérieures à l'organisation - à commencer par les utilisateurs - ont relativement peu d'incitations à améliorer la qualité du service, à le faire connaître, et à le voir croître.

Exemple : le réseau social Steemit

Steemit est une plateforme décentralisée sur laquelle chacun peut poster du contenu et voter pour celui des autres. Il propose à ses utilisateurs de recevoir une récompense pour leurs publications jugées intéressantes par la communauté, non pas (seulement) en « likes » mais également en tokens, créés spécialement pour le service.

La curation de contenus est elle aussi récompensée : les utilisateurs qui votent pour des contenus peuvent eux aussi recevoir des tokens, à condition que ces contenus ne soient pas encore populaires sur la plateforme et le deviennent par la suite.

Ce mécanisme, qui récompense les contributions et l'attention des utilisateurs, permet d'inciter chacun à poster et/ou repérer du contenu intéressant, ce qui doit profiter in fine à la qualité de la plateforme, et donc à son expansion.

⁴² <https://www.linkedin.com/pulse/la-blockchain-agent-de-d%C3%A9centralisation-des-luc-bretones/>

⁴³ Ce mécanisme a été présenté mi-2017 par l'investisseur Chris Dixon dans son billet « Crypto Tokens: une avancée dans la conception de réseaux ouverts » : <https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef>

A noter que les lignes entre les différentes parties prenantes de ces services sont poreuses, ce qui conduit à de nouvelles logiques économiques :

- Un internaute détenteur des tokens peut les avoir acquis dans un pur objectif d'investissement financier, puis décider de les conserver pour devenir par la suite utilisateur, après avoir découvert (plus en détails) l'utilité qu'il peut tirer du service ;
- Inversement, un internaute a pu avoir acquérir les tokens dans l'objectif d'utiliser le service, puis changer d'avis sur celui-ci, et agir alors dans un seul but d'investissement ;
- Autre possibilité : un internaute peut décider d'aider à la construction du service lui-même, afin de faire grandir la valeur du token qu'il possède. Ceci peut s'envisager par exemple via des actions de communication sur le service, ou même avec une aide plus directe (développement technique du code, etc.), ce qui peut donner lieu à une rémunération supplémentaire en tokens décidée par l'organisation qui dirige le service.

En somme, c'est bel et bien un nouveau partage de la valeur créée qui émerge grâce aux tokens, à la fois plus équitable et ouvrant de nouvelles pistes économiques.

b/ L'effet de réseau inversé

Jusqu'alors, figurer parmi les utilisateurs pionniers d'un service numérique n'était pas récompensé ; c'était même le contraire, puisque les grands succès du numérique se sont développés avec l'effet de réseau, règle fondamentale de l'économie numérique selon laquelle la valeur d'un service numérique augmente plus que proportionnellement à chaque nouvel utilisateur. Le plus souvent, un internaute donné a donc tout intérêt à attendre qu'une plateforme numérique gagne en puissance avant de la rejoindre.

BlaBlaCar présentait par exemple peu de valeur à ses débuts, puisque très peu de covoiturages étaient proposés. Plus le maillage territorial de BlaBlaCar s'est affiné grâce à l'arrivée de nouveaux utilisateurs, plus la valeur du service a grandi (de façon exponentielle). Arrivé à un certain stade de développement, BlaBlaCar est devenu incontournable pour le covoiturage : il est désormais pratiquement impossible à un concurrent d'émerger sur le même créneau, sauf proposition de valeur radicalement nouvelle. Toute la difficulté, pour BlaBlaCar comme pour les autres plateformes numériques, a été de faire grandir son nombre d'utilisateurs à ses débuts.

Les tokens bousculent ce paradigme en ajoutant à l'effet de réseau traditionnel un effet de réseau inversé, fondé sur les tokens. Le mécanisme est le suivant : un projet, qui en est souvent à ses premiers pas, décide d'émettre ses propres tokens, ayant pour vocation d'être utilisés dans le service en question – par exemple comme droit d'accès ou d'usage du service, ou comme moyen de paiement, ou comme niveau de réputation, etc. De ce fait, les internautes qui estiment le service prometteur (aussi bien pour eux-mêmes que pour l'ensemble des utilisateurs) sont incités à acquérir le token (et ainsi à rejoindre le réseau) le plus tôt possible, au moment où ce token présente une valeur encore relativement faible par rapport à ce qu'il pourra valoir.

L'intérêt de l'internaute est alors simple : miser sur le développement à venir du service, ce qui permettra d'accroître la valeur du token. Ainsi, il pourra ensuite soit revendre le token à tout moment et réaliser alors une plus-value, soit l'utiliser dans le service en question.

« L'effet de réseau inversé permettra à des services numériques d'émerger bien plus facilement, et de lutter contre l'effet winner-takes-it-all dont bénéficient aujourd'hui les GAFAs »

Le mécanisme de l'effet de réseau inversé permettra à des services numériques d'émerger et de se développer bien plus facilement, et ainsi de lutter contre l'effet winner-takes-it-all dont bénéficient aujourd'hui les GAFAs. Jusqu'ici, les startups tentaient toutes les ruses pour réduire le blocage lié à l'effet de réseau : Facebook avait ainsi débuté en aspirant la base de données des étudiants d'Harvard ; Airbnb avait créé un robot qui postait automatiquement ses annonces de logement sur Craigslist (l'équivalent du site LeBonCoin aux Etats-Unis) ; etc.

Avec les tokens, plutôt que d'attendre qu'un service soit suffisamment développé pour s'y inscrire, les internautes seront encouragés (financièrement) à le rejoindre très en amont, ce qui permettra d'accélérer la création de viralité autour du service, et donc de booster son développement initial. Si un service est jugé utile et apporte une valeur ajoutée, il parviendra ainsi à grandir et donc à rivaliser plus facilement avec les acteurs déjà installés sur le marché.

c/ Les ICO : les levées de fonds du web décentralisé

Le mécanisme des ICO (Initial Coin Offering) vise justement à bénéficier de l'effet de réseau inversé présenté ci-dessus. Il s'agit d'une méthode de levée de fonds qui permet aux fondateurs d'un projet (à but lucratif ou non) de financer et booster les premières étapes de développement du projet - d'où le terme « initial » - sans diluer leur capital. Concrètement, l'organisation à l'origine d'une ICO émet ses propres tokens (qui ne représentent pas des parts de l'organisation), qu'elle vend à des internautes disposant de cryptomonnaies. Les internautes font l'acquisition de ces tokens (sorte de pré-achat) avec l'espoir que le service, et donc le token, prendra de la valeur.

Les ICO ont connu un engouement spectaculaire à partir de 2017, où l'équivalent de plus de 5 milliards de dollars ont été levés via cette méthode –plus que les montants levés en phase d'amorçage en capital-risque par l'ensemble des entreprises Internet ! En ce sens, les ICO constituent pour beaucoup la première « killer app » de la blockchain, c'est-à-dire sa première application (relativement) grand public.

Il est vrai que les ICO offrent plusieurs avantages aux entrepreneurs, outre le fait de ne pas avoir à diluer le capital de la société.

Elles leur permettent d'abord de s'affranchir de certaines contraintes des levées de fonds traditionnelles. Ce mécanisme permet de lever des sommes qui auraient difficilement pu être levées avec le système de capital-risque classique, et ce pour deux raisons :

-les porteurs de projets n'ont la plupart du temps pas encore de premier produit ni même de prototype, lorsqu'ils effectuent leur ICO. Cela correspond donc à la phase d'amorçage en capital-risque, voire pré-amorçage. Or les montants levés en ICO sont régulièrement (pour le meilleur et pour le pire) de l'ordre des montants levés en série A, série B voire parfois série C, en capital-risque !

-les ICO ont une portée globale, ce qui signifie qu'elles permettent de s'adresser aux internautes du monde entier, qui peuvent avoir d'autres critères de jugement que les acteurs du capital-risque (VC). De ce fait, l'accès au capital se fait de façon plus égalitaire. Un projet démarré en Afrique est en théorie sur un pied d'égalité avec un projet démarré dans la Silicon Valley. En particulier, puisque le processus de financement est décentralisé, faire financer son projet par des investisseurs américains, par exemple, n'oblige plus les porteurs de projets à se rendre physiquement aux Etats-Unis.

Les ICO vont cependant au-delà de l'outil de financement, ce qui est parfois oublié. Elles permettent en effet de créer un effet de réseau grâce au token, comme présenté plus haut, ce qui est censé servir de boost pour le projet.

Enfin, les ICO permettent à des projets de construire une communauté de pré-utilisateurs, et d'ambassadeurs, avant même le lancement (et même la construction) de leur service.

Ces atouts ont conduit à une croissance exubérante et irrationnelle du marché des ICO depuis mi-2017, qui se manifeste par des levées considérables pour des projets parfois peu sérieux. Cette tendance, que l'on peut qualifier de bulle, est logique : il s'agit des premiers pas des ICO. Une correction est prévisible. En parallèle, une professionnalisation du marché a commencé à s'effectuer depuis début 2018, avec le développement d'acteurs spécialisés en accompagnement d'ICO, l'arrivée d'investisseurs de la finance « traditionnelle » (family offices, fonds de VC, etc.), et la mise en place de nouvelles exigences par les régulateurs, qui devraient permettre de distinguer les projets sérieux des autres.

Malgré le phénomène médiatique et financier qui les entoure, les ICO ne sont qu'un des outils rendus possibles par cette nouvelle économie numérique. En ce sens, elles constituent l'arbre qui cache la forêt. Le plus important réside surtout dans la notion de token, dont les perspectives sont bien plus vastes. In fine, si les ICO font autant parler depuis l'an dernier, la raison en est principalement quantitative, liée aux montants spectaculaires qui sont levés ; à l'inverse, les progrès des protocoles blockchain et de leurs applications, et le bouillonnement intellectuel sur ces technologies, ne sont pas (aussi) quantifiables, mais mériteraient bien plus d'attention. Du reste, les projets blockchain les plus prometteurs sont loin d'être systématiquement ceux ayant réalisés les plus grandes ICO...

Enfin, deux éléments de réflexion méritent d'être ajoutés sur ce sujet :

-Avec les ICO, le secteur créé sa propre valeur, puisque les entrepreneurs créent leurs tokens ex-nihilo, et s'auto-financent en partie, puisque ces tokens sont achetés en cryptoactifs, dont la possession résulte parfois d'acquisition d'autres tokens (dont la valeur a pu progresser).

-Les ICO, aujourd'hui devenues très médiatiques, se sont développées dans un contexte qu'il est utile de (re)situer : à leurs débuts, les projets blockchain n'avaient pas d'autres choix que de se financer en ICO. Il était en effet quasiment impossible d'être financé par les acteurs traditionnels (banques, fonds de capital-risque...) qui ne comprenaient alors pas ces technologies et jugeaient le risque trop important. Sans ICO, Ethereum n'existerait probablement pas aujourd'hui.

d/ Les « protocoles lourds »

Les protocoles clefs de l'économie numérique, en particulier celui à l'origine d'Internet (TCP/IP) et du web (HTTP), sont nés du travail de chercheurs. Or la grande majorité des chercheurs qui ont créé ces protocoles en ont tiré très peu de gains financiers directs. La captation de valeur s'est faite au profit des plateformes construites par-dessus les protocoles existants (Google, Facebook, etc.), c'est-à-dire au profit des acteurs de la couche applicative et non protocolaire. C'est cette captation de valeur qui a permis aux GAFA d'acquérir la puissance dont ils jouissent aujourd'hui.

« A l'inverse du web actuel, les plus grands gagnants du web décentralisé ne devraient pas être des applications, mais des protocoles »

Dans le web décentralisé, la relation entre protocoles et applications se renverse. C'est la théorie dite des « protocoles lourds⁴⁴ » selon laquelle, dans le monde blockchain, la valeur se concentre dans la couche protocolaire ; seule une partie de la valeur est distribuée tout au long de la couche applicative. Selon cette théorie, la valeur d'un protocole blockchain augmente plus fortement que la valeur combinée des applications construites par-dessus. Ceci s'explique par le fait que le succès d'une application construite sur un protocole blockchain ne fait, logiquement, que renforcer la valeur du protocole lui-même, par rapport aux autres protocoles blockchain. Un protocole sera donc d'autant plus fort (et son token vaudra d'autant plus cher) qu'un grand nombre d'entrepreneurs choisit de construire des applications par-dessus.

44 Joel Monegro, 2016 : <https://www.usv.com/blog/fat-protocols>

Cette notion explique la vive compétition que se livrent aujourd'hui les protocoles dans l'écosystème blockchain. Si la théorie des « protocoles lourds » se vérifie au fil du temps, les plus grands gagnants du web décentralisé ne devraient pas être des applications, mais des protocoles, c'est-à-dire des blockchains publiques (comme Bitcoin ou Ethereum).

e/ Le financement de protocoles open source et non-lucratif

L'architecture technique d'Internet a peu évolué depuis le XXe siècle. Cette architecture, qui n'avait pas été pensée pour une utilisation aussi massive du réseau, présente des fragilités souvent méconnues⁴⁵. En outre, comme expliqué dans la partie deux de cette note, les protocoles publics sur lesquels reposent Internet sont incomplets : il manque en particulier un standard relatif à l'identité numérique (créneau dans lequel s'est engouffré Facebook). Le développement de nouveaux protocoles permettrait de combler certains de ces problèmes. Un tel travail implique cependant des investissements très conséquents, ce qui nécessite souvent une aide publique, étant donné que les acteurs technologiques privés n'ont que rarement intérêt à financer un protocole open source et non-lucratif.

Cette dépendance au financement public est fragile. Il faut non seulement convaincre les pouvoirs publics de l'importance de ces dépenses, mais aussi parvenir à conserver ses financements au fil du temps. Dans les années 1970, des chercheurs français, parmi lesquels Louis Pouzin, travaillèrent sur des protocoles qui se révélèrent ensuite précurseurs à ceux d'Internet, avant de se voir couper l'accès au financement par le gouvernement français, alors persuadé que l'avenir était dans le minitel et pas dans Internet. Les travaux de Louis Pouzin furent repris par deux chercheurs américains, Robert Kahn et Vinton Cerf, qui développèrent le protocole TCP/IP sur lequel repose aujourd'hui Internet.

Internet aurait-il été inventé par un Français si les tokens avaient existé en 1970 ? A minima, Louis Pouzin aurait eu là un moyen de continuer à financer ses travaux, ce qui aurait pu être décisif. En effet, avec l'économie des tokens, les créateurs d'un protocole peuvent désormais monétiser leur travail et ainsi gagner en indépendance financière : ils peuvent faire appel aux internautes, non pas avec un appel aux dons comme avec le crowdfunding, mais avec une émission de tokens que les internautes peuvent acquérir (dans une perspective de spéculation ou d'utilisation future du token dans le réseau).

Ce mécanisme bouleverse la donne en termes d'innovation protocolaire⁴⁶. Les chercheurs et développeurs, d'ordinaire « aspirés » par les géants technologiques qui leur proposent des conditions très avantageuses, peuvent désormais (très bien) gagner leur vie en travaillant de façon indépendante sur des innovations au niveau de la couche protocolaire, et embaucher eux-mêmes les meilleurs talents qui les aideront à construire les protocoles de demain.

En outre, l'incitation à travailler sur les protocoles est d'autant plus forte que tout porte à croire, aujourd'hui, que le géant du monde blockchain de demain sera un (ou des) protocole(s) et non une application, comme expliqué plus haut avec la théorie des protocoles lourds.

Les fondateurs de la blockchain Ethereum ont financé de cette façon le développement de leur protocole via une émission de tokens (appelés « ethers ») en 2014, ce qui leur a alors permis de lever l'équivalent de 18 millions de dollars. En 2014, 1 ether valait 0,145 €. Aujourd'hui (début avril 2018), 1 ether vaut plus de 350€. Les fondateurs du protocole ayant conservé un grand nombre d'ethers, leur force de frappe financière est aujourd'hui considérable. Le magazine Forbes estime ainsi que la fortune personnelle de Joe Lubin, cofondateur d'Ethereum, est comprise entre 1 et 5 milliards de dollars⁴⁷. La valeur de marché d'Ethereum avoisine quant à elle aujourd'hui les 35 milliards de dollars.

45 Voir par exemple le discours de Danny Hillis intitulé « Internet pourrait planter. Il nous faut un plan B » (TED, 2013) https://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b

46 Ce mécanisme a été présenté par l'investisseur Albert Wenger en 2016 : <http://continuations.com/post/148098927445/crypto-tokens-and-the-coming-age-of-protocol>

47 <https://www.forbes.fr/finance/classement-forbes-cryptofortune-les-plus-grosses-fortunes-de-la-cryptomonnaie/>

4/ Un nouveau domaine d'étude : la cryptoéconomie

A/ Qu'est-ce que la cryptoéconomie ?

Les différentes stratégies économiques présentées ci-dessus font partie d'un tout appelée cryptoéconomie. Ce terme constitue un nouveau champ d'étude à part entière. Il peut être défini comme la combinaison de principes notamment cryptographiques, d'incitation économique et de théorie des jeux, visant à concevoir des protocoles et applications décentralisées et robustes.

« Les réseaux pair-à-pair et chiffrés pré-existaient aux réseaux blockchain, mais manquaient jusque-là d'un élément clef : des mécanismes d'incitation économique alignant les parties prenantes vers un objectif commun »

Sous cette perspective, la blockchain ne consiste pas - ou pas uniquement - en un système monétaire indépendant et décentralisé, mais en une technologie et un nouveau champ économique qui utilise des mécanismes incitatifs pour établir de nouveaux types de réseaux : des réseaux dans lesquels les interactions entre les parties prenantes sont construites de façon à faire grandir la valeur du réseau pour tous.

