La Blockchain décryptée

Les clefs d'une révolution

Blockchain France

Publié par l'Observatoire Netexplo
www.netexplo.org
264 Rue du Faubourg Saint-Honoré – 75008 Paris

Mai 2016

Imprimé par Imprimerie de la Centrale de Lens
Rue des Colibris – BP 78 62302 Lens Cedex

ISBN : 978-2-9546672-1-8

Qui sommes-nous ?

Blockchain France (blockchainfrance.net) est né à l'été 2015 suite au constat d'absence d'informations sur le sujet en français, que ce soit sur Internet ou dans les médias généralistes. L'objectif de Blockchain France est de démocratiser la blockchain en faisant comprendre ses enjeux avec pédagogie, et en s'impliquant dans la construction d'applications concrètes.

Concrètement, Blockchain France accompagne les organisations dans la découverte, l'exploration et le déploiement des technologies blockchain. Nos offres vont de la formation aux enjeux de la blockchain à la construction de proof-of-concepts, en passant par des ateliers exploratoires.

Nos offres

Formation	**Exploration**	**Proof-of-Concepts**
Présentation de la blockchain, de ses cas d'usage et enjeux Session d'acculturation d'une heure à trois heures	Ciblage des cas d'usage blockchain pertinents pour votre entreprise 2 ou 3 demi-journées	Création d'un PoC blockchain pour démontrer la faisabilité d'un cas d'usage. En fonction du projet, de 1 à 3 mois.

Nos références

-Grands comptes : Total ; Air France ; BNP Paribas ; Crédit Agricole ; MAIF ; Louis Vuitton ; La Poste ; SNCF ; EDF ; …

-Institutions publiques : Banque de France ; Mairie de Paris ; CCI ...

-Associations : Positive Economy Forum ; ADRA ; …

Pour nous contacter

Envoyez-nous un email à contact@blockchainfrance.net

Remerciements

Nos premiers remerciements sont pour tous les contributeurs de ce livre, sans qui il n'aurait pas pu voir le jour. Ils vont aussi à Thierry, à Guillaume et à toute l'équipe Netexplo, pour la confiance et l'aide qu'ils nous ont prodiguées.

Ce livre est également pour nous l'occasion de remercier ceux qui ont soutenu l'aventure de Blockchain France, en particulier Clément, Nicolas et Axelle qui nous ont mis le pied à l'étrier et nous aident encore aujourd'hui ; Gilles qui nous porte depuis le début par sa bienveillance et son expérience ; et notre école, ESCP Europe, pour son soutien.

Une pensée spéciale pour Quentin, son travail impressionnant sur le forum et Slack CryptoFR, et pour tous les passionnés de la communauté, sans lesquels la blockchain ne serait pas grand-chose en France.

Merci aussi à tous ceux qui apportent leur pierre au projet et nous aident encore, et tout spécialement à François, à Thomas, à Amélie.

Enfin, un grand merci à nos proches qui ont subi cette fameuse révolution blockchain de plein fouet, de jour comme de nuit, et sans (trop) se plaindre. Promis, ce n'est que le début...

Avant-propos

Dans le monde numérique, et au-delà, la blockchain s'est imposée comme le grand sujet de l'année 2016. "Technologie révolutionnaire", "machine à créer de la confiance", "innovation de rupture d'une ampleur inédite"... : les superlatifs s'accumulent peu à peu dans les médias au fil des semaines.

Pourtant, tout comme le phénomène d'"uberisation" avait cannibalisé l'année 2015 en étant employé - parfois - de façon excessive, la blockchain court aujourd'hui le danger de devenir un simple buzzword, brandi comme symbole d'une "disruption ultime", sans être pourtant véritablement compris par ceux qui en parlent.

Ces derniers mois, nous avons entendu beaucoup de choses sur la blockchain, des projections les plus fascinantes aux affirmations les plus douteuses. Huit mois après la Une de *The Economist* ("Comment la blockchain pourrait changer le monde"), que l'on peut considérer comme le départ de l'emballement autour du sujet, il nous a donc semblé important de mettre "pause" sur cette machine médiatique, afin de prendre le recul nécessaire pour analyser les ressorts du phénomène blockchain.

Pour dépasser les effets d'annonce et saisir la réalité du terrain, nous avons rencontré celles et ceux qui font et pensent les blockchains. Leurs points de vue et nos synthèses avaient nourri le site de Blockchain France. Mais pour prendre le temps de l'apprentissage, de la réflexion, et pour inscrire cette technologie dans le temps long de la diffusion et du débat public, il était nécessaire de leur donner la parole plus longuement. C'est l'objet de ce livre.

Nous avons ainsi choisi 20 voix pour vous raconter cette technologie dans sa richesse et sa complexité. Cette combinaison de la parole directe des acteurs de la blockchain et d'un volet de découverte didactique, c'est le panorama d'une révolution. Ce livre est destiné à tous ceux qui veulent découvrir la blockchain, la comprendre en profondeur et élargir leurs horizons.

Préface

De Joël de Rosnay, Scientifique et Conseiller à la Présidence d'Universcience

La Blockchain : un défi aux pouvoirs centralisés

Pour la première fois dans l'histoire des révolutions technologiques, l'une d'entre elle, au-delà de la révolution internet, a la capacité d'agir sur le pouvoir vertical et centralisé exercé par les Etats sur la monnaie, sur celui des banques et les transactions financières, des notaires et les cessions immobilières, des monopoles énergétiques sur la distribution d'électricité ou de carburants. Il semblait impossible d'imaginer de tels bouleversements avant le développement de la Blockchain. Sans en refaire l'historique largement médiatisée, rappelons que la Blockchain est un protocole de gestion numérique de données en "open source", décentralisée, infalsifiable et fondée sur les échanges réalisés en P2P dans des réseaux. Cette technologie va bouleverser le rôle des tiers de confiance et des intermédiaires dans des domaines très variés allant de l'audit des entreprises, à des systèmes électoraux et de votes en général, la gestion des propriétés de terrains dans un cadastre ouvert et transparent, des systèmes d'assurance quasi autonomes et autorégulés, où polices d'assurance et réclamations des assurés seraient automatiquement gérées, la vente de tableaux et d'œuvres d'art sans passer par les grandes galeries ou les maisons de ventes aux enchères internationales. La blockchain permet d'éviter les hackers en gérant les informations critiques de manière décentralisée et encryptée. Une telle gestion par blockchain aurait permis, par exemple, d'éviter le piratage de la société Sony et la révélation de messages électroniques personnels.

Tout transfert d'actifs, conservation de données critiques dans des registres, signatures contractuelles sont bouleversés par la blockchain ; d'où le principe des contrats intelligents (*smart contract*). Une fois lancé, le système gère automatiquement les conditions contractuelles, les termes et les conditions du contrat entre les contractants. Grâce à la transparence et l'infalsifiabilité des blocs, chaque intervenant peut vérifier la réalisation et la justification des termes contractuels et, dans le cas d'une transaction financière, être automatiquement réglée par transfert bancaire.

Dans le domaine énergétique la blockchain va désintermédier les grands pouvoirs centralisés et pyramidaux des énergies fossiles et nucléaires. Grâce à la Smartgrid qui permet l'adaptation de la fourniture d'électricité à l'offre et à la demande et grâce au réseau de distribution de biocarburants produits localement dans des conditions agricoles, des particuliers vont pouvoir, grâce à la blockchain, acheter et vendre de l'électricité ou des biocarburants de manière sécurisée et

sans intermédiaire. Un tel système de vente d'électricité dans la Smartgrid existe déjà à Brooklyn. Il va certainement s'étendre aux ventes d'électricité provenant des voitures électriques en stationnement, dans le cadre du protocole VTG (*Vehicule to Grid*). Ainsi, grâce à la blockchain, Enernet deviendra aussi important, sinon plus, qu'internet, car sur un plan politique il favorisera une véritable démocratie énergétique inexistante aujourd'hui. Même s'il est question de transition énergétique, les grandes décisions restent entre les mains des pouvoirs centralisés.

Mais évidemment face à une telle révolution de nombreuses questions demeurent. Ce livre intelligent, proposé par Blockchain France et édité par Netexplo, qui a prouvé sa compétence en matière de prospective, permet d'apporter les premières réponses. Comment vont réagir les grands pouvoirs étatiques industriels ou institutionnels, aux nouveaux risques de désintermédiation représentés par la blockchain ? Elle instaure une perte de pouvoir incontestable pour les banques sur le marché du crédit, les compagnies d'assurance et la gestion statistique et impersonnelle de leurs clients, les grandes galeries d'art, les sociétés d'auteurs compositeurs, les monopoles de distribution de l'énergie. Il paraît aujourd'hui évident qu'ils ne se laisseront pas influencer pour modifier leurs structures.

Il existe cependant de nombreuses questions à régler. Par exemple, renforcer le cadre législatif de la blockchain, garantir l'interopérabilité des systèmes et des réseaux pour que les registres, la transparence, la confidentialité puissent être assurés dans toutes les conditions. Poursuivre et financer des recherches dans tous les domaines de la blockchain avec la nécessité de réaliser des expérimentations de cas d'usage et surtout continuer à favoriser la transversalité des actions et du pouvoir de décision des particuliers.

La France ne peut manquer de s'impliquer dans une telle révolution à la fois technique et sociétale. Ce livre souligne les grandes voies à suivre pour rester compétitif dans ces domaines. Les mesures récentes prises par le Ministère de l'Economie sont un signe encourageant dans la bonne direction. Mais une nouvelle lutte de pouvoir va s'engager, fondée non plus sur les seuls rapports de force entre structures verticales et centralisées, mais dans le cadre de rapports de flux entre personnes informées et responsables, connectées en réseaux.

On a prédit la prise de pouvoir des robots supprimant et remplaçant le travail des "cols blancs" après celui des "cols bleus". Avec la Blockchain on va assister au contraire à un retour de l'humain dans l'écosystème numérique avec de réelles opportunités de choix, de partages, de liberté d'achat ou de vente, de travail indépendant, avec en même temps la catalyse et le développement de la créativité collective.

1

COMPRENDRE LA BLOCKCHAIN EN DOUZE QUESTIONS

L'objectif de la première partie de ce livre est simple: nous souhaitons donner au lecteur les clefs pour pouvoir appréhender la seconde partie et nourrir ainsi son dialogue avec les acteurs de la blockchain.

Ces clefs sont au nombre de douze ; nous avons choisi de les présenter sous forme de questions, que voici.

1 - Qu'est-ce que la blockchain ?

La blockchain est une technologie de **stockage et de transmission d'informations**. Cette technologie possède en particulier trois caractéristiques majeures : elle est transparente, sécurisée, et fonctionne sans organe central de contrôle.

Transparente, car chacun peut consulter l'ensemble des échanges inscrits sur une blockchain depuis sa création.
Sécurisée, comme nous l'expliquerons plus loin en détails.
Sans organe de contrôle, puisque la blockchain est fondée sur des relations de Pair-à-Pair.

Concrètement, une blockchain est **une base de donnée numérique infalsifiable** sur laquelle sont inscrits tous les échanges effectués entre ses utilisateurs depuis sa création. C'est parce que les échanges successifs y sont enregistrés sous forme de blocs de transactions que l'on appelle ce registre une "blockchain", ou chaîne de blocs.

Différents types de blockchains coexistent. Celles-ci partagent toutes une caractéristique essentielle, qui les distingue des bases de données "classiques" :

ce sont toutes des bases de données distribuées. Cela signifie que différents exemplaires de ce registre existent simultanément sur différents ordinateurs (qui deviennent à la fois clients et serveurs : on parle de "nœuds" du réseau). Lorsqu'un bloc est ajouté à une blockchain, il est ajouté presque simultanément sur chacun des exemplaires de ce registre.

Il existe des blockchains publiques, ouvertes à tous (par exemple : Bitcoin et Ethereum), et des blockchains privées, dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs.

Une blockchain publique peut être assimilée à un grand livre comptable public et infalsifiable. Comme l'écrit le mathématicien Jean-Paul Delahaye, il faut s'imaginer "un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible".

2 - D'où vient la blockchain ?

La blockchain a été créée en 2008 avec la monnaie virtuelle bitcoin. Les deux sont donc historiquement liées : la blockchain est l'infrastructure virtuelle sur laquelle repose le bitcoin.

Le terme Bitcoin (B majuscule) renvoie à la fois à une monnaie numérique utilisant des techniques cryptographiques - le bitcoin (b minuscule) - et au protocole décrivant le fonctionnement du réseau sur lequel cette monnaie circule.

Ce protocole, c'est la blockchain, où la création monétaire et la validation des transactions s'effectuent de manière horizontale et transparente. Ce système fonctionne sans autorité centrale ni tiers de confiance, à l'inverse des monnaies contrôlées par des banques ou des gouvernements.

L'inventeur de Bitcoin (et donc de la blockchain) reste à ce jour inconnu, même si certains ont tenté de revendiquer sa paternité, sans réussir toutefois à présenter les preuves nécessaires. On ne connaît que son pseudonyme, Satoshi Nakamoto, sous lequel il a mis en ligne fin 2008 le *whitepaper* à l'origine de ce qu'il définissait comme un "système de monnaie électronique pair-à-pair". Il pourrait s'agir d'un individu mais aussi d'un groupe et ce mystère entretient une certaine mythologie autour de la figure de Satoshi Nakamoto.

L'historique de Bitcoin a été mouvementé depuis le lancement des premiers bitcoins en 2009 et la première véritable transaction effectuée en mai 2010 (2 pizzas contre 10,000 BTC, ce qui équivaudrait aujourd'hui, au cours actuel, à 2 millions d'euros la pizza !). Début 2011, le bitcoin touche la parité avec le dollar et atteint plusieurs millions de dollars de capitalisation : les premiers articles sur le Bitcoin commencent alors à apparaître dans des journaux majeurs aux Etats-Unis. Après deux phases de bulles, aux printemps 2011 et 2013, le cours du bitcoin a retrouvé plus de stabilité depuis 2014.

L'intérêt porté à la blockchain elle-même, au-delà de son application monétaire qu'est le bitcoin, est venu relativement tardivement, à partir des années 2013-2014. Il n'y a bien sûr pas de date précise étant donné que la blockchain existe depuis la création de Bitcoin. Les pionniers s'y sont intéressés avant 2013-2014, mais ce n'est véritablement qu'en 2015 que la blockchain a commencé à susciter une grande attention.

3 - Comment fonctionne la blockchain ?

Pour une première approche du fonctionnement des blockchain, le plus facile est de raisonner avec une blockchain purement monétaire. On peut prendre l'exemple de Bitcoin, ou d'une blockchain avec des jetons "simples"[1], pour laquelle une transaction se résume en fait à trois informations : qui donne quoi à qui.

Par exemple, on peut imaginer qu'Alexandre veuille donner deux bitcoins à Camille.

Les transactions effectuées entre les utilisateurs du réseau sont d'abord regroupées par blocs. Cette étape passée, il est nécessaire de vérifier qu'Alexandre a les moyens de réaliser cette transaction, avant qu'elle ne soit inscrite dans la blockchain. Le processus est simple, dans la mesure où la blockchain ne tolère pas le découvert : pour qu'Alexandre puisse envoyer ces bitcoins à Camille, il doit les avoir reçus au préalable.

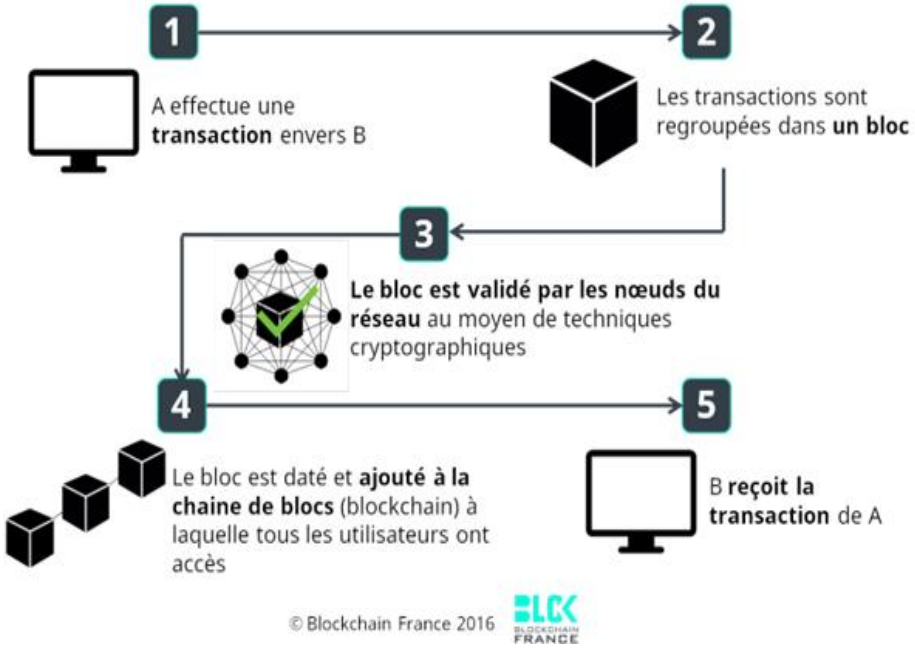
Ceux qui sont chargés de vérifier la validité des transactions sont des acteurs du réseau que l'on appelle des "mineurs".

Lors de la vérification, l'historique des transactions d'Alexandre est remonté pour vérifier que ces 2 bitcoins qu'il a reçus précédemment n'ont pas été réutilisés depuis. On vérifie en fait tout simplement qu'il n'essaye pas de dépenser deux fois l'argent qu'il a reçu.

Une fois les vérifications effectuées, le bloc dans lequel se trouve la transaction entre Alexandre et Camille est validé par les mineurs, selon des techniques qui dépendent du type de blockchain, et qui permettent d'atteindre le consensus distribué, c'est-à-dire le consensus des nœuds sur l'état du réseau. Dans la blockchain Bitcoin, cette technique est appelée le "Proof-of-Work"[2] (preuve de travail) et consiste en la résolution de problèmes algorithmiques très lourds.

Si le bloc est validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau. Camille possède maintenant ses deux bitcoins.

[1] Un jeton est ce qui est échangé sur un réseau blockchain. Le bitcoin est le jeton (en anglais le « token ») de la blockchain Bitcoin, tandis que l'ether est celui de la blockchain Ethereum, par exemple.
[2] Pour plus d'informations sur ce procédé, se référer au Lexique en fin d'ouvrage.



Ce processus prend un certain temps selon la blockchain considérée (environ une dizaine de minutes pour Bitcoin, 15 secondes pour Ethereum). Le protocole modifie la difficulté du calcul afin que celui-ci ait toujours la même durée, celle prévue dans le code source.

4 - En quoi la blockchain est-elle si sécurisée ?

La blockchain peut être considérée comme doublement sécurisée.

Elle est d'abord sécurisée lors la création de nouveaux blocs.

- Un premier élément de sécurité repose sur le couple clé publique/clé privée, qui est un système de cryptographie dite "asymétrique". On peut comparer ce couple à celui RIB/PIN dans le monde bancaire. La clé publique est l'équivalent du RIB : elle est l'adresse publique du compte d'un utilisateur donné. Cette clé n'a pas d'autre fonction que la réception des paiements. En revanche, pour soumettre une transaction dans la blockchain, il est nécessaire de disposer de sa clé privée, unique, équivalent du PIN bancaire. Sans cette clé, il est impossible de signer numériquement ses transactions. Ainsi, personne ne peut signer de transaction au nom d'un autre individu, à moins de disposer de sa clé. Il reste bien sûr à la charge de chacun de faire en sorte que cette clé ne se perde pas et ne soit pas révélée.

- Deuxièmement, la validation des blocs est soumise à un processus que l'on appelle le "minage". Celui-ci vise à certifier certains éléments (l'authenticité des transactions, l'identité des parties, etc.) sans avoir recours à un intermédiaire de confiance ou une autorité centrale. Ceux qui vérifient les transactions sont les mineurs. Ils ne vérifient pas transaction par transaction mais bloc par bloc, un bloc étant constitué de plusieurs

transactions. Des procédés comme la Preuve-de-Travail (Proof-of-Work)[3] assurent l'objectivité de leur validation.

D'autre part, elle est sécurisée grâce à sa réplication sur l'ensemble des nœuds du réseau. En effet, le registre étant dupliqué autant de fois que le réseau comporte de nœuds, il faudrait, pour falsifier une transaction, corrompre simultanément plus de la moitié de ces nœuds. En cas de tentative de fraude, la majorité des serveurs détecterait rapidement une incohérence par rapport à l'historique du système : la fraude serait donc repérée et rejetée.

Il reste certes possible, sur le papier du moins, de corrompre plus de la moitié des nœuds du réseau et d'installer sa propre "vérité" : c'est l'attaque dite des 51 % ("Goldfinger"). Cependant, une telle attaque, en plus d'être extrêmement coûteuse (et donc à la portée d'extrêmement peu d'organisations), n'aurait aucune garantie de réussite. En effet, chaque nœud a toujours le choix de ne pas accepter le nouveau consensus créé par le fraudeur, et de continuer une chaîne de blocs parallèle.

Depuis sa création, la blockchain de Bitcoin n'a ainsi jamais été "hackée". En 2010, soit au tout début du Bitcoin, une faille dans le protocole a permis l'émission de plusieurs milliards de bitcoins frauduleux ; la faille a cependant été repérée immédiatement, et en quelques heures ces bitcoins furent retirés de la circulation.

Par ailleurs, les affaires de bitcoins volés apparues parfois dans les médias s'expliquent simplement par le fait que ce sont les plateformes internet qui contenaient les clés privées des détenteurs de bitcoins qui ont été piratées, et non la blockchain Bitcoin elle-même. Ces utilisateurs n'étaient pas allés au bout de la logique Bitcoin, qui nécessite, pour bénéficier entièrement du caractère sécurisé, de ne pas transiter par un intermédiaire, et de stocker ses clefs privées à froid, sur un disque dur externe par exemple.

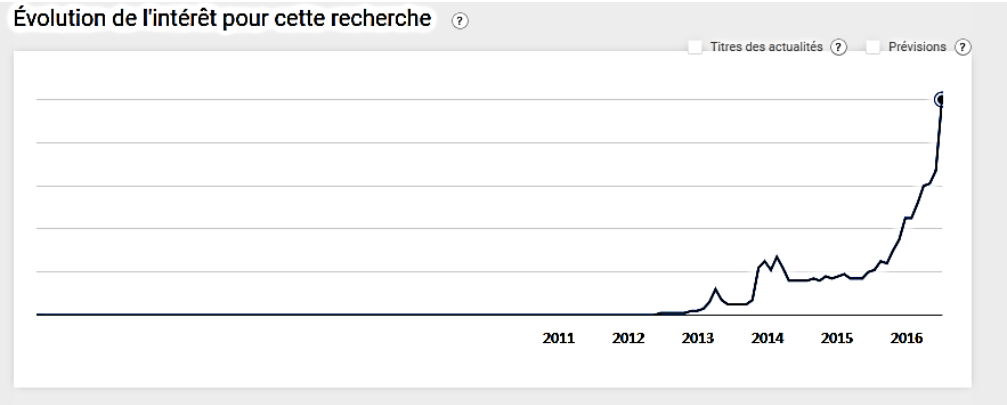
5 - Depuis quand la blockchain fait-elle autant parler d'elle ?

En octobre 2015, l'hebdomadaire *The Economist* fait sa Une sur la blockchain, annonçant que "la technologie derrière le Bitcoin pourrait changer le monde". La réputation du magazine, très lu dans les milieux business, permet alors à la blockchain de sortir des cercles "geek" et "Bitcoin" et lui donne une crédibilité quasi institutionnelle. Rétrospectivement, nombre d'acteurs estiment que cette couverture a constitué l'élément déclencheur de l'emballement médiatique autour de la blockchain. Jusqu'alors, le nombre d'articles sur le sujet dans les médias traditionnels était resté très limité.

A partir de fin 2015, la blockchain commence à être évoquée plus régulièrement. Le véritable emballement n'a toutefois lieu qu'à partir de début 2016, comme le témoigne l'évolution du nombre de recherches sur le mot-clé "blockchain" sur

[3] Pour plus d'informations sur ce procédé, se référer au Lexique en fin d'ouvrage.

Google dans le monde (à noter que la courbe sur Google France pour 2016 est encore plus accentuée) :



Certains pionniers de la blockchain et du bitcoin ont, du reste, assisté avec un regard assez critique à la montée de ce que beaucoup considèrent comme une "hype". Les entreprises traditionnelles et les médias ont en effet eu tendance à établir une séparation tranchée entre blockchain (à l'image vierge) et Bitcoin (associé à des activités illicites), en oubliant un peu vite que la première a été créée avec le second, et que la blockchain la plus robuste et la plus utilisée reste bien celle du bitcoin, malgré toutes ses limites.

6 - La blockchain peut-elle fonctionner sans bitcoin ?

Oui. La Blockchain fonctionne aujourd'hui dans la grande majorité des cas avec une crypto-monnaie associée, qui constitue l'incitation économique de sécurisation du réseau pour les mineurs. Cependant cette crypto-monnaie n'est pas nécessairement le bitcoin. Ethereum fonctionne avec de l'ether, Litecoin avec des litecoins, Nxt avec des nxt, etc.

Rappelons toutefois que la blockchain Bitcoin reste à l'heure actuelle la plus sécurisée. La sécurisation de son réseau s'effectue en effet *via* une puissance de calcul gigantesque : à titre de comparaison, début 2015 l'ensemble de la puissance de calcul de Google représentait 1% de celle de Bitcoin. Depuis, la puissance de calcul de Bitcoin a été multipliée par 4.

Cela étant, Bitcoin affronte aujourd'hui certaines difficultés[4] qui peuvent à terme remettre en jeu sa position de blockchain de référence. Au fond, la question qui agite actuellement la communauté est surtout de savoir si la blockchain Bitcoin a pour ambition de devenir incontournable ou non.

7 - Quels sont les différents types de blockchains ?

Il faut distinguer d'une part les blockchains publiques, d'autre part les blockchains privées.

[4] Ce point est discuté plus loin dans la question "Quels défis pour la blockchain ?".

Les blockchains publiques constituent les blockchains "historiques". Il s'agit de blockchains accessibles à n'importe qui dans le monde : chacun a libre accès au registre. En outre, chacun peut envoyer des transactions et s'attendre à ce qu'elles soient incluses dans le registre (tant que ces transactions respectent les règles de cette blockchain). Enfin, chacun peut participer librement au processus d'approbation (celui qui permet de décider quel bloc sera ajouté à la chaîne et qui définit l'état du système). Bitcoin et Ethereum constituent les deux principales blockchains publiques. D'autres existent également, de moindre ampleur : Litecoin, Dogecoin, etc.

Dans le cas des blockchains privées (parfois appelées "de consortium"), le processus d'approbation est contrôlé par un nombre restreint et choisi de nœuds. Par exemple, une quinzaine d'institutions financières pourraient se mettre d'accord et organiser une blockchain dans laquelle un bloc devrait être approuvé par au moins 10 d'entre elles pour être valide. Il existe donc une double modification au système originel, puisque non seulement les participants au processus d'approbation sont limités et sélectionnés, mais en outre ce n'est plus la règle de la majorité qui s'impose. Le droit de lire la blockchain, c'est-à-dire l'accès au registre, peut-être, lui, soit public, soit réservé aux participants du réseau.

Il existe également des cas de blockchains privées où le processus d'approbation est limité à un unique acteur, bien que les autorisations de lecture par exemple puissent être publiques. Ce peut être le cas par exemple lorsque plusieurs départements d'une même entreprise dialoguent autour d'une blockchain en interne.

A la différence des blockchains publiques, l'existence d'une crypto-monnaie n'est pas nécessaire pour les blockchains privées : ces dernières n'ont en effet pas besoin de rémunérer leurs membres pour la validation des transactions. Les logiques de Proof-of-work n'existent donc pas nécessairement dans ce type de blockchains.

Les blockchains privées présentent certains avantages, qui peuvent expliquer l'intérêt que leur portent notamment les institutions financières : gouvernance simplifiée, acteurs connus, coûts réduits, rapidité, confidentialité, mise en conformité facilitée par les possibilités d'audit y compris par le régulateur... Elles font néanmoins débat car celle-ci réintroduisent des acteurs humains dans la gestion du réseau (gérant l'accès et le fonctionnement) alors que le concept central d'une blockchain (publique) est de supprimer le tiers de confiance. Le consortium R3 qui travaille sur ce sujet et fédère une quarantaine de banques mondiales parle d'ailleurs de "distributed ledger" plutôt que de blockchain.

Qu'est-ce qu'Ethereum ?

Ethereum est une blockchain publique, considérée comme la blockchain "montante", et par certains comme étant la plus prometteuse. Elle permet de construire des applications décentralisées. Son principe est de coupler les caractéristiques de la blockchain avec des "smart contracts", des programmes autonomes capables d'exécuter automatiquement des conditions définies en amont. Sa crypto-monnaie, l'ether, est devenue début 2016 la deuxième plus utilisée derrière le bitcoin.

La blockchain Ethereum est bien plus récente que Bitcoin : elle a été inventée fin 2013 par Vitalik Buterin, un jeune Canadien d'origine russe alors âgé de 19 ans. D'abord passionné par Bitcoin qu'il découvre à 17 ans, il estime après plusieurs mois de travail que celui-ci est très perfectible, d'où la création d'Ethereum. Après avoir levé en 2014 l'équivalent de 19 millions de dollars pour financer le projet, il sort en 2015 une première version, dédiée aux tests des développeurs. Début 2016, les choses s'accélèrent avec le lancement de la phase 2 du projet, la version Homestead, qui apporte plus de stabilité au réseau. Dans le même temps, le cours de l'ether bondit, allant même jusqu'à dépasser un temps le milliard de dollars en termes de valorisation totale.

Ethereum n'a pas été construit pour concurrencer frontalement Bitcoin : il s'agit plutôt de deux utilisations différentes et complémentaires de la blockchain. « *La blockchain Bitcoin a été conçue spécifiquement pour les devises alors qu'Ethereum permet de créer tout type d'applications*" explique Vitalik Buterin, son fondateur.

Microsoft, qui a décidé d'utiliser Ethereum pour sa plateforme Azure blockchain-as-a-service, justifie ainsi son choix: "*Tandis que Bitcoin a de nombreuses utilisations intéressantes en tant que crypto-monnaie, Ethereum apporte la flexibilité que beaucoup de nos clients recherchent. Ethereum possède une communauté vibrante de développeurs, enthousiastes et ouverts à des applications business*".

ethereum

La prochaine étape pour Ethereum sera la sortie de la version intitulée "Metropolis" qui correspondra au lancement grand public et qui est donc très attendue. Elle devrait permettre aux utilisateurs non avertis de bénéficier d'une interface utilisateur quasi complète, et notamment d'un "DApp Store". En outre, dans le but de consommer moins d'électricité, Ethereum a également l'intention début 2017 de passer du proof-of-work (système du bitcoin où les blocs sont validés par le mineur qui a la plus grande puissance de calcul) à un système dit proof-of-stake, moins énergivore[5].