Les systèmes pair-à-pair fondés sur des principes cryptographiques ne sont pas nouveaux : ils pré-existaient à Bitcoin. Citons ainsi les réseaux pair-à-pair Kazaa, Emule et Bittorent. Il manquait cependant un aspect essentiel à ces réseaux décentralisés, qui explique (en partie) le fait qu'ils n'aient pas prospéré : l'existence de mécanismes d'incitation économique alignant l'ensemble des parties prenantes vers un objectif commun. En d'autres termes, l'ensemble des parties prenantes n'étaient pas toutes incitées à participer au bon fonctionnement et à la croissance de ces réseaux.

C'est ce que permet de résoudre la cryptoéconomie, dont l'objectif est de créer des réseaux pair-à-pair sécurisés qui prospèrent au fil du temps. Pour ce faire, la cryptoéconomie s'appuie en effet deux notions essentielles : les tokens, qui permettent d'aligner les parties prenantes vers un objectif commun comme vu précédemment, et la notion de « fork ».

B/ Le fork comme moyen de faire défection

La notion de « fork » est au cœur de la cryptoéconomie. Un fork (un « embranchement ») désigne la création d'une nouvelle « branche » d'une blockchain, à la fois indépendante de la chaîne initiale mais qui se base sur la chaîne développée jusqu'à l'embranchement.

Un fork se produit souvent suite à un désaccord au sein des communautés d'acteurs d'une blockchain (en particulier les mineurs et les développeurs) sur certains choix de gouvernance.

Il peut être vu à travers le prisme de la théorie « Exit, Voice and Loyalty » d'Albert Hirschman, publié dans son ouvrage éponyme en 1970. Hirschman montre (entre autres) que tout individu insatisfait de la gestion d'un groupe auquel il appartient dispose de deux façons de réagir : quitter le groupe (Exit), ou prendre la parole (Voice) pour faire savoir son mécontentement et proposer des améliorations.

Dans le contexte des blockchains, un acteur insatisfait peut décider de quitter une blockchain soit en revendant ses cryptomonnaies (ce qui est une façon silencieuse de faire défection), soit en réalisant un « fork » et en créant ainsi une blockchain concurrente, ou alternative, qui reflète ses préférences et ses valeurs.

Cette nouvelle blockchain disposera de sa propre cryptomonnaie. Si ce nouvel embranchement parvient à attirer une partie importante des acteurs au détriment de la branche originelle, cette dernière devrait voir le cours de sa cryptomonnaie diminuer, au profit de la cryptomonnaie de la nouvelle branche.

Le grand avantage du fork est qu'il permet de répliquer non seulement le code informatique mais aussi l'état des données du réseau jusqu'à l'embranchement. Dans le web 2.0, si un entrepreneur insatisfait souhaite quitter Facebook pour créer un autre réseau social, il doit repartir de zéro, y compris en termes de base de données. Les réseaux blockchains fonctionnent différemment : tout acteur peut quitter un réseau donné et en créer un nouveau, en conservant ce qui a été réalisé jusqu'à la création de la nouvelle branche.

Chacun peut donc tenter de construire ce qu'il considère comme étant un meilleur réseau, de façon permissionless (sans devoir en demander la permission).

Comme l'explique l'entrepreneur Fred Ehrsam, « *dans le modèle actuel [du web], tout le profit et le pouvoir d'un réseau est aux mains d'une seule entreprise. Avec les blockchains, il devient possible de créer des structures de pouvoir complètement différentes. La capacité de forker réduit considérablement l'emprise des systèmes sur les individus et accroît leur diversité, en autorisant bien plus d'expérimentations*⁴⁸ ». La possibilité de forker offre une meilleure « égalité des chances » pour un nouveau compétiteur, puisque celui-ci n'a plus à redémarrer de zéro pour lancer son réseau ; de ce fait, le fork permet de lutter contre l'effet « winner-takes-it-all » présent dans le web actuel.

Une des contreparties du fork est néanmoins qu'il réduit les effets de réseau (qui peuvent conduire d'habitude à cet effet « winner-takes-it-all ») dont aurait pu bénéficier la chaîne initiale si elle n'avait pas été divisée en deux.

Pour cette raison, un des grands défis des communautés blockchains à l'heure actuelle est d'améliorer la capacité des acteurs à prendre la parole (Voice) et à se faire entendre, pour éviter que les choix des acteurs soient réduits au statu quo (Loyalty) ou à la défection (Exit). Cette capacité à pouvoir s'exprimer, être écouté et dialoguer est en effet encore limitée aujourd'hui. Dans cette optique, l'écosystème blockchain doit mettre l'accent sur la mise en place de meilleurs mécanismes de gouvernance, ce sur quoi travaillent plusieurs acteurs comme les fondateurs du projet Aragon⁴⁹.

Un nouveau type de management et de leader

La notion de fork transforme le management des organisations dans le monde des cryptoactifs. C'est ce que présentent les investisseurs Joel Monegro et Chris Burniske ci-dessous, qui expliquent que les choix d'investissements des fonds de capital-risque devront s'adapter :

« En raison de la possibilité des forks, il est critique de sélectionner des fondateurs avec un fort leadership et des compétences de gestion de communauté. Dans le monde des cryptoactifs, l'équipe idéale diffère de celle d'un business traditionnel : un style de management ouvert, transparent, inclusif et collaboratif réussira mieux qu'un management hiérarchique traditionnel. Impliquer la communauté dans le développement du protocole et dans la prise de décision, et leur donner du pouvoir en mettant en place des mécanismes de gouvernance de communauté, est clef pour construire des communautés loyales et engagés qui soutiendront le token sur le long terme.

*L'expertise dans un domaine et la capacité d'exécution restent deux choses importantes, mais tout autant que choisir des équipes dirigées par des fondateurs dont l'engagement à la promesse de la décentralisation est plus fort que leur désir de faire de l'argent. Le marché actuel est rempli d'opportunités cherchant à faire du profit rapidement. Mais les fondateurs qui sont motivés avant tout par le profit ont plus de chances d'être focalisés sur l'appréciation à court terme plutôt que sur la création de valeur à long terme pour le réseau. Ces individus là peuvent réussir à attirer de l'argent rapidement, mais ne peuvent pas engager et diriger des communautés*⁵⁰. »

48 Voir l'article de Fred Ehrsam traduit en français par Philippe Honigman sur Ethereum France <https://www.ethereum-france.com/gouvernance-blockchain-programmer-notre-futur>

49 Voir par exemple <https://blog.aragon.one/thoughts-on-governance-and-network-effects-f40fda3e3f98>

50 <https://ipfs.io/ipfs/QmZL4eT1gxnE168Pmw3KyejW6fUfMNzMgeKMgcWJUfYGRj/Placeholder%20Thesis%20Summary.pdf>

5/ Les cryptoréseaux, un changement de paradigme pour l'économie numérique

Les acteurs au cœur du web décentralisé ne sont pas nécessairement des entreprises, comme le sont les acteurs du web 2.0, mais peuvent être des réseaux, que l'on peut appeler « cryptoréseaux » (du terme anglais « cryptonetworks »). Ceux-ci peuvent être définis comme des « réseaux décentralisés construits sur les protocoles Internet, capables de fournir différents services numériques (stockage de données, puissance de calcul, applications...) », comme le présente l'investisseur américain Nick Grossman⁵¹.

« Certains cryptoréseaux, comme Ethereum, sont des plateformes générales qui peuvent être utilisées pour presque n'importe quel but. D'autres cryptoréseaux sont plus spécialisés, et se concentrent par exemple sur le stockage de fichiers décentralisé [comme le projet Storj présenté plus haut] ou sur l'offre de puissance de calcul décentralisée [comme le projet iExec] » précise l'investisseur Chris Dixon⁵².

Les tokens jouent un rôle clef au sein des cryptoréseaux : ils représentent d'une part les monnaies internes de ces réseaux (dépensées par les utilisateurs pour bénéficier des différents services), d'autre part le moyen d'inciter les acteurs à proposer et faire fonctionner les services en question (ces acteurs étant rémunérés en tokens). En outre, les tokens sont également utilisés pour la sécurité et la gouvernance des cryptoréseaux.

Plus globalement, les tokens, qui sont transférables librement en pair-à-pair et cotés sur un marché ouvert à tous, constituent le liant entre les différents acteurs de ces réseaux. Chaque acteur est incité économiquement à ce que le réseau gagne en utilité et donc en valeur, ce qui est censé être corrélé à l'appréciation du token.

Les cryptoréseaux représentent un changement de paradigme pour l'économie numérique : les services numériques ne sont plus apportés et gérés par des entreprises centralisées, mais par des écosystèmes d'acteurs tous liés par des mécanismes d'incitation économiques.

Le fait que cette coordination des acteurs constitue des réseaux et non des entreprises numériques « classiques » implique plusieurs points :

▪ Un cryptoréseau ne meurt pas comme peut mourir un business

Les entreprises du web peuvent faire faillite. L'éclatement de la bulle Internet au début des années 2000 avait ainsi conduit à de nombreuses faillites de startups. Un cryptoréseau ne connaît pas ce même problème. Son token peut subir des chutes de valeur importantes mais son existence même n'est pas menacée directement car celle-ci repose sur une multitude de points techniques, appelés « nœuds » du réseau (le plus souvent répartis partout dans le monde), sans serveur central pouvant être désactivé : c'est ce qui fait la décentralisation des technologies blockchain. Un réseau peut être très peu utilisé, mais restera existant tant que des nœuds continueront de fonctionner.

▪ Un cryptoréseau n'a pas à proprement parler de business model comme une entreprise classique

Chaque entreprise a son business model. Chaque cryptoréseau a son modèle cryptoéconomique. Les réseaux qui réussiront le mieux seront ceux qui reposent sur des modèles cryptoéconomiques à la fois très bien construits en théorie et très bien mis en place en pratique – de là, par ailleurs, l'importance de l'exploration de la cryptoéconomie pour pouvoir comprendre et analyser finement le web décentralisé.

51 <https://www.nickgrossman.is/2018/cryptonetworks-and-why-tokens-are-fundamental/>

52 <https://medium.com/@cdixon/why-decentralization-matters-5e3f79f7638e>

Parmi les éléments à considérer figurent ainsi la politique monétaire du token ou les mécanismes de gouvernance du réseau.

Pour qu'un cryptoréseau fonctionne de façon optimale, les tokens doivent par exemple être répartis de façon large entre toutes les parties prenantes du réseau : utilisateurs, contributeurs, « mineurs » (acteurs qui valident les transactions sur une blockchain, rémunérés en tokens). De cette façon, chacun est incité à la réussite du réseau. « *Les réseaux qui transfèrent plus de valeur aux utilisateurs ont plus de chances de réussir que ceux qui sur-concentrent la valeur au sein d'un groupe restreint de développeurs ou d'investisseurs* » considèrent ainsi Joel Monegro & Chris Burniske dans leur thèse d'investissement de leur fonds d'investissement dédié aux cryptoactifs⁵³.

• Un cryptoréseau est plus comparable à une ville ou une économie émergente qu'à une entreprise

Les cryptoréseaux sont comparables à des économies émergentes, selon Joel Monegro & Chris Burniske. « Cette analogie permet de savoir où chercher la valeur du token, en considérant des critères similaires à ceux d'une économie nationale : bonne gouvernance, politique monétaire adaptée, faible corruption, faibles inégalités, tendances en termes de productivité, etc. » écrivent-ils.

D'autres observateurs les comparent à des villes. C'est notamment le cas de l'entrepreneur Taylor Pearson : « *Comme une ville, un cryptoréseau est une communauté d'individu plus ou moins liés qui partagent un ensemble de règles sur la façon dont ils vivent et travaillent : les lois pour les villes, les protocoles pour les cryptoréseaux. Contrairement à des entreprises, les villes et les cryptoréseaux sont organisés de bas en haut, plutôt que de haut en bas. Les leaders individuels comptent plus pour les entreprises que pour les villes. Savoir qui est le CEO d'une entreprise joue un rôle important dans une décision d'investissement, alors que savoir qui est le maire d'une ville est rarement un critère important dans le choix d'un individu d'y emménager. De même, la plupart des investisseurs en bitcoins ne sauraient pas nommer le moindre développeur cœur du réseau, mais cela n'est pas un critère majeur de leur décision d'investissement*⁵⁴ ».

En conséquence, il est important de ne pas imiter le modèle de construction de l'entreprise pour construire un cryptoréseau ; Taylor Pearson estime que le modèle de développement de certaines villes clefs doit être considéré de près.

Quelle que soit leur nature, les cryptoréseaux n'en sont encore qu'à leurs premiers stades de développement – même si un réseau comme Bitcoin fêtera prochainement sa première décennie d'existence. Pour Chris Dixon, « *les cryptoréseaux souffrent aujourd'hui de limites qui les empêchent de concurrencer sérieusement les acteurs centralisés* ». Ces limites tiennent en particulier à des dimensions techniques, comme la capacité à réaliser un grand nombre de transactions par secondes. « *Il s'agira ces prochaines années d'essayer de surmonter ces limites. Ensuite, les efforts se concentreront sur la construction d'applications par-dessus ces infrastructures*⁵⁵ ».

6/ De nouveaux questionnements économiques

Les nouvelles logiques présentées ci-dessus font l'objet depuis plusieurs mois d'un bouillonnement intellectuel considérable. S'il serait vain de chercher à le synthétiser ici tant il est foisonnant, certaines questions peuvent être mises en avant à titre d'illustration.

53 Accessible ici en PDF : <https://ipfs.io/ipfs/QmZL4eT1gxnE168Pmw3KyejW6fUfMNzMgeKMgcWJUfYGRj/Placeholder%20Thesis%20Summary.pdf>

54 <https://www.coindesk.com/worst-crypto-networks-will-biggest/>

55 <https://medium.com/@cdixon/why-decentralization-matters-5e3f79f7638e>

Un des grands enjeux de la « token économie » réside ainsi dans les méthodes de valorisation des tokens, qui restent encore à modéliser précisément. Un premier travail a été réalisé en ce sens par l'investisseur Chris Burniske (auteur d'un ouvrage dédié aux cryptoactifs publié fin 2017), prolongé ensuite par d'autres acteurs comme Alex Evans (dans un article intitulé « Sur la valeur, la vitesse et la théorie monétaire : une nouvelle approche des valorisations des cryptoactifs »).

Les recherches actuelles indiquent que la question de la valorisation des tokens est intimement liée à leur "vitesse", qui peut être définie comme le rapport entre le volume total de transactions sur un cryptoréseau et la valeur moyenne de ce réseau. Cette notion de vitesse fait l'objet de nombreuses réflexions (par exemple : « *Understanding token velocity*⁵⁶ »).

Plus globalement, de nombreux travaux portent sur la manière de classer les tokens afin d'aboutir à des distinctions plus fines entre leurs différents types⁵⁷. Plusieurs classifications ont été proposées ; en Suisse, la FINMA (Autorité fédérale de surveillance des marchés financiers) distingue ainsi les tokens de paiement (utilisés comme moyens de paiement), les tokens utilitaires (donnant droit à un accès à des services numériques) et les security tokens (présentés plus ba⁵⁸s).

D'autres questions plus spécifiques se posent également, parmi lesquelles :

- Comment maximiser les chances que les acquéreurs de tokens comptent réellement utiliser le service et n'agissent pas simplement comme des spéculateurs ?
- Comment quantifier concrètement la décentralisation⁵⁹ ?
- Les tokens disrupteront-ils les places de marchés de titres cotés, et si oui dans quelle mesure et à quelle échéance ? Comme l'explique Denis Lafont-Trevisan, cofondateur du projet blockchain Talao, « *de même qu'Internet a bousculé les opérateurs télécoms, cette "infrastructure" peut bousculer les acteurs traditionnels comme le NYSE ou Euronext. Il est possible de résister, réglementer, nier, mais le mouvement semble inéluctable* ».
- A quoi pourrait ressembler la première prise de contrôle hostile d'un cryptoréseau⁶⁰ ? Ou les futures fusions ou acquisitions de cryptoréseaux ? Ces questions se poseront de plus en plus ces prochains mois et prochaines années avec la mise en place opérationnelle des réseaux financés depuis 2017 en ICO.
- Comment faire face au déséquilibre actuel entre l'offre très importante de tokens et une demande qui semble aujourd'hui en partie artificielle⁶¹ ? Comment susciter une demande (naturelle) pour les tokens ?
- Etc.

56 <https://multico.in.capital/2017/12/08/understanding-token-velocity/>

57 Voir notamment ces trois articles <https://thecontrol.co/on-token-value-e61b10b6175e> ; <http://startupmanagement.org/2017/06/10/tokenomics-a-business-guide-to-token-usage-utility-and-value/> ; <http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/>

58 <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/>

59 <https://news.earn.com/quantifying-decentralization-e39db233c28e>

60 https://medium.com/@andy_bromberg/what-the-first-token-hostile-takeover-could-look-like-c40be3ccb6b5

61 https://medium.com/@Melt_Dem/drowning-in-tokens-184ccfa1641a

Avec les tokens, les règles traditionnelles de l'économie numérique sont donc bouleversées. Un nouveau web, que certains appellent web 3.0 ou plus simplement web décentralisé, est en train d'émerger.

Le potentiel des tokens est cependant tel que ses applications potentielles ne se limitent pas simplement au web...

IV. LES IMPLICATIONS DE L'ÉCONOMIE DES TOKENS AU-DELÀ DU WEB

Les mécanismes des tokens permettent d'envisager des usages qui concerneront, bien au-delà du seul web, la finance, les actifs réels et les entreprises déjà existantes.

1/ La tokenisation d'actifs traditionnels, nouvelle frontière de la blockchain

L'économie des tokens peut aller au-delà du web et toucher notamment la finance traditionnelle avec la notion de security tokens.

Ces tokens peuvent être définis comme des actifs financiers digitalisés qui permettent de créer des fractions de propriété et d'effectuer des transactions quasi-instantanées.

Dans le système financier actuel, un individu qui possède 100 euros ne peut pas acheter une action individuelle d'une entreprise qui s'échange à 200 euros. Les parts digitalisés lui permettront de détenir par exemple 0.5 part de l'entreprise. En outre, l'acquisition de cette fraction de part sera réalisée presque instantanément sur une blockchain, à condition que l'acheteur et le vendeur respectent tous deux les réglementations en matière de security token (cette vérification pourra s'effectuer presque instantanément avec les protocoles blockchain).

Les security tokens ouvrent la voie d'une nouvelle ère pour les actifs financiers : leur digitalisation. Selon l'analyse de l'investisseur Anthony Pompliano⁶², ces actifs n'étaient jusqu'ici pas véritablement digitalisés : il parle plutôt d'ère « électronique » pour désigner ce qui a remplacé en large partie à partir des années 1990 la première phase de développement des actifs financiers, alors fondée sur des certificats de propriété papiers (qui devaient être transférés physiquement à chaque échange d'actifs). « *Le monde numérique tel que nous le connaissons aujourd'hui, aussi bien son infrastructure que ses applications, n'étaient pas encore en place* » lors du basculement à l'ère électronique, justifie-t-il.

La digitalisation des actifs qu'ouvre les *security tokens* constitue le pendant de la digitalisation de l'information ouvert par Internet. Il est alors question de « tokenisation », qui désigne le processus d'inscription d'un actif, et de ses droits associés, sur un token afin d'en permettre la gestion et l'échange en pair-à-pair, de façon instantanée et sécurisée sur une infrastructure blockchain.

Security Tokens : quels avantages ?

La tokenisation d'actifs financiers présente sur le papier plusieurs atouts, selon Anthony Pompliano⁶³ :

« **-Réduction des frais de commission.** La plupart des frais liées aux transactions financières viennent des paiements effectués aux intermédiaires. Les security tokens éliminent le besoin d'intermédiaires comme les banques. En outre, l'usage de smart contracts (des programmes autonomes capables d'exécuter automatiquement des conditions prédéfinies et inscrites sur une blockchain) permettra de réduire la complexité et le coût de gestion de ces actifs (processus de collectes, distributions, etc.).

-Exécution des transactions plus rapides. Ces tokens accéléreront les processus en réduisant le nombre d'acteurs impliqués. En outre, la possibilité de réaliser des transactions immédiates sur le marché secondaire des security tokens sera attractif pour les émetteurs d'actifs ainsi que les investisseurs.

-Libre exposition au marché. La plupart des transactions sur le marché de l'investissement manquent aujourd'hui d'exposition à une base mondiale d'investisseurs. Il est par exemple difficile pour les investisseurs en Asie d'investir dans des entreprises privées américaines. Avec les security tokens, les détenteurs d'actifs commercialiseront simplement avec quiconque avec une connexion Internet, à condition de respecter les réglementations. Cette libre exposition au marché devrait conduire à des changements significatifs dans la valorisation d'actifs.

-Accès à une base d'investisseurs plus large.

-Automatisation de certains services. Les émetteurs de security tokens commenceront à utiliser des smart contracts pour automatiser la fonction de fournisseur de services. En conséquence, le rôle des avocats devrait se concentrer sur leurs fonctions de conseil. »

Au-delà des actifs financiers, la tokenisation peut concerner un grand nombre d'actifs du monde réel.

Pour Stephen McKeon, professeur de finance à l'Université de l'Oregon, la tokenisation est particulièrement prometteuse pour les actifs relativement illiquides, dont la valorisation est pénalisée par leur faible liquidité dans des proportions importantes (qu'il estime à « 20% à 30%, soit des montants considérables⁶⁴ »). La tokenisation permettra en effet d'augmenter la profondeur de marché, en ouvrant les marchés à plus de participants, engendrant ainsi plus d'échanges.

Selon lui, « les actifs traditionnels se tokeniseront parce qu'ils perdront la prime de liquidité s'ils ne le font pas » (la prime de liquidité désigne la « rémunération complémentaire versée aux investisseurs afin de compenser le manque de liquidité de l'actif acheté »). Il cite l'exemple d'actifs immobiliers commerciaux, résidentiels, ou encore d'œuvres artistiques. Dans ce dernier cas, des particuliers pourraient ainsi acquérir collectivement un tableau de valeur pour un musée local via une vente de tokens, même si aucun d'entre eux n'a individuellement les moyens d'acheter le tableau.

63 <https://medium.com/@apompliano/the-official-guide-to-tokenized-securities-44e8342bb24f>

64 <https://hackernoon.com/traditional-asset-tokenization-b8a59585a7e0>

Dans une étude parue sur le site du Nasdaq en 2017⁶⁵, l'entrepreneur Addison Cameron-Huff prend de son côté l'exemple d'un grossiste de diamants, Jane, qui en possède l'équivalent de 15 millions de dollars, et d'un investisseur individuel, Joe, qui souhaite investir quelques milliers de dollars dans les diamants sans avoir à gérer la problématique du transfert physique, qui implique notamment des processus de sécurité pour s'assurer qu'un faux n'a pas été introduit. Joe souhaite idéalement posséder une petite part de nombreux diamants dans une logique de diversification, et pouvoir échanger facilement l'une de ses parts à d'autres individus que Jane. Les tokens constituent une solution répondant à ces différents besoins, en permettant d'échanger facilement une fraction de propriété d'actifs et ainsi de démocratiser l'accès à ces actifs.

Deux grands types d'actifs sont distingués par l'étude comme pouvant être plus facilement « tokenisés » que d'autres :

-Les actifs incorporels (brevets, crédits carbone, droits d'auteur...). En raison de leur absence d'existence physique, ces actifs peuvent se prêter plus facilement que d'autres à ce processus de tokenisation, même si les différentes de juridictions peuvent rendre les transferts difficiles.

-Les actifs fongibles. Ces actifs sont eux aussi plus faciles à convertir en tokens car ils peuvent le plus souvent être divisés en plusieurs unités (comme des bitcoins) et parce que l'ensemble des tokens peuvent être associés à un ensemble général de composants d'actifs interchangeable (exemple : 10kg d'or), estime le Nasdaq. A l'inverse, les actifs non-fongibles se prêtent moins facilement à la tokenisation. Lorsqu'ils sont titrisés, les prêts hypothécaires sont par exemple souvent regroupés avec d'autres prêts qui présentent des caractéristiques similaires mais pas identiques.

L'étude souligne le fait qu'il faut distinguer plusieurs sortes de transferts de droits. Dans certains cas, comme les baux, seuls certains droits liés à un actif seront transférés, et non la propriété de l'actif elle-même. C'est également le cas de certains actifs incorporels comme les droits musicaux : lorsqu'un consommateur achète une chanson sur iTunes, il achète en réalité une licence qui l'autorise à accéder à vie à cette chanson, sans la posséder. La licence s'arrête à sa mort, ce qui signifie qu'elle n'est pas transmissible comme héritage par exemple⁶⁶. Des tokens pourraient représenter ce type de droits d'accès au lieu de représenter une propriété totale de l'actif.

65 <https://www.nasdaq.com/article/how-tokenization-is-putting-real-world-assets-on-blockchains-cm767952>

66 Pour plus de précisions, voir <http://master-ip-it-leblog.fr/non-vous-ne-pouvez-pas-heriter-dune-bibliotheque-itunes/>

La tokenisation, un mouvement inéluctable ?

C'est le point de vue défendu par l'investisseur Balaji Srinivasan⁶⁷ :

« La tokenisation s'applique aux actifs rares. Aujourd'hui, la chose la plus appropriée à tokeniser est quelque chose de purement digital. D'ici 2025-2030 je m'attends à ce que de multiples juridictions permettent la tokenisation de n'importe quelle ressource rare, en raison des bénéfices de la digitalisation. Cela comprend les actions, les obligations, les commodités, les maisons, les voitures, les biens digitaux de tout type...Le cadre réglementaire finira par l'accepter. Il suffit que seuls quelques pays l'acceptent, et la création de richesses qui en résultera sera si large que cela poussera un grand nombre d'autres pays à adopter un régime libéral en matière de tokenisation.

Je pense que la tokenisation signifie qu'in fine, chacun peut devenir investisseur, une fois toutes les questions réglementaires fixées – depuis votre ordinateur jusqu'à un enfant Indien qui n'a que dix dollars. Cela signifie aussi que chacun, du business angel à l'investisseur en capital-risque, en passant par les investisseurs sur les marchés publics, commenceront à acheter les mêmes actifs. De la même façon que des formes disparates d'informations (photos, vidéos, audios, textes...) ont été convertis sous forme de « paquets » [avec Internet], la blockchain convertit ces formes disparates de rareté en tokens.

La progression de tous ces tokens et des blockchains publiques signifie qu'Internet deviendra, à long terme, le plus grand marché d'actifs du monde, tout comme Internet est devenu la plus grande bibliothèque du monde. »

Cette analyse est notamment partagée par l'entrepreneur David Sacks, ancien directeur des opérations de Paypal, qui travaille aujourd'hui dans le secteur des cryptoactifs : *« Si vous aviez dit aux gens au début des années 1990 que chaque forme disparate de contenus - TV, films, musique, informations, photographies – serait chacune convertie en paquets sur le réseau Internet, disruptant massivement ces secteurs, les gens vous auraient pris pour un fou ⁶⁸».*

Plusieurs grands défis restent encore à surmonter pour que la tokenisation d'actifs réels se produise effectivement en pratique.

Le premier de ces défis est bien sûr d'ordre réglementaire. De premiers efforts ont été entrepris en ce sens, en particulier par l'initiative Harbor qui a créé un standard spécifique, le Regulated Token Standard⁶⁹. Les tokens créés sous ce standard sont constitués de telle façon à ce qu'ils soient par nature conformes aux différentes réglementations.

Cela étant, le processus de régulation des security tokens reste encore à ses débuts. Selon Stephen McKeon, « l'adoption massive de la tokenisation d'actifs traditionnels prendra des années, possiblement des décennies. La technologie évolue vite, mais pas la régulation. La tokenisation constitue l'une des plus grandes opportunités, et l'un des plus grands challenges, que les autorités de régulation affronteront au cours de la prochaine décennie ».

67 <https://www.cnn.com/2017/09/05/balaji-srinivasan-21-co-interview-on-blockchain.html>

68 <https://www.cnn.com/2018/02/06/ex-paypal-david-sacks-on-craft-fund-and-harbor.html>

69 <https://www.cnn.com/2018/02/06/ex-paypal-david-sacks-on-craft-fund-and-harbor.html>

Parmi les autres défis, citons en particulier les questions de gouvernance des actifs tokenisés et possédés collectivement par des dizaines, des centaines ou des milliers d'investisseurs. Comme l'explique Stephen McKeon, dans le cas d'un bâtiment possédé par une seule entité, celle-ci est incitée à surveiller certains aspects comme la maintenance. Si 10 000 personnes possèdent ce même bâtiment, cette incitation est moins évidente car le coût de surveillance peut dépasser la valeur de leur investissement individuel respectif. Des solutions devront donc être trouvées en termes de gouvernance.

2/ La tokenisation d'activités d'entreprises traditionnelles

Les entreprises traditionnelles elles-mêmes pourraient créer leurs propres tokens pour certaines de leurs activités.

Le token pourrait par exemple représenter un moyen de paiement dans une application. C'est le choix qu'a fait en 2017 l'application de messagerie instantané Kik, qui compte près de 800 millions d'utilisateurs dans le monde. Kik a annoncé la création de son propre token qui aura vocation à être utilisé comme moyen de paiement dans l'application, notamment pour payer des services premium. Pour financer son nouveau projet et booster le lancement de son token, Kik a réalisé une ICO, devenant ainsi la première grande entreprise déjà existante à réaliser une levée de fonds de ce type. L'opération est devenue l'une des dix plus importantes ICO jamais réalisées, et leur a permis de lever l'équivalent de 98 millions de dollars.

Certaines rumeurs évoquent aujourd'hui la possibilité qu'Amazon lance un jour son propre token, nourries par l'initiative du géant américain de déposer fin 2017 le nom de domaine amazoncryptocurrency.com. La mise en place d'un token permettrait à Amazon de proposer un moyen de paiement unifié pour toutes ses places de marché, au lieu de devoir utiliser des monnaies différentes par les différentes places de marché Amazon dans le monde⁷⁰.

Pour encourager l'adoption de ce token, Amazon pourrait alors employer plusieurs méthodes⁷¹ :

- Décider que le token permette de débloquer des services additionnels que les monnaies traditionnelles ne permettent pas.
- Accorder une réduction de par exemple 5% pour tout achat payé avec ce token –sur une période de temps limitée ou non.
- Distribuer gratuitement quelques tokens Amazon à ses 80 millions d'utilisateurs Amazon Prime, pour accélérer leur adoption. Ce principe, appelé « airdrop », est fréquemment utilisé par les nouveaux projets blockchain qui souhaitent développer l'usage de leur token.
- Faire basculer son programme d'affiliation sur ce système en rémunérant ses partenaires en tokens Amazon.
- Faire en sorte que le token soit coté sur des plateformes d'échange. Chacun aurait alors une incitation à acquérir le token au départ, en misant sur l'idée que le token gagnera ensuite en valeur, notamment grâce à la croissance d'Amazon. Imaginons la puissance que représenterait l'annonce du lancement d'un Amazon Coin : la demande pourrait être considérable, pour ne pas passer à côté de ce qui pourrait devenir un token de référence en terme de moyen de paiement numérique.

⁷⁰ Voir <https://bitcoinmagazine.com/articles/op-ed-could-amazon-token-become-viable-worldwide-cryptocurrency/>

⁷¹ C'est ce que présente notamment l'entrepreneur Michael Amar dans une tribune intitulée « La cryptomonnaie Amazon va faire un raz de marée » <https://www.frenchweb.fr/la-cryptomonnaie-amazon-va-faire-un-raz-de-maree/320114>

A terme, il est possible d'aller plus loin en partant du principe qu'Amazon ne souhaite probablement pas se contenter d'être un géant du e-commerce et pourrait se lancer dans d'autres secteurs : le commerce physique (Amazon a ouvert son premier magasin à Seattle en janvier 2018) ; la vidéo en ligne avec le service Amazon Vidéo déjà existant, qui pourrait concurrencer Netflix à terme ; la maison connectée avec ses enceintes intelligentes Echo ; la santé ; etc.

Dès lors, un individu pourrait payer uniquement avec le token Amazon dans l'ensemble de cet écosystème de services, sans jamais utiliser de monnaies traditionnelles. En d'autres termes, Amazon aurait donc créé sa propre monnaie interne. Amazon pourrait même nouer des partenariats avec d'autres entreprises pour qu'ils acceptent son token : des chaînes hôtelières, des restaurants, supermarchés, etc.

Ceci n'est encore qu'un exercice de prospective mais Amazon ayant été pionnier dans un certain nombre de domaines, il n'est pas impossible que l'entreprise menée par Jeff Bezos choisisse d'investir le terrain des tokens en tant que pionnier, en se servant comme atout principal de sa base d'utilisateurs déjà existante. Une étude récente réalisée récemment auprès de 1000 clients Amazon révèle du reste qu'une majorité absolue des sondés seraient prêts à utiliser une cryptomonnaie Amazon si celle-ci venait à voir le jour⁷²...

Au-delà du moyen de paiement, un token créé par une entreprise pourrait représenter d'autres usages. Pensons ainsi aux points de fidélité, comme le prévoit d'ores et déjà le géant du e-commerce Rakuten qui a annoncé début 2018 la création de son propre token pour représenter ses points de fidélité. Ce mécanisme permettra aux entreprises de :

-réaliser un suivi plus fin et en temps réel des points des consommateurs : savoir quel consommateur possède quels points, à quel moment ; comment et où il les dépense ; etc. L'analyse de ce suivi en temps réel permettra à l'entreprise de proposer au consommateur des promotions personnalisées et adaptées à ses besoins, via une application mobile.

-créer des programmes de fidélité multi-enseignes. Les points de fidélité en token pourront être intermarques, c'est-à-dire être valables dans différentes enseignes d'un même groupe. Un groupe pourrait dès lors savoir pour chaque consommateur si celui-ci préfère par exemple acheter un type de produits chez une enseigne A, et un autre type de produits chez une enseigne B, ainsi que bien d'autres informations. Il sera même possible de créer des programmes de fidélité qui rassembleront différents groupes présentant des complémentarités (un loueur de voitures avec un groupe hôtelier, par exemple). Les points seraient en effet enregistrés sur une blockchain qui serait (par nature) contrôlée simultanément par les différents partenaires, sans que l'un d'entre eux ne contrôle le registre plus qu'un autre.