[5] Pour plus d'information sur ce procédé, se référer au Lexique en fin d'ouvrage.

8 - En quoi peut-on parler de désintermédiation ultime ?

La décentralisation induite par la blockchain remet en cause le rôle des tiers de confiance traditionnels. En particulier, la blockchain peut permettre aux utilisateurs et aux travailleurs de se passer des plateformes intermédiaires, qui constituent aujourd'hui le cœur de la révolution numérique. Ces plateformes se rémunèrent le plus souvent au moyen d'une commission, parfois importante (20 % pour Uber, jusqu'à 25 % pour Booking) :

TAUX DE COMMISSION DES PLATEFORMES NUMÉRIQUES

Société	Taux de commission	Type de plateforme
KissKiss BankBank	8%	Financement participatif
Leetchi	de 2,9% à 4%	Financement participatif
Kick Starter	8%	Financement participatif
Airbnb	de 9% à 15%	Logement
Booking	de 15% à 25%	Logement
Uber	20%	Transport
Blablacar	12%	Transport
Drivy	30%	Transport
Ebay	7,50%	Vente de biens
PriceMinister	de 4% à 22%	Vente de biens

Ces taux de commission sont en outre fixés de façon unilatérale par les plateformes qui peuvent décider du jour au lendemain de les modifier. C'est cette dépendance vis-à-vis d'Uber qui a par exemple conduit à la création du projet Arcade City qui ambitionne de devenir un "Uber-killer" [6]. L'enjeu n'est donc pas seulement de permettre aux utilisateurs de bénéficier de taux de commission moins élevés, mais bien aussi de libérer les travailleurs dits indépendants de leur dépendance vis-à-vis des plateformes en matière de prix.

La blockchain permettrait alors de redonner du pouvoir à ces travailleurs, afin notamment qu'ils puissent anticiper leurs revenus sans subir les décisions

[6] Ce projet est détaillé plus loin dans les cas d'usage.

arbitraires et soudaines des plateformes[7]. C'est ce qui conduit certains à parler d'une "uberisation d'Uber" engendrée par la blockchain.

Le transport n'est d'ailleurs pas le seul secteur concerné. Le même raisonnement peut par exemple être tenu pour les hôteliers, aujourd'hui très dépendants de Booking.com. La start-up blockchain Slock.it travaille quant à elle au développement d'un Airbnb-killer[8], tandis qu'OpenBazaar, projet open source décentralisé surnommé "le Ebay de la blockchain", vise à mettre en relation directement acheteurs et vendeurs, sans commissions ni restrictions.

9 - Quels sont les grands types d'usages de la blockchain ?

Il est possible de catégoriser les usages de la blockchain en trois types :

> **Les transferts d'actif**. Bitcoin est le cas d'usage le plus évident en la matière, si l'on pense par exemple au marché des transferts d'argent internationaux. Sur les 440 milliards de dollars par an que représente ce marché (données Banque Mondiale, 2015), près de 10 % de commissions sont prélevés par les plateformes d'échange dans certaines régions du globe. La diaspora africaine perd ainsi 2 milliards d'euros par an juste à cause du coût d'envoi des transferts d'argent[9], et l'Afrique subsaharienne subit même les frais de transferts les plus élevés au monde -12 %, soit quasiment le double de la moyenne mondiale - alors qu'il s'agit d'une des régions les plus pauvres du monde. La blockchain pourrait alors constituer une solution infiniment moins coûteuse (seuls quelques centimes sont prélevés sur chaque transaction) et plus rapide (entre 10 mn à 1h, contre parfois plusieurs jours pour les transferts à l'étranger), notamment pour les pays en développement.

  Mais la blockchain va au-delà du transfert monétaire, et permet de transférer tout type d'actifs : actions, obligations, titres de propriété, votes… En plus de sa valeur propre, chaque jeton peut en effet recevoir des métadonnées contenant des informations de tout type. Ainsi, la start-up Colu (lauréate Netexplo 2016) vise à faciliter des transactions extrêmement diverses, concernant des œuvres artistiques (notamment concernant les droits d'auteur dans l'industrie musicale), des voitures, appartements, billets de spectacle, etc. En pratique, pour un bien donné, Colu attache des métadonnées à un jeton du réseau, qui devient ainsi une preuve de la propriété du bien en question ; ce jeton peut ensuite être affiché pour preuve sur son téléphone sous forme de QR code unique certifié, et transféré si besoin à un autre utilisateur dans le cadre d'une transaction.

> **La blockchain en tant que registre** : le caractère inaltérable et transparent de la blockchain en fait un atout précieux pour des enjeux de traçabilité et de certification. Les documents légaux de tout type sont concernés (par exemple des certificats de naissance, mariage, …). L'ESILV, une école d'ingénieurs

[7] Le 7 octobre 2015, Uber a ainsi annoncé que le prix de son service VTC à Paris diminuerait de 20 % dès le surlendemain, et que le même niveau de chiffre d'affaire des chauffeurs ne serait plus garanti au-delà de six semaines.
[8] Voir la partie "smart contracts" dans le chapitre "Les applications de la blockchain".
[9] Rapport publié en 2014 par l'ONG britannique Overseas Development Institute

située à La Défense, a ainsi annoncé qu'elle certifiera les diplômes de ses étudiants sur la blockchain. Plus généralement, on peut imaginer que des domaines aussi divers que les "social goods", le "Made in France", la fraude alimentaire, la "supply chain" de façon plus globale, soient impactés par la blockchain. Dans la partie "applications", nous présentons ainsi deux cas d'usage en lien avec cette utilisation de la blockchain en tant que registre: les cadastres, et le secteur du luxe. Attention cependant : la blockchain n'apporte pas la preuve en soi qu'un document est un "vrai", mais simplement qu'il existait sous cette forme à date de son enregistrement. Tout dépend de la personne humaine qui introduit le document en amont.

> **Les smart contracts** : présentés ci-après, ils peuvent être considérés comme l'élément de la blockchain au plus grand potentiel applicatif.

10 - Que sont les smart contracts ?

Les smart contrats sont des programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable. Ils fonctionnement comme toute instruction conditionnelle de type "if - then" ("Si" condition vérifiée "Alors" conséquence s'exécute), et présentent trois principaux apports : une vitesse accrue, une meilleure efficacité, et une certitude que le contrat sera exécuté comme convenu. Ces programmes sont capables de surmonter les problèmes d'aléa moral, et de réduire les coûts de vérification, d'exécution, d'arbitrage et de fraude.

L'avantage de mettre en place des smarts contracts dans une blockchain réside dans la garantie que les termes du contrat ne pourront pas être modifiés. Un smart contract qui ne serait pas dans la blockchain serait un programme dont les termes pourraient être changés en cours d'exécution.

Comme l'explique Primavera de Filippi, chercheuse au Cersa (CNRS) et au Berkman Center for Internet & Society à l'Université d'Harvard, "*Un smart contract est un logiciel, une application de la blockchain. Comme on leur a donné l'appellation de "smart contracts", on a tendance à les assimiler à des contrats, mais ils n'ont pas en eux-mêmes d'autorité juridique. Lorsqu'un contrat juridique existe, le smart contract n'est qu'une application technique de ce contrat*." Les smart contracts posent des défis juridiques et éthiques majeurs, qu'il s'agisse de responsabilité légale ou de protection des consommateurs.

Une des start-up les plus prometteuses en la matière s'appelle Slock.it. Elle se définit comme la "future infrastructure de l'économie collaborative", ayant pour slogan : "louez, vendez ou partagez n'importe quel objet - sans intermédiaire". Slock.it vise à rendre certains objets entièrement autonomes : nous pourrions ainsi directement signer des contrats avec eux, sans intermédiaire. Des pistes de travail ont d'ores et déjà été présentées :

> Un "Airbnb-killer" : une porte avec laquelle on pourrait interagir directement pour signer un contrat de location, ce qui déclencherait son ouverture et rémunérerait le propriétaire même si celui-ci se trouve à des milliers de kilomètres. Le mini-ordinateur contenu dans la porte irait regarder en temps

réel les tarifs pratiqués dans la ville ou le quartier pour proposer à l'utilisateur un prix adapté à l'offre et la demande. Slock.it ne travaille pas seulement sur ce prototype de porte mais sur toute l'expérience client qui en découlerait. Parmi ces pistes de travail : le fait pour l'utilisateur de ne payer que pour l'énergie qu'il a réellement dépensée ; ou encore, la possibilité pour la porte lors du départ de l'utilisateur d'envoyer une demande d'intervention à une équipe de ménage.

> Un "Uber-killer" : un prototype de voiture autonome qui se loue elle-même, fondée sur le projet de la start-up Mobtiq, permettant aux passagers de ne payer que pour les kilomètres qu'ils effectuent réellement. L'idée serait qu'une communauté, composée par exemple d'une centaine de personnes, achète quelques voitures, utilisables par tous ses membres, sans appartenir à aucun individu en particulier.

11 - Qu'est-ce qu'une DAO ?

Une DAO (Decentralized Autonomous Organization) est un logiciel, un programme, fonctionnant sur la blockchain, qui fournit des règles de fonctionnement et de gouvernance à la fois transparentes et immuables, à destination d'une communauté s'organisant autour d'un objectif commun. Elle a pour but, à la manière d'un fond d'investissement classique, d'évaluer des projets qui lui sont soumis, de décider collectivement avec les détenteurs de jetons de la DAO de financer ou non ces projets, et de distribuer les risques et récompenses qui y sont relatifs.

Une DAO est donc en quelque sorte à la croisée du crowdfunding, du fond d'investissement et de la fondation. "*Il s'agit d'une organisation incorruptible qui appartient aux personnes qui ont aidé à la créer, à la financer, et dont les règles sont publiques*." détaille Stephan Tual, cofondateur de Slock.it. "*Il n'y a donc pas besoin de faire confiance à qui que ce soit, tout étant dans le code, auditable par chacun*.".

La première véritable DAO a été lancée fin avril 2016 à l'initiative d'une communauté de développeurs parmi lesquels les fondateurs de Slock.it. Elle est devenue en moins de dix jours la deuxième plus grande campagne de crowdfunding jamais réalisée. Les DAO sont considérées comme l'une des applications les plus prometteuses de la blockchain, même si nous n'en sommes encore qu'à ses débuts.

12 - Quels sont les défis qui se présentent pour le développement de la blockchain ?

Le premier enjeu est un enjeu de scalabilité, c'est-à-dire de passage à grande échelle. La blockchain n'est actuellement pas encore véritablement mature. En termes de blockchain publique, la blockchain Bitcoin est considérée comme la seule véritablement robuste à l'heure actuelle, même si celle d'Ethereum progresse rapidement. Cela étant, la blockchain Bitcoin présente des contraintes techniques qui freinent un éventuel déploiement massif et généralisé (ce qui n'est pas forcément son but d'ailleurs) : citons ainsi le temps de dix minutes pour valider

une transaction, qui permet d'assurer une sécurité du réseau mais qui n'est pas adapté pour utiliser le bitcoin en tant que moyen de paiement courant, ou encore la limite des sept transactions maximum par seconde, à comparer aux 2000 en moyenne d'un réseau comme Visa.

En lien avec ces limites techniques figure un enjeu de gouvernance. Les choix technologiques du bitcoin sont en effet décidés par sa communauté. Celle-ci connaît périodiquement des débats voire des conflits sur les décisions à prendre. Début 2016, les acteurs du bitcoin se sont ainsi divisés entre les partisans d'une augmentation de la taille des blocs (limités à 1 mégaoctet à l'heure actuelle) et les défenseurs d'une réduction de la taille de chaque transaction. Parmi ces derniers, certains plaident également pour la création de "sidechains", des blockchains secondaires rattachées à la blockchain originelle qui géreraient notamment les micro-transactions, sans que cette proposition ne fasse elle non plus le consensus. Les débats sont donc aujourd'hui loin d'être tranchés et conditionneront le développement à venir du bitcoin.

A tout cela s'ajoute plus globalement un défi majeur pour les blockchains : parvenir à créer une expérience utilisateur qui leur permettrait d'être utilisée par tout un chacun. Nous en sommes encore loin aujourd'hui mais il s'agit avant tout d'une question de temps, de la même façon que le réseau Internet a préexisté au Web (la principale application d'Internet, qui permet la publication et consultation de documents - textes, sons, images…- et qui utilise les techniques de liens hypertextes) et aux navigateurs internet.

Par ailleurs, un autre enjeu essentiel réside dans la consommation énergétique, très élevée, des blockchains utilisant le système du proof-of-work – c'est-à-dire Bitcoin en premier lieu, et Ethereum jusqu'à 2017, avant le basculement vers un système alternatif intitulé proof-of-stake justement pour réduire cette consommation. Si aucune étude scientifique et académique n'a pu évaluer précisément l'impact du proof-of-work sur l'environnement, il est en tout cas certain que ce processus de sécurisation du réseau passe, par nature, par un gaspillage d'électricité très important. Le développement des blockchains ne pourra s'exonérer de cette question-là.

Enfin, s'ajoutent à tout cela des questions juridiques et éthiques majeures, par exemple en termes de responsabilité, sans parler des enjeux plus culturels et humains liés à l'acceptation des concepts sous-jacents à la blockchain, qui redéfinissent un certain nombres de paradigmes actuels. Ces questions sont largement évoquées dans la troisième partie intitulée "Penser la blockchain".

2

LES APPLICATIONS DE LA BLOCKCHAIN

La blockchain peut sembler abstraite sans exemples concrets. Nous avons choisi de présenter un certain nombre de cas d'usage destinés à illustrer le potentiel de cette technologie complexe et à montrer l'étendue de ses possibilités. Ces cas d'usage sont loin d'être exhaustifs, d'autant que la plupart des applications restent encore à construire. Ils suffisent néanmoins à comprendre l'étendue des possibilités offertes par la technologie.

Assurance

Le secteur de l'assurance est l'un des premiers avec le secteur financier à avoir manifesté son intérêt pour la blockchain. Des entreprises comme Lloyds ou Allianz France ont exprimé assez tôt leur volonté de lancer des expérimentations sur la blockchain, et début 2016, Axa a investi 55 millions de dollars dans la start-up Blockstream, qui doit permettre, entre autres, une interopérabilité entre différentes blockchains.

Alors que des modèles d'assurance peer-to-peer avaient déjà commencé à apparaître (par exemple Friendsurance), la blockchain y donne un nouvel élan grâce à des systèmes d'assurance automatisés fondés sur des smart contracts. Des entités appelées "oracles" permettent ainsi de gérer les données des smart contracts et de déterminer, par exemple, si les conditions sont bien remplies pour déclencher le paiement.

L'exemple souvent cité est celui de l'assurance dite indicielle ou paramétrique, autrement dit l'assurance liée à un indice tel que la température ou le niveau de pluie. Le smart contract conclu entre l'agriculteur et l'assureur peut par exemple stipuler que le paiement est effectué après 30 jours sans précipitations. Le contrat est alimenté par des données externes fiables (par exemple du service national de météorologie), qui permettent aux oracles de déclencher automatiquement le paiement après 30 jours de sécheresse, sans l'intervention d'un expert ni nécessité de déclaration ou revendication de l'assuré.

En automatisant l'exécution des contrats, ces mécanismes permettraient aux assurés comme aux assureurs de s'émanciper des phases déclaratives : formulaires, réclamation, vérification, déclenchement de l'indemnisation… La blockchain, en faisant office de tiers de confiance automatisé, ouvre ainsi la voie à une diminution des coûts de structure tout en fiabilisant et en accélérant les processus de décision. A terme, cela générerait également une plus grande satisfaction des assurés *via* la mise en place de nouveaux services plus intuitifs et plus rapides.

Un autre exemple d'application envisageable concerne les assurances voyage : constatant que 60 % des passagers assurés contre le retard de leur vol ne revendiquaient jamais leur argent, une équipe a créé lors d'un hackathon à Londres en 2015 un système d'assurance automatisé basé sur la blockchain, *via* le service Oraclize. Avec ce service, les passagers sont automatiquement indemnisés lorsque leur vol est en retard, sans avoir besoin de remplir un quelconque formulaire, et donc sans que l'entreprise ne doive traiter les demandes.
L'apport de la blockchain consiste ici à générer la confiance et la sécurité nécessaires pour automatiser les phases déclaratives sans avoir recours à un tiers. Si par le passé les assureurs n'ont pas mis en place ce type de produits, la blockchain apporte aujourd'hui une solution qui pourrait permettre à de nouveaux acteurs de pénétrer ce marché.

En allant plus loin dans la prospective, il est possible d'envisager des liens entre assurance et DAO (Decentralized Autonomous Organization), c'est-à-dire des entités autonomes fonctionnant sur la blockchain et dont les règles de fonctionnement sont inscrites dans du code informatique. Elles pourraient créer des groupements d'assurés sans organisation centrale de contrôle, chaque groupe étant gouverné par les assurés eux-mêmes. Dans ce genre de système, les primes versées par chaque assuré formeraient un capital, utilisé pour payer les indemnisations ; les sommes non-utilisées à la fin de l'année seraient redistribuées automatiquement aux assurés, grâce à la réduction drastique des frais de structure.

Ce modèle collaboratif déplace en outre le pouvoir de décision du tiers parti assureur vers les assurés : des systèmes de vote peuvent être mis en place pour permettre au groupe de décider collectivement de valider ou non une indemnisation ou de redistribuer le surplus.

La grande question soulevée par ces modèles est celle de la régulation : avec des contrats sans territorialité et une forme de pouvoir décisionnel donné à des lignes de code, les enjeux juridiques sont considérables. Déterminer qui est légalement responsable du code contenu dans les DAO est une problématique qui, à l'heure actuelle, n'a pas véritablement été tranchée par les systèmes législatifs.

La blockchain n'en reste pas moins un outil au potentiel important pour mettre en place des systèmes plus sûrs, plus intuitifs et plus collaboratifs, capables de créer un système assurantiel recentré sur ses utilisateurs.

Banques

Certains pronostics avancent que la blockchain pourrait entraîner la fin des banques telles que nous les connaissons. La blockchain serait en effet de nature à rendre caduque, en théorie, toutes les activités fondées sur l'existence d'un tiers de confiance : bon nombre de services financiers figurent en très bonne place dans cette définition.

Dès les origines du bitcoin, voué à servir de monnaie numérique sans intermédiaire, la fin des banques a été évoquée. Aujourd'hui encore l'idée qu'un certain nombre de métiers bancaires pourraient demain disparaître au profit soit d'une automatisation soit d'acteurs fonctionnant sur une blockchain reste un futur envisageable.

De fait, un certain nombre de facteurs poussent à imaginer une remise en question du rôle des banques dans la société et l'économie.

Pour David François par exemple, Chief Technical Officer de la plateforme bitcoin Paymium, "*Un des grands avantages de la blockchain Bitcoin réside dans le fait qu'il n'existe aucune barrière à l'entrée : n'importe qui peut créer un service qui fonctionne sur la blockchain. En particulier, n'importe qui, moyennant un important capital confiance, peut créer une banque en bitcoin qui accepte les dépôts des clients et émet des crédits en bitcoins. C'est en ce sens que le bitcoin peut disrupter la banque sur l'activité de crédit, en faisant tomber cette barrière à l'entrée"*. L'aspect clé réside dans la confiance qu'obtiendront les plateformes bitcoin de la part des utilisateurs : "*Les acteurs qui réussiront le mieux seront ceux qui auront réussi à générer un capital confiance très important et à capitaliser dessus*" juge-t-il.

Autre exemple, l'économiste Philippe Herlin, auteur de "La fin des banques ?", qui considère quant à lui que "*les banques sont uberisables en tant que très grosses structures, très hiérarchisées et centralisées*". En argument-clef, "*les coûts d'intermédiation très faibles des services fondés sur le bitcoin, par rapport aux frais bancaires*"[10]. Du fait des puissantes barrières règlementaires, et notamment sur les activités de crédit au cœur du métier bancaire, il pronostique toutefois avant tout le développement du bitcoin dans des pays où la monnaie est mal maîtrisée, et où la crypto-monnaie peut constituer une valeur refuge, comme on a pu le constater d'ores et déjà en Argentine ou dans les pays à difficulté comme la Grèce.

Il faut également ajouter que diverses tendances se conjuguent au même moment et plaident pour une redéfinition du rôle des banques. Tout d'abord la crise de confiance durable instillée par les crises et les diverses affaires (Kerviel, Libor, évasion fiscale…), qui correspond à une certaine hostilité idéologique de la communauté originelle du bitcoin -et de certaines blockchains- vis-à-vis des établissements financier.

[10] Propos recueillis lors de la conférence 'le Big Bang Blockchain', en janvier 2016.

Ensuite, le monde des "Fintech", c'est-à-dire des start-up qui se positionnent sur le marché de la finance, est en pleine explosion. Ces multiples entreprises ont toutes pour cible un ou plusieurs métiers traditionnels des intermédiaires financiers, réinventés notamment grâce aux outils numériques. Ce monde des Fintech attire non seulement l'attention des entreprises et des particuliers à la recherche de services à moindre coûts, mais également des investisseurs qui dépensent des fortunes pour alimenter la croissance de ces start-up.

Sous cette pression multiforme qui gagne sans cesse en ressources et en visibilité, la législation tend à s'adapter plus rapidement qu'on ne l'aurait appréhendé pour permettre à ces jeunes entités de croître rapidement, tandis que les acteurs financiers traditionnels et particulièrement les acteurs bancaires "généralistes" sont contraints de faire évoluer en parallèle et à toute vitesse simultanément toutes leurs pratiques du métier ou presque. Les Fintech blockchain, très représentées à Londres, s'inscrivent ici dans une tendance lourde qui par sa rapidité d'évolution menace mécaniquement les acteurs traditionnels, qui peinent parfois à s'adapter.

Face à cette évolution, pourtant, il est nécessaire de nuancer malgré tout le propos.

Tout d'abord, plusieurs limites techniques rendent aujourd'hui la blockchain Bitcoin – la plus sécurisée des blockchains publiques à ce jour - difficilement utilisable à grande échelle, rendant sa menace pour les banques assez limitée à court terme : citons ainsi la limite des sept transactions par seconde, qui n'est certes pas gravée dans le marbre mais qui constitue un réel frein.

Certains développeurs estiment que la taille des blocs validés, qui commande directement le nombre de transactions effectuées en moyenne, devrait être augmentée afin de faciliter le passage à l'échelle du Bitcoin. Les débats sont vifs dans la communauté, et du fait de la gouvernance complexe du bitcoin, il faudra sans doute un peu de temps avant que cette restriction des sept transactions moyennes ne soit assouplie.

Par ailleurs, la relative volatilité des crypto-monnaies peut rendre complexe leur utilisation dans un certain nombre d'opérations financières. Dans la mesure où les atouts de la blockchain se composent 1- d'une réduction des délais de transaction et 2- d'une réduction des coûts, ne pas pouvoir s'assurer de la stabilité de la monnaie peut obliger à des surcoûts importants qui menacent cet avantage.

Un exemple classique : le marché des remises, c'est-à-dire de l'envoi d'argent à l'étranger (typiquement dans un contexte d'un travailleur renvoyant une partie de son salaire dans son pays d'origine) ; sur le papier, le bitcoin avec ses frais de transactions négligeables et fixes (par opposition aux pourcentages très élevés pratiqués par certains opérateurs en situation de quasi-monopole), et son délai de transaction faible (se comptant en minutes tandis qu'un acteur traditionnel comptait jusque-là en jours), paraît une situation idéale. Mais en réalité les frais nécessaires pour changer au départ et à l'arrivée l'argent en bitcoin, et les risques inhérents à la volatilité de la monnaie qu'il faudrait théoriquement couvrir par une assurance, représentent des frais qui, additionnés, rendent la compétitivité de la

solution moins évidente. Ainsi malgré de nombreuses tentatives, seule la start-up BitPesa perce vraiment aujourd'hui sur le marché Africain par exemple.

De leur côté, les banques ne restent de toute façon pas inactives, et tentent de transformer la menace en opportunité. La méthode retenue est globalement toujours la même : s'approprier la technologie pour l'adapter au sein des systèmes actuels.

Par exemple, le consortium formé autour de la start-up blockchain R3 CEV réunit plus d'une quarantaine de banques de grande envergure, dont Goldman Sachs, UBS, JP Morgan, ainsi que la BNP côté français, afin de définir des standards communs de mise en place de blockchains interbancaires. L'objectif affiché est de "remplacer" en réalité Swift, le système de transaction interbancaire, même si dans la pratique les expérimentations retenues par le consortium s'intéressent d'abord à des utilisations à plus courte échéance.

Ce mode de fonctionnement décrit assez bien l'état d'esprit des banques, forcées sous la menace de coopérer (dans une certaine mesure), mais aussi d'expérimenter plus ou moins discrètement en interne pour ne pas se laisser dépasser par la technologie. Afin de garder le contrôle sur leurs systèmes, les expérimentations se concentrent d'ailleurs autour des "blockchains" de type privé, où seul un nombre limité d'acteurs peuvent enregistrer des transactions ou disposer du registre. Les blockchains publiques sont en effet plus compliquées à utiliser pour les banques qui ne souhaitent guère perdre la main sur leur contenu, et qui doivent respecter des réglementations telles que les KYC (Know Your Customer – l'identification des parties prenantes) peu compatibles avec le caractère pseudonyme des transactions sur une blockchain publique.

Or si l'on se concentre sur une blockchain privée, par exemple dont les nœuds seraient concentrés dans quelques établissements choisis, ou même au sein des différents départements d'une même banque, l'attrait de la blockchain pour la banque est tout simplement celui d'une réduction des coûts. Selon un rapport de la banque Santander, l'utilisation de la blockchain pourrait faire économiser aux banques 15 à 20 milliards de dollars par an d'ici 2022, grâce à la réduction des "coûts d'infrastructure liés aux paiements internationaux, au trading et à la mise en conformité".

Cette réduction des coûts pourrait permettre à certains métiers bancaires de se réinventer suffisamment vite et efficacement pour éviter de tomber aux mains d'outsiders (venus des Fintech ou du monde des grandes entreprises innovantes). Pour cela, il faudra que les acteurs concernés soient capables non seulement de collaborer efficacement entre eux, de montrer une grande agilité de transformation, et surtout de prolonger le cadre réglementaire protecteur le temps d'être prêt pour la concurrence.

En France, la première initiative bancaire ayant dépassé le stade du prototypage a été rendue publique par la BNP. Conçue en interne avec l'aide de la start-up Labo Blockchain, elle s'appuie sur la plateforme de financement participatif SmartAngels, dont l'émission de certaines contreparties aux investissements sera désormais enregistrée sur une blockchain.

La logique des blockchains privées va bien sûr à rebours du modèle libertaire pensé par les précurseurs de cette technologie, et des principes mêmes de la blockchain "historique", dont le cœur du potentiel repose justement sur l'ouverture et l'absence de contrôle centralisé - par un ou plusieurs acteurs. Pour autant, les blockchains publiques ne sont pas forcément incompatibles avec les blockchains privées, au contraire. La cohabitation semble possible, tant les atouts des unes complètent les limites des autres : d'un côté, une révolution capable de toucher de façon importantes les banques mais dont l'horizon ne semble pas à court terme; de l'autre, une logique d'optimisation interne au monde bancaire, sans être toutefois de nature à bouleverser le secteur.

Energie

L'énergie possède de nombreuses facettes, de l'extraction à la consommation, susceptibles de rendre l'utilisation des blockchains intéressante. Or la période est favorable : la multiplication des auto-producteurs (les foyers dotés de panneaux photovoltaïques par exemple) pose d'important problèmes aux réseaux de distributions traditionnels, conçus historiquement de façon univoque. La solution prônée pour y répondre est celle de la multiplication des réseaux locaux intelligents, les smart-grids. Deux projets encore en développement résument aujourd'hui une partie du potentiel de la technologie blockchain dans cette perspective.

La première utilisation est celle de SolarCoin, et concerne les garanties d'origines. Ces garanties, qui visent à promouvoir la production et la consommation d'énergies propres, sont aujourd'hui concentrées au main d'un acteur central (Powernext pour la France). L'idée de SolarCoin est de donner pour chaque MWh d'énergie solaire 1 SolarCoin au producteur. Ces jetons s'échangeront ensuite sur une place de marché, rendant liquide et efficient l'échange de ce qui est finalement une garantie d'origine 2.0. A terme, l'idée est de parvenir à un véritable marché de l'énergie locale désintermédié, où offre et demande seuls fixeront les prix de l'énergie. Cette ambition est également celle que poursuit la start-up Grid Singularity, qui fonctionne directement sur Ethereum.

Transactive Grids, le projet emblématique de la plateforme LO3 (alliée pour l'occasion à Consensys, une structure développant de nombreuses applications sur la blockchain), est un second exemple devenu assez célèbre des applications de la blockchain à l'énergie. Son objectif réside dans la réappropriation par les citoyens de leur production énergétique, par l'établissement de mini-grids, c'est-à-dire de mini communautés énergétiques autonomes ; pour cela des capteurs enregistrent l'historique de la création énergétique à un point précis, et l'enregistre aussitôt sur la blockchain Ethereum. Des smart contracts pourront ensuite régir les règles d'utilisation de cette énergie, et naturellement les tarifs des producteurs.

Transactive Grids développe aujourd'hui une expérimentation pilote à Brooklyn, où 5 maisons de producteurs vendent à 5 foyers "consommateurs". Cette expérimentation, largement médiatisée, explique en partie les manifestations d'intérêt de grands groupes énergétiques sur le sujet, mais aussi les tests en cours rendus publics par ces derniers.

Le conglomérat allemand RWE a ainsi annoncé une expérimentation avec la start-up Slock.it autour d'une nouvelle génération de bornes de rechargement électrique. En France, Engie conduit des expérimentations sur le sujet, notamment dans la traçabilité des flux (eau, gaz, électricité), le combinat capteur-blockchain permettant par exemple une gestion plus fine de la consommation et de la maintenance.

De façon générale, l'énergie est un terrain propice au déploiement de la blockchain, mais au vu de la complexité du sujet, de la régulation et de la prégnance des acteurs traditionnels, il faudra probablement encore un certain temps avant que les projets actuels puissent se déployer à grande échelle.

Santé

Plusieurs cas d'usage sont envisageables dans le secteur de la santé. La blockchain pourrait notamment servir à la traçabilité des médicaments, à la sécurisation des données de santé, et à la gestion des données des patients.

On estime aujourd'hui qu'au moins 10 à 30 % des médicaments fournis dans les pays en développement sont des "faux médicaments", ce qui pose des problèmes de santé considérables : l'Organisation Mondiale de la Santé estime ainsi à 700.000 le nombre de décès par an provoqués par des médicaments contrefaits. Un moyen de lutter contre ce phénomène serait de créer un système universel garantissant la traçabilité des médicaments. La blockchain, en tant que registre distribué, pourrait permettre aux différentes entreprises pharmaceutiques, aux régulateurs et même aux particuliers d'utiliser la même base de données, sans qu'une seule entreprise ou institution n'en soit propriétaire.

Ce mécanisme de "certification" des médicaments pourrait être étendu aux données de santé au sens large. En certifiant les dossiers médicaux sur une blockchain, on ajoute une couche supplémentaire de sécurité : toute mise à jour d'un document est enregistrée dans la blockchain, sans que les documents eux-mêmes aient besoin d'y être stockés. Il est ainsi impossible pour qui que ce soit (pouvoirs publics, institutions de santé, patients) de "couvrir" un changement dans un dossier médical. Dans cette optique, Guardtime, une start-up spécialisée, a conclu un partenariat avec le gouvernement estonien afin de sécuriser le million de dossiers médicaux estoniens sur la blockchain[11].

Mais l'application la plus impactante sur le quotidien des patients et des professionnels de santé pourrait concerner la gestion des données médicales, notamment en permettant au patient de se réapproprier ses données et d'en gérer l'accès. Chaque patient pourrait ainsi paramétrer son dossier médical de façon à en autoriser l'accès (total ou partiel) aux personnes de son choix (médecin traitant, famille…). Il pourrait également requérir un certain nombre de signatures (clés privées) pour en ouvrir l'accès. C'est en partie ce qui motive le projet Enigma[12].

[11] Business Insider, Oscar Williams-Grut, "*Estonia is using the technology behind bitcoin to secure 1 million health records*", 3 mars 2016
[12] Voir la partie sur le Cloud et la blockchain.

Prenons une situation concrète, celle d'un patient inconscient après un malaise : il ne peut donc pas débloquer l'accès à ses données médicales. Celles-ci peuvent toutefois être accessibles par l'hôpital, à la condition qu'elles soient débloquées par 3 clés accréditées différentes : celles du médecin de l'hôpital, de l'ambulancier, et d'un parent du malade. Utiliser la blockchain pour ce système garantirait entre autres l'absence d'organe central de contrôle qui pourrait accéder à toutes les données.

En enregistrant par la suite les étapes du parcours de soins dans une blockchain regroupant institutions de santé et assureurs, il serait également possible d'automatiser le paiement des prestations médicales nécessaires, grâce à des smart contracts[13].

En ayant une vision à plus long terme, il serait même imaginable que les patients puissent anonymement monétiser leurs données auprès des industries pharmaceutiques, permettant à celles-ci d'étudier les résultats de leurs traitements sur une population plus large. De leur côté, les patients seraient automatiquement indemnisés lorsque l'entreprise accèderait aux données souhaitées. A la clef un échange gagnant-gagnant pour les patients qui ont un contrôle accru sur leurs informations comme pour les laboratoires qui pourront préciser leurs recherches avec le traitement d'échantillons statistiques à la fois plus larges et plus pertinents.

Cadastre

La blockchain, en tant que registre à la fois transparent et sécurisé, intéresse d'ores et déjà plusieurs pays pour y héberger leur système de cadastre, document qui recense l'état de la propriété foncière sur le territoire. Nous vous en proposons deux exemples, similaires dans la technologie mais assez différents dans leur application.

Le Ghana tout d'abord, où la start-up Bitland, qui fait partie des 10 lauréats Netexplo 2016, travaille à enregistrer les titres de propriété sur la blockchain et à résoudre les conflits fonciers. Près de 90 % des terres rurales ghanéennes ne sont pas enregistrées dans une base de données officielle, et de nombreux citadins n'ont pas encore d'adresse officielle.

Cette situation, loin d'être propre au Ghana, se retrouve dans de nombreux pays en développement, posant ainsi de nombreux problèmes administratifs et économiques. Le développement rural par exemple en souffre puisque l'absence de sécurité foncière freine en partie les investissements nécessaires au développement de la productivité agricole ; mais de nouveaux domaines économiques sont également concernés, à l'image du e-commerce, puisqu'il est tout simplement impossible aux foyers de se faire adresser des colis…

Sur le plan individuel, l'absence de titre de propriété rend également impossible l'hypothèque et limite fortement le recours à l'emprunt, tout en étant source de potentiels problèmes lors de conflit ou de succession. Ces multiples problématiques entravent la prise d'initiative personnelle et l'accumulation de

[13] Voir également le cas d'usage sur l'assurance

capital, et constituent de façon générale un frein au développement économique de ces pays.

Le projet Bitland, en phase de lancement, a bénéficié d'une reconnaissance légale de l'Etat ghanéen. "*Nous travaillons avec tous les bords politiques pour que le projet ne soit pas impacté en cas d'éventuel changement de gouvernement*" explique Chris Bates, Chief Security Officer de Bitland.

"*Notre plus grande ambition serait de contribuer à faire en sorte que le Ghana et l'Afrique développent leurs terres grâce à des registres transparents, des systèmes écologiques, et en coopération avec les gouvernements. Le but est de créer un système capable de réduire la corruption humaine dans les conflits fonciers. Ce projet dépasse largement Bitland. Les citoyens ont besoin d'un système qui empêche leur gouvernement de profiter d'eux injustement. Le projet pourrait apporter de la richesse à des communautés entières, pas seulement aux mains de quelques-uns.*"[14]

Bitland projette de signer un contrat de 4 ans avec le gouvernement pour couvrir la totalité du pays, et est déjà en discussion pour s'étendre à d'autres Etats.

Une initiative similaire se développe par ailleurs en Géorgie. A la différence du Ghana toutefois, elle est portée directement et officiellement par le gouvernement. En avril 2016, l'Agence Nationale du Registre Public et l'entreprise BitFury spécialisée dans le bitcoin ont en effet annoncé, lors d'une cérémonie au Ministère de la Justice géorgien, la signature d'un partenariat pour désigner et piloter un projet de titres fonciers sur la blockchain. Le but est de permettre aux citoyens d'enregistrer leur propriété sur la blockchain.

"*La blockchain apportera trois éléments essentiels*", explique le directeur de BitFury : "*D'abord, elle permettra de sécuriser les données pour qu'elles soient incorruptibles. Ensuite, elle donnera la possibilité de réaliser un audit public quasiment en temps réel : l'auditeur pourra auditer le registre non pas une fois par an, mais toutes les 10 minutes par exemple. Enfin, elle réduira la friction dans l'enregistrement et le coût d'enregistrement des droits de propriété, puisque les citoyens pourront utiliser le service sur leur smartphone. La blockchain sera ainsi utilisée comme un service de notariat*".

L'économiste péruvien Hernando De Soto, inventeur de la théorie du "capital mort"[15], devrait faire partie de l'équipe du projet, qui place la Géorgie au rang des rares pays ayant annoncé une expérimentation gouvernementale sur ce sujet.

Covoiturage

Arcade City est un projet emblématique de la façon dont la blockchain pourrait complètement réinventer l'économie de plateforme que représentent les modèles économiques du type Uber, Airbnb, Booking, etc. Ces modèles, qui reposent sur une plateforme qui centralise l'information et les interactions des utilisateurs, ont

[14] Interview réalisée en Mai 2015.
[15] Pour plus d'informations, lire le texte de Julien Lévy dans la partie "Penser la blockchain".

également en commun de capter au passage une partie plus ou moins importante de la valeur qui transite.

Dans le cas d'Uber, deux éléments cristallisent la critique et ont donné naissance au projet d'Arcade City : d'une part la totale mainmise sur les prix pratiqués par les utilisateurs, et d'autre part les 20 % prélevés en commission sur chaque trajet. Arcade City, née de l'idée de créer une sorte de coopérative des chauffeurs Uber fonctionnant sur blockchain, a été créée en février 2016 et a connu très rapidement un certain succès, avec 1800 chauffeurs inscrits en moins de deux semaines. En l'espace d'un mois, plus de 1000 trajets ont été effectués dans une centaine de villes aux Etats-Unis, au sein de 27 Etats différents, ainsi qu'en Australie. Au cœur du projet, une plateforme ouverte où conducteurs et passagers peuvent être mis en relation directement, sans intermédiaire.

"*Le talon d'Achille d'Uber est son management centralisé des prix. Chaque jour les chauffeurs d'Uber se préoccupent de la diminution des prix fixés de façon centralisée au QG d'Uber à San Francisco, ou de la prochaine action coercitive menée par un gouvernement centralisé contre des échanges pair-à-pair. En décentralisant la décision pour la porter au niveau du chauffeur et du passager, Arcade City libère le chauffeur et permet au passager d'avoir le contrôle sur l'expérience entière de son trajet"* explique Christopher David, fondateur du projet.

Début avril 2016, les membres du projet ont retiré provisoirement l'application des différents App Stores, le temps de travailler plus en profondeur à une version complète. Ils ont notamment annoncé vouloir intégrer la blockchain Ethereum dans leur service, pour que les systèmes d'identité, d'évaluation et de réputation d'Arcade City reposent sur celle-ci. Des smart contracts pourraient également déterminer les règles de calcul de la réputation des chauffeurs. En parallèle, l'équipe du projet cherche à développer une assurance optionnelle pour les conducteurs. L'ambition affichée est qu'à terme la blockchain puisse gérer entièrement la plateforme, qu'il s'agisse des paiements ou des contrats d'assurance. La communauté blockchain regarde toutefois Arcade City avec une certaine mesure, le projet n'ayant notamment encore rien prouvé en termes d'intégration à la technologie.

Au-delà de ce projet particulier et de ses caractéristiques propres, l'idée même d'un service de covoiturage décentralisé reposant sur la blockchain est une idée très emblématique des applications possibles de la technologie. Avant Arcade City, un projet israélien intitulé La'Zooz avait déjà cherché à mettre en place un tel service. Il allait plus loin qu'Arcade City puisqu'il n'était pas détenu par ses fondateurs, mais par la communauté de ses utilisateurs. L'application devait rémunérer ses conducteurs en jetons appelés "Zooz" (une monnaie basée sur le bitcoin), avec l'idée qu'ensuite les utilisateurs dépensent leurs jetons en commandant une course à un tarif unique, proche de 0,1 dollar/km. Le projet n'avait toutefois pas été porté à son terme. Le covoiturage version blockchain reste donc encore bel et bien à construire.

Produits de luxe

Everledger est une start-up créée en 2015 emblématique des enjeux de traçabilité et de certification, qui utilise la blockchain pour combattre la fraude dans le domaine du luxe. Son marché premier est celui de l'industrie du diamant.

L'idée est de construire un registre numérique qui recense les transactions diamantaires, avec comme objectif de rendre le marché du diamant plus transparent. Les fondateurs d'Everledger misent ainsi sur l'effet de réseau pour obtenir à terme un système dissuasif pour la fraude : une fois la base de donnée suffisamment développée, si un vendeur n'est pas capable de prouver par preuve cryptographique qu'il possède bien les droits sur le diamant, la valeur du joyau diminuerait considérablement.

L'utilisation de la blockchain qui est faite ici est celle d'un registre, dont l'atout principal réside dans son caractère immuable : de la même façon qu'une transaction bitcoin inscrite sur la blockchain ne peut pas être altérée, il est impossible de changer une entrée écrite sur le registre d'Everledger.

Concrètement, pour l'enregistrement de chaque diamant, Everledger recense 40 attributs (taille, couleur, pureté, poids en carat, lieu d'extraction…), qui constituent 40 métadonnées à partir desquelles un numéro de série unique est créé. Ce numéro de série est ensuite gravé microscopiquement sur la pierre d'une part, et d'autre part ajouté à la blockchain avec les 40 métadonnées. Toutes ces données et le numéro de série sont cryptés et répliqués sur chacun des nœuds du réseau Everledger, ce qui constitue de fait une protection contre toute attaque qui viserait à altérer le registre.

Le marché du diamant est un choix judicieux, dans la mesure où la fraude et les problématiques de provenance sont prégnantes, par exemple avec les fameux "diamants de sang" qui financent les groupes armés en Afrique. Des certificats papiers prouvant la provenance de diamants avaient été mis en place, mais le registre d'Everledger est inaltérable, mis à jour continuellement et accessible depuis n'importe quel endroit dans le monde, grâce à la blockchain, ce qui constitue un pas en avant décisif. Plus encore, le fait que le registre ne soit pas aux mains d'un acteur unique (un gouvernement, ou un assureur, etc.) mais redistribué, a permis de rassembler plusieurs grands acteurs du secteur.

La start-up a ainsi commencé à travailler avec plusieurs compagnies d'assurance, intéressées au premier chef puisque le coût pour les assureurs de la fraude dans le marché diamantaire est évalué à près de 50 milliards de dollars annuels. Everledger est également en discussion avec des sites de e-commerce, comme Amazon ou Ebay, pour empêcher la revente de produits volés sur leurs plates-formes, ainsi qu'avec Interpol et Europol. Dans ce contexte porteur, plus de 900.000 diamants ont été enregistrés par Everledger en seulement quelques mois.

La start-up a toutefois l'ambition d'aller au-delà du marché du diamant et d'investir tout le champ du secteur du luxe : bijoux, montres, sacs haut de gamme… Elle réfléchit également à la mise en place de blockchains privées pour de la

certification d'œuvres d'art. La cofondatrice Leanne Kemp esquissait en mai 2016 la forme que prendrait une telle blockchain : "*Il est tout à fait possible d'imaginer un consortium de quinze institutions artistiques, où chacune gèrerait un nœud et où dix d'entre elles devraient signer chaque bloc dans le bon ordre pour que le bloc soit validé*". Dans cette optique, les métadonnées pourraient être constituées d'un historique propre à la pièce (attributs physiques, provenance, historique des expositions et référencement littéraire par exemple).

Everledger a d'ores et déjà signé un partenariat avec Vastari, une société qui sert d'intermédiaire entre les musées qui recherchent de nouvelles pièces et les collectionneurs privés qui cherchent à accroître la valeur de leurs œuvres en les présentant au public, pour progresser sur ce marché.

Cloud

Une des applications les plus inattendue mais néanmoins prometteuse de la blockchain concerne ce qu'on appelle le *cloud computing*, qui consiste à exploiter la puissance de calcul ou le stockage de serveurs informatiques situés à distance *via* Internet. Aujourd'hui, c'est une activité qui va du simple hébergement de données (Infrastructure As A Service) à la mise à disposition de logiciels comme par exemple Gmail (*Software As A Service*). Bien que très populaire, le cloud soulève d'importantes questions de sécurité des données, mais aussi de confidentialité : toutes les données hébergées par des entreprises américaines sont par exemple susceptibles d'être consultées à tout moment par des agences gouvernementales américaines.

De nombreuses initiatives visent à utiliser la blockchain dans le domaine du cloud. Nous avons choisi de nous arrêter sur quelques cas emblématiques.

Blockchain As A Service

La course est lancée entre deux géants que sont Microsoft, qui a annoncé dès octobre 2015 un partenariat avec Ethereum pour sa plate-forme de cloud généraliste Azure, et IBM, qui a annoncé en février 2016 s'intéresser également à cette solution. L'idée ? Pouvoir accéder directement et à moindre coût à n'importe quelle blockchain depuis une plate-forme de développement cloud, et pouvoir notamment développer des applications utilisateurs liées, qu'il sera possible de rendre disponibles ensuite sur ces mêmes plateformes. L'objectif pour ces deux entreprises est donc de parvenir à créer le plus rapidement possible un écosystème applicatif blockchain intéressant autour de leurs plates-formes respectives, pour attirer par la suite d'autres développeurs, et donc *in fine* d'autres applications pour leurs clients.

Storj, Filecoin et autres : le stockage en cloud distribué

Une des utilisations "de base" du cloud est aujourd'hui la simple location de serveurs. Ce qu'achètent les entreprises à travers des offres comme celles de Amazon Web Services, et les particuliers indirectement à travers des outils comme Dropbox, est d'abord de l'espace de stockage. Ce stockage permet certes de mutualiser et d'externaliser les coûts sans se soucier de l'entretien, et d'accéder à ses données depuis n'importe quel lieu, mais il a un prix : les questions d'éventuelle perte de données et de responsabilisation des opérateurs

qui en découlent, les enjeux de confidentialité, et les vulnérabilités causées par les constants allers-retours avec ces serveurs *via* des réseaux externes.

Des start-up comme Storj proposent de réinventer ce modèle du cloud grâce à la blockchain. Partant du constat qu'une partie importante des limites du système actuel provient en réalité de la centralisation des données, ces projets proposent de louer l'espace disque des utilisateurs qui le souhaitent, et distribuent dans ces espaces les fragments des données de ceux qui souhaitent utiliser Storj.
Ainsi, si quelqu'un souhaite héberger par exemple un fichier de musique, celui-ci sera distribué entre plusieurs serveurs, et seul l'individu en question sera en mesure de reconstituer le document pour son utilisation, grâce au système de clé privée de la blockchain. Les possesseurs des différents serveurs, quant à eux, seront rémunérés pour héberger un fragment inutilisable à lui seul. Ces plateformes de mise en relation entre offre (capacités de stockage) et demande (besoin d'un stockage externalisé) pourraient constituer le nouveau visage du cloud de demain, moins coûteux, plus rapide, et plus sûr.

Enigma, le cloud au service de la vie privée
Ce projet en cours de développement du MIT Media Lab consiste en une plateforme cloud décentralisée sur une blockchain. La particularité du protocole est que son design est tout entier tourné vers la protection de la vie privée : l'objectif affiché est de rendre aux internautes le contrôle de leurs données personnelles. Les données sont pour cela chiffrées et éclatées sur différents serveurs. Cette double protection (chiffrement et morcellement des informations) assure que nul ne peut lire de lui-même le contenu inscrit sur Enigma : l'internaute, maître des clefs, peut lui seul conférer à des tiers l'accès à une partie ou à la totalité de ses données, à ses propres conditions.

Supposons par exemple que les données issues d'un capteur (telle qu'une montre connectée) soient inscrites sur Enigma ; l'utilisateur pourra vendre l'accès d'une partie de ces données à une application, qui sera alors libre de les analyser. Non seulement l'application sera alors limitée aux seules données concédées par l'utilisateur, mais elles ne pourront être ensuite réemployées ou revendues, puisqu'elles resteront chiffrées. Si Enigma remplit ses promesses de confidentialité et de contrôle autonome, de nouvelles possibilités devraient s'ouvrir pour des domaines très consommateurs en données, comme la santé (notamment pour la recherche pharmaceutique)[16] ou l'intelligence artificielle (par exemple pour alimenter un programme de *deep learning*).

Ethereum et l'ordinateur mondial
Pour comprendre pleinement le potentiel d'Ethereum, il est nécessaire de s'extraire un instant de la vision de cette blockchain comme d'un registre distribué pour revenir à celle de son fondateur Vitalik : Ethereum a l'ambition d'être le *World Computer*, c'est-à-dire l'ordinateur mondial. De ce point de vue-là, la blockchain peut être considérée comme une *Virtual Machine* : son objectif est de fournir tous les services d'un ordinateur à distance, et constitue donc une nouvelle dimension distribuée du cloud. Dans ce projet, la mutualisation des coûts d'infrastructure (au fondement de toute blockchain publique) pourrait réduire de façon importante la

[16] Voir les applications de la blockchain dans la santé.

facture pour l'utilisateur sur un certain nombre de cas d'usage. Payer des ethers pour faire tourner des smart contracts est, en dernière analyse, ce qui est à l'origine de l'idée de *Cloud Computing* : la location de puissance de calcul.

IPFS & Swarm : le règne à venir des applications distribuées ?

Si IPFS ne constitue pas à proprement parler un projet blockchain, puisqu'il repose sur une autre utilisation des briques technologiques offertes par le Pair-à-Pair, ses interactions avec les projets blockchain s'annoncent si fructueuses que ne pas le citer ici serait une erreur. Il s'agit d'une des technologies aujourd'hui en développement les plus prometteuses en terme d'impact attendu, puisque l'objectif d'IPFS est de proposer une solution décentralisée pour remplacer HTTP.

L'HyperText Transfer Protocol est au cœur d'Internet dans son fonctionnement actuel ; lorsque l'on se rend sur un site web par exemple, c'est ce protocole qui est suivi pour aller chercher sur un serveur le contenu du site (le code, les images) et l'afficher. Ce protocole, qui s'est avéré crucial pour le développement d'Internet, présente toutefois des limites : en particulier, le fait de lier un site à un serveur unique implique que, si le serveur cesse de fonctionner, le lien est brisé[17].

IPFS propose de réinventer ce procédé en ne stockant plus le contenu hypermédia sur un serveur unique mais sur un réseau de serveurs décentralisés, qui fourniraient l'information demandée par une transmission P2P. De ce fait, il devient possible de construire des applications[18] décentralisées, c'est-à-dire un tout nouveau paradigme dans le fonctionnement des systèmes numériques que nous connaissons et utilisons tous les jours.

Dans cette optique, IPFS résonne absolument avec l'ambition de la blockchain (et notamment d'Ethereum) d'amener un nouvel internet enfin décentralisé. C'est pour cela que le projet Swarm développé sur Ethereum reprend les constatations faites sur HTTP pour construire une réponse distribuée semblable à celle d'IPFS, mais fonctionnant sur la blockchain d'Ethereum.

Si les deux équipes travaillent à des rapprochements, certains éléments différencient pour le moment les deux projets, notamment le fait qu'IPFS, dont le protocole de distribution est le plus avancé, ne possède pas encore les mécanismes d'incitation que peut posséder Swarm (celui-ci fonctionnant sur Ethereum, il a la possibilité de convaincre les utilisateurs de louer de l'espace disque contre des ethers). Mais ces débats sur la mise en place du protocole ne doivent pas cacher l'intérêt sans cesse croissant porté à ces initiatives dont l'ambition, à moyenne ou longue échéance, n'est rien de moins que de remplacer le protocole internet aujourd'hui dominant pour ouvrir l'ère des applications distribuées.

[17] C'est la fameuse « Erreur 404 – File not found ». Au-delà du simple vieillissement, ces serveurs en centralisant l'information sont non seulement vulnérables aux attaques classiques dites de « dénis de service» (attaques brutales par saturation du réseau), mais également soumis aux éventuels blocages par un gouvernement (pare-feu aux frontières, comme en Chine), ou tout simplement aux requêtes des agences gouvernementales du territoire sur lesquels ils se trouvent, à l'image de celles de la NSA pour les Etats-Unis. A ces problèmes s'ajoutent une vulnérabilité vis-à-vis du réseau physique lui-même, puisqu'un simple accident météorologique qui arrache un câble bien placé peu ralentir toute une partie du trafic des serveurs du secteur.

[18] C'est-à-dire des sites webs, mais de façon plus générale, tout ce qui fonctionne avec HTML, CSS, JavaScript…

3

PENSER LA BLOCKCHAIN : ENJEUX SOCIAUX, ETHIQUES, JURIDIQUES, POLITIQUES

La blockchain, une horizontalisation du monde

Par Gilles Babinet, multi-entrepreneur, Digital Champion de la France à la Commission Européenne :

Il est frappant de constater à quel point la blockchain passionne autant de monde. La question que l'on peut se poser est de savoir si cet intérêt est de nature économique, lié par exemple à une envie de créer des start-up blockchain pour faire fortune, ou d'une nature plus politique. La blockchain semble en effet avoir des implications nettement plus profondes que les autres technologies. J'ai même la tentation de comparer la blockchain à l'invention du protocole TCP/IP, à l'origine d'Internet.

L'invention d'Internet était déjà d'une ampleur comparable à l'invention de l'imprimerie par Gutenberg. L'arrivée du TCP/IP a ainsi écroulé le coût de l'information : en 1980 une adresse IP et l'ordinateur associé valaient 100.000 dollars ; 20 ans plus tard, 1500 dollars ; encore 10 ans plus tard, 300 dollars ; et aujourd'hui, 30 dollars. La nature même de l'information s'est également transformée, bouleversant considérablement l'organisation de nos sociétés. C'est pour cette raison que je parle souvent d'une révolution anthropologique au-delà de la seule révolution numérique.

Un problème se pose toutefois au moment d'évoquer cette révolution : l'ère de l'hyper-capitalisme. On le constate depuis la globalisation des marchés financiers. Contrairement à une idée commune, les marchés financiers globalisés ont commencé à apparaître en 1985 non pas, en premier lieu, parce que les gouvernements se sont entendus pour retirer les barrières douanières, mais bien avant tout parce que la technologie a permis cette apparition. Or depuis 1985 les revenus de la classe moyenne américaine ont justement fondu. 40 % de la richesse des Etats-Unis est aujourd'hui concentrée sur 70 personnes. Cette globalisation permise par le numérique porte un nom : les plates-formes, que l'on

voit aujourd'hui dans tous les domaines, bien au-delà de la capacité de levier sur les marchés financiers.

Une nouvelle ère commence cependant à émerger, dont les références pionnières s'appellent Wikipédia, l'open source, les fablabs. L'espoir qui prévaut derrière est que ce ne soient plus seulement les capitalistes, les concentrateurs de richesse, qui bénéficient de cette révolution digitale, mais bien tout un chacun, à commencer par les citoyens. La blockchain s'inscrit dans ce mouvement, en faisant à la transaction ce que le protocole TCP/IP a fait à l'information. La blockchain permet en effet de certifier du transfert d'informations - un processus qui nécessitait jusqu'ici de passer par l'intermédiaire de plateformes. Il s'agit d'un changement majeur puisque la capacité à certifier des transactions, jusqu'ici source de concentration de richesse, se déconcentre très fortement grâce à la blockchain.

Des services de toute nature, décentralisés, peuvent alors émerger. Les premiers exemples de projets sont nombreux : pensons ainsi à Arcade City, sorte d'Uber mettant en relation directement conducteurs et passagers, sans la plateforme centrale qui vient prélever une richesse ; à Synereo, un réseau social où les utilisateurs reprennent le contrôle sur leur identité et leurs données personnelles grâce à la blockchain ; à Moneytis, un Western Union décentralisé. Ce dernier exemple présente un potentiel considérable, car les flux des diasporas vers l'Afrique de l'Ouest représentent aujourd'hui plusieurs milliards d'euros par an, dont environ 10 % sont prélevés par Western Union. Si cet argent était directement envoyé aux familles, il serait sans doute employé plus justement plutôt qu'entre les mains d'acteurs qui concentrent les richesses. Les gouvernements sont également concernés : Factom construit ainsi un cadastre au Honduras et empiète de ce fait sur les plates-bandes des services publics, en apportant plus de sécurité et une meilleure certification.

A ce stade de la réflexion, la question à se poser est de savoir si nous ne sommes pas victimes de la courbe de la hype théorisée par Gartner : celle-ci stipule que les technologies connaissent, au cours de leur développement, une courbe d'ascension initiale très forte, puis une désillusion également marquée, avant de remonter plus lentement mais plus sûrement. Il est probable que nous soyons en quelque sorte victimes de cette courbe dans le cas de la blockchain. Celle-ci comprend en effet encore plusieurs limites : son nombre de transactions par seconde, encore très limité dans le cas du bitcoin ; sa consommation énergétique, très élevée, due au minage ; le délai d'exécution de ses transactions, encore loin d'être instantané, ce qui empêche pour le moment le développement de nombreux services. Pour toutes ces raisons, il est possible que la blockchain suive actuellement la courbe de la hype.

La comparaison avec le TCP/IP est là encore intéressante : au début des années 2000, suite à la promesse extraordinaire représentée par Internet, une bulle avait fini par se former, avec de très grandes attentes et des millions de dollars investis; en 2002, suite à l'explosion de la bulle, le discours ambiant était à l'extrême inverse, à savoir que tout ceci n'aurait finalement été qu'une illusion, et qu'il fallait arrêter de croire dans les start-up. On voit aujourd'hui, quatorze ans plus tard, ce

qu’il en a réellement été : plus personne ne remet en question l’importance du numérique. La blockchain pourrait donc suivre un chemin similaire.

Cela étant, même s’il existe peut-être actuellement une "hype" autour de la blockchain, son potentiel, lui, est bien réel. La blockchain, grâce à sa capacité d’horizontaliser le monde, est en effet de nature à renforcer la révolution anthropologique que nous vivons. Cette tendance se pressent depuis quelques temps déjà ; il est notamment de plus en plus question d’organisations agiles et de modèle holacratique, qui obligent les entreprises à devenir plus plates, poussées par la révolution digitale. Les conséquences de cette transformation sont majeures, notamment dans un pays comme la France qui reste fasciné par l’élitisme, la verticalité, et la vision d’un pouvoir quasi-thaumaturge, auquel nous sommes trop coutumiers.

La terre est plate : sa géographie n’a plus d’importance. Ce qui compte désormais est la capacité d’empowerment des communautés, qui nous oblige à repenser l’organisation des sociétés humaines. "Il n’y a rien de plus puissant qu’une idée dont l’heure est venue" affirmait Victor Hugo. Avec le TCP/IP et la blockchain, il existe maintenant des technologies capables de faire cette révolution anthropologique. A nous de faire en sorte que cet aplatissement du monde devienne réel.

Perspectives et enjeux des blockchains de demain

Par Primavera de Filippi, Chercheuse au Cersa (CNRS) et au Berkman Center for Internet & Society à l'université d'Harvard

Vers une intelligence collective humaine

Il existe dans la nature des exemples impressionnants de ce que l'on appelle l'intelligence collective. Les termites, par exemple, qui travaillent ensemble à l'établissement de leurs immenses monticules ; ou les oiseaux migrateurs, qui fonctionnent en parfaite coordination sur des distances phénoménales sans que nulle part un être ou un groupe d'individus n'émette d'ordre à ce sujet.

On sait aujourd'hui que cette coordination est produite indirectement, par le fonctionnement et la lecture notamment de traces, y compris hormonales. C'est donc la lecture *a posteriori* de ces traces laissées par les autres membres du groupe qui permet l'émergence de ce qu'on appelle "l'intelligence collective", sans que nulle part on ne puisse vraiment rencontrer cette intelligence elle-même. Les biologistes l'appellent la stigmergie. Elle est à la fois le fruit de la somme des intelligences individuelles du groupe, et plus que cela à la fois.