-donner aux consommateurs la possibilité de s'échanger ces tokens en quelques clics, en pair-à-pair (c'est-à-dire sans intermédiaire). L'entreprise pourrait visualiser les transferts de points entre consommateurs, ce qui pourrait là aussi lui apporter des données intéressantes notamment en termes de marketing communautaire.

De façon générale, les usages des tokens pour entreprises restent encore à inventer, construire et expérimenter. Les prochaines années verront certainement de plus en plus d'entreprises explorer et tester ce modèle, comme en témoigne la déclaration récente d'Alexandre Bompard, PDG de Carrefour : « *Je réfléchis beaucoup [aux cryptomonnaies et aux tokens] en ce moment. On ne pourra pas passer à côté de cette transformation-là*⁷³ »...

72 Etude LendEDU, février 2018 <https://www.cnn.com/2018/02/28/majority-of-shoppers-are-open-to-amazon-cryptocurrency-survey-shows.html>

73 <https://twitter.com/ArnaudLeRoux/status/978695148845617154>

3/ L'émergence d'organisations d'un nouveau genre : les DAO

La blockchain et l'économie des tokens transforme le concept même d'entreprise.

C'est le concept de DAO : Decentralized Autonomous Organization, définissable comme une organisation décentralisée dont les règles de gouvernance sont automatisées et inscrites de façon immuable et transparente dans une blockchain.

L'automatisation de ces règles est effectuée par des smart contracts (ces programmes autonomes qui exécutent automatiquement des conditions définies à l'avance).

Une DAO apporte au moins trois nouveaux éléments par rapport à une entité traditionnelle :

- Une DAO ne peut pas être arrêtée ou fermée.
- Aucune personne ou organisation ne peut à elle seule contrôler l'entité ou modifier unilatéralement ses règles ou ses données.
- Toutes les transactions effectuées au sein de la DAO et entre la DAO et d'autres acteurs sont transparentes et auditables, dans un cadre supranational.

Comme l'explique l'entrepreneur Philippe Honigman (Partner de Tribute, CEO de ftopia), « *l'organisation décentralisée correspond à la topologie du réseau blockchain, qui autorise des interactions directes entre tous les acteurs, sans dépendance à un acteur central. Le côté "autonome" fait référence aux règles qui régissent le réseau, y compris celle qui en modifient le fonctionnement ; elles sont à la fois définies formellement et implémentées sous la forme de smart contracts, c'est-à-dire de programmes exécutés sur la blockchain selon un mode décentralisé. La DAO est auto-référente, son mode de fonctionnement et son évolution sont décidées par le réseau lui-même. On peut ainsi entrevoir un Facebook sans Facebook, un Uber sans Uber, un eBay sans eBay, etc. L'activité conduite dans ces plateformes serait régulée directement par les participants, et la valeur créée répartie entre leurs membres* ».

La transformation du modèle de l'entreprise centralisée

Philippe Honigman montre que la nature actuelle de l'entreprise comme « opérateur central de toute plateforme » tient à trois grandes dimensions, qui relèvent toutes de la « capacité de l'entreprise d'agir en tant que tiers de confiance entre les agents du réseau⁷⁴ » :

« - les flux financiers : la garantie d'être payé lorsqu'on fournit un service via une plateforme nécessite des mécanismes de séquestre et de sécurisation des paiements que seul un tiers est en mesure de fournir ;

- l'identité : s'assurer que l'identité de notre interlocuteur n'est pas susceptible d'être à tout moment usurpée requiert un gestionnaire d'identité tiers, fonction assurée aujourd'hui par tous les services en ligne pour le compte de leurs utilisateurs (banques, réseaux sociaux, messageries, e-commerce, services publics, etc) ;

- la réputation : savoir que nous pouvons faire confiance à la personne avec laquelle nous envisageons d'effectuer une transaction est capital ; ceci impose de faire certifier l'historique des transactions et des évaluations entre pairs par un tiers arbitre.

A l'heure des cryptomonnaies et de la blockchain, ces trois aspects essentiels de la fonction de confiance peuvent s'appréhender différemment. Le paiement direct de pair à pair, éventuellement assorti de conditions de déclenchement, est la fonction même des cryptomonnaies. Les nouveaux modèles d'identité décentralisée (ou Self-Sovereign Identity) recalibre les rôles des tiers de confiance, qui deviennent des validateurs d'attributs ("verifiable claims") plutôt que les détenteurs de nos identités. Enfin, les systèmes de décentralisation de la réputation s'appuient sur la blockchain pour dériver de l'historique infalsifiable de nos transactions les preuves que nous souhaitons échanger avec d'autres personnes physiques ou morales. »

Avec les DAO et les tokens, il ne s'agit plus de capter la valeur par une entité centralisée, hiérarchique, sensible aux décisions arbitraires et unilatérales d'un individu ou d'un groupe restreint d'individus. Il s'agit désormais de partager cette valeur dans une organisation décentralisée, entre les détenteurs des tokens, qui peuvent détenir le pouvoir sur les décisions stratégiques de l'organisation. Ce partage de valeur plus distribué, et donc équilibré, peut permettre également de gagner en efficacité : chaque détenteur de token est en effet incité économiquement à faire grandir le projet, puisque le développement du projet entraîne logiquement une hausse de valeur du token associé.

Aujourd'hui, les DAO sont avant tout encore au stade expérimental. Plusieurs obstacles restent encore à lever, parmi lesquels l'expérience utilisateur des applications décentralisées, et par-dessus tout, la gouvernance de ces organisations. Le projet Aragon, entre autres, travaille sur ces aspects essentiels pour le développement du web décentralisé.

Illustration : Talao, une DAO pour le travail à la demande

⁷⁴ <https://fr.linkedin.com/pulse/la-blockchain-agent-de-d%C3%A9centralisation-des-luc-bretones>

Talao est un projet français qui vise à construire la première plateforme décentralisée dédiée aux travailleurs indépendants. Cette plateforme, en cours de levée de fonds (en ICO), deviendra une DAO à la suite de sa mise en place, et disposera de trois grands atouts par rapport aux plateformes existantes :

- elle supprimera entièrement les commissions (aujourd'hui de 15% à 20%) de mise en relation freelances-entreprises prélevées par les plateformes centralisées ;
- elle redonnera aux freelances la possession de leur réputation (aujourd'hui contrôlée par les plateformes) et certifiera leurs compétences sur la blockchain ;
- elle permettra aux freelances de voter pour les choix de gouvernance de l'organisation (politique tarifaire, etc.) grâce au token Talao.

L'ambition de Talao est d'entrer dans le top 3 mondial des plateformes de travail à la demande, en commençant par les secteurs industriels et technologiques.

V. LES CRYPTOACTIFS FACE AU MÊME SCEPTICISME QU'INTERNET À SES DÉBUTS

L'économie des tokens et les cryptoactifs peuvent donner l'impression d'un charabia difficilement digeste pour un néophyte. L'accent y est pourtant mis ici car des milliers d'entrepreneurs avancent en ce moment même sur ces questions, sans nous attendre en France. Partout dans le monde, des projets se créent tous les jours, se testent, se développent, se confrontent au regard du secteur blockchain, qui ne cesse de s'agrandir.

En parallèle, ces technologies font l'objet d'un bouillonnement intellectuel peu commun, invisible de l'extérieur, loin de l'attention portée aux mouvements quotidiens de hausse ou de baisse des cours des cryptomonnaies, qui ne relèvent le plus souvent que de l'anecdote. Ce bouillonnement se manifeste par une production d'idées qui déborde largement des aspects purement technologiques, et touche à la finance, au droit, à la monnaie, à l'histoire, à l'économie numérique...

A ce titre, la déconnexion frappante entre une partie du discours médiatique et politique sur les cryptoactifs et sa réalité contribue à la propagation d'idées reçues sur le sujet, de la même façon qu'Internet était souvent présenté dans les années 1990 au mieux comme une invention peu utile, si ce n'est comme le lieu de tous les dangers et de tous les vices.

En 1995, seuls 30 à 40 millions de personnes utilisaient Internet⁷⁵. Une large partie des investisseurs restaient sceptiques sur son potentiel. La blockchain et les cryptoactifs, encore aujourd'hui marginaux dans leurs usages, font face aujourd'hui au même scepticisme, auquel il est nécessaire de répondre.

⁷⁵ Source Internet World Stats

1/ Des technologies trop complexes ?

Il est parfois dit que ces technologies sont trop complexes d'utilisation pour tout-un-chacun. C'est effectivement le cas aujourd'hui...tout comme c'était le cas pour Internet dans les années 1990. Internet était alors avant tout un outil de « geek », comme le raconte Le Monde Diplomatique en novembre 1995⁷⁶ : « *Il n'y a pas de grande diversité humaine dans le cyberspace, qui est habité par des hommes de moins de cinquante ans disposant en abondance de temps d'accès à des ordinateurs, très habiles sur des claviers, aux opinions bien ancrées, et d'une épouvantable timidité dans les contacts directs, surtout avec des personnes du sexe opposé.* »

Les interfaces étaient très sommaires, pour ne pas dire laides.



Pages d'accueil deBay et Altavista (moteur de recherche de référence aux débuts du web) dans les années 1990

Cette complexité s'est avérée un obstacle uniquement provisoire. Dans les années 2000, les entrepreneurs du numérique ont commencé à faire de l'expérience utilisateur leur priorité. Internet a alors véritablement décollé, en s'ouvrant largement au-delà du cercle des passionnés d'informatique. Nicolas Colin et Henri Verdier le soulignent bien dans leur ouvrage « L'Age de la multitude » : le cœur de la révolution numérique réside dans l'expérience utilisateur simplifiée, intuitive, qui a été proposée aux internautes. C'est ce qui a permis le succès de BlaBlaCar, AirBnb, et bien d'autres, à partir de la moitié des années 2000.

La blockchain et les cryptomonnaies sont appelées à suivre la même évolution. De façon schématisée, la plupart des entrepreneurs du secteur se concentrent aujourd'hui sur les couches technologiques, les plus basses, qui doivent d'abord être construites et renforcées avant de pouvoir travailler sur les couches applicatives qui s'y grefferont et sur lesquelles les internautes se connecteront. Le travail sur l'expérience utilisateur est un des grands défis du monde blockchain, mais il viendra naturellement.

76 Article « Faut-il brûler Internet ? » paru en novembre 1995 dans Le Monde Diplomatique (<https://www.monde-diplomatique.fr/1995/11/TORRES/6781>)

2/ Les cryptoactifs, une simple bulle ?

Combien de fois le bitcoin a-t-il été comparé à la tulipomania de 1637 aux Pays-Bas, considérée comme l'une des premières bulles spéculatives de l'Histoire ? Suffisamment pour qu'émerge dans l'écosystème blockchain le « prix tulipe », décerné régulièrement à ceux qui usent et abusent de cette comparaison. Une large partie des économistes invités à s'exprimer sur le sujet, jusqu'à Jean Tirole, prix Nobel d'économie, l'affirment en effet avec conviction (tout en reconnaissant souvent « ne pas maîtriser » le sujet⁷⁷) : le bitcoin est une bulle sans fondement, fermez le ban ! Une recherche dans les archives de The Economist permet ainsi de montrer que les articles affirmant que 'le bitcoin est une bulle sur le point d'éclater' sont publiés par le magazine sans discontinuer depuis plus de six ans - y compris dès 2011, quand celui-ci ne valait que quelques dollars...

La thèse de la tulipomania a pourtant déjà été largement déconstruite⁷⁸, même si le propos reste encore inaudible, manquant d'oreilles à l'écoute. Rappelons que le bitcoin est un actif programmable, rare, fongible, pérenne, divisible jusqu'à huit chiffres après la virgule, et transférable à quiconque dans le monde en quelques minutes, à coût minime, et de façon sécurisée. Très loin, donc, d'un contrat à terme sur un bulbe de tulipe au 17e siècle...

En réalité, une grande partie des économistes qui s'expriment sur les cryptoactifs font preuve non seulement d' « une certaine méconnaissance du sujet », comme l'écrivent les économistes Nicolas Houy et François Le Grand dans une tribune du Monde⁷⁹ (qui n'a sans doute pas plu à tous leurs confrères), mais surtout d'un manque d'écoute des arguments adverses, qui laisse songeur.

« Les vives réactions suscitées [envers les cryptomonnaies] sont surtout émotionnelles, et expriment largement la peur instinctive de tout ce qui est nouveau, inhabituel, disruptif » analysent Gonzague Grandval (entrepreneur) et Yorick de Mombynes (fin connaisseur du sujet et par ailleurs conseiller référendaire à la Cour de Comptes), pour qui « l'hyperinflation » dont il est question n'est pas tant celle des cours des cryptoactifs que celle « des doutes, sarcasmes et préjugés » à leur encontre⁸⁰. Ce point de vue est partagé, de façon moins attendue, par Guillaume Maujean, rédacteur en chef de la rubrique Finance et Marchés du quotidien Les Echos, qui écrit dans une analyse parue en décembre 2017 qu'« il faut prendre le bitcoin très au sérieux : notre incrédulité face à ce phénomène est sans doute la même que celle que nous avons devant l'avènement d'Internet⁸¹ ».

En France, des spécialistes comme Jacques Favier et Adli Takkal Bataille tentent depuis plusieurs années de faire entendre un discours plus construit et argumenté que celui de la « tulipomania » (porté jusque par la Banque de France !⁸²), en particulier dans leur ouvrage « Bitcoin, la monnaie acéphale » (CNRS Éditions, 2017) qui fait aujourd'hui référence. Ils ont été rejoints récemment dans leur défense des cryptoactifs par de penseurs extérieurs à cet écosystème comme Gaspard Koenig ; ce dernier écrit ainsi, dans une tribune récente au titre explicite et un brin provocateur (« Le bitcoin, c'est mieux que l'euro⁸³ »), que « le bitcoin a le mérite d'être plus tangible et rassurant qu'une monnaie gérée arbitrairement par une banque centrale et des Etats insolubles ».

77 Jean-Marc Daniel, invité sur BFM Business en novembre 2017 www.youtube.com/watch?v=IVUBnYkzZz4

78 Entre autres, lire « Bitcoin, les faits contre les fantasmes » par Gonzague Grandval et Yorick de Mombynes www.latribune.fr/opinions/tribunes/bitcoin-les-faits-contre-les-fantasmes-760650.html et « La bulle Bitcoin, parlons-en » par Ouriel Ohayon <https://www.presse-citron.net/bulle-bitcoin-parlons/>

79 http://www.lemonde.fr/idees/article/2017/12/05/bitcoin-les-economistes-font-preuve-d-une-certaine-meconnaissance-du-sujet_5224960_3232.html

80 La bulle des arguments anti-bitcoin, La Tribune, janvier 2018 <https://www.latribune.fr/opinions/tribunes/la-bulle-des-arguments-anti-bitcoin-764804.html>

81 https://www.lesechos.fr/04/12/2017/lesechos.fr/030975681185_pourquoi-il-faut-prendre-le-bitcoin-tres-au-serieux.htm

82 Voir la note de la Banque de France publiée début mars 2018 : https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf

83 <https://www.lesechos.fr/idees-debats/editos-analyses/0301291294173-le-bitcoin-cest-mieux-que-leuro-2153263.php>

Un point en particulier mérite ici d'être souligné, d'abord parce qu'il est directement lié à l'économie numérique sur laquelle cette note se focalise, mais surtout pour son caractère contre-intuitif.

Il semble clair que les cryptoactifs, le bitcoin en tête, ont connu fin 2017 un mouvement haussier violent et sans doute excessif, rapidement corrigé ensuite comme cela s'était déjà produit en 2014, et qui pourra se reproduire à l'avenir. Cette spéculation ne justifie pourtant en rien l'idée d'actifs « tulipes ». Internet avait lui aussi connu une forte bulle, explosée en 2001, sans pour autant empêcher son développement par la suite. Rappelons du reste la prédiction de Jack Ma, fondateur du géant chinois du e-commerce Alibaba, dans l'un de ses tout premiers pitch en 1999 : *"Tout le monde sait qu'Internet est une bulle qui ne fait que grossir. Quand va-t-elle exploser ? (...) Ne vous inquiétez pas : le rêve d'Internet n'explosera pas⁸⁴"*.

En réalité, non seulement cette bulle n'avait pas freiné le développement d'Internet, mais elle l'avait probablement favorisé. C'est ce que démontre l'économiste vénézuélienne Carlota Perez, méconnue du grand public mais à la pointe sur les questions d'économie numérique, qui a étudié les grandes innovations technologiques depuis l'ère industrielle dans son ouvrage « *Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages* » paru en 2002. Ses conclusions sont claires : la spéculation est souvent le moteur de l'adoption des technologies. Les bulles nourrissent l'innovation en attirant du capital, qui permet en particulier de financer les infrastructures techniques et les efforts coûteux de recherche et développement. En ce sens, la spéculation est non seulement utile, mais nécessaire. Ce qu'il faut combattre n'est pas la bulle, mais les arnaques et les tromperies.

« La spéculation est souvent le moteur de l'adoption des technologies. Les bulles nourrissent l'innovation en attirant du capital »

Ces arnaques, nombreuses dans le domaine des cryptoactifs, doivent être combattues, et leurs auteurs punis sévèrement lorsque cela est possible. Cette politique implique cependant d'adopter une nouvelle démarche intellectuelle : entrer dans une analyse plus fine de ces actifs que celle souvent réalisée, et opérer une distinction entre les centaines, désormais milliers, d'actifs qui composent cette nouvelle économie numérique. Aujourd'hui, seule une petite partie d'entre eux font véritablement sens (bitcoin, ether...), et une majorité doit être évitée, étant au mieux peu utilisables, au pire relevant de véritables escroqueries (OneCoin par exemple). Les autorités de régulation ont bien entendu un rôle essentiel à jouer dans la dénonciation de ces fraudes, à condition de ne pas jeter le bébé avec l'eau du bain.