Cette idée d'agréger une multitude de petits travaux individuels pour réaliser quelque chose de supérieur à la somme des parties n'est certes pas nouvelle pour les humains, qui se sont très tôt constitués en organisations destinées à accomplir certains objectifs. Mais si on se penche sur les réalisations les plus imposantes et les plus immédiatement visibles, les Pyramides d'Egypte ou des domaines Aztèques, la Grande Muraille, le Colisée, et plus récemment nos gratte-ciels partout dans le monde, on constate qu'aucune n'est le fruit d'une intelligence collective humaine. Elles sont pratiquement toujours le fruit des ordres données par une ou plusieurs personnes, bien souvent complètement absente de la mise en œuvre technique.

Aujourd'hui le mode de décision prôné dans la majorité des discours est devenu celui du marché, du *Winner takes all*, réputé plus efficient qu'une prise de décision hiérarchique. Pourtant, la compétition (puisque c'est elle qui est au cœur de la logique de marché) n'est pas toujours le meilleur moyen d'allouer les ressources. On peut prendre comme exemple très simple la Recherche et Développement sur les sujets pharmaceutiques, aujourd'hui compartimentée en autant de silos qu'il existe de laboratoires, tous lancés dans une course dont les termes sont simples: le premier qui dépose le brevet gagne. Se demander si la mutualisation des ressources et des hommes sur ces sujets-là ne serait pas meilleure pour le bien public, c'est prendre conscience des limites de la gouvernance systématique par le marché.

La question qui se pose est donc de savoir s'il nous est possible, à nous humains, d'atteindre en partie cette forme d'intelligence collective déployée par d'autres espèces, et de l'appliquer à des buts plus ambitieux que la création d'une termitière. Ce ne serait pas la première fois que l'on imiterait la nature dans ce qu'elle sait le mieux faire. Elle nous a donné envie de voler ; pourrait-elle nous conduire vers des formes d'organisations plus horizontales et plus efficientes ?

A mon sens, la blockchain est un outil capable de nous amener vers cette intelligence collective.

Un outil particulier, au croisement de plusieurs mondes

Reste encore à préciser la nature de cet outil.

Ce qui paraît très clair lorsque l'on observe la blockchain, et notamment le projet d'ordinateur global d'Ethereum, c'est que la blockchain ne constitue pas simplement une "nouvelle technologie", c'est-à-dire en économie classique une simple transformation des facteurs de production et une hausse transversale de la productivité. Elle possède une capacité de transformation à même de proposer de nouvelles formes d'organisation et de gouvernance économique.

Prenons les marchés : ce sont des organisations décentralisées qui ont montré leur efficacité pour la gouvernance de systèmes qui reposeraient simplement sur des contrats ponctuels, c'est-à-dire pour une économie qui se concentrerait sur de simples échanges entre les entités qui la composent. Mais dès que l'activité économique a besoin de coordonner des investissements sur le temps long, met en contact régulièrement les mêmes acteurs, ou fait face à des éléments totalement imprévisibles qu'on ne peut pas traduire par des contrats, on s'aperçoit que le marché ne suffit pas, et on en revient à d'autres modes d'organisations, par exemple plus hiérarchiques.

Ainsi jusqu'à il y a peu, on considérait que la transaction "travail contre salaire" avait davantage vocation à exister au sein d'une entreprise que sur un marché, même si l'économie de plateforme est venue revisiter cet *a priori*. Demain, les caractéristiques des blockchains pourront leur permettre d'abriter à leur tour un certain nombre de transactions aujourd'hui réalisées dans les entreprises, sur les marchés ou ailleurs, voire permettre des transactions qui jusqu'ici n'existaient pas faute de structure appropriée.

Sous cet angle-là, les blockchains sont donc concurrentes des organisations. Pourtant il est difficile de les qualifier elles-mêmes "d'organisations" ; comme l'expliquent S. Davidson et J. Potts dans un récent travail[19], les blockchains sont davantage ce qu'on appelle des "organisations spontanées", avec des caractéristiques proches des marchés, mais sans l'être tout à fait puisqu'elles permettent et facilitent des transactions qui vont plus loin que le simple échange. Elles se rapprochent en fait de ce qu'Hayek décrivait dans les années 1960, sans connaître bien sûr la blockchain, comme une catallaxie, un ordre spontané particulier qui répond à une diversité de besoins individuels dans le respect notamment de la propriété et des contrats[20].

Pourtant, une fois encore, on ne peut pas réduire les blockchains à cette vision-là.

[19] Davidson, Sinclair and De Filippi, Primavera and Potts, Jason, *Economics of Blockchain* (2016).
[20] Hayek, F.A. The Constitution of Liberty (1960).

Si l'on se penche sur l'histoire des biens communs par exemple, on s'aperçoit que la blockchain fait tout-à-fait sens dans une telle grille de lecture. Historiquement[21], on peut dire que les Communs 1.0 se sont concentrés sur les ressources naturelles communes (forêts, systèmes d'irrigation…), tandis que les Communs 2.0 ont cherché à analyser les communs de l'information et du savoir (notamment dans les secteurs du numérique, comme les logiciels open-source ou le Pair-à-Pair). Les Communs 1.0 ont prouvé la possibilité d'une gouvernance efficace à petite échelle sur ces sujets, tandis que les Communs 2.0 ont démontré que les enjeux d'image et de réputation pouvaient permettre de dépasser les problèmes de "passagers clandestins" pour parvenir à une gestion durable des biens publics.

Dans cette perspective, la blockchain peut apparaître comme un Commun 3.0, en ce qu'elle propose une solution technique (le consensus cryptographique) à un problème simple : comment faire coopérer à large échelle un groupe dans l'optique d'une production concrète, tout en maintenant les bénéfices d'une gouvernance qui respecte les principes des communs ? La difficulté du passage à l'échelle de la gouvernance peut être résolue par la blockchain, qui constitue elle-même un commun de par son code open-source, et grâce à laquelle la gouvernance peut se fonder par le biais de "smart contracts" directement inscrits et sécurisés par la technologie - pour peu que ces règles inscrites dans la blockchain respectent les règles de la gouvernance des communs, comme par exemple les 8 principes définis par Elinor Ostrom[22].

La blockchain est donc bien plus qu'une simple nouvelle technologie dans une économie faite de marchés et d'organisations. Si on considère par exemple un complexe formé à la fois d'Ethereum, de Backfeed [un système de gouvernance décentralisée sur la blockchain] et d'une communauté, qu'est-ce que serait finalement la blockchain ? La réponse est du côté d'une organisation spontanée, qui s'auto-organise avec les propriétés de coordination d'un marché, les propriétés de gouvernance d'un commun, et une capacité de prise de décision semblable à celle d'un Etat.

Mais ce modèle théorique n'est pas encore en action, loin de là. Deux obstacles importants doivent d'abord être surmontés.

Les deux obstacles fondamentaux de la confiance et de la gouvernance

Le premier obstacle, que l'on perd trop rapidement de vue lorsque l'on traite de la blockchain, est le sujet de la confiance.

La blockchain élimine le besoin de confiance entre individus qui interagissent entre eux ; c'est de cette promesse dont parlait *The Economist* en titrant "Trust Machine" (la machine à créer de la confiance). Ce qui est désormais envisageable grâce à cette technologie, ce sont les échanges commerciaux entre des individus

[21] Cf E.Ostrom sur le sujet, notamment: Governing the Commons. The Evolution of Institutions for Collective Action (1990) et A Framework for Analysing the Knowledge Commons (2006).

[22] Elle identifie huit principes caractéristiques des communautés pérennes de gestion de ressources communes, parmi lesquelles la définition claire de l'objet de la communauté et de ses membres, la participation des utilisateurs à la modification des règles concernant la ressource commune, l'accès rapide à des instances locales de résolution de conflits, ou encore le fait que la communauté soit reconnue comme autonome sur ces sujets par les autorités extérieures.

ou organisations qui ne se connaissent pas et qui ne se font pas confiance en amont, sans nécessiter d'opérateur centralisé ou de tiers de confiance. Et cela va bien plus loin encore dans des domaines encore assez peu explorés mais qui seront fondamentaux demain, comme l'Internet des Objets et la communication entre humains et machines ou machines-machines.

Mais derrière cette promesse, il existe une réalité qu'on ne peut pas ignorer : malgré tout, dans le cadre des interactions humaines les individus ressentent tout de même souvent l'envie de savoir qu'ils peuvent faire confiance à autrui. Lorsque je loue un espace sur Airbnb, la transaction n'est pas purement comptable ou financière : elle touche à quelque chose de plus important, à savoir le besoin de placer une certaine confiance en la personne avec qui je vais contracter.

Ma conviction est donc la suivante : plus le curseur de la confiance sera déplacé sur la technologie, plus il sera nécessaire de développer des relations sociales et des organisations pour appuyer et certifier cette confiance. Dès que la technologie va nous amener vers des applications plus sociales, ou qui impliquent des relations humaines, il deviendra nécessaire de développer au-dessus de la blockchain une nouvelle couche, un nouveau protocole, qui permettra de gérer les relations humaines et de réintroduire cette confiance. Sans cette surcouche, la blockchain ne parviendra pas à prendre en charge avec succès toutes les applications qu'aujourd'hui on projette parfois un peu vite dans un avenir proche.

Il s'agit donc du premier obstacle. Le second est celui de la gouvernance.

Le bénéfice d'une technologie décentralisée ne peut être totalement exploité que si l'on arrive à déployer au-dessus une gouvernance décentralisée. La blockchain ne pourra pas concurrencer les marchés ou les organisations traditionnelles et ne sera pas non plus un commun ou un outil de gestion des communs sans modèle de gouvernance approprié.

Ce qu'il est nécessaire de construire, c'est donc une nouvelle couche de gouvernance au-dessus de la blockchain. Elle partira de l'idéologie de l'open source, mais devra nécessairement inclure un processus de récompense, pour inciter le plus grand nombre à rejoindre la blockchain et à la développer pour la rendre compétitive vis-à-vis des autres systèmes.

C'est tout le projet de Backfeed. Backfeed est un protocole en développement qui se fonde sur un système de réputation et de gouvernance décentralisée, pour obtenir à une autre échelle et sur un fonctionnement humain la coordination horizontale –la stigmergie- des différentes organisations présentes dans la nature. Concrètement, cette gouvernance est assortie d'un mécanisme de création et de redistribution de la valeur, qui dépend de la valeur effectivement apportée par des individus dans un projet ou une organisation : plus j'apporte relativement aux autres de valeur ajoutée au projet auquel je participe et qui utilise Backfeed, plus mon influence et mes gains tirés du projet seront importants.

L'objectif de Backfeed, c'est donc d'obtenir une couche d'interaction humain-humain au-dessus d'un protocole qui permet naturellement le dialogue des machines, et de transformer la blockchain, qui est - on l'a vu - une organisation

spontanée fonctionnant sur des principes de marché, en une organisation en propre, tournée vers des buts bien déterminés. Tant qu'une telle entreprise n'aura pas réussi, le potentiel de la blockchain ne pourra pas être totalement réalisé.

C'est pour cela que les DAO, les Organisations Autonomes Décentralisées, sont si importantes.

En permettant à des individus de se coordonner de façon décentralisée et de coopérer pour fournir un service dont ils vont bénéficier eux-mêmes, ces applications décentralisées collaboratives se développeront de façon plus autonome encore que ne le font les applications blockchain "classiques". En effet, outre la figure de l'intermédiaire, les DAO s'attaqueront à un autre tiers de confiance, à savoir les administrateurs.

Gérées par des logiciels, basés sur la blockchain, et indépendantes de toute intervention humaine, elles éviteront les principaux écueils des organisations verticales, tout en assurant leur autosuffisance et donc leur résilience. En effet, la grande force des DAO est leur capacité à aller récupérer les ressources nécessaires à leur propre survie – par exemple, pour payer elles-mêmes un loyer sur la blockchain. Cette force et cette résilience promettent donc une nouvelle étape dans la conception d'une organisation distribuée. Mais ce n'est pas leur seul avantage : elles permettent également de mettre en lumière les enjeux juridiques fondamentaux des technologies blockchain.

La régulation et la responsabilité en question

D'un point de vue juridique, en effet, les DAO soulèvent deux problématiques essentielles que sont les questions de responsabilité et de régulation. Davantage que des obstacles, ces problématiques recèlent plutôt une multitude de questions dont les réponses pourront s'avérer cruciales pour l'élaboration de nos sociétés à venir.

En ce qui concerne la responsabilité, plusieurs interrogations apparaissent d'emblée : comment gérer le cas où une DAO serait utilisée à des fins illicites ? Qui serait responsable pour les activités d'une organisation qui n'aurait pas d'administrateur ni d'opérateur ? Si intuitivement, on pourrait avancer que la responsabilité engagée est celle des créateurs du logiciel, le problème qui s'ensuit est double : d'une part, ces créateurs sont bien souvent anonymes ; d'autre part, à supposer que l'on parvienne à les identifier, comment ensuite bloquer les opérations d'une organisation qui agit de façon complètement autonome ?

En fait, les smart contracts risquent de nous obliger à une régulation typiquement *ex ante* (avant leur écriture) plutôt qu'*ex post* (*a posteriori*, avec par exemple l'intervention d'un juge en fonction des conséquences de l'écriture du smart contract). C'est un exercice complexe : tous ceux qui ont vu Minority Report comprennent les problèmes posés par une justice qui interviendrait avant l'acte[23]…

[23] Dans ce film, la police arrête les criminels avant qu'ils ne commettent le crime, en se fondant sur les dons de prescience de mutants.

S’agissant de régulation, la blockchain suscite des espoirs et des craintes car elle est vue comme une technologie capable d’échapper aux règles actuellement en vigueur et à la domination des Etats. Tout cela nous ramène en quelque sorte à la déclaration d’indépendance du cyber espace de John Perry Barlow, et à cette croyance d’un espace dans lequel les Etats n’auraient ni le droit ni la capacité d’imposer leur souveraineté. Or on voit à présent qu’Internet qui devait être un outil d’émancipation est aujourd’hui davantage un moyen de contrôle des internautes, par les gouvernements ou par les entreprises… En réalité on réitère les mêmes promesses. Les "cyberpunks", notamment Satoshi Nakamoto, ont souvent présenté Bitcoin comme une continuation des objectifs d’indépendance promus par le cyberespace.

Or davantage encore que sur Internet, le code fait désormais effet de loi ("code is law") : non seulement le code peut dicter l’architecture qui nous entoure, mais il peut désormais créer des relations contractuelles et de nouveaux cadres techno-juridiques indépendants du monde physique. Ce qui nous amène donc à un vieux débat : faut-il ou non un cadre juridique dédié à ce nouvel objet blockchain ? Vieux débat, parce qu’il est exactement le même que celui qui s’était posé à l’époque sur l’environnement légal du cyberespace ; est-ce qu’exiger un cadre juridique dédié n’est pas tomber dans un travers qui consisterait à proposer un cadre juridique pour chaque exception ?

A mon sens, il n’est ni possible ni souhaitable d’appliquer les règles du droit traditionnel à l’environnement numérique ; il est donc nécessaire d’établir un nouveau cadre juridique spécifique à cet environnement, et ce d’autant plus pour la blockchain, pour laquelle on ne sait pas encore où elle nous conduit, quels en sont les champs d’exploitation, et quels en sont les dangers. Chercher à réguler la blockchain avec des règles traditionnelles serait risqué car cela pourrait limiter voire éliminer son potentiel.

Au cœur des problèmes opérationnels de l’écosystème des start-up bitcoin, par exemple, se trouve le statut du bitcoin. Monnaie ? Actif ? Autre ? Le plus souvent, un peu des trois, et cela change d’un pays à l’autre. Difficile d’opérer quand on est au croisement de multiples réglementations. Or la raison pour laquelle la blockchain a besoin d’un cadre juridique propre est justement parce qu’elle se trouve à la croisée de multiples champs aujourd’hui distincts. Ce qu’il faudrait écrire, ce n’est donc pas une déclaration d’indépendance, mais bien une déclaration d’interdépendance de la technologie blockchain...

La seule façon de comprendre comment avancer sur un sujet qui est si intrinsèquement imbriqué avec une multitude d’autres est de mieux étudier l’écosystème et de collaborer avec tous les acteurs qui travaillent autour de cette technologie. Il faut casser le cercle vicieux que l’on ne cesse d’observer avec les nouvelles technologies, où des outils de libération, ou disruptifs, cherchent à échapper à la régulation, ce qui conduit le droit à devenir de plus en plus strict pour tenter de s’en emparer, ce qui pousse à son tour la technologie à devenir encore plus décentralisée et disruptive pour lui échapper à nouveau. Il faut inventer un nouveau mode de dialogue entre juristes et développeurs, et inclure toute la société dans ce dialogue.

Plaidoyer pour une éthique des protocoles

La blockchain est un outil puissant, à même de soutenir ou accompagner le droit, en permettant par exemple une plus grande transparence pour les gouvernements, une optimisation du fonctionnement des entreprises ou de l'administration publique, et le développement d'une société bien plus collaborative que compétitive.

Internet, ce formidable outil d'autonomisation des personnes, est aujourd'hui le sujet d'une surveillance qui par certains aspects pourrait rappeler 1984 de Georges Orwell, à ceci près que dans 1984, les outils de surveillance et d'influence étaient visibles et connus. La situation dans laquelle nous nous trouvons tous, celle de fournir gratuitement des données à quelques entreprises qui n'hésiteront pas à les transmettre aux autorités à leur demande, contraste terriblement avec les promesses d'internet des années 1990.

Il faut donc se poser la question : que se passera-t-il si demain les communications que nous avons avec nos machines, avec les multiples capteurs qui peupleront notre environnement, passent toutes par une ou deux entreprises tierces ? Aujourd'hui il reste possible de limiter les données que l'on donne sur internet à ces géants bien connus. Que se passera-t-il si demain ils viennent les prélever directement sur les capteurs, à la source ?

Si les communications entre machines, ou humain-machines passent par des protocoles au code clair, et sans intermédiaire pour piller les données, nous aurons peut-être participé à la préservation des droits de chacun et notamment des libertés individuelles. La relation entre humain et machine dépendra tout simplement de la façon dont sont élaborés les codes qui régissent leurs interactions[24]. C'est, plus immédiatement, dans ce sens d'un cyberespace aux libertés retrouvées que vont des projets simples comme NameCoin, qui visent à remplacer l'ICANN dans son rôle de gestion des noms de domaines (l'ICANN est une ONG américaine).

Les décisions techniques prises aujourd'hui auront donc un impact sur nos sociétés demain. Il n'y a pas de technologie neutre. La blockchain est un outil qui peut être employé pour le meilleur comme pour le pire. Il faut donc comprendre que faire du code revient à faire de la politique : la blockchain peut tout aussi bien être une technologie de libération et d'émancipation qu'être reprise par les pouvoirs en place pour renforcer le cadre actuel. En conséquence, il est essentiel de commencer à réfléchir aux implications éthiques de la blockchain, aujourd'hui trop souvent oubliées : qui va bénéficier de cette technologie ? Qui y aura accès? Qui pourra la contrôler ? Quels seront les rapports de force qui se développeront? Quels acteurs se renforceront et s'affaibliront ? La blockchain favorisera-t-elle l'émergence d'une société plus juste, ou renforcera-t-elle les écarts entre ceux qui ont le pouvoir et ceux qui ne l'ont pas ? Les décisions prises aujourd'hui définiront le futur de la blockchain, et ce futur déterminera une partie importante de l'avenir de notre société.

[24] Sur ces sujets, on retrouve finalement avec une étonnante acuité les projections d'Asimov et les trois lois de la robotique exposées dès 1942.

Les deux visages de la blockchain

Par Michel Bauwens, Théoricien du pair-à-pair, Fondateur de la Peer-to-peer Foundation

Tout d'abord, une petite mise en contexte.

Mon approche, c'est le rejet de ce qu'on peut appeler le déterminisme technologique. Ce déterminisme, que l'on appelle aussi les approches technocratiques, c'est une croyance selon laquelle la technologie est univoque. Ce discours consiste à dire : parce que demain nous pourrons techniquement faire ceci ou cela, alors nécessairement notre société sera comme ceci ou comme cela. C'est le genre de discours par exemple que peut tenir Jeremy Rifkin dans son livre *The Zero Marginal Cost Society*, où il associe la montée en puissance de l'Internet des Objets et des économies collaboratives avec un déclin du capitalisme. Or à mon sens la technologie ne peut pas être univoque ; il est extrêmement important de la problématiser.
Je vais donc essayer de problématiser la blockchain dans cette optique. Il me semble que l'on peut en dire à la fois du bien, et du mal. Je vais commencer par la critique, avant de développer ce qui me plait dans cette innovation.
J'avais donné en 2014 pour Ouishare une keynote dans laquelle je proposais une analyse politique de la technologie. Pour qualifier les technologies Pair à Pair (P2P), j'avais réalisé une simple grille à double entrée. Première entrée du tableau: une technologie peut soit être sous contrôle central et globale, soit décentralisée et donc locale. Deuxième entrée, elle peut avoir soit un but de profit, soit un but social. J'avais mis dans ce tableau un certain nombre de technologies P2P.

Une technologie à la fois P2P, sous contrôle centralisé, et avec un but de profit peut bien sûr paraître contre-intuitive, mais Facebook en est un bon exemple. Avec Facebook, plus de 2 milliards de personnes peuvent se connecter en P2P, ce qui crée de formidables capacités d'auto-organisation ; pourtant, les utilisateurs ne contrôlent ni le design, ni les données, et l'entreprise en capte tout le profit monétaire.

La blockchain, elle, à cause de son association avec Bitcoin, se place dans un autre croisement. A mon sens, elle est pour l'instant une technologie P2P dédiée au profit et avec un contrôle décentralisé : c'est ce que j'appelle le capitalisme distribué.

Ce n'est pas un secret : Bitcoin est très influencé par la théorie politique qu'on appelle anarcho-capitaliste (qui est aussi un anarcho-totalitarisme, puisque ce mouvement prône le marché total, et par une théorie économique qui est l'école de Vienne, celle de Friedrich Hayek). Tout le design du Bitcoin, on le voit, est tourné vers l'intérêt personnel : j'investis dans le bitcoin car je pense que sa valeur va augmenter. Cette vision, ce rêve politique tourné vers soi, rejaillit de la genèse du Bitcoin sur chaque Blockchain qui le suit ; nombre de gens s'approchent du Bitcoin et de ses dérivés précisément à cause de ce rêve politique là.

C’est dans ce rêve même que se tient ma critique de la blockchain, car ce rêve politique est une vision hyper-individualiste. Ce qu’il figure, ce sont ces individus atomisés, séparés absolument, qui créent des contrats entre eux, en fonction de leurs volontés individuelles. A première vue, rien de problématique là-dedans puisque c’est ce qu’est Bitcoin par essence.

Mais la réalité, c’est que la société ne marche absolument pas comme cela. Aucune société ne le fait. On naît toujours quelque part, dans un contexte, dans un ensemble, avec des parents. Il y a toujours du collectif ; ce collectif présent dans les faits, il disparaît dans cette idéologie Bitcoin, dans ce rêve politique et dans ses développements technologiques.

Sans argent, dans le Bitcoin, on ne joue pas. Un paysan de l’Utthar Pradesh [Etat indien] n’a pas 450 dollars pour s’acheter un Bitcoin, ni même une fraction de Bitcoin. Il y a dans l’idée de Bitcoin une certaine démocratisation de la rente, par le biais de la spéculation. Le rêve n’est pas d’abolir les revenus spéculatifs et le pouvoir de bénéficier d’une rente divorce de la spéculation, mais d’ouvrir l’accès à ce jeu-là. C’est le rêve de Thatcher et de Reagan qui ont voulu la propriété immobilière et la participation de tous comme actionnaires.

La blockchain dans ce contexte bien spécifique a donc un message simple à faire passer : nous en avons fini avec l’Etat et nos autres organisations, et nous pouvons désormais créer de la confiance sans passer par des systèmes démocratiques et sans avoir confiance en personne ; la confiance est placée dans la cryptographie, dans l’algorithme, dans la technologie.

En ce sens, je trouve la blockchain dangereuse. Parce que ce qu’elle nous annonce, c’est un totalitarisme libertaire, effrayant, terrible. Cette politique "cachée" qui se tient derrière le Bitcoin, c’est elle que je critique. Si la question est celle de la confiance, alors il existe d’autres philosophies que l’on peut opposer à la *Trustlessness*, en particulier celle de la *Trustfullness* : c.a.d. j’ai confiance en toi, tu as confiance en un tiers, et donc j’ai confiance en ce tiers. C’est par exemple du système *Couchsurfing*, c’est la ‘mise en échelle’ de la confiance (*scaling trust),* aussi appeler le *web of trust*, l’internet de la confiance. Voilà à mon avis une philosophie préférable à celle de la Blockchain. Attention, je ne veux pas dire que ces solutions ne sont pas appropriées dans certains contextes, ce que je vise c’est plutôt la vision sociétale qui se cache derrière, qui veut rendre absolu cette individualisation complète.

Mais on l’a dit : une technologie n’est jamais univoque. Et tout n’est pas mauvais dans Blockchain.

A nouveau, il est nécessaire mettre les choses dans le contexte. On peut considérer qu’il y a toujours au moins trois couches dans l’élaboration d’une technologie. Il y a d’abord celle des financeurs de projets, qui ont une influence déterminante sur le design, puisque ce sont eux qui vont donner les ordres à ceux qui travaillent. Ensuite, il y a ceux qui développent la technologie ; ceux-ci ne sont pas des exécutants passifs, des esclaves, mais sont des créatifs, à l’image de la communauté des développeurs blockchain, et vont donc influencer fortement sur le design de la technologie. Il s’agit d’un groupe social fortement influencé par

l'éthique 'hacker'. Enfin, il y a les utilisateurs qui ont en tout temps 'subverti' les technologies pour les adapter à leur besoin. La technologie est donc bien un terrain de lutte, ou des influences variées essayent d'adapter les fonctionnalités à leurs propres besoins.

Prenons l'exemple d'Internet. A l'origine, Internet est né de l'idée de militaires qui cherchaient des moyens de communications pouvant survivre à une destruction nucléaire. Puis ce sont les scientifiques qui ont repris l'idée pour en faire un réseau de partage des connaissances. Tim Berners-Lee, en inventant le World Wide Web, a ensuite crée une couche civique, qui a démocratisé l'Internet. Enfin est arrivé le commerce, qui est venu se greffer dessus et a fait tout pour qu'il y ait des contrôles, de la surveillance sur les accès utilisateurs, etc.

Internet n'est donc pas quelque chose de simple ; il y a des aspects P2P, des aspects décentralisés, des aspects centralisés, et ce sont ces couches successives qui ont fait que l'on a aujourd'hui un système finalement assez contradictoire dans son idée sous-jacente. La blockchain suit le même chemin des différentes couches de développement et de leurs motivations contraires.

Dans la blockchain, une chose m'intéresse en particulier : la promesse d'une nouvelle organisation. Il faut bien comprendre qu'Internet a pourtant déjà fait baisser considérablement les coûts de l'auto-organisation humaine, et que les individus n'ont pas attendu la blockchain pour commencer à s'organiser ; certaines études témoignent d'une croissance exponentielle des organisations citoyennes depuis une dizaine d'années. Cela étant, si nous n'avons pas besoin de la blockchain pour nous auto-organiser, celle-ci peut renforcer ce mouvement.

A mon sens, la blockchain peut représenter une deuxième couche, une seconde baisse des coûts de publication, de communication, de transaction. En créant une banque de données universelle, en créant une sécurité universelle, la technologie a le potentiel de faciliter encore davantage l'auto-organisation humaine. C'est une seconde vague d'accélération qui pourrait se dessiner, et en ce sens, il serait intéressant que des forces disons progressistes, ou émancipatrices, qui sont concernées par des valeurs comme la durabilité de la planète et une équité dans la distribution de la richesse, apprivoisent et s'approprient à leur tour le potentiel de la blockchain.

Mais dans ce cas la blockchain revêt une coloration différente. On quitte en effet le technocratique et l'individu, pour entrer dans le domaine des coopératives, des communautés productives pour soutenir des domaines comme la pêche ou l'agriculture éthiques. Dans cette approche, on réinvestit le collectif et il y a une forme de gouvernance démocratique. La blockchain pourrait être utilisée pour automatiser les accords de ces organisations-là.

On peut également trouver à la blockchain un potentiel intéressant autour de la transparence. Aujourd'hui, il existe deux principales façons dans nos sociétés d'allouer les ressources : en faisant choisir l'Etat, c'est-à-dire hiérarchiquement, ou en faisant choisir le marché, c'est-à-dire compétitivement. Mais lorsque l'on atteint un système véritablement transparent, une troisième option émerge de façon très forte : la coordination mutuelle libre.

Cette coordination mutuelle libre est déjà en action sur Wikipédia et pour Linux. L'économie de l'immatériel connait donc déjà ce qu'on appelle la stigmergie, cette possibilité pour chacun de gérer son propre effort et donc de collaborer, et ce parce que tous les signaux sont lisibles. En appliquant la transparence à la comptabilité ou à la logistique, et c'était la proposition du Livre Blanc de Provenance par exemple, il devient théoriquement possible grâce à la blockchain de passer à une économie matérielle qui fonctionne elle aussi selon le principe de la coordination mutuelle libre.

C'est une vision à mon sens très émancipatrice, puisqu'elle permet l'émergence d'un système où chaque individu peut librement allouer son temps et son énergie, et la création du même coup des ressources partageables.

Ce qui m'intéresse dans la blockchain, c'est donc son potentiel d'encapacitation ("*empowerement*") de l'organisation collective de l'humanité.

Des projets comme ArcadeCity, ou Backfeed, sont des projets qui peuvent être interprétés sous cet angle-là. Pour qu'ils se multiplient, il est important d'aller éduquer les forces égalitaires au potentiel de la blockchain. Car dans la blockchain comme ailleurs le constat est le même : aussi bien les investisseurs à risques que les défenseurs de l'idéal propriétaire et libertarien se montrent toujours plus rapides dans l'adoption de la technologie que d'autres parties de la société. L'enjeu de la blockchain est de s'assurer qu'elle ne s'engage pas dans une voie unique, celle de l'individu atomique et égocentré, mais qu'elle investisse bien, aussi, des valeurs qui sont celles de liberté, d'égalité de fraternité.

Prenons deux exemples pour montrer à quel point les choix de développement sont révélateurs d'un choix de société.

Prenons par exemple les inégalités sur Bitcoin. Le coefficient de Gini, qui est un instrument utilisé par tous les pays pour mesurer l'écart de richesse au sein de leur population, est infiniment plus élevé dans Bitcoin que dans nos sociétés modernes, pourtant passablement inégalitaires ; plus révélateur encore, il continue de croître avec la montée en puissance du réseau. En réalité, nous assistons à un jeu de Monopoly : au départ, nous étions tous égaux devant Bitcoin, mais ceux qui ont pris de l'avance en début de jeu gagnent à la fin. "Plus tu gagnes, plus tu gagnes" : il n'existe dans Bitcoin aucun mécanisme redistributeur qui permet de protéger des distributions de valeur plus équilibrées.

Or ce choix-là n'est pas une nécessité. On peut faire appel à d'autres systèmes, comme ceux décrits par Christopher Boehm (*Hierarchy in the Forest*) ou Pierre Clastres (*la Société contre l'Etat*), pour comprendre l'importance des systèmes de contre-hiérarchie. Ainsi dans ces sociétés de chasseurs-cueilleurs les femelles et les mâles bêta prennent le pouvoir contre les mâles alpha et mettent en place des mesures pour limiter leur domination. Ce sont des exemples connus mais qui illustrent un fait : un système qui n'a pas de contre-pouvoir va nécessairement virer au monopole. Il s'agit d'un choix à faire au moment d'en fixer les règles.

Un second exemple pourrait être la fameuse "longue traîne" décrite par Chris Anderson. Il s'agit de cette idée de dissocier d'une part les "gros succès", qui

attirent individuellement l'attention, et la multitude de petits succès qui viennent ensuite, mais dont la somme peut être collectivement supérieure à celle des " hits" en terme d'impact. Cette économie secondaire, alternative, crée à son échelle un système fondé sur des micro-choix.

Or cette longue traîne n'est pas permise par Amazon, ni Google et consorts parce qu'en leur cœur réside un algorithme qui crée de la concentration. A l'inverse, Jamendo avait mis en place des contre-mesures qui la protégeait. Là encore, la technologie est affaire de choix, et ce choix n'est pas univoque.

Il est urgent pour nous tous de réapprendre cette vérité, puisqu'il me semble que nous l'avons oubliée. Dans les milieux technologiques, les développeurs, les hackeurs, ne la connaissent pas assez. Et une fois cette prise de conscience faite, viendra l'heure des choix : c'est ce qu'on appelle *value sensitive design*, c'est-à-dire prendre conscience lors de la création que celle-ci prend place dans un système de valeur, et effectuer ses choix en conscience.

Il est urgent de commencer à développer des financements de projets plus égalitaires - par exemple *via* les coopératives -, des algorithmes plus égalitaires, des gouvernances de plateforme - par exemple par les utilisateurs - plus égalitaires. Des exemples comme ceux du collectif Inspire en Nouvelle-Zélande sont à suivre.

On constate aujourd'hui une sorte d'automatisme, de passage apparemment obligé pour les créateurs : des jeunes, qui veulent créer une technologie, sont très vite poussés par une certaine valorisation sociale dans la culture extractive. Cette culture extractive, c'est celle des start-up, avec la volonté unique de réussir une *Licorne (Nb : start-up dont la valorisation boursière dépasse 1 milliard de dollars)* ou un *Exit (Nb : sortie du capital rapidement après lancement et avec forte plus-value)*. Or une autre voie existe, même si elle n'est pas très visible. Il y a tout un travail à faire aujourd'hui envers les développeurs pour leur montrer cette autre voie.

Il faut dénaturaliser l'idée du développement de la technologie, l'idée que ce développement est naturel, que le capitalisme est naturel … Il faut se rendre conscient qu'il s'agit de choix humains.

Or la blockchain arrive vite. Une sorte de consensus informel prédisait les prototypages en 2016, et les premiers systèmes utilisables en 2017. Sans se placer dans ce débat, je crois important de rappeler que l'on a toujours tendance à exagérer l'importance des technologies quant au potentiel de développement sur le court terme, et à les sous-estimer sur le long terme.

Souvenons-nous de la hype autour de l'intelligence artificielle, comme de celle autour de la réalité augmentée. Si cela n'a pas pris sur le moment 20, 25 ans après, nous y sommes. Il est tout à fait possible que la blockchain soit l'éléphant qui accouche d'une souris. Mais ce ne sera pas grave, et ce n'est pas pour cela que la blockchain n'aura pas d'importance ensuite, le temps qu'elle se déploie réellement. Cela peut arriver vite: on a vu avec le moteur de recherche par exemple *(Nb: inventé au début des années 1990, il décolle véritablement au début*

des années 2000) que ce délai de montée en puissance se réduit constamment avec l'accélération technologique. Il faut s'attendre à ce que la blockchain compte vraiment dans moins d'une dizaine d'années.

Les grandes entreprises et les défenseurs du capitalisme seront les premiers à s'en saisir mais je ne pense pas que cela soit un mal. Quand on regarde l'histoire des grandes évolutions sociales, comme la grande révolution féodale du X^{e} siècle ou la grande révolution capitaliste du XV^{e} siècle, le scénario est un peu le même : on est face à un système épuisé qui ne marche plus, et où tout le monde va chercher des alternatives, aussi bien les gens qui ont les moyens que les gens qui sont au bas de l'échelle.

C'est justement parce que les éléments ultra-capitalistes investissent dans ce changement qu'il pourra avoir lieu. C'est à l'intérieur des structures romaines en déclin que se sont formées les graines du changement qui allaient former la féodalité, et c'est à l'intérieur des grains du système féodal que les grains qui allaient devenir le capitalisme se sont développés. Il est naturel de penser que c'est à l'intérieur du système capitaliste en déclin que les graines des communs vont se développer.

Ce qui peut d'ailleurs amener des paradoxes, comme Facebook, parfait produit du capitalisme d'extraction et en même temps puissant encapaciteur d'auto-organisation en P2P. Le changement n'est peut-être pas encore totalement là où on voudrait qu'il aille, mais il va dans la bonne direction, et il faut s'en saisir. Ne refusons pas un outil sous le prétexte qu'il a été développé pour les mauvais motifs ; il faut garder en tête Luther au XV^{e} siècle lorsqu'il voit à sa juste valeur le potentiel de l'imprimerie pour la diffusion de ses idées. Il faut se saisir et s'approprier les potentiels des technologies, même si elles sont en partie dominées par des forces qui ne sont pas nécessairement émancipatrices.

La blockchain, catalyseur de décentralisation des organisations

Par Philippe Honigman, Entrepreneur, Fondateur de ftopia

Il est toujours surprenant de se souvenir que l'entreprise telle que nous la connaissons n'a pris son essor qu'il y a deux cents ans. La prédominance de cette forme sociale est telle aujourd'hui qu'il est difficile de penser la production économique en dehors de son cadre. En 1980, la part de l'emploi salarié a atteint 90 %[25] aux Etats-Unis !

Les économistes se sont préoccupés des raisons de ce succès fulgurant. Les travaux nobélisés de Ronald Coase, en particulier, ont montré que la firme disposait de l'avantage de coûts de transaction moins élevés que le marché libre, lorsqu'il est nécessaire de faire travailler ensemble de nombreuses personnes de façon prolongée. La recherche de ressources qualifiées et la négociation de conditions satisfaisantes pour les parties entraînent des coûts élevés. Embaucher et débaucher des travailleurs en fonction de la demande devient une stratégie plus coûteuse que leur intégration à long terme sous la forme d'un contrat de travail.

On peut du coup se poser la question de la limite à la croissance de la firme. Si ce modèle d'organisation sociale de la production est plus efficace que le marché libre, comment se fait-il que nous constations des limites à la croissance des entreprises ?

Une réponse tient aux limitations humaines en matière de planification et de coordination. Nos ressources cognitives ne nous permettent de travailler étroitement qu'avec un petit nombre d'individus. Une autre limite bien connue, celle du nombre de Dunbar, rappelle que nous ne pouvons entretenir de relations directes qu'avec environ 150 personnes, au maximum.

Face à ces limitations, nous avons inventé la hiérarchie de commandement et de contrôle, s'appuyant sur des procédures opératoires standardisées, associées à des fiches de postes elles-mêmes insérées dans un organigramme structurant l'ensemble de l'entreprise.
L'efficacité de ce dispositif a largement fait ses preuves. Cependant, l'accroissement de la taille d'organisations hiérarchiques va de pair avec une complexification des systèmes de décisions, des coûts de coordination interne élevés, et un manque d'agilité, en particulier dans des environnements marqués par des changements rapides.

A partir d'une certaine taille, tout se passe comme si l'organisation est peu à peu paralysée par son propre poids, et devient incapable d'identifier les opportunités nouvelles dont des structures plus lestes savent se saisir.

Chefs d'entreprise et théoriciens ont tenté d'adresser cette limite de multiples manières : formes plus sophistiquées d'organisations comme le management

[25] "Cloudworker Economics", Venkatesh Rao
http://www.ribbonfarm.com/2008/10/29/cloudworker-economics

matriciel, tentatives d'aplatir la structure hiérarchique en la réduisant à 3 ou 4 niveaux, dispositifs d'innovation ouverte rassemblant des équipes hybrides au sein de réseaux non hiérarchiques.

On a vu encore émerger des formes nouvelles de coordination, plus coopératives et plus fluides, telles que l'holacratie ou la sociocratie, ainsi que des organisations ouvertes comme Linux ou Wikipedia.

La nouvelle donne : les plates-formes

Au cœur de la révolution numérique : les plates-formes, et leur capacité à extraire une valeur économique de la coordination de millions d'individus et d'entreprises.

La plate-forme présente un caractère hybride. D'un côté, une firme traditionnelle, souvent sur-capitalisée afin de lui permettre de passer à ses clients les économies d'échelle encore virtuelles lors du déploiement de son modèle. De l'autre, un réseau ouvert associant les usagers, dont les actions sont coordonnées par du logiciel, plutôt que par des équipes opérationnelles.

Dans le monde des plates-formes telles qu'Uber, Facebook, Youtube ou eBay, chacun est encouragé à participer au réseau, en tant que contributeur, évaluateur, producteur. Plus le réseau s'étend, plus sa valeur d'usage s'accroît. Puisque les actions de millions d'agents peuvent être automatiquement coordonnées, le coût de changement d'échelle est négligeable.

Mais si les plates-formes s'appuient sur des réseaux gigantesques, les firmes qui les contrôlent sont de taille modeste, comparées aux entreprises dominantes de l'ère pré-digitale. La valorisation boursière d'Amazon dépasse celle de Walmart, avec des effectifs 10 fois inférieurs – 155.000 employés contre 2,2 millions. Airbnb, avec 1400 collaborateurs, dispose de plus d'un million de chambres aujourd'hui, plus que certaines chaînes d'hôtels internationales comme le groupe Hilton group, qui compte… 110 fois plus d'employés !

Dans le modèle de la plateforme, la firme organise le réseau de façon à en extraire une valeur économique optimale, conformément au mandat que lui assignent ses actionnaires. La valeur est largement coproduite par les agents du réseau - que serait Facebook sans les contributions de ses utilisateurs, ou Airbnb sans les appartements de ses hôtes - mais ceux-ci ne sont jamais en capacité de peser sur les mécanismes de gouvernance et de distribution de la valeur d'échange.

Parachevant une évolution qui s'est appuyée sur le logiciel pour mobiliser une multitude[26] active et génératrice de valeur, nous pouvons envisager l'émergence d'organisations dont la gouvernance serait **interne** au réseau, et où la distribution de la valeur d'échange se ferait **au profit des contributeurs**.

[26] "L'Age de la Multitude", N. Colin et H. Verdier, Ed. Armand Colin

Ces organisations existent, au moins à l'état de projet ou d'expérimentation. Elles ont toutes en commun le fait de s'appuyer sur la blockchain pour atteindre leur objectif de gouvernance décentralisée.

La blockchain, technologie émancipatrice ?

L'internet et la capacité à publier des pages Web dynamiques - ou Web 2.0, évolution du Web vers des usages sociaux construits à partir du contenu généré par l'utilisateur - ont rendu possible l'apparition des plateformes.

Aujourd'hui, de nouveau, une technologie est perçue comme "disruptive", c'est-à-dire susceptible de transformer en profondeur les systèmes d'organisation sociale, notamment en matière de production économique : la blockchain. Sa caractéristique principale réside dans sa faculté à établir un consensus entre des acteurs n'ayant *a priori* pas de raison de se faire confiance, ni mis dans l'obligation d'agir de concert par la force d'une autorité surplombante.

En tant que "machine à fabriquer du consensus", la blockchain semble autoriser la constitution de systèmes d'information décentralisés et transparents, à l'opposé de l'asymétrie des plates-formes où le pouvoir et l'information sont concentrés du côté de la firme.

L'utilisation de la blockchain pourrait ainsi favoriser une émancipation de l'individu dans son activité contributive auprès d'organisations diverses, dans la mesure où la valorisation de ses contributions (en termes monétaires ou non monétaires) donnerait lieu à une trace incontestable, incorruptible et surtout échangeable dans d'autres réseaux, *via* l'interopérabilité de tokens émis sur la blockchain.

On peut ainsi envisager de s'appuyer sur cette technologie pour outiller de nouvelles formes collectives de production de valeur sociale et économique. En garantissant la transparence et en renforçant la résilience des mécanismes de distribution de valeur et de gouvernance, la blockchain pourrait fournir la solution au problème d'auto-organisation des réseaux, et inaugurer l'ère des organisations collaboratives décentralisées (DCO), successeurs des plateformes.
Ainsi, le projet **Reposium**[27] vise à auto-organiser des collectifs producteurs de connaissance, en combinant des mécanismes d'incitations économiques et d'établissement de la réputation des contributeurs. Le modèle décrit par son créateur, Dominik Schiener, pourrait s'appliquer à de nombreuses communautés ouvertes, réunies autour du contenu généré par les participants, telles que Wikipedia ou Reddit. En ligne de mire, un fonctionnement économique équilibré et autonome, alternatif aux options actuelles du financement par le don ou par la publicité.

Le projet **Backfeed** a pour objectif de généraliser cette approche, en fournissant des outils d'établissement du consensus au sein de tous types d'organisations décentralisées. En l'absence de hiérarchie pour allouer les tâches, évaluer les

[27]"Reposium: The future of Wikipedia as a DCO", Dominik Schiener
https://medium.com/college-cryptocurrency-network/reposium-dco-the-future-of-wikipedia4be080cfa027#.sx16rtb3u

contributions et décider du mode de répartition de la valeur, il est critique de disposer d'un mécanisme d'alignement favorisant la cohérence dans l'action, quelle que soit la taille d'un réseau ouvert par nature à toute contribution de valeur.

Backfeed élabore son protocole dans ce dessein, en s'efforçant de coupler réputation et rétribution monétaire. Le mécanisme de *proof-of-value* consiste à définir les conditions de validation collective de la valeur des contributions, sous la forme de tokens propres à l'organisation et enregistrés sur la blockchain. Dans les premiers temps d'un projet décentralisé, ces tokens peuvent être vus comme une forme de parts sociales, promesse de valeur future. Lorsque l'organisation mature et qu'elle offre ses services sur un marché, les tokens deviennent liquides et acquièrent une valeur d'échange.

De façon plus générale, et en l'absence à ce jour de modèles éprouvés, l'intérêt de la blockchain pour les organisations décentralisées nous semble justifié par trois considérations :

a. Des modes de **gouvernance** implémentés sous la forme de DAO et de smart contracts moins susceptibles de détournement au profit d'un petit nombre disposant des avantages que confère l'information asymétrique. Les conditions d'une rétribution plus juste de tous les contributeurs de valeur deviennent plus sûres et plus transparentes ;

b. La sanction de la **contribution** sous la forme de tokens (monétaires ou non) enregistrés sur la blockchain renforce l'autonomie de l'individu, qui dispose ainsi d'une trace intangible de son activité ; dans un monde où le salariat décline et où nous sommes amenés à multiplier les participations à des projets hétérogènes, la capacité à valoriser et établir vis-à-vis de tiers l'historique de nos contributions devient constitutive de notre identité ;

c. Une capacité intrinsèque à porter l'interopérabilité entre organisations distinctes, et *in fine* à estomper les frontières artificielles entre organisations; la blockchain est un système d'information universel, qui a vocation à servir de lingua franca.

La nouvelle frontière organisationnelle

Rêvons un peu. Imaginons que demain, le lien de subordination constitutif du salariat soit brisé, non au profit d'une régression vers le travail à la tâche, mais au bénéfice du libre choix de participer à des projets satisfaisant aux objectifs de chacun.

En tant qu'initiateur d'un projet, je souhaite réunir les collaborateurs qui partagent mes valeurs et dont les compétences complètent les miennes. En tant que participant, je cherche à combiner en diverses mesures la nécessité de subvenir à mes besoins matériels, l'aspiration à servir une cause désirable, le besoin de développer du lien social et l'envie d'utiliser et d'accroître mes compétences. Ce faisceau de motivations peut me conduire à me concentrer sur un seul projet, ou bien à participer à plusieurs. Dans le cadre d'un même projet, je peux être aussi invité à endosser de multiples rôles.

Nous voyons se constituer aujourd'hui de nouveaux réseaux sociaux tels que Colony ou Part-up[28] dont le but est précisément d'offrir l'accès à ce nouveau Web collaboratif, cet univers fluide où nos aspirations et nos compétences trouvent à s'ancrer dans des projets, aussi simplement que nous hélons virtuellement un chauffeur Uber depuis notre mobile.

Au bout du compte, comment caractériser ces nouveaux modes d'organisation que la blockchain pourrait outiller ? Ils devraient tout d'abord être **ouverts**. Les firmes actuelles sont dotées de dispositifs de protection renforcée vis-à-vis de l'extérieur. Une organisation décentralisée se doit d'être poreuse, afin de laisser son réseau atteindre naturellement et rapidement son optimum. Cette porosité n'est pas un simple état passif, mais une capacité dynamique à inviter chaque acteur à exprimer son potentiel[29].

La résilience de l'organisation n'est pas affectée par son ouverture, car elle ne dépend pas d'une sélection initiale, incertaine et coûteuse ; l'accès à une position d'influence au sein de l'organisation dépend de la validation consensuelle de contributions effectives. L'influence reconnue au participant se doit d'être proportionnelle à l'engagement effectif, ainsi qu'à l'alignement vis-à-vis des valeurs du groupe. La forme naturelle de la structure de décision de telles organisations est donc **méritocratique**, plutôt que démocratique - même si rien n'empêche d'introduire des formes plus égalitaires de prises de décision.

Lorsqu'une rémunération rétribue l'activité des participants, il convient également qu'elle soit proportionnelle aux contributions effectives, afin de prendre en compte la diversité d'implication. Là encore, **l'équité** ne peut s'assimiler systématiquement à l'égalité, sauf à en faire explicitement une valeur cardinale du réseau. Des mécanismes complémentaires de redistribution - tel que le revenu universel d'existence, par exemple, - peuvent être trouvés en dehors de l'organisation.

Ouverte, méritocratique, équitable : tels pourraient être les attributs d'organisations décentralisées collaboratives. Exceller dans ces dimensions ne saurait dépendre uniquement d'une technologie, aussi puissante soit-elle. On touche ici à l'humain et au social, qui débordent de toute part l'approche techniciste. Mais il faut reconnaître le caractère transformatif de la blockchain dans cette évolution, et s'en saisir comme d'un outil irremplaçable pour substituer au pouvoir descendant de la hiérarchie la forme du consensus entre pairs, à une échelle inédite dans l'histoire des organisations.

[28] www.colony.io - www.part-up.com

[29] Voir les attributs d'angularité et d'adhésion des objets liens, in "Les communs, l'open source, les objets liens et l'Art de la Guerre", Gabriel Plassat - http://lafabriquedesmobilites.fr/articles/la-fabrique/communs/

Politique des blockchains

Par Yves Moreau, Professeur à l'université de Leuven

"Architecture is politics", Mitch Kapor, 2006

La blockchain permet de créer une relation de l'ordre du contrat social. Elle permet de connecter des individus les uns avec les autres, en créant une architecture adaptée. "Architecture is politics" affirmait en 2006 Mitch Kapor, à l'origine du logiciel Lotus (qui a fortement contribué à l'arrivée de l'ordinateur personnel au sein des entreprises). Toute architecture, toute façon de créer un système, qu'il soit ou non informatique, est une forme de politique. Par exemple, la façon d'aménager les rues pour ralentir les conducteurs constitue une manière de réguler les comportements des individus.

En matière d'architecture informatique plus spécifiquement, la création de systèmes informatiques, en permettant de connecter des individus ensemble, de les mettre en réseau, de les faire s'échanger des informations, n'est pas sans influence. Cette influence peut être négligeable à l'échelle de quelques individus, mais à l'échelle de l'ensemble du réseau, ces petites influences vont créer de grandes forces.

Autrement dit, construire un système en réseau revient toujours à créer des forces entre les individus. Il est essentiel que les développeurs qui construisent ces systèmes aient cette notion en tête. On entend souvent des scientifiques ou ingénieurs dire qu'il n'y a pas de dimension morale et politique dans la création des systèmes techniques, et que ce sont ce que les utilisateurs en feront. Cela peut être plus ou moins vrai pour les technologies classiques, mais cela n'est jamais vrai pour les technologies de réseau. L'exemple de Facebook le montre bien : ses créateurs ont développé un système intolérant vis-à-vis de la nudité et très tolérant vis-à-vis de la violence verbale et ce qui relève plus globalement de la liberté d'expression. Ils imposent ainsi un système de norme américain aux utilisateurs du monde entier. En somme, à chaque fois que des infrastructures de réseau sont déployées, il y a bien une dimension politique.

Tout réseau entre individus constitue un système complexe

Quand le système grandit, il devient difficile de prévoir ce qu'il s'y passera. Quand on développe le design d'un système, on ne peut jamais totalement être sûr de la façon dont il fonctionnera et sera utilisé. Au moment de la création du Bitcoin, la possibilité d'une attaque des 51 % a été jugée très improbable, quasi impossible. Pourtant, on s'est rendu compte par la suite que Bitcoin était assez vulnérable à cette attaque des 51 %, en raison du développement d'intérêts économiques qui conduisent à la concentration du minage.

Il est donc important de comprendre que lorsque l'on crée un réseau, seule une approche empirique peut gérer la croissance de celui-ci. C'est en effet seulement au fur et à mesure de son développement que l'on se rend compte des problèmes auxquels on est confronté. On peut certes essayer d'anticiper ces problèmes en mettant en place certaines mesures, mais on ne peut pas prévoir si celles-ci auront ou non des effets secondaires non escomptés. Il faut donc suivre le

développement du réseau et agir et compenser au fur et à mesure, dans une logique d'itération.

"Vote with your feet" : l'adhésion au réseau comme facteur démocratique

La période de croissance des différents réseaux, avant qu'ils n'atteignent une taille critique, constitue une opportunité démocratique intéressante. La compétition entre chaque réseau offre en effet aux individus la possibilité de ce qu'on appelle "voter avec leurs pieds" ("vote with their feet"), une notion très américaine qui consiste pour des individus à quitter des situations qui ne leur conviennent pas ou à rejoindre des situations qu'ils pensent être plus bénéfiques. Cette démarche est décrite par le chercheur Ilya Somin comme un "outil pour favoriser la liberté politique, puisqu'il permet aux citoyens de choisir le régime politique sous lequel ils aimeraient vivre".

Dans cette période où des réseaux comme Bitcoin et Ethereum se développent, chacun a la possibilité d'adhérer ou non au réseau de son choix. Cette situation contraste avec la réalité du réseau de la vie de tous les jours, l'Etat, puisque chaque citoyen est sujet d'un Etat en fonction de critères notamment géographiques, ce qui n'est pas un choix véritablement démocratique : pour pouvoir changer de règles, l'individu doit déménager. Les réseaux blockchains actuels, dans la période où ils grandissent, offrent donc une véritable opportunité démocratique en autorisant chaque personne à choisir le ou les réseaux qu'elle souhaite rejoindre.

Effets fondateurs et croissance de réseaux

Cette opportunité démocratique s'inverse lorsque les réseaux deviennent dominants. L'exemple phare pour l'illustrer est Facebook : il y a peu de sens aujourd'hui pour un utilisateur de migrer vers un autre réseau social que Facebook car le coût d'opportunité est trop important. Chaque individu, en faisant ce même calcul, renforce le réseau dominant. En d'autres termes, tant que les réseaux restent de taille modeste, les possibilités d'en changer sont réelles, mais lorsque l'un d'entre eux prend une certaine ampleur, la liberté de choix des individus se réduit alors fortement.

Quelle blockchain obtiendra la première la masse critique suivante et sortira victorieuse du phénomène du "winner-takes-all" ? Rappelons-nous de la compétition initiale entre Myspace et Facebook : les deux coexistaient en tant que réseaux sociaux. Puis Myspace s'est retrouvé complètement dépassé. Nul ne sait si Bitcoin est l'équivalent de Facebook ou Myspace ou, autrement dit, si un réseau pourrait émerger qui marginalisera Bitcoin. Peut-être qu'Ethereum ou un autre système de blockchain encore à venir deviendra cet acteur dominant à la Facebook, mais il est impossible de le prédire pour le moment. En outre, il est aussi tout à fait envisageable que plusieurs types de blockchains coexistent sans que l'une ne l'emporte nettement sur une autre.

Seuil de viralité des réseaux

Avec la croissance des réseaux comme la blockchain se produit un effet de viralité: au début cette croissance reste modérée, mais celle-ci s'accélère à partir d'un certain seuil. Là encore, Facebook en est un bon exemple. Cet effet de viralité pose un problème en particulier : une fois un certain seuil atteint, il devient très difficile de changer les paramètres du système au cas où un effet ne conviendrait pas. Il faut donc essayer d'adresser les problèmes avant que ne se produise cette inflation. Mais le paradoxe est le suivant : tant que le réseau reste de taille modeste, la tendance naturelle est de se dire qu'il n'y a aucune urgence à adresser ces problèmes, d'autant qu'il n'y a alors aucune certitude que ce réseau et non un autre devienne dominant.

Les choix fondateurs sont politiques

Si l'une des blockchains devient dominante, alors ses choix politiques sous-jacents se répandront avec elle. Dans le cas de Bitcoin, même si les intentions de Satoshi Nakamoto ne sont pas connues, il est clair que ce système implique une conception politique libertarienne. Dès lors si Bitcoin devient dominant, la vision libertarienne qui la sous-tend deviendra elle aussi dominante. Il faut donc se demander si cette vision politique correspond véritablement à notre souhait. Par exemple, il faut se demander si l'idée de déplacer de l'argent très facilement et rapidement est conciliable avec la notion d'impôts. Il peut être problématique qu'en une fraction de secondes il soit possible de transférer mon argent ailleurs dans le monde ; sans parler des protocoles entièrement anonymes, tels Dash ou Monero que certains veulent développer.

Ces questions politiques doivent se poser maintenant : ensuite, il sera trop tard.

La gouvernance des projets de blockchain

La question essentielle à se poser est de savoir comment gérer le développement des réseaux blockchains, et donc leur gouvernance - plus précisément la façon de se mettre d'accord sur les décisions. Les conflits dans la communauté bitcoin pour déterminer s'il faut ou non lever les restrictions techniques actuelles du protocole (taille des blocs par exemple) témoignent de la difficulté à résoudre ces questions. De multiples avis et intérêts divergent à ce sujet ; les mineurs chinois, par exemple, affirment qu'ils ne sont pas capables d'absorber de profonds changements.

Ces conflits montrent les limites de modèle de gouvernance de Bitcoin. Le pouvoir a été transféré à un groupe restreint qui décide des directions auxquelles le projet peut aller. Il existe certes toujours la possibilité de créer un fork, c'est-à-dire une version alternative qui découle d'un modèle existant, mais la réussite d'un fork dépend du nombre de personnes qui choisissent d'y basculer, qui se révèle en pratique souvent très limité.

Cette situation pose un réel problème de gouvernance à l'heure où Bitcoin est déjà devenu un projet avancé, avec une capitalisation conséquente (bien qu'encore réduite par rapport à ce que Bitcoin pourrait devenir). La majorité des

bitcoins sont aujourd'hui détenus par une infime partie d'utilisateurs ; et par "infime", il n'est pas question de 1 % mais plutôt de 0,001 %. Parmi les 2,5 millions d'adresses bitcoin utilisées à ce jour, les 100 adresses avec le solde le plus important représente à elles seules 20 % de toutes les bitcoins en circulation. Derrière l'idée libertarienne, démocratique, égalitaire, qu'on retrouve initialement dans le Bitcoin, se cache donc une réalité très différente dans les faits.

Démocratie des blockchains

Malgré ses promesses, la blockchain peut tout à fait être utilisée de façon non-démocratique.

Sur le papier, si l'on considère la notion de consensus distribué, la dimension démocratique est indéniable. Mais ce ne serait pas exact d'affirmer que la blockchain par nature permettra toujours la participation et la reconnaissance de chacun dans le système. La blockchain, malgré sa capacité à supprimer la notion de plateforme intermédiaire, ne garantit pas forcément une gouvernance démocratique du système. L'existence d'un système de décentralisation n'apporte pas la garantie que ce système ne sera pas oppressant et que les individus garderont le contrôle.

En réalité, la question n'est pas tant de savoir si le système est décentralisé mais qui le contrôle. Si ce contrôle reste centralisé entre un petit nombre de personnes, alors le fait que le système général soit décentralisé n'apporte pas grand-chose - au contraire, cela risque même d'engendrer des structures encore plus oppressives. La gouvernance est donc un enjeu clé pour parvenir à un système ouvert et transparent.

Le besoin d'un système de défense pour les technologies de rupture

Puisque personne ne possède la blockchain, une question se pose : qui va la défendre ? Le manque d'incitations à défendre le système constitue une de ses vulnérabilités. La seule façon qu'a aujourd'hui Bitcoin de se défendre repose sur des "évangélistes" qui vont promouvoir son concept. Mais devant les institutions traditionnelles, ces évangélistes ne vont pas avoir les leviers institutionnels des plateformes classiques.

Il manque donc un lobbying organisé à la blockchain, alors même qu'elle représente déjà des montants très conséquents en termes d'investissements. Si ne serait-ce qu'un pour mille de ces montants était attribué à la défense de la blockchain, beaucoup de choses pourraient déjà se faire ; mais la façon dont le système a été construit n'a pas intégré cette notion. Uber a par exemple très bien intégré, très tôt, l'importance du lobbying, des relations publiques, mais Uber est une entreprise, ce dont n'est bien sûr pas la blockchain.

Quelle transparence ?

Une autre dimension fondamentale est la transparence : la blockchain apporte bien plus de transparence que ce dont on a l'habitude. Le système financier actuel, malgré des progrès certains ces dernières années, reste ainsi très opaque.