3/ Les technologies du « dark web » ?

L'accusation revient de façon régulière : les cryptoactifs seraient essentiellement utilisés pour des activités occultes ou illégales (blanchissement d'argent, terrorisme...). L'économiste Joseph Stiglitz a ainsi déclaré fin novembre 2017 non seulement que le bitcoin est une bulle, mais surtout qu'il s'agit d'un produit pour trafiquants et évadés fiscaux, et qu'il devrait à ce titre être interdit.

84 https://www.youtube.com/watch?v=Up9-C4_8dVo

« Utiliser le bitcoin pour des activités illégales serait aujourd'hui particulièrement risqué »

Ces poncifs habituels n'étonnent plus dans la communauté blockchain, habituée depuis des années à ce type de discours. Rappelons que l'historique des transactions est entièrement public, ce qui permet à plusieurs entreprises, comme Elliptic ou Chainalysis, de travailler avec les pouvoirs publics pour retracer les transactions frauduleuses. En réalité, utiliser le bitcoin pour des activités illégales serait aujourd'hui particulièrement risqué ! Et ce d'autant plus que les progrès techniques ne feront que s'accroître en matière de transparence.

C'est ce qu'écrit Tracfin lui-même dans son rapport « Risques de blanchiment de capitaux et de financement du terrorisme en 2016 » : « *une caractéristique essentielle de la blockchain bitcoin reste la traçabilité. Au fur et à mesure que l'utilisation de la blockchain bitcoin se banalise, les outils logiciels d'analyse des transactions se développent*⁸⁵ ».

Ainsi, BitFury, l'une des plus grandes entreprises du secteur blockchain dans le monde, a récemment annoncé qu'un nouveau produit, Crystal, permettra aux enquêteurs de « tracer les transactions bitcoin et de noter la probabilité qu'une adresse bitcoin spécifique reçoive de l'argent sale » en analysant le web, les forums et d'autres sources d'informations.

« Le fonds d'origine illicite concerne moins de 1% des transactions en bitcoin, et ne font que diminuer »

De fait, les rares études réalisées en la matière montrent que les activités illicites représentent une fraction extrêmement limitée des échanges de bitcoins. Le think tank américain « Fondation pour la défense de la démocratie » a publié en janvier 2018 une étude détaillée sur le réseau Bitcoin de 2013 à 2016. Ses résultats montrent que les fonds d'origine illicite représentent moins de 1 % du volume des transactions du réseau Bitcoin, et qu'ils n'ont fait que diminuer au fil des années pour atteindre 0,1% sur la dernière année considérée⁸⁶. Une étude d'Europol abonde dans le même sens : selon elle, la part des transactions en bitcoins liées à un commerce illégal ne représentent que 3% à 6% du total.

In fine, un constat s'impose : **ces accusations sur les dangers des cryptoactifs relèvent de la même peur que celle exprimée envers Internet dans les années 1990.**

Le parallèle entre la réputation des cryptoactifs aujourd'hui et la réputation d'Internet à ses débuts est en effet saisissant. Dans le documentaire « Une contre-histoire des Internets », Laurent Chemla, fondateur de Gandi, raconte qu'en 1995, la première fois qu'une émission de télévision évoque Internet, elle le décrit comme « un repaire de pirates, de néo-nazis, de pédophiles ».

85 une caractéristique essentielle de la blockchain bitcoin reste la traçabilité. Au fur et à mesure que l'utilisation de la blockchain bitcoin se banalise, les outils logiciels d'analyse des transactions se développent

86 <http://www.defenddemocracy.org/media-hit/yaya-j-fanusie-bitcoin-laundering/>

« Le parallèle entre la réputation des cryptoactifs aujourd'hui et la réputation d'Internet à ses débuts est saisissant »



Les archives de l'INA se révèlent précieuses pour corroborer ces souvenirs. En 1995 Daniel Bilalain fait ainsi écho, lors d'un journal télévisé présenté sur France 2, du risque terroriste ouvert par Internet, un « réseau que personne ne contrôle » : « On a découvert que sur le fameux réseau de communication international, Internet, n'importe qui pouvait trouver la recette destinée à confectionner des bombes. C'est aussi simple et terrifiant que cela⁸⁷ ». Le reportage présente d'ailleurs un numéro de La Revue des directeurs administratifs financiers affichant en couverture : « Internet: le réseau de tous les dangers? ».

L'année suivante, un reportage de France 3 évoque à son tour brièvement Internet, cette fois-ci pour témoigner des risques qu'il présente en termes de pédophilie⁸⁸ ; de même, France 2 présente de nouveau Internet quelques mois plus tard, sur les risques liés au terrorisme là encore⁸⁹.

En 1997, un rapport dédié à Internet, mené par le député Patrice Martin-Lalande, est remis au gouvernement. Si sa tonalité est positive et incite l'Etat à agir en faveur du développement d'Internet, une phrase reste révélatrice de l'image que le réseau porte encore alors : « L'Internet est souvent présenté comme un réseau transportant une grande quantité d'images pornographiques ».

Au même moment, Amazon commence à se développer aux Etats-Unis. Deux faces d'une même pièce. Deux façons de considérer l'innovation de rupture.

Aujourd'hui, même si Internet continue de susciter des craintes, légitimes, sur son rôle dans les activités terroristes notamment, il n'est plus question de nier les multiples opportunités positives ouvertes par le réseau, pourtant insuffisamment considérées dans ses premières années. Les cryptoactifs semblent aujourd'hui suivre le même chemin...

4/ Des technologies vouées à l'échec ?

Les cryptomonnaies agissent comme un révélateur : à force d'irriter, elles dessinent en creux tous les défauts du royaume des « experts ». Un de ces principaux défauts tient à la question de la prédiction.

« La croissance d'Internet va ralentir drastiquement, car la faille de la loi de Metcalfe [selon laquelle l'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs] deviendra apparente : la plupart des gens n'ont rien à se dire ! D'ici 2005 environ, il deviendra clair que l'impact d'Internet sur l'économie n'est pas plus grand que celui du fax. »

87 <http://www.ina.fr/video/CAB95042655/recette-bombe-internet-video.html>

88 <http://www.ina.fr/video/CAC96019023/tout-images-internet-et-pedophilie-video.html>

89 <http://www.ina.fr/video/CAB96041748/internet-et-terrorisme-video.html>

Ces pronostics ont été écrits par Paul Krugman en 1998, dans un article intelligemment intitulé « Pourquoi la plupart des prédictions des économistes sont fausses⁹⁰ ». Sûr de son fait, il ajoutait ensuite : « avec le ralentissement du taux de changement technologique, le nombre d'offres d'emploi pour spécialistes IT décélèrera, puis se renversera ; dans dix ans, l'expression « économie de l'information » semblera stupide ».

Dix ans plus tard exactement, en 2008, Paul Krugman remportait le prix Nobel d'économie, pour d'autres analyses fort heureusement.

Cette anecdote est loin d'être un cas isolé en termes de prédiction réalisée parmi des « experts » du monde économique. Un exemple est resté célèbre en la matière : le cas AT&T et McKinsey. Au début des années 1980, l'opérateur téléphonique AT&T demanda au célèbre cabinet de conseil McKinsey d'estimer environ combien de téléphones portables seraient utilisés dans le monde au tournant du siècle. La conclusion de McKinsey fût claire : en raison de leurs défauts majeurs (poids trop important ; batteries trop faibles ; coût exorbitant ...), le téléphone portable ne deviendra pas un succès. McKinsey estima que seuls environ 900 000 personnes utiliseraient en l'an 2000 un téléphone portable, et que personne n'utiliserait ce type d'appareil si une ligne téléphonique fixe était disponible à proximité. McKinsey recommanda donc à AT&T de se retirer du marché des téléphones portables (coûtant à l'entreprise, des années plus tard, plusieurs milliards de dollars). Au tournant du siècle, le téléphone portable compta finalement plus de 100 millions d'utilisateurs, soit plus de cent fois le pronostic réalisé.

**“ « Internet ? Ça ne marchera jamais ! »
tranchait Pascal Nègre en 2001 ”**

Dans cet exemple comme dans de multiples autres qui auraient pu avoir leur place ici, **le problème ne tient pas tant à l'erreur d'analyse, qui peut tout-à-fait s'entendre, qu'à l'absence de doutes sur les pronostics exprimés.** "Internet ? On s'en fout, ça ne marchera jamais" tranchait ainsi Pascal Nègre, PDG d'Universal Music, dans une conférence en 2001⁹¹.

En réalité, la capacité d'accélération ou de retournement d'une tendance est souvent sous-estimée. Ainsi, phénomène inédit, en 2018 la majorité (absolue) des foyers américains n'a désormais plus de téléphone fixe. Il y a trente ans, un tel pronostic aurait été jugé inconcevable, en témoignent les certitudes de McKinsey à l'époque.

Aujourd'hui, les cryptoactifs voient un nombre important d'experts être « victimes » du même biais cognitif que celui vécu au moment des débuts du web. Ce biais est énoncé par l'**effet dit Dunning-Kruger : les moins qualifiés dans un domaine donné ont tendance à surestimer leur compétence dans ce domaine.** Ce biais les empêche de reconnaître objectivement le fait qu'ils ne maîtrisent pas le sujet donné. Les cas d'Internet et des cryptoactifs sont similaires voire identiques : il s'agit, pour tous les deux, d'innovation de rupture – un domaine que les acteurs traditionnels ont toujours eu du mal à appréhender et à détecter en avance de phase.

Les exemples cités ci-dessus incitent donc à la plus grande prudence s'agissant des prédictions fatalistes sur des tendances émergentes. Les cryptoactifs constituant aujourd'hui une tendance émergente forte, chacun serait bien avisé de prendre certaines pincettes avant d'exprimer des pronostics tranchés, pourtant régulièrement entendus à leur sujet...

⁹⁰ <http://web.archive.org/web/19980610100009/www.redherring.com/mag/issue55/economics.html>

⁹¹ <https://archive.org/details/RNBM2013MichelDeSouzaPascalNegreInternet>

Il n'est d'ailleurs pas interdit de changer d'avis au cours du temps, comme Christine Lagarde récemment. Alors que ses déclarations en la matière étaient plutôt critiques en 2015 et 2016⁹², la directrice générale du Fond Monétaire International (FMI) semble avoir reconsidéré sa position, comme elle l'exprimait dans un discours prononcé en octobre 2017 :

« Beaucoup d'obstacles des monnaies virtuelles pourront être réglés avec le temps. Il n'y a pas si longtemps, certains experts ne croyaient pas à l'adoption du PC ou prédisaient que les tablettes feraient office de plateaux à café. Je pense donc qu'il ne serait pas sage de négliger les monnaies virtuelles.

Ces nouvelles monnaies seront peut-être un jour moins risquées et plus facile à obtenir que la monnaie papier, surtout dans les régions reculées. Elles pourraient devenir de plus en plus stables. Les transactions pourraient être complètement transparentes et gouvernées par des règles prédéfinies par un algorithme.

A bien des égards, les devises virtuelles pourraient donc donner du fil à retordre aux monnaies existantes et à la politique monétaire. Les gens préféreront peut-être un jour les monnaies virtuelles parce qu'elles seront potentiellement aussi peu coûteuses et aussi pratiques que le cash, sans risque de règlement, sans délai de compensation, sans enregistrement central et sans intermédiaire pour vérifier votre compte ou votre identité ».

Ces déclarations font aujourd'hui figures d'exceptions pour une dirigeante de ce niveau, dans la sphère financière. Christine Lagarde n'affirme pourtant rien de définitif : elle ne fait simplement qu'envisager une possibilité, celle que les cryptomonnaies atteignent effectivement leurs promesses dans le domaine monétaire, à l'encontre de nombre de pronostics exprimés par les économistes qui les voient aujourd'hui mourir à court ou moyen terme...

Comment les cryptoactifs pourraient-ils, dès lors, parvenir bel et bien à s'imposer ?

L'investisseur Chris Dixon estime que *« les réseaux décentralisés peuvent remporter la troisième ère de l'Internet en gagnant les cœurs et les esprits des entrepreneurs et des développeurs⁹³ »*. Il prend l'exemple de la bataille au début des années 2000 entre Wikipédia et les encyclopédies centralisées comme Encarta. *« Si vous comparez les deux produits au début des années 2000, Encarta était un bien meilleur produit. Mais Wikipédia s'est amélioré à un rythme bien plus rapide, parce qu'il avait une communauté active de contributeurs volontaires qui ont été attirés par ses valeurs décentralisées. En quelques années, Wikipédia s'est imposé comme l'encyclopédie la plus populaire sur Internet. Encarta a fermé en 2009 »*.

Pour lui, la question de savoir qui des systèmes décentralisés ou centralisés s'imposera dans la prochaine ère de l'Internet dépend d'une chose : lesquels de ces systèmes attirera le plus de développeurs et d'entrepreneurs de talents. *« Les Gafa ont de nombreux atouts, comme des réserves financières, des bases d'utilisateurs larges, et des infrastructures opérationnelles. Les cryptoréseaux ont une proposition de valeur nettement plus attractive pour les développeurs et les entrepreneurs. S'ils peuvent gagner leurs cœurs et leurs esprits, ils pourront mobiliser bien plus de ressources que les Gafa, et dépasser rapidement leur développement de produits »* juge-t-il.

5/ Les cryptoactifs, des actifs sans utilité réelle ?

« Si vous demandiez aux gens en 1989 ce dont ils avaient besoin pour améliorer leur vie, il est peu probable qu'ils vous auraient répondu un réseau décentralisé de nœuds liés les uns aux autres, qui utilise hypertexte » (Sep Kamvar)⁹⁴

Les chapitres précédents doivent justement permettre de répondre à cette question en montrant en quoi les cryptoactifs constituent la clef d'une nouvelle économie numérique, avec les usages protéiformes des tokens.

92 Voir <https://bitcoin.fr/lagarde/>

93 <https://medium.com/@cdixon/why-decentralization-matters-5e3f79f7638e>

94 <http://farmerandfarmer.org/mastery/builder.html>

Le lecteur pourrait toutefois rester sur sa faim en termes d'exemples concrets d'applications. Ceci n'est pas un oubli, mais la volonté de ne pas se prêter au jeu de la futurologie. Il est toujours facile d'affirmer que dans cinq, dix, quinze ans, tel usage se sera massivement développé au point d'avoir supplanté tel ou tel autre usage ; par exemple, de prédire le remplacement de Facebook par un réseau social décentralisé où les utilisateurs resteraient maîtres de leurs données, ou encore le remplacement d'Uber par une application de mise en relation directe entre conducteur et passager sans intermédiaire, ce qui constituerait une véritable « uberisation d'Uber ».

L'honnêteté intellectuelle incite plutôt à se garder de prédictions sensationnalistes. **Peu auraient pu prédire dans les années 1990 les chemins pris par le web, au-delà du seul e-commerce, et en particulier l'émergence quinze ans plus tard de Facebook, Uber, BlaBlaCar, Twitter, etc. La blockchain et les cryptoactifs suivront probablement la même logique.**

Si l'on devait tout de même se livrer au jeu du pronostic, celui-ci serait le suivant. Les GAFAs ont habitué les individus à des services intuitifs, simples d'utilisation, parfois même addictifs dans le cas de Facebook. Les GAFAs sont certes loin d'être éternels, et le réseau social Facebook semble aujourd'hui voir son utilisation baisser drastiquement chez les nouveaux adolescents au profit d'autres applications (Snapchat et Instagram), mais ils disposent de moyens tels qu'il semble difficile, si ce n'est impossible, de les dépasser avec un service similaire, comme montré dans la première partie. Dans cette perspective, il ne s'agit pas de vouloir créer un nouveau Facebook, mais simplement d'autres concepts. Autrement dit, les cryptomonnaies et les tokens ne remplaceront pas forcément les usages existants : ils créeront de nouveaux usages, dont la plupart sont encore à imaginer et à développer.

« Les cryptomonnaies et les tokens ne remplaceront pas forcément les usages existants : ils créeront de nouveaux usages »

Ce qui créera le plus de valeur résidera sans doute dans des solutions trouvées en-dehors des paradigmes existants. C'est ce qui s'est passé avec Internet. 98% des 50 sites web les plus visités au monde sont le fait d'entreprises nées avec le web lui-même (la seule exception étant le site de Microsoft). Les applications les plus intéressantes du web décentralisé seront celles qui permettront des modèles qui n'étaient pas possibles jusqu'à présent, comme Storj (location d'espace de stockage libre sur un réseau décentralisé) et iExec (location de puissance de calcul inutilisée sur un réseau décentralisé).

« 98% des 50 sites web les plus visités au monde sont le fait d'entreprises nées avec le web »

Tout est donc à inventer. *C'est justement la virginité de cet immense nouveau terrain pour l'innovation de rupture qui doit susciter l'intérêt de nos entrepreneurs, développeurs, chercheurs, innovateurs de tout type, et, au-delà, celui des pouvoirs publics, dont une des missions clefs est de préparer l'avenir et permettre à la France et l'Europe de faire partie, cette fois-ci, des leaders de la nouvelle économie.*

VI. UNE OPPORTUNITÉ À SAISIR RAPIDEMENT

« La révolution blockchain est déjà là. Cette tendance avance fortement. Surfez sur la tendance et vous prospérerez. Opposez-vous à cette tendance et vous êtes condamné. C'est une subversion complète de la tradition, bien plus forte qu'Internet et l'Internet mobile » (Bob Xu, l'un des investisseurs en capital-risque les plus réputés de Chine)⁹⁵.