La question est toutefois de savoir dans quelle direction la transparence s'effectue, car celle-ci constitue un rapport de pouvoir.

Jusqu'ici cette transparence s'est surtout portée sur le citoyen, contre sa vie privée : Facebook et Google ont ainsi accès à d'immenses données sur les citoyens sans que ceux-ci en aient forcément conscience. Or les citoyens voudraient que cette transparence s'effectue dans l'autre sens, vers l'Etat et les entreprises, dans la perspective d'une société plus équilibrée, où les plus faibles gardent un certain contrôle sur les plus forts. La blockchain pourrait constituer un moyen d'y arriver. Mais il est essentiel de réfléchir à la transparence du système dès le design de celui-ci.

Cela étant, la transparence absolue n'est pas forcément souhaitable. Hal Finney, pionnier du Bitcoin (il est celui qui a reçu la première transaction), a été victime alors même qu'il était gravement malade de maîtres-chanteurs qui ont cherché à lui extorquer ses bitcoins. Le besoin de plus de transparence de façon générale ne signifie donc pas qu'il ne faille pas poser certaines limites à celle-ci.

Les smart contracts et les risques de l'arbitrage privé

Le concept de smart contract est très attirant, et permettra sans doute nombre de choses intéressantes, mais il faut se rendre compte des pouvoirs et des asymétries que ses contrats pourraient avoir. Aujourd'hui personne ne lit réellement les contrats des logiciels et services téléchargés ou utilisés sur Internet. Par exemple, peu d'utilisateurs de Facebook savent qu'en utilisant le réseau social ils accordent à Facebook le droit d'utiliser leurs photos personnelles, notamment pour les publicités du site.

Les smart contracts vont plus loin encore puisqu'ils peuvent s'exécuter avec un effet financier. Là réside un potentiel danger. Prenons le cas des factures téléphoniques actuelles. Périodiquement, les médias font état de clients de téléphonie mobile qui découvrent une facture de plusieurs milliers d'euros après un séjour à l'étranger. Dans ces cas-là, le plus souvent l'utilisateur plaide au tribunal qu'il n'est pas capable de payer la somme demandée, et le juge peut alors lui demander de ne payer qu'une somme réduite : une régulation par la loi s'effectue donc.

Cette régulation risque de ne pouvoir s'effectuer que beaucoup plus difficilement avec le smart contract, qui prélève par nature automatiquement les montants : ce sera alors à l'utilisateur d'aller poursuivre l'autre partie pour tenter de récupérer une partie de la somme, sans aucune garantie de succès. Les smart contracts contiennent donc le risque d'une asymétrie entre une partie forte et une partie faible.

On sort dans ce cas du système légal classique pour se retrouver dans un système d'arbitrage privé, ce qui me semble très dangereux. Le cas des Etats-Unis constitue une bonne illustration de ce qu'une sortie du système légal classique peut engendrer. Ces dernières années s'est en effet développée là-bas une tendance forte à l'arbitrage privé, qui prévoit qu'en cas de conflit, les parties

prenantes se rendent non pas devant un tribunal classique mais devant un panel d'arbitrage. Cela aboutit parfois à des histoires surréalistes.

Les smart contracts risquent d'engendrer ce phénomène au carré. L'individu, après avoir donné son accord, se retrouvera face à des mécanismes automatiques qui l'obligeront en cas de problème à devoir se plaindre *a posteriori* devant les tribunaux. Il faudra surveiller ce risque avec beaucoup d'attention.

Le rêve libertarien

L'idéologie libertarienne consiste en une réduction de l'Etat au strict minimum : sa responsabilité se limiterait à la garantie de non-agression (le fait que l'Etat doive intervenir en cas d'agression) et la garantie d'exécution du contrat privé. Autrement dit, l'idée est que toute la société soit gérée par des contrats privés, et qu'en cas de conflit, l'Etat intervienne pour assurer leur exécution. C'est bien sûr très différent du droit européen où le juge a toujours la possibilité de décider que telle ou telle clause est abusive. Dans l'idéologie libertarienne la liberté individuelle est fondamentale ; à chacun d'assumer par la suite ses choix, qu'ils aient été bons ou mauvais. La notion de salaire minimum n'existe par exemple pas : si un individu est prêt à travailler pour une bouchée de pain, il en a la possibilité.

L'étape qui vient au-dessus du rêve libertaire, et qui se rapproche des idées anarchistes, est l'idée selon laquelle il est possible et souhaitable de se soustraire à l'Etat. C'est par exemple le cas du Darknet et de certaines utilisations de réseaux anonymes comme Tor (ce qui n'exclut pas que Tor ait de nombreuses utilisations légitimes). D'où le souhait des crypto-anarchistes d'adapter le protocole Bitcoin comme point de départ pour développer des transactions complètement anonymes entre les individus, ce qui empêcherait totalement les institutions de pouvoir y avoir accès.

Tout système informatique avec des "effets de bord" ("side effects") dans la vie réelle peut être réglementé

L'idée selon laquelle il est possible de se soustraire totalement à la régulation est à mon sens fausse. Pour y parvenir, il faudrait rester entièrement dans le cyberespace, puisque dès qu'on en sort et qu'on rentre dans le monde réel, les transactions sont observables. Un individu qui s'enrichirait d'un millier de bitcoins [Nb : l'équivalent de 400.000 euros] et qui s'achèterait avec des voitures de sport se remarquerait nécessairement. De la même façon, s'il achète avec ses bitcoins des substances illégales, celles-ci doivent de toute façon lui être envoyées dans la vie réelle.

Cela étant, la capacité de l'Etat à taxer de tels mécanismes est plus restreinte et ce même s'ils sont en grande partie légaux – tout comme nombre de constructions financières permettant aux entreprises de payer moins d'impôts sont légales en soi. En conséquence, si des crypto-monnaies plus ou moins anonymes venaient à prendre une ampleur globale, on assisterait à un affaiblissement encore plus marqué de la capacité de l'Etat à prélever l'impôt. Ceci pourrait mener à une

réaction particulièrement violente pour endiguer ce qui serait une menace quasi existentielle pour des états déjà vacillants.

Recréer l'Etat grâce à la blockchain

La concentration de richesse de Bitcoin est bien plus importante encore que dans la société actuelle, où cette concentration est pourtant déjà forte. L'idéal libertarien n'a donc rien amélioré de ce côté-là.

L'attirance de certains pour le rêve libertaire relève plutôt d'une déconnexion entre les structures de gouvernance et les individus : ces derniers ont l'impression de ne plus avoir de poids dans les discussions et les décisions, et que leur vote ne change plus rien, dans une sorte de faillite du système démocratique classique.

Or il faut comprendre que l'Etat n'est rien d'autre que nous : il faut donc utiliser la blockchain pour recréer l'Etat et non le détruire. Evidemment, cela ne peut pas se faire en quelques mois, mais seulement par un processus très progressif. Le but serait d'utiliser la technologie pour créer des mécanismes de contrats sociaux (mécanismes de solidarité, de transparence, de rééquilibrage, etc.) afin d'atteindre un "meilleur" entre les individus. En d'autres termes, il ne faut pas essayer de s'échapper de la notion d'Etat, mais au contraire se le réapproprier pour affirmer que "l'Etat, c'est nous", dans un contexte où les citoyens ont de moins en moins l'impression que l'Etat les représente.

La blockchain, une base possible pour construire des systèmes de communs

Comment parvenir à cette réappropriation de l'Etat par les citoyens ? Par exemple en créant des communs. Pensons au cadastre établi sur base des transactions notariées : ce registre des propriétés, qui constitue une fonction centrale de l'Etat, est quelque part un commun, avec un accès relativement transparent, ouvert à tous. Ce commun peut être perçu comme banal, cependant si on pense à des états où un tel mécanisme n'existe pas ou est déficient (et il ne faut pas aller plus loin que la Grèce pour l'observer), on se rend compte à quel point ce mécanisme est essentiel.

Plus généralement, la blockchain peut aider à créer un certain nombre de communs ; pensons par exemple à un registre d'informations importantes, de propriétés, d'activités économiques, d'œuvres artistiques, etc. Ces communs seraient construits de façon collective ; l'intérêt de la blockchain est alors d'apporter un retour à la personne qui a contribué. Si l'on prend l'exemple du design, lorsque quelqu'un utilise un design, un retour financier s'opérerait automatiquement vers son créateur.

Ce mécanisme pourrait fonctionner pour le design, la production d'objets, l'impression 3D, l'architecture électronique, les créations artistiques, etc. En somme, d'une part le commun serait accessible à tous, et d'autre part des mécanismes de redistribution vers ceux qui auraient contribué à sa construction seraient mis en place *via* la blockchain, ce qui permettrait de vaincre la "tragédie des communs".

La blockchain, une menace pour les institutions ?

Par Julien Lévy, Professeur affilié à HEC Paris, Directeur du Centre Digital d'HEC, auteur de l'étude annuelle *Netexplo Trend report*

Traditionnellement, le titre de propriété est garanti par une institution. Ainsi, la monnaie est garantie par la banque centrale ; les titres de propriété fonciers sont garantis par les notaires et le cadastre de l'administration publique ; les transactions monétaires sont garanties par les banques ; etc. La confiance dans le système de propriété repose donc sur la confiance dans les institutions. Jusqu'ici, ce sont les institutions qui ont créé la propriété. Quand les institutions sont gravement défaillantes, la propriété est menacée et les transactions s'opèrent par le troc ou les monnaies étrangères.

La blockchain est de nature à renverser ce paradigme. Avec cette technologie, les titres de propriété et les transactions peuvent être en effet garanties par un *réseau* (duplication en masse de l'information) et un *protocole* (qui garantit la protection et la cohérence entre les doubles).

Autrement dit, le réseau et le protocole se substituent à l'institution.

Quelles en sont les conséquences ?

Les coûts de traitement et de validation de la blockchain sont sans commune mesure avec les systèmes institutionnels existants. Le système est très léger (encore que la consommation de temps de traitement de machine s'alourdit avec le succès de la technologie) et complètement décentralisé. Il est aussi conçu pour être entièrement automatisé. Ce qui aurait réclamé la mise en place d'organisations et d'une cohorte d'experts, de contrôleurs, de managers, d'employés est géré par le réseau et le protocole.

La blockchain permet de réduire les coûts de transaction à deux titres : par la réduction des coûts de traitement comme on vient de le souligner, et par la réduction des risques. Cette technologie, par sa facilité d'utilisation et son faible coût, peut réduire les risques associés à de nombreuses transactions, par exemple celles entre particuliers ou celles générées par les plateformes collaboratives.

Par conséquent, on peut s'interroger sur l'obsolescence de certaines institutions. Ne peut-on numériser, "blockchainer" une grande partie des processus existants? Les notaires vont-ils succéder aux chauffeurs de taxi comme les victimes de la révolution numérique ? Toute une partie de l'activité des banquiers ne sera-t-elle pas touchée ? La blockchain ne crée-t-elle pas en fait un modèle alternatif, plus performant que les modèles institutionnels existants (le cas de Bitland au Ghana en offre une belle illustration) ?

Ainsi en Afrique, jusqu'à 90 % des terres sont non-documentées et donc en dehors du système juridique. Même dans les villes, les adresses ne sont pas toujours formalisées, et un même lieu peut avoir plusieurs adresses.

Cela soulève un enjeu économique fondamental. L'économiste péruvien Hernando de Soto a montré qu'un frein majeur au développement économique des pays pauvres est qu'une bonne partie du capital est, selon, son expression, du "capital mort". Dans ces pays, la plupart des habitants sont par exemple propriétaires de leur maison ou de leur terrain. Mais ces propriétés ne sont pas légalisées, en raison de l'inefficience des systèmes d'enregistrement en place, de la longueur des procédures, de leur coût, de la difficulté à aboutir, de la corruption. Ce capital n'étant pas légalisé, il n'entre pas dans les statistiques nationales et il est exclu du système financier local. Les banques ne prêtent pas, faute de capital qui serve de caution, alors qu'un financement même réduit permettrait le développement de nombreuses activités.

La blockchain ne suffira pas à elle seule à résoudre l'enjeu de la "résurrection" du "capital mort" dont parle Hernando de Soto (il y faut aussi une volonté politique et des conditions juridiques), mais en réduisant considérablement les coûts de constitution d'un cadastre, elle peut y contribuer.

De façon plus générale, comme toute technologie la blockchain est un "enabler", et non une solution. Elle ne pourra pas fonctionner sans une volonté politique et une validation par la justice des dispositifs créés. Il est donc peu probable que la blockchain se passe des institutions.

Face à la blockchain, l'Etat est Janus : d'un côté, il aura la tentation d'interdire et de contrôler, d'autant que les professions menacées comme celles des notaires ne resteront pas sans rien dire. Mais tout l'intérêt du caractère décentralisé de la blockchain risquerait alors d'être atténué.
D'un autre côté, il faudra bien, à moins de rester dans le virtuel, qu'une jonction se fasse entre d'une part ce que la blockchain permet et d'autre part la vie réelle - notamment en termes de reconnaissance juridique -. Certains technophiles ou utopistes imaginent certes un monde sans Etat ; mais dans le cas des titres de propriété, par exemple, ces titres devront bien être reconnus juridiquement.

La technologie n'est jamais une solution : celle-ci ne vient que des usages. L'important est donc de voir ce que rend possible la technologie, et de développer des stratégies qui intègrent les possibilités apportées par la blockchain.

Blockchains et démocratie : deux mesures d'une même confiance

Par Louis Margot-Duclot, Directeur des affaires juridiques de Democracy Earth

Aux yeux d'une blockchain, notre système légal et administratif n'est rien d'autre qu'une succession de choix binaires. À y regarder de près, le droit n'est en effet qu'une série de décisions très simples, réalisées en continu par des acteurs connus, et selon une procédure spécifique. Cet ensemble de choix binaires est organisé en une pyramide, dont la Constitution et les valeurs fondamentales de la République sont placées au sommet, et qui exprime le fait que certains choix réalisés par certains acteurs prévalent sur d'autres.

Ainsi, si l'on cherchait à créer un système informatique qui tenterait de reproduire notre droit, on programmerait ce système de sorte que chaque règle juridique choisisse en premier lieu un comportement humain ou une action humaine ; qu'elle choisisse ensuite si elle autorise ou interdit cette action ou ce comportement ; et qu'elle détaille enfin à qui et dans quelles conditions cette interdiction ou cette autorisation s'appliquent.

Par exemple, il est autorisé à tous de fonder une entreprise. Au sein d'une entreprise, il est interdit d'employer des enfants. Cependant, il existe certains cas dans lesquels cette interdiction ne s'applique pas, lorsqu'il s'agit d'un travail réalisé dans le cadre de leur formation ou de leur éducation par exemple. Il est alors autorisé à certains acteurs, dans des circonstances bien définies, d'émettre des conventions de stage, prouvant qu'ils sont bel et bien autorisés à employer un enfant pour une certaine période. Tout le cheminement intellectuel conduisant à l'établissement de ces règles strictes encadrant le travail des enfants peut donc être ramené à un ensemble organisé de choix binaires, répartis entre des actions qui ont été soit autorisées soit interdites.

D'un point de vue juridique, la seule véritable valeur, c'est donc la réalité des faits: cette réalité-là est binaire. Soit les faits ont eu lieu, et alors la condamnation est prononcée, soit ce n'est pas le cas, et l'accusé est relâché. Entre les deux subsistent des conditions particulières, qui vont moduler l'une ou l'autre possibilité, mais la valeur fondamentale, elle, est bien binaire. Se dressent ainsi une distinction entre, d'une part, des règles administratives, qui détaillent les conditions selon lesquelles une administration est autorisée à agir, et de l'autre, les valeurs politiques d'une société, qui reflètent le refus collectif que certains actes, jugés "immoraux", soient accomplis par ses membres.

L'État, un système binaire décentralisé ?

En droit français, ces deux ensembles, règles procédurales et valeurs politiques, sont exprimés par un même objet, le texte de loi. Ils recouvrent pourtant des réalités bien différentes, et cette confusion prend aujourd'hui de l'importance dans la mesure où, avec une blockchain, la "logique" du texte de loi, la manière dont les règles sont intégrées au reste du système, peut être exprimée non par des simples mots, mais par un code informatique. Les règles "procédurales" pouvant

être réduites à l'exécution d'un programme lu par des milliers d'ordinateurs en même temps, seuls seraient laissés aux soins des citoyens et des élus les choix collectifs exprimant les valeurs morales qui définissent le système – par exemple le refus qu'un enfant travaille.

Bien entendu, cela ne signifie pas que l'appréciation des valeurs communes ni l'exercice de la justice doivent être laissés à un système informatique. Certaines informations demeureront toujours du texte, car elles expriment une vision du monde, une intersubjectivité dont l'appréciation nécessitera toujours des juges. Dans un souci de transparence et d'efficacité de l'action publique, nous pouvons malgré tout considérer que toutes les dispositions légales qui ne font qu'exprimer par du simple texte une règle de procédure devraient être formulées dans un langage qui pourrait être lu par un ordinateur. La constitution d'un tel modèle pourrait en effet permettre de se passer d'une masse administrative considérable, tout en ouvrant certains processus d'élaboration des politiques publiques à de nouveaux modèles de gouvernance.

La notion de *smart contract* pourrait permettre cette translation de dispositions textuelles vers un langage dynamique de manière particulièrement efficace. Le réseau Ethereum obéit par exemple aux mêmes contraintes fondamentales qu'un système légal : les *smart contracts,* comme les textes de loi, ne sont que des objets qui visent à énoncer une règle. Le support de cette règle ne devrait servir qu'à faciliter son exécution et sa diffusion dans la société.

Ainsi, un *smart contract* va tout d'abord utiliser une **adresse**. C'est l'identifiant unique d'un objet sur la blockchain, qui prend en charge la question de l'identité d'un objet : c'est la réponse à la question du "qui". Un *smart contract* va ensuite exprimer une **causalité**. "Si l'événement X se produit, alors la conséquence Y se produira également". Cet aspect est utile dans la mesure où il va nous permettre de programmer à l'avance des enchaînements complexes de décisions, selon une procédure bien précise et en un temps et un coût minimes. Pour assumer ce coût, un *smart contract* va enfin se voir attribuer une **puissance de calcul**, afin de permettre l'exécution au sein d'une blockchain des règles que ce contrat énonce. La question de savoir si l'événement X s'est produit ou non est quant à elle laissée aux **mineurs**, des instances de contrôle décentralisées sur tout le réseau.

C'est exactement la manière dont un Etat de droit fonctionne[30].

Le législateur définit souverainement un acte qu'il considère délictueux, et lui attache une **sanction**. Si une **personne identifiée** commet cet acte, un **juge** aura pour rôle de déterminer si, oui ou non, le comportement constaté correspond bien à la définition de cet acte donnée par la loi, et modulera la gravité de la peine prévue par elle en fonction des circonstances. La sentence qu'il prononce autorisera alors la **puissance publique** à déployer les ressources nécessaires à l'application de cette peine.

Un environnement constitué de *smart contracts* qui se reconnaissent mutuellement, s'organisent et se synchronisent selon des règles spécifiques

[30] H. Kelsen, Théorie pure du droit, Titre premier, 6, a : "Le droit, ordre de la conduite humaine".

pourrait ainsi, en théorie, reproduire une "pyramide des normes" tout à fait semblable à celle qui est en vigueur en France – aussi complexe et développée soit-elle. Cela ne signifie pas que nous n'aurions plus besoin de juges, seulement que l'autorisation qu'ils délivrent à l'administration devra être transmise par voie numérique. Ce changement peut sembler anodin, mais il permet cependant de constituer des organisations d'un genre nouveau[31], et ouvre un potentiel encore inexploré pour notre démocratie.

Blockchains et constitution de nouveaux biens communs

Fondamentalement, l'intérêt d'une blockchain pour une administration pourrait ainsi se comparer à un horodateur géant pour toutes les transactions dont elle pourrait avoir la connaissance. C'est une base fondamentale de coordination, une vérité partagée, qui va attester, pour le compte de tous, que l'événement X a bien eu lieu à telle heure, qu'il a impliqué tels acteurs, et que par conséquent l'événement Y va pouvoir se produire.

En distribuant des identités et en organisant la nature des échanges qui peuvent avoir lieu entre ces différents acteurs, qu'il s'agisse d'un vote, d'une part dans une société ou d'un titre de propriété, un système de *smart contracts* remplit en réalité la définition qu'on pourrait avoir d'une institution : un jeu de règles partagées et acceptées souverainement par un ensemble d'acteurs donné, constituant un socle de *valeurs communes*.

On peut désormais constituer des organisations autonomes, publiques, décentralisées, ces "DAOs" qui remplissent finalement toutes les caractéristiques d'une administration publique. Elles n'appartiennent à personne en particulier, suivent leurs propres règles, et se donnent les moyens de leur exécution. Une question qui vient est donc de savoir si certaines de ces organisations ne pourraient pas être utilisées par des administrations pour réaliser une mission de service public, voire, pourquoi pas, réunir l'ensemble des règles qui gouvernent l'action publique et remplacer notre vieille conception de l'État ?

Les "DAOs" permettent non seulement de réaliser ces missions de manière efficace et transparente, mais également de revoir la manière même dont nous envisageons leur accomplissement. Elles ouvrent la voie à de nouveaux types de coopération, plus horizontaux, permettant à des millions de personnes de travailler ensemble en étant coordonnées, voire rémunérées, non par un responsable de programme ou une armée de managers, mais par une suite de *smart contracts*.

Une telle organisation permettrait l'automatisation de certaines procédures, mais également l'évolution de certaines modalités de l'engagement démocratique. Les exemples d'applications de la technologie blockchain en dehors du secteur financier[32] se sont ainsi très rapidement portés sur le vote électronique, et sur la possibilité d'organiser des consultations plus fréquentes, plus riches et plus

[31] Vitalik Buterin, DAOs, DACs, DAs, and more: An incomplete terminology guide
[32] Ethereum State of the Dapps

faciles, tout en maintenant un niveau d'exigences élevé en matière de sécurité et d'anonymat.

Un exemple : des institutions numériques pour une démocratie liquide

Les perspectives de renouvellement démocratique *via* les concepts de démocratie liquide par exemple, s'imposent aujourd'hui avec d'autant plus de force que la notion de blockchain se démocratise. Certaines revendications émergent ainsi pour dénoncer le caractère restrictif des modes de suffrages utilisés dans les élections nationales[33], l'argument de certains consistant à dire que le scrutin majoritaire à deux tours limite la capacité des électeurs à exprimer un choix sur des mesures spécifiques, et les obligent à voter en bloc pour un programme porté par un candidat. Une solution serait donc d'affiner les possibilités de choix présentes sur les bulletins de vote[34], ou alors d'augmenter la fréquence des élections au cours du temps.

La démocratie liquide est un système de délégation de vote qui propose de faire les deux[35]. Le vote d'un électeur est considéré comme un jeton qui peut être confié à n'importe quel candidat afin qu'il décide en son nom. Chaque candidat peut à son tour confier ses jetons à qui il le souhaite, en gardant à l'esprit que chaque électeur lui ayant confié son vote peut également le retirer à tout moment s'il est mécontent de ce second niveau de délégation. Chaque votant peut ainsi déléguer son vote autant de fois qu'il le souhaite, en continu, et exprimer ses opinions de manière plus libre que si son vote était "bloqué" par un même candidat, pour cinq ans.

La difficulté de mettre en place un tel système réside dans le fait qu'il nécessite la certification d'un grand nombre de transactions en temps réel. Or il se trouve que le caractère de "jeton" du vote liquide s'accommode particulièrement bien avec l'architecture d'une blockchain, et le caractère informatique de ces "jetons" ouvre la voie à un suffrage qui serait "programmable". On pourrait par exemple diviser le jeton en parts qui représentent un certain pourcentage du vote, et les répartir en fonction de sujets d'intérêts déterminés par le votant.

Bob pourra ainsi attribuer 15 % de son vote aux questions environnementales, pour lesquelles il délibère directement, 20 % aux questions économiques, pour lesquelles il délègue son vote à Mike, un ami économiste avec qui il s'entend bien, et déléguer le reste de son vote sur les autres sujets à Alice, l'élue locale de sa circonscription. Bob peut également décider qu'Alice a le droit de déléguer son vote à un tiers, alors que Mike doit voter directement sur les questions liées à l'économie. Si Mike préfère déléguer son vote sur une de ces questions, le jeton de Bob lui sera retiré automatiquement, et Bob pourra à nouveau l'utiliser comme bon lui semble.

Bien entendu, un tel système n'est possible que si les questions de sécurité du vote, d'anonymat et de transparence sont résolues de manière robuste, ce qui n'est pas le cas aujourd'hui. En tout état de cause, s'il est toujours difficile

[33] The Economist, dossier "What's gone wrong with democracy?"
[34] Voir par exemple Claude Tardif, Les systèmes électoraux : le vote unique transférable
[35] Voir http://liquidfeedback.org/ ou http://democracy.earth

d'assurer l'anonymat d'un votant sur une blockchain qui permet à chacun de vérifier soi-même son vote, il demeure clair que cette technologie rend possible des usages qui étaient tout simplement impossibles il y a encore quelques années, et qui remettent profondément en question certains processus d'élaboration et de mise en œuvre de l'action publique.

Quelques propositions pour un Etat 2.0

Dans les faits, nous pourrions par exemple prendre appui sur les succès du déploiement du Réseau interministériel de l'État (RIE), infrastructure physique désormais commune à l'ensemble des ministères, et placée sous l'autorité du Premier ministre[36], pour déployer une véritable "blockchain d'État". Cette blockchain pourrait constituer le laboratoire de l'État pour des applications décentralisées de service public en tout genre, et enverrait un signal fort dans le sens de la co-construction d'un bien commun numérique, un "code source" de l'État, ouvert et transparent.

Il serait également envisageable de faire de France Connect (l'actuelle plateforme d'identification de l'État) le point d'entrée de cette blockchain pour les citoyens français. Au compte France Connect de chaque citoyen serait ainsi attachée une adresse permettant d'effectuer des transactions avec les institutions connectées, et de gérer la certification de nombreux documents officiels émis par l'État (comme c'est aujourd'hui le cas en Estonie[37]) à savoir l'état civil, les registres du commerce, les diplômes et autres certificats en tout genre.

À partir de ce socle d'identification commun et sécurisé, il sera ensuite plus aisé de développer des services supplémentaires au fur et à mesure que d'autres administrations ou des collectivités territoriales adopteront le protocole. On permettra ainsi la prestation de certains services sociaux (dans le domaine de la santé, des transports ou du logement par exemple) ou même fiscaux (prélèvement à la source, assurances chômage, retraites). Ces adresses pourront alors servir de fondation à des développeurs indépendants, leur permettant de proposer de nouvelles applications de service public ou la correction de bugs, et pourquoi pas des expérimentations en matière de démocratie liquide ou de nouvelles formes de consultations citoyennes.

Une fois constituée cette "mission blockchain" au sein de l'État, on pourra alors pousser la logique encore plus loin pour l'étendre à des organisations internationales, ou à la gouvernance d'organisations croisant plusieurs échelles indépendantes, entre un échelon local, national et international. Cette démarche pourrait ainsi contribuer à promouvoir la constitution d'infrastructures publiques supranationales, à l'image d'un récent projet de la Commission européenne visant à augmenter la participation citoyenne *via* le développement d'applications sur la blockchain[38]. Il pourrait alors être possible de voter pour des élections qui dépassent notre seul cadre national, ou pourquoi pas d'utiliser une crypto-monnaie européenne indexée sur l'euro par exemple.

[36] Décret n° 2014-879 du 1er août 2014 relatif au système d'information et de communication de l'Etat
[37] Voir https://e-estonia.com/tag/blockchain/
[38] Appel à projets ICT-12-2016 de la Commission européenne pour le développement de blockchains et d'architectures décentralisées

La promesse d'une construction commune

La force politique des technologies de la blockchain, c'est donc peut-être leur capacité à mettre en lumière le rôle essentiel d'une *mesure commune de la valeur*. Que cette valeur soit économique (la monnaie) ou politique (le vote), les progrès de la technologie ne doivent pas occulter que ces différents types de valeurs sont tous dépositaires d'une même valeur commune : la confiance. Par la mesure de cette valeur sociale, et sa confrontation à une échelle mathématique, la blockchain crée un étalon universel qui constitue lui-même une valeur, un bien public que l'État et la société civile se doivent de cultiver s'ils souhaitent réduire la distance qui les sépare.

Organiser les pouvoirs entre des institutions indépendantes est désormais grandement facilité par ces technologies, tout comme certaines interactions directes entre citoyens. Ce que la blockchain promet à nos démocraties, c'est la possibilité d'une redéfinition de notre rapport aux institutions, pour lui substituer une intersubjectivité partagée de pair à pair, un rapport direct à des règles communes, au sein d'un espace public, ouvert à tous et n'appartenant à personne. Les règles qui définissent la gestion d'un bien commun font partie de ce bien, et il est aujourd'hui possible, voire souhaitable, de voir certaines de ces règles prendre la forme d'un code distribué sur une blockchain, pour faciliter leur lisibilité, leur évolution et leur diffusion. Le développement de telles applications est rapide et peu coûteux, des modalités de financement public existent et son potentiel pour l'administration peut se révéler considérable[39]. Reste donc à savoir si l'État saura saisir cette opportunité.

[39] Voir l'article de Blockchain France, "Blockchain : le Royaume-Uni prend les devants en Europe", 26 janvier 2016.

Interview avec Jérôme Giusti, Avocat fondateur du cabinet "11.100.34. Avocats Associés", spécialiste en droit des nouvelles technologies

Quels sont les impacts envisageables de la blockchain sur le droit ?

On peut imaginer trois domaines juridiques impactables par la blockchain :

> le droit de la preuve, qui peut être complètement modifié ;
> tout ce qui relève de la notarisation et du tiers de confiance. Cela peut impacter le formalisme juridique, notamment tout ce qui est contractuel, puisque le droit impose aujourd'hui, dans bien des cas, des contrats écrits, signés, avec des clauses qui doivent être démontrées par écrit ;
> tout ce qui relève de l'exécution automatique de clauses contractuelles.

Il s'agit toutefois seulement de prospective. Nous avons commencé à réaliser dans notre cabinet des études sur la blockchain pour savoir si elle pourrait valoir contrat ou s'apparenter à une signature électronique. Nous sommes en cours d'expérimentation à ce sujet. Nous avons par exemple déjà créé un générateur de contrat automatique ; la blockchain pourrait en être un prolongement, dans l'idée de notarisation de ces contrats.

La blockchain n'est-elle pas difficilement compatible avec des problématiques de réglementation (Know Your Customer…) ?