A/ Pourquoi il faut agir (vite)

La France et l'Europe ont raté le (premier) train d'Internet. Les Etats-Unis et la Chine dominent aujourd'hui le classement des licornes, ces startups nées après l'an 2000 valorisées plus d'un milliard de dollars. Malgré des progrès manifestes ces dernières années, notamment en financement des startups, la France et l'Europe peinent à rattraper l'immense retard accumulé au fil des ans.

Comme expliqué précédemment, le web décentralisé ouvre la voie d'une nouvelle économie numérique, qui renverse les règles et les stratégies connues jusqu'à présent dans le numérique. De nouveaux acteurs, et donc de nouveaux champions, vont émerger. Les GAFA, fondés sur des logiques de centralisation, n'ont sans doute pas leur place dans ce web. De la même façon que Microsoft n'avait pas vu venir le tournant Internet, le paradigme qui a suivi l'informatique, les GAFA sont aujourd'hui complètement absents du web décentralisé. C'est une chance inouïe pour la France et l'Europe, qui luttent aujourd'hui pour combler leur retard face aux géants du numérique actuel.

Plus encore : **ce nouveau web est aligné avec les valeurs portées par la France et l'Europe, que ce soit en termes de privacy, de partage de la valeur créée, ou de juste concurrence dans l'innovation.** Contrairement aux plateformes des GAFA, le créateur d'une application décentralisée fondée sur la blockchain n'en est pas le maître absolu : il ne contrôle pas, par exemple, les données de ses utilisateurs. Les internautes redeviennent maîtres de leurs données et plus largement de leur identité numérique. L'internaute est remis au centre du jeu. De même, le créateur d'une application décentralisée ne peut pas changer ses conditions générales ou ses fonctionnalités de façon brusque et unilatérale, comme Facebook l'a imposé aux médias récemment. Enfin, comme expliqué précédemment, le web décentralisé permet d'une part de partager plus équitablement la valeur créée, d'autre part d'introduire une concurrence plus équitable entre ses acteurs, en réduisant l'effet « winner-takes-it-all ».

« Ce nouveau web est aligné avec les valeurs portées par la France et l'Europe, que ce soit en termes de privacy, de partage de la valeur créée, ou de juste concurrence dans l'innovation »

La France dispose d'atouts sérieux pour devenir l'un des pôles de référence en matière de cryptoactifs, grâce à l'excellence de ses ingénieurs, mathématiciens, cryptographes, mais aussi grâce son dynamisme entrepreneurial et la présence d'une communauté très active autour de ces technologies (constituée autour du forum CryptoFR créé par Quentin de Beauchesne, de l'association Chaintech présidée par Alexandre Stachtchenko, du Cercle du Coin créé notamment par Jacques Favier ou encore de l'association Asseth présidée par Jérôme de Tychey). Elle compte un nombre croissant d'entreprises dans ce secteur, dont des acteurs réputés mondialement comme Ledger et Acinq. Le nombre d'offres d'emplois en France liés aux cryptoactifs a du reste triplé en 2017 par rapport à 2016, et la tendance devrait se poursuivre, si ce n'est s'accélérer, en 2018⁹⁶.

⁹⁵ <http://news.8btc.com/charles-xue-diss-bob-xu-i-was-not-so-pumped-on-blockchain-investment-as-him>

⁹⁶ <https://joblift.fr/Presse/crypto-monnaies-offres-demploi-triples-en-2017-mais-des-postes-qui-peinent-tre-pourvus>

Ledger, tête de proue de l'écosystème français des cryptoactifs

Ledger, le leader mondial de la sécurisation des cryptoactifs, est un acteur français dont l'usine se trouve à Vierzon, dans le Parc Technologique de Sologne. Ce centre logistique est l'un des principaux pourvoyeurs d'emploi de la région. De 15 employés en 2016 (CA 650k€), l'entreprise est passée à 90 employés en 2017 (CA : 46 millions d'euros soit +7 000 %) avec une prévision de 200 employés en 2018, pour la plupart en France. Après une levée de fonds de 61 millions d'euros en janvier, elle est considérée comme l'une des startups les plus crédibles pour devenir la future licorne française.

Dès lors, il est indispensable de saisir sans attendre les opportunités de cette nouvelle innovation de rupture. Ne reproduisons pas l'erreur du Minitel à la fin du siècle dernier, lorsque l'Etat avait choisi de soutenir le réseau Transpac, support technique du Minitel mené par la Direction générale des télécommunications (future France Télécom), au détriment du réseau Cyclades, qui posait les prémisses du protocole TCP/IP à l'origine d'Internet. Dans les années 1990, France Télécom et le gouvernement avaient même souhaité interdire Internet⁹⁷, dont l'architecture ouverte s'opposait à la fermeture du réseau du Minitel, alors vue comme un atout (par les opérateurs télécoms) ; une opposition comparable à celle aujourd'hui entre les réseaux ouverts que représentent les blockchains publiques (qui suscitent des inquiétudes, justement pour ces mêmes raisons) et les réseaux fermés que sont les blockchains privées.

La blockchain suscite les mêmes crispations qu'Internet il y a 25 ans

« Internet est célébré pour son orientation démocratique. Aucune distinction n'y est faite entre un « serveur » délivrant des informations et un « terminal » à partir duquel un usager les consulte. Une telle particularité frappe l'utilisateur du Minitel (où la séparation est totale). Sur Internet, tout consommateur est potentiellement producteur (et vice versa) » (Astrad Torres, « Faut-il brûler Internet ? » paru en novembre 1995 dans Le Monde Diplomatique⁹⁸).

Internet a décentralisé l'information. La blockchain décentralise la valeur. Elle suscite donc logiquement les mêmes crispations qu'il y a vingt-cinq ans. A l'époque, comme le rappelle Patrice Martin-Lalande, ancien député auteur du rapport "L'internet : un vrai défi pour la France" paru en 1997, « il y avait le danger de l'inconnu. Internet était un bouleversement total des modes de communication. C'est un outil qui ignore les frontières, les distances, et par rapport aux États, c'était la remise en cause de l'un des fondements de leur autorité ⁹⁹ ». Les mêmes réflexions peuvent être faites aujourd'hui vis-à-vis de la blockchain et des cryptoactifs : celles-ci bouleversent effectivement la création et les échanges de valeur, et remettent en cause les institutions qui contrôlent aujourd'hui cette création et ces échanges.

97 <https://www.youtube.com/watch?v=dO4GaUmGdHY>

98 <https://www.monde-diplomatique.fr/1995/11/TORRES/6781>

99 <http://www.slate.fr/story/136043/rapport-internet-france-1997>

La comparaison entre d'une part blockchains privées et Minitel, d'autre part blockchains publiques et Internet, a d'autant plus de sens que les réseaux fermés connaissent souvent au départ plus de réussite : ceux-ci sont en effet (bien) moins ambitieux et font face, de ce fait, à moins d'obstacles. Ainsi, les blockchains privées commencent déjà à être mises en place et exploitées par de grands acteurs économiques, alors que les blockchains publiques ne sont pas encore réellement utilisées par le grand public. De la même façon, le Minitel avait lui aussi connu un certain succès en France bien avant Internet. Rappelons-nous cette phrase de Jacques Chirac en 1997 : « *La boulangère d'Aubervilliers sait parfaitement interroger sa banque par Minitel, alors que la boulangère de New York en est incapable* ».

Ironie de l'Histoire : à l'origine, la France était bien partie dans la révolution Internet puisque le projet Cyclades, précurseur du réseau Internet, était porté par un chercheur français, Louis Pouzin. Louis Pouzin s'est toutefois vu couper les subventions publiques accordées à ses travaux. En conséquence, ces derniers ont été réutilisés par deux Américains pour développer ce qui est devenu ensuite Internet...

Avec l'émergence du web décentralisé, il est essentiel, cette fois-ci, de ne pas rater le coche. La France n'est pas condamnée à avoir fatalement un train de retard. **Les autres puissances ne nous attendent cependant pas. En Russie, Vladimir Poutine a rencontré dès juin 2017 le fondateur de la blockchain Ethereum, Vitalik Buterin**, en marge du Forum économique de Saint-Petersbourg. Dans des déclarations récentes, en février 2018, il exprimait sa compréhension des enjeux de ces technologies : « *Ce n'est pas la première fois que nous parlons de ce sujet. Certains peuvent se demander : « Pourquoi en avons-nous besoin ? Nous avons tout : pétrole, gaz, charbon, métaux de toutes sortes, or, platine, argent... ».* Mais nous devons aller plus loin. L'âge de pierre ne s'est pas terminé à cause d'un manque de pierres, mais parce que d'autres technologies sont apparues. Aujourd'hui de nouvelles technologies apparaissent dans le monde. Si nous sommes en retard dans cette course, alors très vite nous serons sous la dépendance totale des leaders de ces processus. La Russie ne peut pas se le permettre¹⁰⁰ ».

Vladimir Poutine souligne ici l'enjeu stratégique représenté par ces technologies : celles-ci constituent non seulement un nouveau terrain pour l'innovation de rupture mais également une bataille qui touche à la souveraineté de chaque grande puissance.

Outre l'enjeu de souveraineté, ces technologies constituent aussi et d'abord une bataille de compétitivité et d'attractivité. Celle-ci semble s'accélérer depuis ces derniers mois. En mars, le groupe américain BitFury a installé une ferme de « minage » de bitcoins en Norvège. L'inauguration a été applaudie directement par le Ministre du Commerce et de l'Industrie norvégien, qui a pu se féliciter de la création de trente emplois locaux grâce à cette seule installation. De même, lorsque quelques jours plus tard la première plateforme mondiale d'échange de cryptoactifs, Binance, a annoncé son installation à Malte, le Premier Ministre de Malte en personne a salué publiquement cette décision. Bien d'autres exemples pourraient être cités ici mais tous convergent vers le même constat : les acteurs des cryptoactifs choisissent de s'installer dans les pays où ils peuvent s'assurer de la bienveillance des pouvoirs politiques à l'égard de ces technologies. La bataille d'attractivité, qui ne fait que commencer, sera remportée par les pays qui auront su attirer tôt les acteurs du secteur, par des décisions ou prises de position incitatives.

100 Voir vidéo de ses déclarations : <https://t.co/i7dQCb6Dms>

B/ Une question de choix, de vision et de méthodes

Qu'en est-il en France ? Le gouvernement affiche sa volonté de faire du soutien à « l'innovation de rupture » une priorité, avec la création d'un fonds de dotation de 10 milliards d'euros (...dont la capacité de financement sera en réalité proche de 200 à 300 millions d'euros par an). Trois remarques peuvent être faites ici à ce sujet.

1/ Les pouvoirs publics doivent prendre conscience que **devenir leader dans une innovation de rupture nécessite de faire des paris, et donc de prendre des risques**. Aujourd'hui, la quasi-totalité de l'effort en termes d'innovation de rupture semble porté vers l'intelligence artificielle (IA). Or l'IA n'est plus un pari : plus personne ne doute aujourd'hui qu'il s'agit bel et bien d'une grande technologie d'avenir. La France se positionne très tard pour tenter d'être leader en IA. C'était lorsque l'IA était encore un pari, lorsqu'elle était loin des projecteurs, qu'il fallait produire l'effort pour s'emparer du leadership. Il est bien sûr crucial de tenter aujourd'hui de rattraper notre retard en IA ; mais si nous ne voulons pas, demain, nous retrouver dans cette même situation lorsque les futures innovations de rupture émergeront, il nous faut repérer ces innovations en amont, et nous y préparer avant les autres – ou du moins, pas après...

2/ Ce problème de retard à l'allumage est un mal bien connu en France. Gérard Berry, l'un des plus grands informaticiens français, professeur au Collège de France, médaille d'or 2014 du CNRS, raconte ainsi : « *En France, on n'a pas cru en l'informatique. On a dit que c'était une mode et que ça allait passer. Dans les années 80, dans les grandes écoles, on se demandait si l'informatique était un sujet ou pas. En 1985, à Polytechnique, on se demandait encore s'il fallait l'enseigner* ».

Lorsqu'il est devenu ensuite évident que l'informatique allait être incontournable, est arrivé Internet. Les grands acteurs économiques et politiques ne savaient pas s'il fallait considérer au sérieux ou non cet ovni. Pour se faire un avis, le gouvernement d'Edouard Balladur a commandé à un rapport, le rapport Théry, intitulé « Les autoroutes de l'information », et remis en 1994¹⁰¹. Sa conclusion est explicite : « *il n'existe aucun moyen de facturation sur Internet, si ce n'est l'abonnement à un service. Ce réseau est donc mal adapté à la fourniture de services commerciaux. Le chiffre d'affaires mondial sur les services qu'il engendre ne correspond qu'au douzième de celui du Minitel. Les limites d'Internet démontrent ainsi qu'il ne saurait, dans le long terme, constituer à lui tout seul, le réseau d'autoroutes mondial* ».

Erreur sur toute la ligne. Pour l'informatique comme pour Internet, la France n'a pas su écouter les bonnes personnes, celles capables de porter une vision de l'innovation de demain. Faire de la France une terre d'innovation nécessite donc de changer de lunettes, en écoutant des sons de cloche différents venant d'acteurs moins établis : l'innovation de rupture vient en effet rarement des élites, mais bien souvent de la marge...

3/ Ce raisonnement vaut non seulement pour le choix des innovations à soutenir, mais également ensuite pour la méthode de soutien. Décider d'investir 200 à 300 millions d'euros par an dans l'innovation de rupture est une chose (discutable par ailleurs au vu du faible montant comparé à ceux investis par les autres puissances) ; savoir où injecter cet argent en est une autre. En la matière, les erreurs de jugement peuvent se produire facilement, en imitant les choix faits par le passé, en particulier au XXe siècle. Ainsi, dans le monde des cryptoactifs, l'innovation est venue jusqu'ici principalement des communautés de développeurs, ce qui est sensiblement différent d'autres vagues d'innovation parfois plus issues des universités et du monde de la recherche.

Dès lors, si les pouvoirs publics décident de faire des cryptoactifs un enjeu de développement important, ce sont en priorité les communautés de talents en cryptoactifs (entrepreneurs et développeurs) qui doivent être soutenues. Si le travail de ces talents n'est pas soutenu, ou a minima si les obstacles qu'ils connaissent ne sont pas levés, la France ne pourra pas devenir un acteur important du web décentralisé.

101 Encore accessible en ligne : <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000675.pdf>

Pour que cette prise de conscience se produise effectivement, encore faut-il néanmoins savoir écouter ces communautés, qu'un acteur politique présentait récemment en privé comme des « réserves d'Indiens » devant l'auteur de cette note... Là encore, un changement de lunettes s'impose. Il est évident que les innovations de rupture ne sont pas créées et portées par des personnalités « classiques », typiques. Si les acteurs économiques et politiques n'acceptent pas d'écouter, d'inviter et de dialoguer avec des personnalités plus marginales, le gouffre entre politique et innovation de rupture ne risque pas de se réduire.

Dans le cas de la blockchain, si les pouvoirs publics écoutent en priorité les acteurs très établis, en particulier du secteur bancaire et financier (ce qui reviendrait à demander à l'industrie musicale en 2000 ce qu'elle pense d'Internet), soyons-en certains : la France se retrouvera avec un rapport Théry bis, qui recommandera probablement de privilégier des blockchains privées, dont on imagine qu'elles pourront être qualifiées de « meilleur compromis entre innovation et sécurité »... Pour s'en convaincre, il suffit de lire la note de la Banque de France de mars 2018 qui consacre un portrait au vitriol des cryptoactifs, caricatural tant il est orienté. Les cryptoactifs sont parés de tous les dangers par la Banque de France : en plus d'être comparés à la tulipomania de 1637 aux Pays-Bas, ils sont accusés entre autres d'être « vecteurs de risques de cyber-attaques, de blanchiment d'argent et de financement du terrorisme, tout en ayant un coût environnemental ¹⁰²»....

Cette prise de position est emblématique : jusqu'ici, la France a eu tendance à considérer les cryptoactifs sous le seul spectre des dangers. Comme présenté dans la partie précédente, le parallèle entre la réputation des cryptoactifs aujourd'hui et la réputation d'Internet dans les années 1990 est saisissant.

Internet était présenté en 1995 comme un lieu de tous les dangers (pédophilie, terrorisme, Ponzi...). En 2000, comme Bitcoin aujourd'hui, Amazon était même présenté comme un schéma de Ponzi par certains commentateurs¹⁰³ ! Tout comme Internet facilite effectivement certains dangers, les cryptoactifs présentent eux aussi des risques inhérents à leur usage, qu'il convient de prendre à bras-le-corps en refusant le développement d'un far-west. Mais un équilibre doit être trouvé, au risque, à défaut, de tuer toute perspective d'innovation en la matière en France. En tout état de cause, contrairement à ce que certaines déclarations publiques peuvent affirmer, il n'est pas possible de réguler le protocole Bitcoin lui-même : ce sont les acteurs des cryptoactifs qu'il est possible de réguler.

Pistes de régulation face aux risques posés par les cryptoactifs

a. La protection des investisseurs et des particuliers, via des actions de pédagogie, une lutte contre les arnaques, et des sanctions fortes

Ceci passe en particulier par l'éducation et la promotion de bonnes pratiques, ainsi que la lutte contre les escrocs qui pullulent sur le marché des cryptoactifs. Quentin de Beauchesne, fondateur de CryptoFR, explique ainsi : « **Nous disposons actuellement d'une liste de plus de 250 sites de fausses plateformes d'échange, disponible sur le forum CryptoFR et déjà reprise par divers acteurs francophones. Une partie de cette liste a été signalée par la FSMA, le régulateur belge, qui nous a remercié de cet effort contre les arnaques et qui nous a demandé de lui rediriger toute victime belge de ce genre de site afin qu'elle puisse ajouter de manière officielle ce faux site à sa liste de mise en garde.**

Nous attendons par contre toujours un signe de la part des régulateurs français, qui n'ont pour le moment pas communiqué sur ces sujets. Nous recevons un nombre croissant d'investisseurs en panique, totalement perdus, émettant le souhait de poursuivre ces arnaqueurs. »

102 https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf

103 http://www.slate.com/articles/business/moneybox/2000/02/amazon_ponzi_scheme_or_walmart_of_the_web.html

Une coordination avec les représentants de CryptoFR est donc essentielle pour conjuguer les efforts en matière de lutte contre les arnaques (schémas de Ponzi, cryptomonnaies frauduleuses, etc.), qui peut encore être nettement renforcée.

En outre, des sanctions exemplaires doivent être prises contre les escrocs pour faire bien comprendre aux différents acteurs qu'il n'y aura aucune impunité en la matière.

b. L'application des dispositions de lutte anti-blanchiment

Aujourd'hui, les opérateurs français appliquent les obligations relatives à la lutte contre le blanchiment et le financement du terrorisme (LCB/FT). En particulier, les plateformes de change, comme La Maison du Bitcoin à Paris, appliquent les standards bancaires :

- Identification du client dès le 1er euro,
- Mesure de contrôle de l'origine des fonds pour les transactions importantes,
- Déclaration de soupçon auprès de TRACFIN en cas de doute.

Cet établissement développe même des outils d'intelligence artificielle pour limiter au maximum les risques de blanchiment. Pourtant, la situation est complexe en l'absence d'autorité de régulation désignée par les textes : ni l'AMF, ni l'ACPR, ni la DGCCRF ne supervisent ni n'accompagnent officiellement ces opérateurs.

La solution proposée est donc faire entrer expressément les opérateurs "crypto" dans le champ de compétence des autorités de régulation.

c. L'octroi d'un agrément aux opérateurs français

Comme en matière de lutte anti-blanchiment, les opérateurs français se présentent, dans leur grande majorité, volontairement auprès des autorités de régulation¹⁰⁴. Pourtant, aucun agrément n'existe aujourd'hui pour ces activités. Un agrément adapté aux spécificités des cryptoactifs permettrait d'améliorer la protection des clients en contrôlant :

- La compétences et la respectabilité des porteurs de projets;
- La structuration juridique (gouvernance) et capitalistique (fonds propres et capital social) des projets;
- Et, plus généralement, la légalité des dispositifs employés.

Pour les entrepreneurs, cet agrément aurait l'avantage de leur permettre d'être identifiés comme acteurs légitimes auprès des clients et des tiers (banques, avocats, experts-comptables, administration...). Attention cependant à ne pas entraver l'émergence des acteurs légitimes en fixant un agrément excessivement strict.

Les mentalités commencent heureusement à évoluer depuis peu. Jusqu'alors critique quant aux risques posés par les cryptoactifs, le Ministre de l'Economie, Bruno Le Maire, semble avoir nettement évolué sur le sujet : en mars 2018, il publiait ainsi une déclaration d'amour aux blockchains et cryptoactifs, qui a été remarquée bien au-delà de nos frontières¹⁰⁵. Il y écrivait notamment ceci : « *nous avons permis en décembre dernier, grâce à une ordonnance, l'utilisation de la blockchain pour la transmission de titres financiers. Pourquoi s'arrêter là ? Oui, sur les crypto-actifs également, nous entendons bien rester à la pointe ! Ne soyons pas de simples spectateurs : devenons acteurs de cette révolution* ». Pour la première fois, ce n'était pas simplement le mot générique de « blockchain » qui était mis en avant, mais bien aussi celui, bien moins

104 L'ACPR a déclaré lors de son audition au Sénat le 7 février 2018 avoir reçu plus de 200 projets.

105 <https://www.numerama.com/politique/336943-tribune-cryptoactifs-blockchain-ico-comment-la-france-veut-rester-a-la-pointe-par-bruno-le-maire.html>

consensuel, de cryptoactifs.

Au-delà du gouvernement, les choses progressent aussi du côté des parlementaires. Deux missions ont été lancées début 2018 à l'Assemblée Nationale sur ces technologies, l'une dédiée à la blockchain, l'autre (menée au sein de la Commission des Finances) aux cryptomonnaies. La première aboutira à des recommandations en septembre 2018 après avoir auditionné près de 200 experts¹⁰⁶. La seconde est destinée à faire adopter des mesures législatives à brève échéance. Chacune de ses missions est portée par des rapporteurs qui ont montré jusqu'ici leur bonne compréhension des enjeux de ces technologies. Il est heureux que l'Assemblée compte en ses rangs en particulier deux députés qui suivent ces sujets depuis plusieurs années, Laure de la Raudière et Pierre Person, dont les points de vue sur les blockchains et les cryptoactifs sont aiguisés, comme le démontre leurs déclarations respectives récentes¹⁰⁷.

Pour le Président de l'AMF, « le développement des crypto-actifs est une tendance lourde, qu'il convient non de combattre mais d'accompagner »

Enfin, du côté des régulateurs, il faut saluer la démarche d'écoute et de dialogue de la Direction Générale du Trésor ainsi que de l'Autorité des Marchés Financiers (AMF) avec sa consultation publique sur les ICO, qui s'est achevée en décembre, et qui devrait déboucher sur la création d'un visa optionnel pour les porteurs de projets d'ICO - une excellente nouvelle. La prise de position du Président de l'AMF, Robert Ophèle, le 5 avril 2018 devant la mission d'information sur les cryptoactifs de l'Assemblée Nationale est du reste d'une tonalité inédite : « *Le rôle de la monnaie, la place de l'intermédiation bancaire, le rôle des marchés financiers, la protection des investisseurs, doit être revisité à la lumière des ruptures que peuvent apporter les crypto-actifs. Le développement des crypto-actifs est une tendance lourde, qu'il convient non de combattre mais d'accompagner via un encadrement qui permette son essor dans un cadre plus sécurisé qu'aujourd'hui* ¹⁰⁸ ».

Ces initiatives et déclarations vont bien sûr dans le bon sens (même si les pouvoirs publics présentent encore des voix discordantes comme en témoignent les prises de position répressives de la Banque de France en matière de cryptoactifs). Il reste maintenant à passer aux actes. Par ailleurs, en dépit du très bon choix effectué pour le cadre réglementaire des ICO, la France accuse un retard certain dans la course mondiale, que le visa optionnel ne règlera pas à lui seul : comme expliqué plus haut, les ICO ne sont qu'un pan parmi d'autres des cryptoactifs.

D/ Comment agir (vite)

Pour faire de la France une nation en pointe sur le web décentralisé et la « token économie », les politiques publiques doivent cibler en priorité les talents en blockchain et cryptoactifs. Dans cette perspective, trois objectifs doivent être poursuivis : faire émerger des talents à l'intérieur du pays, retenir nos talents déjà formés, et attirer les talents étrangers.

a/ Faire émerger des talents

Les startups blockchain françaises, comme leurs homologues à l'étranger, font face à une pénurie de talents, en particulier une pénurie de développeurs blockchain. Par ailleurs, l'écosystème français des cryptoactifs, bien que grandissant mois après mois, reste encore relativement petit. Dans cette perspective il est crucial de faire émerger des vocations dans ce secteur naissant qui est appelé à connaître un boom important au cours des prochaines années.

106 <https://www.jeanmichelmis.fr/blockchain-revolution-france-ne-rater>

107 Ici <https://bitcoin.fr/laure-de-la-raudiere-blockchain-et-cryptomonnaie-cest-difficile-a-dissocier> et ici <https://www.journaldunet.com/economie/finance/1208344-appliquer-le-prelevement-forfaitaire-unique-sur-les-crypto-actifs-n-est-pas-incoherent>

108 Voir ses déclarations en intégralité sur le site de l'AMF : <https://t.co/AgAm4iYneB>

Toute action de communication du gouvernement en la matière (évoquer plus régulièrement ces technologies de façon positive lors des discours politiques, effectuer des visites médiatisées de startups du secteur ou de lieux emblématiques comme La Maison du Bitcoin, etc.) permettra déjà de commencer à agir en ce sens sans nécessiter de dépenses. Dans cette perspective, **la reconnaissance par les acteurs publics des actions de la communauté française (en particulier des efforts de CryptoFR et de la Chaintech), accompagné d'un soutien financier, serait utile.** Celle-ci réalise en effet un travail essentiel d'éducation, de pédagogie, de déconstruction des idées reçues et d'alerte face aux arnaques.

Un enjeu essentiel est de faire comprendre au plus grand nombre, et en particulier aux jeunes appelés à rentrer prochainement sur le marché du travail, l'importance du web décentralisé et des cryptoactifs, et le fait qu'ils constituent des opportunités d'entrepreneuriat et d'emploi considérables. « *Le jeune Bill Gates construirait aujourd'hui une entreprise blockchain* » écrivait ainsi récemment l'investisseur américain Naval Ravikant.

Plus particulièrement, il est important de **soutenir les initiatives de création de cursus spécialisé en blockchain et en cryptoactifs, en particulier dans les écoles d'ingénieurs et d'informatiques.** Certaines écoles ont commencé à ouvrir ce type de cursus, comme l'ESILV à La Défense grâce à l'action d'acteurs pionniers comme Cyril Grunspan, ainsi que l'ESGI avec la création d'un Bachelor en Ingénierie de la Blockchain (sans oublier l'ECE qui a organisé plusieurs « hackathons » dédiés), mais elles restent trop peu nombreuses.

Au-delà des seuls ingénieurs, l'écosystème français (comme les autres ailleurs dans le monde) a besoin de profils très diversifiés pour se développer de façon riche et équilibrée. **Les cryptoactifs et la « token économie » nécessitent en effet des compétences certes technologiques, mais aussi business, économiques, cryptographiques, financières, monétaires, juridiques, sociologiques, géopolitiques, historiques, énergétiques, statistiques,** mais aussi, de façon plus pratico-pratique, graphiques et de design pour améliorer l'expérience utilisateur qui fait aujourd'hui encore souvent défaut dans cet univers. Ces technologies auraient également **besoin de spécialistes des enjeux de gouvernance, de réseaux, de théories des jeux, d'éthique du numérique, et de cybersécurité,** entre autres.

Dans cette perspective, il convient en particulier d'inciter les chercheurs des disciplines citées ci-dessus à travailler sur ces sujets. Les publications de recherche spécialisées en cryptoactifs se développent, comme en témoigne le lancement récent du LedgerJournal, « *revue dédiée à la recherche sur la blockchain et les cryptomonnaies* », publiée en ligne par l'Université de Pittsburgh¹⁰⁹. Comme présenté dans la troisième partie de ce rapport, avec les cryptoactifs émerge un nouveau domaine de recherche, **la cryptoéconomie.** Ce domaine, à la croisée de plusieurs disciplines (économie, blockchain, théorie des jeux, gouvernance...), **mériterait la création de chaires de recherches dédiées.** Une telle initiative permettrait de **placer la France en pointe sur ce domaine.**

De nouveaux métiers verront certainement le jour. Pensons ainsi à celui d'économiste des tokens, qui sera capable de comprendre, d'analyser, voire de prévoir les dynamiques à l'œuvre dans cette nouvelle économie. Si le monde du droit a commencé depuis plusieurs mois à s'intéresser à ces technologies - de nombreuses conférences ont été organisées en ce sens, des cabinets d'avocats ont publié des études, etc. -, les économistes ne se sont pas encore emparés du sujet en profondeur : leurs expertises seraient pourtant essentielles. A l'étranger, plusieurs économistes commencent ainsi à se pencher sur la valeur des tokens¹¹⁰.

De même, le web décentralisé mériterait des recherches fines sur le plan géopolitique, tant il y aurait à étudier et analyser en la matière ; sur le plan financier, étant donné les nouveaux questionnements qu'introduisent les tokens ; ou encore sur le plan énergétique, de façon à pouvoir aller au-delà des idées reçues quant au coût écologique réel des cryptoactifs dont il est beaucoup question.

109 <http://ledgerjournal.org/ojs/index.php/ledger>

110 Exemple : « Initial Coin Offerings and the Value of Crypto Tokens » de mars 2018 <https://www.nber.org/papers/w24418> présenté ici <https://www.coindesk.com/right-way-think-crypto-tokens/>

Dans l'objectif de faire émerger des talents, un point mérite en particulier d'être souligné : la nécessité d'une plus grande diversité des profils. Socialement, les acteurs français des cryptoactifs ne présentent pas, semble-t-il, une homogénéité comparable à celle du milieu des startups « classiques », où les entrepreneurs sont nombreux à venir de milieux privilégiés et à avoir fait des grandes écoles. En revanche, **le déséquilibre entre femmes et hommes est considérable** – un aspect qui n'est d'ailleurs absolument pas propre à la France. Une étude montre que **près de 97% des recherches "Blockchain" et "Bitcoin" sur Google sont effectuées par des hommes**. Il sera vital dans les années à venir de réduire ce gouffre. Là encore, la puissance publique a un rôle important à jouer en la matière, via des actions de communication et de pédagogie, pouvant être conjointes avec les initiatives déjà menées dans le secteur numérique plus globalement.

b/ Retenir les talents

Les talents partiront si la France n'est pas accueillante. Ils s'exporteront dans les pays où :

- d'une part, la régulation et le discours porté sur les cryptoactifs sont équilibrés et font la part entre les opportunités et les risques qu'ils représentent.
- d'autre part, la fiscalité sur les cryptoactifs est considérée comme plus claire et plus juste. C'est le cas dans l'ensemble des autres pays européens, dont l'Allemagne, la Belgique, etc.

Une première vague de départs de talents s'est produite en 2013-2014. Aujourd'hui **une seconde vague de départs, plus forte, est en cours**, pour développer des activités blockchain à l'étranger. A Lisbonne a ainsi émergé récemment un « Blockchain Café » lancé et tenu par des Français nouvellement expatriés. **Ces départs posent problème car il s'agit majoritairement des individus pionniers qui maîtrisent le mieux ces technologies.**

Pour endiguer ces vagues de départs, les remèdes sont donc ceux évoqués ci-dessus :

- Assouplir la fiscalité des cryptoactifs pour les particuliers. L'application actuelle du barème de l'impôt sur le revenu (régime BIC/BNC) sur les gains réalisés en cryptoactifs est en effet à la fois complexe¹¹¹ et peu adapté : le taux effectif maximum d'imposition atteint 62.5% alors que les autres biens incorporels bénéficient du Prélèvement Forfaitaire Unique au taux de 30%.

Dès lors, **il convient d'assujettir les gains en cryptoactifs au Prélèvement Forfaitaire Unique**. Le régime de la plus-value sur biens meuble peut être envisagé comme mesure transitoire : il ne requiert qu'un changement de doctrine fiscale.

- Pour les entreprises, **clarifier le traitement comptable des cryptoactifs ainsi que l'exonération de TVA en cas d'opération de change**. Une partie des difficultés des entreprises du secteur provient en effet de l'absence de règles comptables, ainsi que d'une incertitude sur l'application de la TVA pour certaines opérations. En outre, des mesures d'incitations fiscales doivent être envisagées si la France entend prendre le leadership en Europe.
- Du côté des pouvoirs publics, **adopter un discours plus positif sur les cryptoactifs**, qui ne met pas seulement en avant leurs risques mais aussi les opportunités qu'ils ouvrent.

Ce dernier aspect permet d'évoquer un autre point de blocage majeur qui doit impérativement être levé : **l'extrême difficulté actuelle pour un entrepreneur du secteur des cryptoactifs de trouver une banque acceptant d'ouvrir un compte pour sa société**. Les témoignages se suivent et se ressemblent d'entrepreneurs français retardés, voire bloqués, par ce problème dans leur création et développement d'activités liées aux cryptoactifs. Certains, découragés après avoir fait le tour des différentes banques, se tournent même vers des méthodes atypiques, comme devenir e-résident estonien pour tenter d'ouvrir un compte bancaire à distance en Estonie (pays roi des services numériques pour les citoyens). D'autres, plus simplement, créent leur entreprise dans des établissements étrangers...

111 Voir, par ex. : "Fiscalité des cryptomonnaies : un régime complexe et inadapté", Blockchain France, 17.01.2018

Face aux différents refus des banques françaises de leur ouvrir un compte, La Maison du Bitcoin et Ledger (entreprises situées à Paris dans le quartier du Sentier), qui constituaient il y a peu une seule et même entité juridique, ont même été contraintes il y a quelques années d'ouvrir leur compte bancaire en Allemagne, chez la banque Fidor (par ailleurs filiale de BCPE) ! Ledger, fleuron français des cryptoactifs, reconnu mondialement pour la qualité de ses produits, a dû attendre sa levée de fonds très récente (66 millions d'euros en janvier 2018) pour pouvoir disposer d'un compte bancaire en France. Mais derrière ce champion, de multiples jeunes entreprises et entrepreneurs voient les portes des banques toujours fermées...