C'est tout le sujet. Aujourd'hui la blockchain n'est pas réglementée, mais elle le sera certainement. C'est toujours la même chose : il faut que l'usage soit assez fort pour pouvoir imposer sa loi au législateur. Il faut que nous, juristes, puissions faire en sorte que la blockchain, malgré son côté très libertaire, ne soit pas totalement loin du droit.

La nature même de la blockchain (la pseudonymie par exemple) ne s'oppose-t-elle pas à cette exigence de réglementation ?

Je ne crois pas qu'il y ait une incompatibilité par nature entre les nouvelles technologies et le droit. Il y a toujours un moyen de marier les deux. Si la technologie se veut en dehors du droit, elle sera à un moment rattrapée. Et si le législateur comprend mal la technologie, ensuite il va mal agir et donc mal réglementer. C'est pour cela qu'il est nécessaire de développer une culture commune entre les mondes juridique et technologique.

Comment y parvenir ?

C'est quelque chose de générationnel. Les gens qui sortent des écoles d'avocat et des facultés de droit n'ont pas encore assimilé la technologie dans leur pratique, et c'est un vrai problème. A l'inverse les jeunes diplômés en licence commencent, pour certains, à avoir cette compétence. La nouvelle génération semble donc aller dans le bon sens à ce niveau-là.
Cela nécessite en tout cas une vraie volonté de la part des juristes d'intégrer des compétences qu'ils n'ont pas, en le faisant soit personnellement, soit en

intégrant dans leur cabinet ou leur équipe des profils techniques comme nous l'avons fait chez nous, et de se poser la question de savoir comment leur métier va évoluer dans les 20 ans à venir.

La blockchain va-t-elle uberiser le métier d'avocat ?

Nous ne sommes uberisables que sur les tâches sur lesquelles nous ne sommes pas agiles. Certaines fonctions, qui concernent les tâches de répétition, vont effectivement être uberisables, automatisables, et doivent d'ailleurs l'être : d'abord parce qu'il n'y a pas de raison que le client continue de payer pour des prestations qu'il pourrait obtenir pour moins cher, ensuite pour une question de rentabilité du cabinet. Notre *credo* est en fait de dire que nous allons automatiser ce qui peut l'être, afin de revaloriser notre conseil. Cela nous amène à nous uberiser nous-mêmes. Aujourd'hui la profession s'échine à vendre cher des prestations qui ne valent plus rien. A l'inverse, sur notre plateforme Jurismatic, nous offrons nos contrats gratuitement. Ce qui fait l'avocat aujourd'hui et bien plus demain, c'est un conseil à forte valeur ajoutée: par exemple, savoir quel contrat choisir pour une situation donnée, faire bénéficier son client d'un accompagnement juridique personnalisé, inclure une stratégie juridique dans son développement, faire du droit un avantage économique et un atout concurrentiel, etc. Nous ne sommes plus des faiseurs de contrat, mais nous sommes autre chose et c'est cela que les clients vont chercher.

N'y a-t-il pas, avec la blockchain, un danger en termes de protection des consommateurs, d'absence de responsabilités ?

Il y a effectivement des dangers, qui seront comblés par la pratique, par les cas qui feront jurisprudence. On n'est jamais loin du droit. Pour le moment personne ne comprend ce que c'est, et les juristes encore moins que le reste. Il y aura forcément une autorégulation et même, à terme, une régulation.

Que penses-tu des DAO (Decentralized Autonomous Organisations) ?

Cela peut être une manière de refaire du droit. Je travaille beaucoup sur les communs juridiques et sur l'idée de se réapproprier par le contrat sa propre régulation. Il n'y a là rien de nouveau : le contrat est ce qui permet à des gens de travailler et de collaborer ensemble. Le nom de notre cabinet, 11-100-34, renvoie justement à un article du code civil de 1804 qui dit que "les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites" : en d'autres termes, le fondement de notre cabinet repose sur l'idée que les gens sont acteurs de leur propre droit, et créent leurs propres lois. Dans les DAO les individus pourraient créer leur propre communauté, leur propre charte, leurs propres règles, de façon autogérée et autorégulée. Cela va dans le sens de l'autonomisation des individus.

Interview de Marc Lipskier, Avocat, Fondateur du Cabinet Bamboo & Bees dédié aux entreprises innovantes et aux technologies.

Comment vois-tu la compatibilité entre la blockchain et le droit ?

On a la chance en France d'avoir un droit assez robuste et flexible, et ce d'autant plus qu'entrera en vigueur un nouveau droit des obligations à la fin 2016, qui sera utile pour la blockchain notamment sur les questions de preuves. A mon sens, la valeur probante des blockchains ne devrait guère poser de difficulté en droit positif français.

En effet, tout d'abord, les articles 3-2° et 8 a) du décret du 30 janvier 2013 sur la preuve électronique prévoient la reconnaissance en droit interne français des modes de preuves électroniques d'autres Etats membres de l'Union Européenne. Or, l'Estonie, Etat membre de l'Union Européenne, a annoncé l'utilisation d'une blockchain pour la conservation des dossiers médicaux de ses citoyens. De ce fait, les blockchains deviennent des modes de preuve admissibles dans toute l'Europe.

Par ailleurs, pour ce qui concerne uniquement la France, les articles 1359, 1365 et 1366 du Code civil (dans la rédaction qui entrera en vigueur le 1er octobre 2016) ouvrent grand la porte à la recevabilité des blockchains comme mode de preuve électronique sans qu'il ne paraisse nécessaire de recourir à une validation de la norme probatoire par l'Agence Nationale de la Sécurité des Systèmes d'Information comme c'est le cas actuellement.

Sur les plans du droit civil, du droit commercial et du droit processuel, la blockchain, technologie inédite, ne pose pas de problème juridique radicalement inédit, pour une raison simple : on a derrière nous désormais plus de quinze ans de droit de l'Internet. Toutes les questions qui se sont posées pour construire le droit de l'Internet - quelle est la juridiction compétente, quel est le droit applicable, etc. - ont donc déjà été résolues.

Qu'en est-il des DAO ?

On entend parfois que s'il y a potentiellement des milliers de serveurs qui contribuent à une DAO, il n'y aurait pas de droit applicable. C'est une hérésie puisque le droit français, tant en matière pénale, qu'en matière contractuelle ou en matière quasi délictuelle propose des critères de rattachement au droit français qui n'ont rien à voir avec la localisation ou le nombre de serveurs. Ainsi, en matière pénale, il suffit qu'une victime d'une DAO soit français(e) pour que les juridictions françaises soient compétentes.

Prenons quelques exemples. En matière contractuelle, l'article 4 de la Convention de Rome du 19 juin 1980 sur les obligations contractuelles prévoit que la loi est celle avec laquelle "le contrat présente les liens les plus étroits", c'est-à-dire avec le lieu d'exécution de la "prestation caractéristique". Quatre exceptions sont prévues, en matière immobilière – c'est en ce cas le lieu de situation de l'immeuble qui détermine la loi applicable - , en matière

d'expéditions de marchandises – la loi de l'expéditeur ou la loi du lieu de déchargement sont applicables - , en matière de droit du consommateur - dont la loi du lieu de résidence est applicable, et enfin en matière de contrat de travail – la loi du lieu de prestation habituel du contrat de travail étant applicable.

Ainsi, dans tous les cas où une DAO produirait un dommage contractuel, un rattachement à une loi nationale applicable est possible, indépendamment du nombre et de la localisation des serveurs qui interviennent dans la DAO litigieuse. Il en va de même si la DAO est à l'origine de dommages quasi délictuels. S'applique le principe antique et intangible de la "*Lex loci delicti*", c'est-à-dire de l'application de la loi du lieu de survenue du dommage.

Supposons même que la DAO ou la blockchain serve de support à des objets connectés, dans le cadre de l'Internet des Objets. On aura alors tendance à appliquer la Convention de La Haye du 2 octobre 1973 sur la responsabilité des produits. Cette convention internationale propose quatre critères de détermination d'une loi applicable, dans l'ordre suivant : la loi du lieu du fait dommageable, la loi du domicile de la victime, la loi du lieu du domicile du fabricant ou du producteur, la loi du lieu du distributeur.

Il y a donc nécessairement une loi applicable dont la détermination est possible en fonction de la situation de faits considérés. Bien plus complexe en revanche sera la question de savoir qui poursuivre en justice sur le fondement de la loi dont l'application aura été déterminée. Ce sera l'objet de la jurisprudence à venir.

Qui est responsable en cas de problèmes dans une DAO ?

C'est la question à laquelle on ne peut pas répondre aujourd'hui mais à laquelle les tribunaux répondront lorsqu'ils seront saisis. Mais la question de l'identification des responsabilités dans des systèmes technologiques complexes n'est en rien nouvelle : dans bon nombre de systèmes technologiques imbriqués, les avions par exemple, les juridictions, généralement après expertise technique, finissent par désigner comme responsable tel ou tel acteur parmi la multitude des intervenants. Par exemple dans le cas des logiciels, la jurisprudence au fil du temps s'est aiguillée vers la responsabilité du plus professionnel, parce que c'est le professionnel qui est assuré. Il y a donc des chances qu'on aille dans la même direction.

Au début, la jurisprudence va osciller. Mais elle finira par se stabiliser. On aura déjà résolu les questions essentielles qui sont de savoir quelle est la loi applicable et la juridiction compétente : on ne les résoudra pas en fonction de la nationalité potentielle d'un serveur qui ne nous importe peu, mais en fonction des critères que je viens de vous indiquer. Imaginons que ce soit à l'occasion d'une transaction immobilière : le critère prévu par la loi est le lieu de situation de l'immeuble. Peut-être que tous les intervenants de la DAO seront des serveurs situés partout dans le monde, sauf au lieu de l'immeuble qui constituera l'objet de la transaction. La loi raisonnera alors en fonction de la

situation de l'immeuble. Et de la désignation d'une loi applicable découleront les règles applicables à la situation de fait dont le tribunal est saisi.

Dans le cas des smart contracts, n'y a-t-il pas des problèmes de protection des consommateurs ?

Je ne crois pas, d'abord parce qu'on est encore loin d'avoir des smart contracts susceptibles de s'appliquer à des consommateurs. Les premiers cas de smarts contracts pour consommateurs seront probablement des contrats d'assurance. Comme pour tous les contrats électroniques, il y aura des conditions générales, qui stipuleront que les obligations contractuelles sont telles et telles. Ces conditions générales formeront un premier cadre contractuel qui régira le smart contract. Ensuite parce que le consommateur, en Europe tout du moins, est particulièrement protégé par la loi.

L'automatisation des smart contracts n'est-elle tout de même pas dangereuse pour le consommateur ?

Là encore, la situation des smart contracts n'est pas très différente de celle que nous connaissons depuis l'avènement d'Internet. Le même cadre réglementaire, notamment la directive commerce électronique du 8 juin 2000 et les textes nationaux qui en découlent me semblent suffisants pour protéger le consommateur. Le "consommateur de smart contract" sera protégé comme maintenant et, comme maintenant, il pourra exercer des recours devant ses juridictions nationales en cas de litige.

Si jamais votre opérateur téléphonique, ou votre banque que vous n'avez jamais vue parce que vous avez contracté avec elle en ligne, vous débite trop d'argent, vous irez comme aujourd'hui vous plaindre à la banque, et si celle-ci ne vous donne pas raison, vous saisirez un tribunal, qui pourra constater ou non que la banque a effectivement trop débité. Ce n'est pas parce que la technologie qui sert de support à l'engagement contractuel porte un nouveau nom – smart contract plutôt que commerce électronique – que c'est un phénomène très différent. A l'égard des consommateurs, je ne vois pas grand-chose de différent du point de vue du droit.

Quel est l'apport de la blockchain pour le droit ?

Les blockchains sont un moyen de transporter très facilement de l'argent et de l'information ; plus exactement, d'assimiler de l'argent à de l'information. C'est ça qui fait la nature du smart contract et qui les rend très intéressants conceptuellement. Je ne sais pas encore ce qui en sera déduit du point de vue du droit, mais c'est intéressant comme nouveauté à penser.

Que le droit doit-il faire face à l'émergence de la blockchain ?

Si par "le droit" vous entendez le législateur, rien ; surtout, rien. Laisser les acteurs apparaître et produire des cas d'usage ; laisser le consommateur s'en emparer ; laisser les premières casses se produire pour faire en sorte qu'il y ait de la jurisprudence pour qu'on aille plaider devant les tribunaux. Comme on a

fait dans les années 1990 aux débuts de l'Internet. Si par "le droit" vous entendez le droit concret, libre, produit par les tribunaux, la jurisprudence donc, celle-ci sera en pointe dans l'émergence pratique d'un droit des blockchains.

La loi doit-elle reconnaître les documents certifiés par la blockchain ?

Ce n'est pas nécessaire puisque la loi reconnaît déjà parfaitement la certification électronique des documents. Dont la loi fiscale, d'ailleurs, puisqu'il est dorénavant obligatoire d'être en capacité d'émettre des factures électroniques, et de pouvoir les conserver et attester de cette conservation. Quant à la certification apportée par la blockchain, il s'agit finalement d'horodatage, qui n'a rien de nouveau.

Encore une fois, ce n'est pas parce que c'est un procédé technologique différent que c'est réellement différent du point de vue du droit. Le droit du travail repose déjà en bonne partie sur l'horodatage, en tout cas en ce qui concerne la durée du travail. Ce sont des questions on ne peut plus banales. Il faut simplement avoir le réflexe de penser ces choses-là sur la base du droit existant sans pousser des cris d'orfraies et crier au "vide juridique". Le vide juridique, ça n'existe pas. C'est un réflexe de peur qui conduit à une sur-régulation, sur un trop-plein juridique.

On n'a pas, ou très peu, besoin de normes supplémentaires. Il faut se garder de faire intervenir trop vite le régulateur. Par définition le régulateur a peur. Or quand il a peur, il crée des institutions, qui souvent coûtent cher pour pas grand chose. L'exemple le plus flagrant est l'Hadopi, qui aura existé pendant 6-7 ans et coûté une somme colossale par rapport à son efficacité, pour un problème qui n'en pose désormais plus grâce à la blockchain. Les problèmes posés par le droit de la propriété intellectuelle et la circulation des œuvres sont en effet résolus avec la blockchain. C'est là où le lien entre circulation de l'argent et circulation de l'information est très pertinent, puisqu'on est maintenant capable de savoir avec la blockchain qui est l'auteur de tel élément de propriété intellectuelle, et de conditionner automatiquement l'usage de l'œuvre à un paiement qui peut être instantanément ventilé entre les différents ayants droit. Le problème est résolu par la blockchain, ou plutôt les blockchains.

N'y a-t-il pas un manque de compétences technologiques dans le monde juridique ?

Il y a un manque général en France d'appétence, pour les questions de technologie, comme si elles nous étaient étrangères, alors qu'elles sont permanentes, partout prégnantes. Les questions de traçabilité, de suivi des citoyens, devraient faire hurler tout le monde, mais personne ou presque ne s'insurge, en raison d'un manque de conscience des enjeux en termes de liberté individuelle, et parce que le régulateur est intervenu trop vite, avant que n'arrivent des scandales. Attendons qu'il y ait des cas scandaleux pour que les gens s'en emparent, se rendent devant les tribunaux et obtiennent des condamnations.

Pour qu'émergent des normes cohérentes, du temps doit s'écouler. Pendant cette période de latence entre l'apparition d'une technologie et sa régulation, les acteurs passent des accords avec les plateformes de leur choix pour faire ce qu'ils souhaitent. Si quelqu'un trouve à se plaindre, il va voir le juge et le juge tranche au regard du droit actuel, qui est suffisant. La solution est donc bien le juge : c'est celui qui est le plus proche des besoins et nécessités des parties qui ont éventuellement à se plaindre. Aussi longtemps que les parties ne se plaignent pas, où est le problème ? Le principe de l'Etat de droit, c'est que tout est autorisé sauf ce qui est interdit. Si les choses sont autorisées et qu'elles ne portent préjudice à personne, c'est-à-dire que personne ne s'en plaint devant le juge, pourquoi faudrait-il que l'autorité réglementaire ou le Parlement intervienne ? Et si des parties se plaignent devant un juge, l'océan du droit positif suffit à trancher l'essentiel des cas avant que le législateur n'ait éventuellement à intervenir.

Regards croisés sur la blockchain

Nicolas Loubet, Expert de l'écosystème blockchain. Il a notamment cofondé Cellabz, un accélérateur d'écosystème technologique.
Marc Tirel , Chercheur spécialiste des mutations sociales et des mouvements émergents, et auteur de l'ouvrage "Voyages en Emergences".

Quel regard portez-vous sur la blockchain ?

Nicolas : Il faut regarder derrière la blockchain, ce qui se joue dans les marges. Arrêtons de regarder le futur, soyons dans le présent : que peut-on faire ensemble ici et maintenant ? C'est cette question-là qui doit nous guider, en tant que citoyens, vis-à-vis de la blockchain, et non la question de savoir quand est-ce que la blockchain arrivera, quand est-ce qu'on fera des choses avec, etc.

Lorsque la catastrophe de Fukushima est arrivée, Joi Ito (entrepreneur japonais, aujourd'hui directeur du MIT Media Lab) a construit un collectif qui a permis de créer un capteur libre, open source, open hardware. Ce n'est pas l'Etat japonais qui a pris ces mesures ; ce sont des citoyens comme vous et moi. Il existe maintenant au Japon plus de 17 millions points de mesure, qui ont été construits par des citoyens, des autodidactes, des non-experts qui se sont formés. Et ce phénomène a largement dépassé les frontières du pays.

Voilà le type de phénomènes que la blockchain peut démultiplier. Et c'est en cela que la blockchain est intéressante d'un point de vue citoyen. La blockchain n'est qu'une technologie parmi beaucoup d'autres. De nombreux mix sont envisageables. La chance qu'on a, c'est que ce sont des biens communs, c'est-à-dire des ressources partagées, qui engagent un certain nombre de contributeurs, et avec des règles et processus définis par une communauté. Les blockchains comme Bitcoin et Ethereum reposent sur les principes des communs; on peut même dire qu'elles constituent des biens communs. Il est pour cela essentiel d'aller chercher les zones d'utopie, où des gens qui ne sont pas experts s'approprient la notion de blockchain, dans les universités, les espaces de communauté, etc.

Marc : La blockchain produira-t-elle du bien commun ou sera-t-elle accaparée par les grandes entreprises actuelles ? Voilà la question que je me pose actuellement. Je n'ai pas l'impression que les pouvoirs publics en France ont compris l'enjeu d'intérêt public. L'initiative annoncée fin mars par le cabinet d'Emmanuel Macron se focalise au secteur financier [un assouplissement de la législation pour permettre une expérimentation dans le cadre des "mini-bons", dans une optique de financement plus souple des PME] ; du reste la BNP a annoncé juste après le lancement d'un projet à ce sujet.

Or à mon sens l'Etat devrait plutôt réfléchir à l'idée de développer des services publics fonctionnant grâce à la blockchain. Il serait par exemple intéressant d'envisager la mise en place d'un Blablacar public de la blockchain.

Nicolas : Le gouvernement britannique a d'ailleurs sorti en janvier un très bon rapport sur la blockchain, qui soulignait l'opportunité de repenser le secteur public, le rapport à l'Etat, grâce à cette technologie. Ce rapport est passé assez inaperçu en France, ce qui est dommage.

Quels sont les aspects de la blockchain qui vous intéressent ?

Marc : Le plus intéressant dans la blockchain n'est à mon sens pas la technologie elle-même mais bien son potentiel. Ses promesses font rêver, or beaucoup de gens ont justement besoin de rêver à un nouveau monde. Le potentiel en germe de la blockchain est au moins du même acabit que celui d'Internet, or on sait qu'Internet a bouleversé un certain nombre de choses. Ce potentiel est même peut-être plus important encore, car la blockchain est de nature à bousculer le modèle capitaliste tel qu'on le connaît aujourd'hui. Bien sûr, nous en sommes encore loin : nous n'en sommes qu'aux balbutiements. Mais on pourrait tout à fait imaginer une mutation du capitalisme, ou l'émergence d'un système en parallèle.

Quand une entreprise veut innover, elle a le choix d'innover en interne, ou de travailler avec une start-up. De la même façon, on peut soit vouloir faire changer le capitalisme de l'intérieur, soit tenter de faire naître un nouveau système par ailleurs. La blockchain pourrait contribuer à la mise en place de ce nouveau système. Il s'agirait de revenir en quelque sorte aux sources d'Internet pour arriver à une meilleure répartition des richesses.

A mon sens, un enjeu clef est de savoir comment réussir à faire comprendre la blockchain sans perdre de sa richesse, de sa complexité. Je pense que cela passe par le jeu, le ludique, et l'art. Si on arrive à faire en sorte qu'il y ait un enthousiaste qui aille au-delà du monde business, pour investir le champ de la passion, de l'art, du beau, on aura réussi quelque chose d'intéressant. Pensons par exemple le Plantoïd construit par Primavera de Filippi[40].

Nicolas : Je partage entièrement ton avis. Les utilisations les plus insolites des innovations relèvent de l'hybridation technologique et artistique, bien qu'elles restent assez peu visibles car peu portées par les relations publiques. Le Plantoïd est en ce sens un extraordinaire cas d'usage de la blockchain. Participer à ce type de projets permet d'apprendre énormément, sur des domaines très divers, au-delà de la blockchain elle-même : monnaie, électronique, biomimétisme… le tout de façon très pédagogique, sur des bases interdisciplinaires, de libre pensée.

Pensons aussi au Projet "Tree Coach", qui vise à mettre en lumière les arbres comme êtres vivants, et à les faire communiquer entre eux, *via* une blockchain. Le principe est de donner à chaque arbre une identité inscrite sur la blockchain et de créer des cadres de gouvernance différents, sans organe centralisateur, afin de rendre visible le fonctionnement invisible d'une forêt et questionner les processus de déforestation. L'idée derrière, c'est de tenir compte de la réalité

[40] Le Plantoïd est à la plante ce que l'androïd est à l'humain : à mi-chemin entre une œuvre d'art, une plante et un robot, il détient un compte sur la blockchain, reçoit des dons, et est capable de se reproduire en émettant un appel d'offre auquel des artistes peuvent répondre pour réaliser leur propre plantoïd.

biologique d'un écosystème, là où les cadres de gouvernance actuels sont très anthropocentrés. Il s'agirait donc de donner un pouvoir de gouvernance à ces entités pour changer les itinéraires qu'on veut emprunter en termes de transition écologique. Un projet comme celui-ci résiste à toutes les formes de stress économiques traditionnelles.
Pour compléter le propos de Marc, je suis convaincu que ce sont comme bien souvent les plus jeunes qui ont l'esprit le plus vif et le plus pointilleux sur le système actuel et ses évolutions. Je pense là à des enfants de 10-12 ans qui jouent à Minecraft [jeu vidéo de construction et d'exploration, comptant plus de 100 millions d'utilisateurs dans le monde, et utilisé comme outil pédagogique par de nombreux enseignants en mathématique, histoire-géographie, biologie…] et sont vigilants et malins dans la manière d'interroger nos économies.

Vitalik Buterin [fondateur d'Ethereum] a écrit à 17 ans, dans la revue Bitcoin Magazine qu'il a fondée, un de ses articles qui m'a le plus étonné. C'est le tout premier article qu'il a écrit. Il y parle de l'adoption de Bitcoin. Son propos est le suivant : pour la majorité des individus qui vivent avec des cartes de crédit, prêts et hypothèques, c'est une souffrance d'aller vers le Bitcoin. Mais ce dont on ne se demande pas, c'est si ce n'est pas une souffrance pour les nouveaux venus, les nouveaux entrants, de rentrer dans ces systèmes-là[41].

Que peut-on attendre de la blockchain pour les années et décennies à venir?

Marc : Beaucoup de tâches et de fonctions pourraient être déléguées à des systèmes informatiques, sur lesquelles repose la blockchain. Mais laisser les machines et les intelligences artificielles décider de tout comporte des risques. On en est de toute façon encore loin, mais il faut y réfléchir en amont. Surtout, plus encore qu'y réfléchir, il faut tester, faire des expérimentations, non pas aveuglement en se disant qu'on a trouvé LA solution, mais avec pragmatisme.

La blockchain va à mon avis solutionner un certain nombre de problèmes, notamment des questions de corruption, qui ne se poseront plus pour les générations futures. Il y a bien sûr un enjeu immense dans le domaine de la finance, au niveau de la traçabilité de l'argent ; on l'a encore vu avec les Panama Papers. Mais évidemment on trouvera aussi beaucoup de gens pour lutter contre ces changements, car ces derniers remettent en cause des positions, des privilèges.

Nicolas : Si on voit uniquement la blockchain comme une technologie devant servir à résoudre des problèmes, on se trompe d'emblée dans la façon de

[41] Verbatim : *« Les adolescents représentent l'avenir. Ils ne sont pas encore embourbés par la façon dont nous menons actuellement nos vies, avec nos cartes de crédit, prêts, hypothèques, etc. Alors que pour la plupart des gens, passer au Bitcoin est une souffrance à court terme car ils sont déjà à l'aise avec le fait d'utiliser des cartes de crédit, pour les adolescents c'est à l'inverse tout le processus d'ouverture de compte et de carte de crédit qui leur pose problème. Ils préféraient simplement pouvoir commencer à gagner et dépenser quelques « coins ». En outre, ils ne sont pas encore corrompus par la psychologie du système de carte de crédit, qui veut qu'il est bien plus simple d'obtenir de l'argent rapidement et temporairement en suppliant plutôt qu'en produisant. La psychologie que ces jeunes adopteront sera, dans 10 ou 20 ans, celle qui conduira la psychologie de la société. »*
Vitalik Buterin, https://bitcoinmagazine.com/articles/bitcoin-adoption-opportunity-teenager-1330407280, 28/02/2012

l'aborder. Voir dans la blockchain une solution aux problèmes de gouvernance, c'est oublier les deux siècles qui nous ont précédé. Heureusement, grâce à tous les flops qu'on a connus ces dernières années et décennies, on commence à avoir une bonne approche vis-à-vis de l'innovation, pas seulement technologique. On sait notamment maintenant qu'il faut faire attention à l'appropriation, ou aux principes d'inclusion (par exemple je n'attends pas que le fondateur de Slock.it me dise comment utiliser les smart contracts : j'attends qu'il soit ouvert). On a parfois été dans des impasses intellectuelles mais l'important est d'en tirer les leçons.

Il faut considérer la blockchain au sein d'une vision systémique, et non pas comme une opportunité de marché pour prendre le pouvoir. Le basculement réside vraiment dans cette vision systémique, et non dans la technologie elle-même. Ce qui est intéressant, c'est de s'interroger sur la valeur de tous ces métiers qui ont permis aux institutions traditionnelles d'exister, que ce soit la Banque de France, la Caisse des Dépôts... La Caisse des Dépôts a 200 ans. Est-ce qu'elle existera encore dans 200 ans ? 20 ans ? 2 ans ? Personne ne peut répondre par l'affirmative avec certitude. Tous les fondamentaux sont remis en question.

Ce qui est vu comme prévisible et robuste doit toujours être interrogé. A-t-on profondément confiance dans les formes d'autorité qui paraissent aujourd'hui légitimes dans tout un ensemble de nos vies (en ce qui concerne par exemple l'aménagement du territoire, le montant de TVA, etc…) ? C'est ça qui est en défi depuis au moins 10 ans.

Nicolas, toi qui connais bien l'écosystème blockchain, quel est ton regard sur le projet Ethereum et plus particulièrement sur son fondateur, Vitalik Buterin ?

C'est intéressant de comparer les conditions d'émergence de Bitcoin et celles d'Ethereum car elles sont très différentes : pour Bitcoin, elles se caractérisent par le foisonnement et l'imprévu, alors que pour Ethereum, elles sont très scolaires, tout un ensemble d'articles ont précédé, dont les anciens articles de Vitalik qui avait été le cofondateur de Bitcoin Magazine et qui a arrêté ses études pour se concentrer à plein temps sur ces sujets.

Avec la campagne de prévente, la création du wiki, les forums très instruits, etc., on a l'impression que Vitalik est le bon élève, qu'il a 20/20 du début à la fin. Quand on met en confrontation ces histoires, on a presque l'impression que Bitcoin est né par hasard (je grossis volontairement le trait), alors qu'Ethereum semble un projet quasiment académique, avec des étapes successives très construites. La gouvernance d'Ethereum, tout comme pour Bitcoin, est certes loin d'être idéale, mais les core developers se sont mis d'accord sur un cap, une feuille de route dessinée sur 3 à 4 ans. Au-delà, les questions sont encore ouvertes, et relèvent de la recherche.

Vitalik semble parti pour travailler toute sa vie dessus. Dans un contexte où on est confronté à des impératifs de délivrables de très court terme, il a une sérénité du temps long qui est bluffante. Il porte une vision de très long terme,

qui consiste à travailler sur quelque chose qui dépassera les contingences de la mode. Dans le monde de la technologie contemporaine, c'est très rare.
Il y a finalement peu de différences entre un Vitalik Buterin et un Elon Musk. Ce sont des gens passionnés, qui s'amusent dans ce qu'ils font, qui sont portés par des projets avec une réalité matérielle, et qui vivent leur passion à plein temps, pas seulement le soir en rentrant du travail. Quand Vitalik dit qu'il a arrêté l'université parce qu'il passait beaucoup de temps sur Bitcoin, c'est un choix de raison. Il s'est auto-éduqué, a appris, s'est mobilisé dans une communauté de pairs… Il a une plasticité qui fait sa force, et n'hésite pas à reconnaître quand il se trompe ; du reste je ne l'ai jamais vu se fâcher.

Chose intéressante : il a décidé d'apprendre le mandarin. C'est très malin puisqu'il s'ouvre ainsi à 1,6 milliards de personnes en plus. La DevCon2, en septembre, aura du reste lieu à Shanghai. Ce n'est pas un choix anodin.

Alors que la plupart des évangélistes technologiques sont clivants et affirment qu'il y des choix à faire (par exemple "le Bitcoin, ou rien"), Vitalik a une plasticité et une ouverture qui font sa force.

A titre personnel, l'idée que la blockchain s'impose partout ne me plaît pas, et même me déplaît profondément. Je dois dire que j'ai été très rassuré par Vitalik, ainsi que par l'équipe de Slock.it.

4

LA BLOCKCHAIN VUE DE L'INTERIEUR : LA PAROLE AUX ACTEURS

Interview de George Hallam, Directeur des relations publiques de la Fondation Ethereum

D'où viennent les développeurs d'Ethereum ? Viennent-ils du monde du bitcoin ?