Les pouvoirs publics ont un rôle décisif à jouer sur cette question clef. Eric Larchevêque, fondateur et CEO de Ledger, relatait ainsi sa discussion en 2014 avec le président de sa banque de l'époque, HSBC, qui justifiait sa décision de fermer les comptes de l'entreprise : « *J'ai rencontré le président de la banque, qui a affirmé qu'il n'avait pas le choix et qu'il devait 'choisir ses combats'. Le régulateur français lui met une pression considérable pour fermer toutes les activités liées au Bitcoin¹¹²* ». Ce témoignage souligne bien le poids des régulateurs dans les positions des banques sur le sujet. Il est donc crucial que les régulateurs et le Ministère de l'Economie et des Finances prennent des positions officielles encourageantes, et non répressives, sur les cryptoactifs.

En réalité, le danger ne se situe pas forcément là où l'on croit : plus encore que dans certains usages illicites des crypto-actifs, le risque réside avant tout dans la pénalisation de l'écosystème français face aux écosystèmes étrangers. Autrement dit, le risque est avant tout de passer à côté d'une innovation de rupture qui ouvre la voie de l'économie numérique de demain...

Un chiffre est éloquent à ce titre. Alors que la France a mis des bâtons dans les roues des entrepreneurs qui avaient souhaité développer des plateformes d'échange de cryptoactifs, la Corée du Sud a adopté une approche très différente : elle a favorisé l'innovation tout en protégeant les citoyens des arnaques et en prélevant une juste part des bénéfices du secteur. Ainsi, en 2017 la Corée du Sud a prélevé 24% des 300 millions de dollars de bénéfice des échanges de crypto-actifs coréens, soit 72 millions de dollars.

c/ Attirer les talents

Voyons grands ! Si l'objectif est bel et bien de devenir une nation leader en termes de cryptoactifs, comme proclamé par Bruno Le Maire, alors nous ne pouvons pas nous contenter de nos talents nationaux : il faut également attirer les talents étrangers et encourager l'éclosion de champions français tout en attirant les projets européens et mondiaux. A l'heure du Brexit, un certain nombre d'entre eux pourraient choisir Paris comme tête de pont pour se développer en Europe.

Les mesures préconisées ci-dessus pour retenir nos talents sont donc entièrement valables pour cet objectif-ci. La France connaît aujourd'hui un momentum avec la présidence d'Emmanuel Macron, reconnu à l'étranger comme un dirigeant particulièrement favorable à l'innovation. Profitons donc de cette bonne image pour accueillir les développeurs, chercheurs, entrepreneurs étrangers du secteur des cryptoactifs à la recherche d'une terre bienveillante pour leurs activités ou pour rejoindre un projet français existant. Dans cette perspective, la mise en place à venir du visa optionnel pour les ICO de la part de l'AMF est une première pierre à saluer. Au-delà, il est indispensable de mettre en place des politiques clairement incitatives en faveur des cryptoactifs si la France souhaite bel et bien devenir une leader du web décentralisé.

112 https://www.reddit.com/r/Bitcoin/comments/2nxv6v/hsbc_severs_links_with_bitcoin_firm/

Comment faire émerger une « Europe de la blockchain » ?

A l'heure actuelle, la réalité est encore loin d'une « Europe de la blockchain » : les pays européens sont avant tout concurrents, plus qu'alliés, dans le secteur des cryptoactifs.

Une grande raison l'explique : la grande hétérogénéité des fiscalités nationales en matière de gains en cryptoactifs.

Ainsi, alors qu'en France le taux effectif maximum d'imposition sur ces gains atteint 66,5%, l'Allemagne présente actuellement un régime très avantageux. Si le bitcoin cédé est détenu moins d'un an, la plus-value dégagée est exonérée à hauteur de 600 euros, le reste étant imposé à l'impôt sur le revenu à des taux allant de 15 % à 45 % selon la tranche ; si le bitcoin est cédé après plus d'un an de détention, la plus-value échappe en totalité à l'impôt. Pour cette raison et pour d'autres, Berlin se positionne aujourd'hui en « hub » des cryptoactifs en Europe¹¹³.

De même, en Belgique, lorsque les gains sont qualifiés de revenus relevant d'une gestion normale privée (c'est-à-dire lorsque ces opérations ne sont pas effectuées dans un but de spéculation et qu'elles n'acquièrent pas, par leur fréquence, le caractère d'une occupation lucrative), les gains sont totalement exonérés d'impôt.

Une politique européenne volontariste en matière de cryptoactifs implique nécessairement une harmonisation fiscale entre les différents pays. C'est à cette condition qu'une « Europe de la blockchain » pourra véritablement émerger. Au-delà, il est évidemment souhaitable d'aller plus loin, par exemple en agissant pour que les banques européennes acceptent d'ouvrir un compte aux entrepreneurs du secteur des cryptoactifs, ou encore en établissant une réglementation harmonisée en matière d'ICO.

Cette direction ne semble toutefois pas celle prise aujourd'hui : chaque pays européen mène des politiques différentes en matière de cryptoactifs et de blockchain, le plus souvent de façon non-coordonnée. En Espagne le Premier Ministre Mariano Rajoy a par exemple annoncé début 2018 la préparation d'une loi incluant de possibles réductions fiscales pour attirer les entreprises du secteur¹¹⁴...

Avec les mesures récapitulées dans l'encart ci-dessous, la puissance publique peut être un accélérateur pour cette innovation de rupture. In fine, face à l'émergence du web décentralisé la France et l'Europe se situent aujourd'hui à un carrefour. Ce web est naissant, et donc logiquement encore inachevé, voire bancal. C'est pourtant justement ces périodes d'ébullition qui sont décisives. L'histoire du Web montre que c'est durant ces premiers temps que nombre d'enjeux clefs se jouent : rappelons-nous qu'Amazon a été créé dès 1994, et Google dès 1998. Dès lors, c'est durant ces phases préliminaires et mouvantes qu'il faut produire les efforts pour prendre de l'avance, ou a minima ne pas laisser de retard se creuser. Les champions du web décentralisé ne sont pas encore installés : tout est donc encore possible. Chacun peut encore prendre en marche le train de la blockchain, qui vient tout juste de s'élaner. La France et l'Europe peuvent faire partie de la locomotive...à condition d'agir rapidement.

113 <https://venturebeat.com/2018/01/10/berlins-full-node-wants-to-be-europes-largest-blockchain-coworking-space>

114 <https://www.bloomberg.com/news/articles/2018-02-15/rajoy-s-party-weighs-tax-breaks-for-spanish-blockchain-companies>

SYNTHÈSE DES 15 PROPOSITIONS

Proposition générale

- Apporter un soutien public spécifique à l'écosystème blockchain français en portant l'accent sur les acteurs qui créent et construisent l'innovation : startups, développeurs, entrepreneurs.

Fiscalité et comptabilité

- Pour les particuliers, assujettir les gains en cryptoactifs au Prélèvement Forfaitaire Unique. Le régime de la plus-value sur biens meuble peut être envisagé comme mesure transitoire (il ne requiert qu'un changement de doctrine fiscale).
- Pour les entreprises, clarifier le traitement comptable des cryptoactifs ainsi que l'exonération de TVA en cas d'opération de change. En outre, des mesures d'incitations fiscales spécifiques doivent être envisagées si la France entend prendre le leadership en Europe.

Prises de positions publiques

- Adopter un discours officiel encourageant sur les cryptoactifs, qui ne met pas seulement en avant leurs risques mais aussi les opportunités qu'ils ouvrent. Un objectif doit être visé en priorité : lever le blocage qui empêche les entrepreneurs du secteur de créer un compte bancaire dans un établissement français.
- Mettre en place des actions de communication pour faire comprendre l'importance du web décentralisé et ses opportunités en termes d'emploi et d'entrepreneuriat – ceci afin de susciter plus de vocations dans ce secteur naissant.

Education et recherche

- Encourager les créations de cursus spécialisés en blockchain et en cryptoactifs, en particulier dans les écoles d'ingénieurs et d'informatiques, pour lutter contre la pénurie de talents dans le secteur.
- Inciter le monde de la recherche (en économie, cryptographie, finance, droit, développement durable, géopolitique, histoire, gouvernance des organisations...) à investir ces sujets (blockchains publiques et cryptoactifs). En particulier, soutenir la création de chaires de recherches dédiées au nouveau champ d'étude que représente la cryptoéconomie.

Lutte contre les risques

- Renforcer la protection des investisseurs et des particuliers contre les arnaques, via des actions de pédagogie, des sanctions exemplaires (pénal...), et une coordination en amont avec les représentants de la communauté CryptoFR, qui identifie et répertorie les projets frauduleux (fausses plateformes d'échange, schémas de Ponzi, etc.).
- Mettre en place un agrément (équilibré) pour les opérateurs de cryptoactifs qui contrôlerait les compétences et le sérieux des porteurs de projets, leur structuration juridique et capitalistique, et la légalité des dispositifs employés.
- Faire entrer expressément les opérateurs "crypto" dans le champ de compétence des autorités de régulation.

Ecosystème

- Pour les prochaines réflexions et décisions en matière de cryptoactifs, adopter une posture d'écoute et dialogue systématique avec les acteurs historiques de l'écosystème français : l'association Chaintech qui représente les acteurs des blockchains et cryptoactifs en France, l'association Le Cercle du Coin, et les représentants de la communauté CryptoFR.
- Soutenir le travail réalisé par ces communautés via une reconnaissance publique de leur rôle et un financement minimal, afin de leur permettre de continuer leur travail d'éducation, de pédagogie, de déconstruction des idées reçues et d'alerte face aux arnaques (effectué aujourd'hui en parallèle du travail réalisé au sein des startups blockchain françaises).
- Encourager l'engagement des femmes dans le secteur blockchain et cryptoactifs via des actions de pédagogie et de communication (pouvant être conjointes avec les initiatives déjà menées dans le secteur numérique plus globalement), pour lutter contre le manque de diversité du secteur.

Europe

- Favoriser une harmonisation des différentes politiques fiscales en Europe en matière de cryptoactifs, dont l'absence empêche aujourd'hui la constitution d'une « Europe du web décentralisé ».
- Encourager une coordination, aujourd'hui inexistante, des différentes politiques menées par les pays européens en matière de cryptoactifs.

CONCLUSION

La blockchain est souvent citée comme l'une des grandes technologies de demain, avec l'intelligence artificielle. Une précision importante mérite cependant d'être apportée : contrairement à l'intelligence artificielle, dont les usages spectaculaires et révolutionnaires (voiture autonome, etc.) sont loin d'être prêts, la blockchain est déjà fonctionnelle, depuis 2009. Elle n'en est certes qu'à ses débuts, et ses usages révolutionnaires ne sont certes pas encore développés massivement, mais ces derniers sont déjà existants, au moins en partie.

Loin d'être une bulle sans fondement, les cryptoactifs, malgré des mouvements spéculatifs évidents, sont déjà une réalité financière non-négligeable. La valorisation d'Ethereum est aujourd'hui proche de 35 milliards de dollars, loin devant les 26 milliards de Twitter et les 21 milliards de Snapchat.

A l'issue de cette note, nous pouvons donc affiner le propos introducteur, qui soulignait qu'aucun nouveau géant du numérique n'était apparu dans la décennie 2010 : ceci n'est vrai que dans l'économie numérique « traditionnelle ». Dans l'économie numérique ouverte par la blockchain et les tokens, la décennie 2010 a vu l'émergence d'Ethereum, qui constitue à la fois un protocole blockchain, une plateforme à laquelle se greffent d'ores et déjà des centaines d'applications et des milliers de tokens, et une communauté de dizaines, si ce n'est centaines, de milliers d'acteurs à ce jour.

Ethereum n'a toutefois pas encore gagné la bataille du web décentralisé à ce stade, bien qu'ayant plusieurs (grandes) longueurs d'avance. D'autres protocoles se développent, certains cherchant à concurrencer frontalement Ethereum (comme NEO, surnommé le « Ethereum chinois »), d'autres cherchant plutôt la complémentarité (DFinity). Il est d'ailleurs intéressant de constater que plusieurs fonds de capital-risque américains cherchent aujourd'hui à trouver et financer le nouvel Ethereum de la même façon qu'ils essayaient il y a quelques années de dénicher le nouveau Google.

Le protocole qui l'emportera (à supposer qu'il n'y en ait qu'un) sera celui qui sera porté par la communauté la plus dynamique et talentueuse. La puissance et le potentiel de développement d'un protocole blockchain dépendent en effet très étroitement de la force de sa communauté.

Dès lors, suivre l'évolution du monde blockchain et des cryptoactifs nécessite de changer de lunettes : l'important n'est pas l'évolution quotidienne des cours, mais l'évolution des communautés et des talents de cette nouvelle économie. Depuis plusieurs mois, un nombre croissant d'individus choisissent justement d'entrer de plein pied dans ce secteur émergent, certains ayant décidé de quitter leur précédent travail et de se reconverter, d'autres, précédemment étudiants, ayant choisi de commencer directement leur carrière professionnelle dans le domaine qui les passionne.

Une tendance, en particulier, est frappante et révélatrice : la façon avec laquelle « l'économie des tokens » aspire, peu à peu, les meilleurs talents jusqu'ici attirés par les GAFAs et la Silicon Valley. Ce basculement silencieux, doux, est difficilement quantifiable, mais est souligné par plusieurs acteurs importants de la Silicon Valley, comme l'investisseur Naval Ravikant.

Cette arrivée croissante de talents et le bouillonnement technologique et intellectuel qui accompagne la blockchain doit conduire les pays qui souhaitent devenir leader dans cette nouvelle économie à viser un objectif : attirer les talents du monde des cryptoactifs. Politiquement, cela ne peut passer que par un discours résolument positif sur leurs opportunités (sans compromis, pour autant, sur les enjeux de protection des investisseurs et de lutte contre les activités frauduleuses), par une politique fiscale encourageante, et par une clarté et une stabilité des politiques publiques relatives à ces actifs.

Ce nouveau web prendra certainement du temps à se déployer entièrement à grande échelle, et à réaliser, peut-être, toutes ses promesses - les blockchains et les cryptoactifs sont aujourd'hui avant tout des expérimentations. Mais que ces promesses se réalisent ou non, les fondations posées, le bouillonnement intellectuel engagé et les expérimentations réalisées resteront quoi qu'il arrive et ouvriront la voie d'usages fondée sur la décentralisation. La décentralisation est un nouveau paradigme de l'économie numérique, et l'on voit mal comment ce mouvement en cours de développement pourrait être stoppé.

Dès lors, toute politique purement répressive ou attentiste sur ces technologies serait une erreur de jugement que la France et l'Europe ne pourraient que regretter dans quelques années. « **La France ne peut se permettre de manquer le grand rendez-vous de la société de l'information et doit faire le choix de s'y préparer dans les meilleures conditions** » pouvait-on lire dans un rapport remis au gouvernement en décembre 1998, intitulé « L'Internet : un vrai défi pour la France ». Frilosité et myopie ont finalement conduit la France à rater l'opportunité de faire émerger les leaders du web. Avec la blockchain, nous sommes aujourd'hui face à un embranchement similaire. Voulons-nous suivre la même trajectoire qu'avec Internet ?



L'ÂGE DU WEB DÉCENTRALISÉ

CLÉMENT JEANNEAU

LA DIGITAL NEW DEAL FOUNDATION

LE THINK TANK DE LA NOUVELLE DONNE.

La Digital New Deal Foundation a pour vocation d'éclairer de la manière la plus complète possible les évolutions à l'œuvre au sein du phénomène de « digitalisation », dans l'acception la plus large du mot, et d'élaborer des pistes d'actions concrètes à destination des entreprises et des décideurs publics français et européens. Portés par l'expertise de leurs rédacteurs et leur insertion dans le débat public, les travaux de la Fondation pourront participer à l'élaboration d'une pensée française et européenne de la régulation digitale au service de la mise en place d'un cadre équilibré et durable.

Le Conseil d'administration

Les membres du Conseil d'administration de la Digital New Deal Foundation sont tous membres fondateurs. Ils sont issus d'horizons divers tout en étant en prise directe avec la transformation digitale des entreprises et des organisations. Forts de leur intérêt commun pour les questions numériques, ils ont décidé d'approfondir leurs débats en formalisant un cadre de production et de publication au sein duquel la complémentarité de leurs expériences pourra être mise au service du débat public et politique. Ils s'impliquent personnellement dans la vie de la Digital New Deal Foundation.

Un délégué général (Arno Pons) assure par ailleurs la coordination de l'ensemble des activités du think-tank et pilote avec le président fondateur (Olivier Sichel) les orientations stratégiques de la fondation.

Contact : contact@thedigitalnewdeal.org | **Site** : www.thedigitalnewdeal.org

Olivier Sichel

Président Fondation Digital New Deal
DGA Caisse des Dépôts



Laurent Alexandre
Fondateur de Doctissimo et de
DNA Vision



Sébastien Bazin
PDG AccorHotels

Michel Combes
ex-PDG SFR



Nicolas Dufourcq
DG de Bpifrance



Yves Poilane
DG Telecom Paris Tech



Judith Rochfeld
Professeur agrégée de Droit,
Panthéon Sorbonne



Alain Minc
Président AM Conseil



Robert Zarader
PDG Equancy