> Il y en a seulement quelques-uns qui viennent de l'univers bitcoin, peut-être environ 10 % ou 20 %, mais la majorité ne vient pas du tout de cet univers : ils ont travaillé auparavant sur d'autres technologies, ce qui est positif car cela nous permet de compter sur une diversité de savoirs très intéressante.
> A l'origine, Ethereum comptait un certain nombre de personnes auparavant impliquées dans le bitcoin, mais après avoir levé nos 18,4 millions de dollars [en 2014], nous avons engagé certains des meilleurs développeurs du monde (pour construire la meilleure blockchain du monde, il nous fallait les meilleurs développeurs qui soient) donc nous avons ouvert les profils à des horizons très différents.

Recevez-vous beaucoup de candidatures de développeurs qui voudraient intégrer la Fondation Ethereum ?

> Nous recevons des multiples candidatures de façon permanente, mais généralement ces personnes souhaitent s'investir dans la communauté Ethereum en général [et non la Fondation spécifiquement]. Nous avons travaillé dur pour que les développeurs puissent facilement se mettre à coder sur Ethereum ; beaucoup de documentation leur est accessible. C'est aujourd'hui relativement facile pour une organisation avec une communauté interne de développeurs de s'auto-former sur le sujet. A la Fondation Ethereum nous essayons de rester en dehors des activités de consulting que font certaines organisations : ce n'est pas notre rôle et nous préférons voir la communauté utiliser les ressources disponibles.

Comment fonctionne la gouvernance d'Ethereum ?

A l'origine le développement du protocole était seulement porté par la Fondation Ethereum, mais il existe maintenant de nombreux groupes extérieurs qui construisent des clients Ethereum comme Ethcore, ConsenSys, Ether.Camp etc. Pour cette raison, nous étudions actuellement différents scénarios. Ce que nous souhaitons faire, c'est donner à chacun une voix et une opportunité de discuter de la façon dont le protocole doit changer à l'avenir, tout en conservant notre capacité à faire avancer et se développer Ethereum.

Avec le bitcoin, la gouvernance est devenue une question très sérieuse ; sa technologie n'a pas réussi à se développer à une vitesse suffisante. Nous ne voulons pas connaître les mêmes problèmes durant le développement continu d'Ethereum. C'est pour cela que nous souhaitons faire avancer cette technologie du plus vite que nous pouvons mais de la façon la plus sécurisée possible dans le même temps. La sécurité reste extrêmement importante à nos yeux.

Chez Ethereum nous ne croyons pas forcément aux deadlines ; quand vous travaillez sur un système comme le nôtre, où l'aspect transactionnel est essentiel, la sécurité ne doit pas avoir de deadline, elle doit simplement être certaine. Si quelque chose se produit qui doit requérir toute notre attention, nous devons lui accorder cette attention pour que le système continue d'être sûr. C'est pour cela qu'on préfère ne pas indiquer de chiffres précis sur les dates de sorties des prochaines versions.

La blockchain Ethereum est-elle désormais fiable en termes de sécurité ?

Absolument. Pour la sortie de la première version, "Frontier" [août 2015], nous savions qu'il y avait encore quelques bugs à résoudre, ce qu'on a annoncé très clairement pour que les gens soient bien au courant. Et effectivement nous avons notamment connu un bug fin août 2015 ; mais nous avons pu identifier le problème et le traiter très rapidement. Personne n'a perdu d'argent à ce moment-là.

Quand nous sommes passés à notre version actuelle, "Homestead" [mars 2016], nous avons retiré le "warning sticker" de notre site, car nous étions bien plus certains de la fiabilité du réseau. C'est pourquoi nous avons abaissé le temps de confirmation d'une transaction à environ 3 mn. Dans Ethereum, chaque bloc est validé en 14 secondes environ contre 10 minutes dans le Bitcoin. Dans le Bitcoin, vous devez attendre 6 confirmations, soit 1h, pour qu'une transaction soit bel et bien confirmée, contre 3 minutes pour Ethereum. Nous travaillons avec de nombreux chercheurs en sécurité dans diverses universités du monde, et nous avons dépensé beaucoup d'argent en audit de sécurité avant la sortie de la première version. Les auditeurs ont travaillé main dans la main avec nous pour s'assurer qu'il n'y avait pas de problèmes importants.

Nous avons aussi un programme très actif où quiconque trouvant un bug peut être rémunéré en échange des informations trouvées. Notre souhait est

d'inciter toujours les gens à collaborer avec nous pour rendre Ethereum sécurisé.

Quelles sont les prochaines étapes pour Ethereum ?

Nous avons une certaine idée de là où nous allons pour ces cinq prochaines années. Nous avons en effet assez d'argent pour ne pas avoir à chercher d'autres sources de financement pendant environ cinq ans.

En étant réaliste, la plupart de notre travail de recherche est focalisé sur les deux trois années à venir. Il implique notamment le passage du Proof-of-work au Proof-of-stake[42], ainsi que des recherches sur le passage à grande échelle, sur le "sharding", et sur l'idée que chaque nœud du réseau n'ait plus nécessairement à valider chaque transaction.

Pour notre prochaine version, intitulée Metropolis, nous essaierons de faire en sorte qu'il soit bien plus simple pour des utilisateurs moyens d'interagir avec l'écosystème Ethereum. Ensuite, normalement en 2017, d'une part nous sortirons la version Serenity où nous commencerons à appliquer les résultats de nos recherches sur le passage à grande échelle, d'autre part nous basculerons vers le Proof-of-Stake. A partir de là, nous passerons à l'Ethereum 2.0, qui constituera le moment où le réseau commencera véritablement à grandir très rapidement, puis Ethereum 3.0, etc.

Dans l'année qui vient, nous serons probablement focalisés en grande partie sur nos recherches sur le passage à grande échelle, parce qu'il s'agit d'un des principaux enjeux du monde des crypto-monnaies à l'heure actuelle, et c'est quelque chose que nous pensons pouvoir résoudre : permettre à des milliards d'utilisateurs d'accéder à la blockchain et d'interagir avec elle, au-delà d'être simplement spectateurs.

Quelles applications vous semblent les plus prometteuses ?

Question difficile tant la palette d'applications possibles d'Ethereum est large… En termes de ce qui est déjà en train d'être construit, je suis avec attention les projets de marchés prédictifs, Augur et Gnosis, qui sont très intéressants. Je pense qu'ils veulent lancer leur première version pour les élections américaines. Leur version est encore en bêta ; ils travaillent pour résoudre certains bugs.

Slock.it repousse toujours plus loin les limites : ce qu'ils font est impressionnant. Ils ont développé des partenariats avec des structures importantes comme Samsung et RWE, et ils peuvent compter sur un groupe très solide de développeurs.

[42] Voir le Lexique en fin d'ouvrage pour les explications sur ces deux mécanismes. Le fait de passer au Proof-of-Stake doit permettre à Ethereum de réduire fortement la consommation énergétique de son réseau. Le Bitcoin utilise le Proof-of-Work ce qui lui vaut des critiques sérieuses pour le gaspillage d'électricité qu'il engendre.

Je suis aussi très impatient de voir ce que donneront les projets dans le domaine énergétique, en particulier Transactive Grid à New York. Le but est de permettre aux gens qui possèdent des panneaux solaires, des petites éoliennes, de faire partie d'un véritable réseau d'énergie décentralisé. En termes de résilience je pense que c'est incroyable et que ça constitue le futur du marché de l'énergie.

Quels sont les pays qui dirigent le mouvement blockchain dans le monde ?

Je pense que le Royaume-Uni a développé une approche à la fois proactive et intelligente car non-interventionniste en termes de législation et de régulation de la blockchain. Les membres de l'UKDCA (l'Association britannique de monnaies numériques) ont beaucoup travaillé avec les politiques et les législateurs pour que ceux-ci comprennent ce dont il est question et pourquoi cette technologie va être importante pour l'économie britannique à l'avenir. Grâce à ce travail, les politiques ont été très ouverts sur le sujet.

De la même façon, à Singapour le gouvernement est très avant-gardiste. Il a compris l'importance de la Fintech pour le futur de Singapour, et est par conséquent très désireux de s'impliquer dans la blockchain.

Concernant les Etats-Unis, c'est bien entendu un pays majeur du secteur de la blockchain. Si vous regardez sur ethernodes.org, vous verrez que la très grande majorité des nœuds du réseau Ethereum sont situés aux Etats-Unis. En revanche, la Bitlicense instaurée par l'Etat de New York [qui encadre strictement les activités liées aux monnaies virtuelles] est prohibitive, et la structure juridique Etat par Etat peut être frustrante pour ceux qui veulent développer des activités dans tout le pays.

De grands groupes aux Etats-Unis comme Microsoft travaillent de près avec l'écosystème Ethereum. Mais les Google, Amazon etc, n'ont pas l'air de faire quelque chose avec la blockchain.

C'est étonnant, comment l'expliquez-vous ?

Je pense qu'ils attendent peut-être que les applications blockchain soient utilisables à grande échelle. Une grande partie de leurs revenus provient des internautes grand public, or la blockchain n'est pas encore prête à ce niveau : il n'est pas encore possible de répondre à la demande pour la base d'utilisateurs de Google par exemple. Mais je pense tout de même qu'ils réfléchissent à la question, sans communiquer dessus ; du reste, parmi les personnes qui développent des choses intéressantes sur Ethereum, certains d'entre eux sont d'anciens employés d'Apple ou de Google.

Pour le moment, ce sont plutôt les grands groupes financiers qui s'intéressent à la blockchain, comme le montre les initiatives du consortium R3 [qui inclut une quarantaine de grandes banques mondiales, dont Goldman Sachs, Barclays, UBS…et travaille à la mise en place de standards communs], de JP Morgan [qui a annoncé avoir testé un transfert d'argent *via* la blockchain pour 2000 de leurs clients], etc.

Comment voyez-vous la France ?

> Cela se passe bien, il y a des progrès. Stratumn a récemment levé 600.000 euros; désormais il faut qu'ils fassent encore plus parler d'eux. La barrière de la langue est peut-être un enjeu. L'anglais est la première langue dans le domaine de la blockchain. Mais bientôt le mandarin prendra une place importante.

Quelle est votre position sur le débat autour des blockchains privées ?

> Le débat autour des blockchains publiques et privées ne doit pas être binaire. Il y a tout un spectre de différentes choses. A court terme, quand la confidentialité est nécessaire, les blockchains privées permettent des premières opportunités - notamment pour les institutions financières - au regard des obligations légales en termes de protection des données et de vie privée des clients. Par exemple, on peut imaginer une blockchain de banque capable de communiquer avec une blockchain publique. Cela signifie qu'une sidechain Ethereum/Bitcoin pourrait être construite, avec certains critères imposés mais certains avantages de la blockchain Ethereum tout de même conservés. En revanche je ne trouve pas que les blockchains purement privées apportent une énorme valeur ajoutée.

Quels secteurs seront les plus concernés par la blockchain à votre avis ?

> Si la blockchain concrétise toutes ses promesses, alors pratiquement chaque secteur sera affecté. On peut penser par exemple à la finance bien sûr (settlement, chambres de compensation…), mais aussi au secteur caritatif, dont on parle moins mais qui a besoin de transparence, ou encore à la supplychain, même s'il faudra encore des humains puisque les données inscrites sur la blockchain ne sont bonnes que si les humains qui les ont inscrites le sont, ce que les gens ont parfois tendance à oublier ! Je pourrai en citer de multiples autres, notamment l'économie du partage où l'on peut imaginer un Uber décentralisé géré par une DAO, mais à mon avis, les meilleurs cas d'usage n'ont probablement pas encore été inventés.

Interview de Gavin Wood, Cofondateur d'Ethereum et Fondateur et actuel CTO de Ethcore.

Quelles sont les différences entre Ethcore et la Fondation Ethereum ?

> Je dirais que la Fondation Ethereum a pour buts d'éduquer et de faire avancer le protocole. Chez Ethcore, nous nous situons essentiellement entre le protocole et les applications business ; le fossé est assez large. Nous construisons la couche nécessaire aux applications business.

Les règles d'Ethereum sont-elles définies par la Fondation ?

> Les seules personnes qui peuvent pousser des solutions sont les nœuds du réseau. A de nombreux égards, la fondation n'a pas de pouvoir face à une volonté de changement. C'est la même chose que dans le Bitcoin à ce niveau-là ; les seules personnes qui peuvent faire changer le protocole sont les mineurs. C'est pareil pour Ethereum.

Quels types d'applications blockchains vois-tu prendre de l'ampleur ?

> Comme aux débuts d'Internet, il est nécessaire d'avoir une certaine infrastructure avant que les applications soient utilisées à grande échelle. Par exemple, détenir des tokens qui gardent une valeur stable est essentiel avant de développer des choses en *crowdfinance* ou *crowdbanking*. Ces exemples deviendront importants, de mon point de vue, mais probablement pas avant un moment pour une question d'infrastructure.
>
> La chose la plus disruptive dans un avenir très proche à ma connaissance réside dans les marchés prédictifs sur Ethereum. Les marchés prédictifs pourraient bouleverser un certain nombre d'aspects de notre société, par exemple les élections en politiques.
>
> Je peux aussi penser aux contrôles d'accès des ressources du monde réel : construire des cas d'usage autour de cela pourrait être intéressant.
> Concernant l'assurance, je pense que cela prendra un peu plus de temps car cela nécessitera d'abord d'avoir une stabilité dans la valeur des tokens.

Penses-tu qu'il y a une bulle autour de la blockchain qui ne serait pas justifiée ?

> Nous sommes dans le cycle de la hype, mais on ne sait pas combien de temps celle-ci va durer. Cela étant, je pense qu'il y a fondamentalement quelque chose de spécial dans la technologie blockchain. Elle permet d'une certaine façon à des gens qui sont connectés par internet de faire des affaires directement entre eux ; dans l'histoire de l'humanité, c'est quelque chose qui a seulement été possible dans la société en général par le biais d'un intermédiaire de confiance. Désormais, de façon inédite nous avons un moyen de le faire sans intermédiaire de confiance. C'est le cœur de la proposition de valeur de la blockchain.

Que penses-tu des blockchains privées ?

> Je pense qu'elles ont un rôle ; cependant un registre privé doit nécessairement conserver une relation de confiance. Dès lors j'ai des doutes sur l'apport substantiel d'une blockchain privée comparé à un système IT standard. Cela étant, je reste ouvert d'esprit. Mais *in fine*, je pense que ce type de blockchain restera à un coin de l'histoire, et que la réelle avancée proviendra des chaînes publiques.

A propos des pouvoirs publics : penses-tu qu'ils ont un rôle dans le développement de la blockchain ?

> C'est possible mais ce n'est pas très clair. Je pense que quand les organisations veulent aider, c'est génial, mais ce qui n'est pas clair pour moi est la façon dont cela pourrait fonctionner étant donné la nature très décentralisée de cette technologie et la nature très libertaire de ses participants. Ce qui est en tout cas essentiel, c'est que les pouvoirs publics ne nuisent pas au développement de la blockchain.

Interview de Stephan Tual, Cofondateur de Slock.it

Quel message faut-il faire passer aujourd'hui à ceux qui veulent comprendre la blockchain ?

> La première chose à faire, c'est de faire attention aux amalgames. L'affaire de MTGox[43] a causé beaucoup de tort à Bitcoin par exemple, parce qu'il y a eu amalgame entre les applications de la technologie et la technologie elle-même. Au-delà de cet exemple, les médias se sont acharnés sur Bitcoin pour de nombreuses raisons, qui n'étaient jamais les bonnes : l'achat d'armes, de drogue… qui non seulement ne sont pas de vrais arguments contre Bitcoin, mais créent en plus un amalgame destructeur dans l'esprit du grand public. Dans mon entourage, les premiers retours que j'ai eus en parlant de Bitcoin, avaient tous trait à la drogue...
>
> En tant que communauté, c'est ce genre de chose qu'on essaye absolument d'éviter, et notamment chez Slock.it. On a demandé par exemple à Vitalik *[Buterin, le fondateur d'Ethereum]* d'aller lui-même revoir nos smart contracts, pour ne pas entrer dans l'histoire comme la société qui lèverait 30 m$ et qui les aurait perdus dans la foulée. Si une application aussi emblématique pour le réseau qu'est Slock.it se retrouvait dans cette situation, les conséquences en matière d'image pour tout le projet seraient redoutables.

Un mot sur la France ?

> La communauté française est remarquable, parce que très active. Le paradoxe français, c'est que même si les gens sont moins nombreux qu'au Royaume-Uni, ils sont bien plus actifs. Répéter sans cesse que l'on est mauvais est un peu une spécialité nationale, mais en réalité on se rend compte que dans la blockchain comme ailleurs, il y a bien des domaines où on les français ont une longueur d'avance...
>
> Pour illustrer cette bonne dynamique, je peux même donner un exemple concret. Je me souviens que lorsque le slack[44] Slock.it comptait à peu près 1500 utilisateurs, il s'y échangeait moins de messages que sur le slack de CryptoFr[45] qui devait au même moment compter une quarantaine de membres. Cela montre à quel point en France les gens peuvent être actifs, par rapport à l'Angleterre où il y a davantage d'observateurs.

Quel est pour toi le rôle à venir des pouvoirs publics dans la blockchain ?

> Ils ont un rôle énorme à jouer. Par exemple, ma situation parle d'elle-même : vers mes 18 ans, à l'époque où je voulais absolument monter ma boîte pour faire du web, lorsque je lisais des magazines comme Wired, je me rendais bien compte que tout se passait aux Etats-Unis. En France, en revanche, on voulait

[43] Mt. Gox a été pendant un moment la plus importante plateforme d'échange de Bitcoins en volume; elle a été placée en liquidation en avril 2014 après avoir révélé la perte de près de 650 000 bitcoins, soi-disant suite à une attaque. Son PDG, soupçonné d'avoir aidé au détournement, a été arrêté en août 2015.
[44] Slack est un outil de travail collaboratif, très prisé dans l'univers des start-up et des makers.
[45] CryptoFR est la principale communauté francophone regroupant les passionnés du Bitcoin, de la blockchain et des crypto-monnaies, notamment grâce à ses forums et son slack.

en rester au minitel. C'est une des raisons pour lesquelles je suis parti de France, et je n'y suis plus retourné, en tout cas pour travailler.

Quand je vois que l'intégralité de mes amis d'enfance sont aussi partis de France pour bosser à l'étranger, je trouve que c'est dommage. Je me demande aussi si aujourd'hui en 2016 on ne risque pas d'avoir le même phénomène : des jeunes, peut-être de l'Ecole 42 ou peut-être d'ailleurs, qui travaillent sur ces sujets-là et parce qu'ils se disent que ça n'avance pas assez vite en France, songent à partir. Pour éviter qu'ils ne partent en Angleterre, en Allemagne, ou dans n'importe quel pays dont les régulations seraient plus accueillantes vis-à-vis de leurs projets, les pouvoirs publics ont effectivement un rôle important à jouer. L'enjeu, finalement, c'est tout simplement d'éviter un second *brain drain*.

Ce que tu dis, c'est qu'il faut empêcher la régulation de limiter la création d'entreprises sur ces sujets ?

Exactement ! Prenons un exemple concret. Supposons une boîte qui essaierait d'utiliser la blockchain en tant que système de gouvernance pour une société qui n'aurait rien à voir avec la finance, par exemple une société qui ferait de l'import-export. C'est-à-dire qu'elle n'utilise la blockchain qu'en interne, pour ses processus, et pas du tout dans ses produits. Que se passera-t-il ? Elle va tenter d'ouvrir un compte en banque qu'on lui refusera, à cause de l'équation absurde blockchain = bitcoin = argent sale.

Ce n'est pas un exemple dans le vide. En Angleterre à l'époque, quand Ethereum projetait de se structurer et d'embaucher du monde sur place, l'ouverture d'un compte en banque a été refusé, simplement parce que les banquiers avaient vu sur le site web qu'il y avait eu une levée de fonds en bitcoins. En France, d'après les échos que j'ai eus, la situation est un peu similaire. Un signal du gouvernement sur ces sujets aiderait énormément.

Il y a malheureusement d'autres cas pratiques à donner. Pour financer son projet d'Ethereum Computer[46], Slock.it va demander à la The DAO un financement d'environ 30 millions de dollars. La question qui se pose est en fait la suivante : que mettre sur la facture ? DAO, domicile : la blockchain ? Dans la plupart des pays d'Europe, l'adresse est une condition *sine qua non* pour produire une facture… Dans les faits, il a fallu faire transiter les fonds par une société Suisse, où la législation n'a pas les mêmes contraintes, pour que notre société de droit allemand puisse obtenir son financement en toute légalité. C'est le genre d'obstacles idiots qui peuvent faire gagner ou perdre beaucoup d'argents à un État. La question, ce n'est pas les taxes, parce que ça me semble normal de payer des taxes, blockchain ou pas blockchain. C'est de savoir si les législations sont adaptées ou pas.

[46] L'Ethereum Computer est le premier produit que souhaite développer Slock.it. L'idée est de centraliser au sein de chaque foyer dans l'Ethereum Computer le dialogue entre les différents objets intelligents et la blockchain Ethereum.

Pour toi il y a une bulle autour de la blockchain ?

> Il y a une hype de la blockchain, mais je ne dirais pas forcément qu'il y a une "bulle". Une bulle sous-entend qu'il y aurait un surinvestissement, avec des valorisations d'entreprises trop importantes, ce que je n'ai pas observé de mon côté. Par contre, j'ai vu beaucoup de gens qui parlaient de la blockchain comme si c'était une solution miracle, alors que ce n'est pas du tout le cas.
>
> Il ne faut pas tomber dans le solutionnisme : il faut trouver les cas d'usage qui seront bien adaptés à la blockchain, ou plutôt vice versa, raisonnablement. Il y a un danger je pense à laisser croire aux gens qu'à chaque problème on va pouvoir utiliser la blockchain pour tout résoudre, à la façon d'une poudre magique. C'est dangereux, parce que tous ces gens vont être très déçus, et il y aura nécessairement une sorte de sur-réaction négative par la suite qui les poussera à jeter le bébé avec l'eau du bain.

On annonce beaucoup de choses autour de la blockchain. Est-ce qu'au milieu de ces effets d'annonce il y a des cas d'usage qui te semblent surfaits?

> Oui il y a effectivement beaucoup d'effets d'annonce. Il ne faut pas perdre de vue que la blockchain est limitée pour deux raisons principales aujourd'hui.
> La première est la mise à l'échelle, qui est très difficile. Un exemple tout bête : si on voulait avoir sur la blockchain un service de type visa ou facebook, il faudrait que chaque nœud détienne l'équivalent des données de facebook ou de visa, ce qui est impossible. Il y a des solutions bien sûr, qui sont prometteuses mais qui ne seront pas là avant deux ans, en étant optimiste. C'est le cas du sharding[47] par exemple sur lequel se fondent plusieurs projets dont Ethereum, et sur lequel Vitalik travaille en particulier.
>
> Pour résumer, si la question est de savoir si dans 20 ans on regardera la blockchain en se disant que c'est ce qui nous a permis de créer ce qui sera alors l'équivalent d'internet, je répondrais oui sans hésiter. Dans ce cadre-là, la hype est complètement méritée.
>
> En revanche si la question est de savoir si c'est pour demain ou même après-demain, certainement pas ! Il est absolument impossible de mettre la blockchain d'aujourd'hui à l'échelle d'un réseau comme internet. A court terme, y a de la place pour des Preuves d'Existence (POC), et il y a des cas d'usage qui se révéleront pertinents dans des cas précis, voilà tout.
> Il ne faut pas pour autant que cela empêche les organisations de s'y mettre. Le premier arrivé aura quoi qu'il arrive un avantage compétitif décisif.

[47] Le Sharding est encore au stade exploratoire puisqu'il nécessite le passage à la Preuve-d'Existence (Ethereum est toujours à la Preuve-de-Travail). La technique devrait concrètement permettre de ne pas faire transiter toutes les transactions par tous les nœuds du réseau, augmentant mécaniquement sa capacité.

Est-ce que les blockchain privées ne seraient pas une solution à ce défi de la mise à l'échelle ?

Les blockchains privées sont en fait une réponse au second problème de la blockchain, qui est l'absence de confidentialité.

Dans la blockchain, en effet, toutes les données sont inscrites en clair, notamment pour que les smart contracts puissent interagir avec elles. Si on demande à un programme d'additionner 2+X, il faut bien lui donner X, sinon il ne peut pas travailler ! C'est pour cela qu'on ne peut pas réellement chiffrer les données dans la blockchain tout en voulant profiter des bénéfices des smart contracts. Il y a donc beaucoup de cas d'usage qui *a priori* ne sont pas possibles sur les blockchains publiques, dans des situations où les entreprises ne veulent pas que les données soient inscrites en clair avec le risque que leur pseudonyme soit levé.

La solution que ces entreprises ont trouvée n'est pas bien nouvelle dans l'histoire d'internet : c'est de tout mettre derrière un VPM, et d'appeler ça une chaîne "privée". Fondamentalement, cela ne me dérange pas : c'est un peu comme internet et les intranets. L'un n'empêche pas l'autre, et les deux trouvent leur utilité.

Mais je pense que dans 4 ou 5 ans on verra apparaître des technologies comme le chiffrement homomorphe, ou les preuves à divulgation nulle de connaissance (zero-knowledge-proof), qui auront le potentiel de chiffrer des données tout en laissant les programmes autonomes les utiliser. Il y aura alors beaucoup moins besoin d'utiliser des blockchains privées, puisque les entreprises pourront aller mettre de la data chiffrée très simplement dans une blockchain publique, et donc sans avoir besoin de payer pour l'infrastructure… ce qui est quand même un peu le but de la blockchain !
D'ici là, on devrait effectivement assister à la multiplication des blockchains privées, mais d'avantage pour des raisons de confidentialité que pour d'autres raisons.

Sur ce sujet-là, que penses-tu de l'initiative Hyperledger[48] ?

Je pense qu'ils s'y mettront avec succès et qu'ils trouveront un cas d'usage rapidement. Mais du point de vue du public, les blockchains privées seront effectivement moins intéressantes d'ici 4 ou 5 ans.

Ceci étant dit, je trouve malgré tout un intérêt plus limité à ces outils qu'aux blockchains publiques. Parce que, quelle que soit la blockchain, il y a quand même un moment où le consensus doit être réalisé ; or s'il se fait sur des ordinateurs qui sont tous sur le cloud de Microsoft, ou d'IBM, ça veut dire en dernière analyse que l'on fait de fait confiance à IBM. Ce qui, pour un système qui promettait d'être trustless [de reporter la confiance sur l'algorithme] n'est pas forcément l'idéal …

[48] Hyperledger est un consortium porté par la Linux Foundation et où figure notamment IBM, et qui vise à construire des blockchains privées.

Quelle organisation, coopération ou opposition vois-tu du coup à l'avenir entre les différentes blockchains ?

> Le fait que les gens opposent Bitcoin et Ethereum montre à quel point il existe des méconnaissances de la façon dont la technologie sous-jacente fonctionne.
>
> Bitcoin est un registre qui se contente d'additionner des chiffres et de réaliser l'équilibre des comptes, dans un but très clair : remplacer l'argent. Il suffit de lire le document de Nakamoto pour le comprendre. Ce projet découle d'une longue tradition, notamment des cyberpunks des années 1990 qui cherchaient à trouver un remplacement à l'argent, avec des systèmes fondés sur des choses comme e-gold, et avec toute la recherche qui s'est faite quant à la façon d'assurer la confiance. A aucun moment dans le document de Satoshi, on ne lit que le projet est celui d'une blockchain globale, ou de la mise en place de smart contracts … non. Dans ce papier, tout est toujours une question d'argent. Et sur ces questions, je dirais que Bitcoin remplit sa fonction, malgré toutes les remarques qu'on peut avoir sur le minage et ses limitations, et malgré tous les commentaires très justes formulés par Mike Hearn dans son article de janvier 2016[49]. Il ne faut pas forcément abandonner la technologie, il faut trouver des solutions pour l'améliorer, tout en gardant en tête qu'il s'agit d'un cas d'usage très différent de celui d'Ethereum.
>
> Ethereum a eu dès le début l'objectif d'être le plus générique possible, et applicable à n'importe quelle opération qui puisse être représentée de façon mathématique. Ethereum couvre donc des cas comme l'assurance, l'Internet des Objets, l'énergie... mais aussi avec l'ambition d'être applicable à toutes ces verticales de marché. Bitcoin et Ethereum sont donc fondamentalement séparés.
>
> Si la question est de savoir s'il est possible aujourd'hui d'utiliser l'ether comme on utilise le bitcoin, alors il faut bien dire que oui, on peut. Mais à mon sens la vraie question est de savoir si on a intérêt à le faire. Ce n'est pas forcément le cas. La plupart des vendeurs en ligne par exemple ont installé des systèmes de paiement qui fonctionnent avec bitcoin, et je ne suis pas certain qu'ils aient envie de rajouter un second système de paiement pour l'ether.

Vis-à-vis du bitcoin et des réformes du protocole que tu évoques, quelle est ta vision des évolutions du type *colored coins*, ou Rootstock ?

> Pour moi ce sont des projets qui n'ont pas vraiment de futur. Franchement, intéressons-nous à la chronologie : Colored Coins, c'était un projet sur lequel travaillait Vitalik avant de partir pour créer Ethereum[50]. S'il a jugé nécessaire de développer un autre système, c'est bien qu'il y avait des raisons de le faire. Quant à Rootstock, très honnêtement, je n'ai pas suivi ce qu'ils font, donc j'ai regardé rapidement mais je n'ai pas été convaincu pour l'instant.

[49] "La conclusion de l'expérimentation Bitcoin", article où le développeur reconnu de la communauté explique pourquoi il jette l'éponge et se dissocie du projet Bitcoin qui, à son sens, ne peut plus réussir. https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.sn5jqw66i

[50] Colored Coin est la principale innovation qui a permis d'utiliser la blockchain bitcoin pour enregistrer d'autres actifs que la simple monnaie.

En revanche, des projets comme ENIGMA sont extrêmement intéressants. J'avais échangé avec ceux qui sont à l'origine du projet, il y a un certain temps maintenant, et ils n'avaient pas trop de visibilité sur leurs prochaines étapes et sur la façon de passer à la mise à l'échelle de la technologie. Mais leurs idées sont très intéressantes, avec un système de chiffrement assez avancé, une Virtual Machine (l'EVM d'Ethereum) et une équipe apparemment compétente. C'est un exemple de gens qui bossent sur certains petits problèmes de la blockchain et font avancer les solutions pour les résoudre.

Personnellement je pense qu'il y aura une blockchain qui va s'imposer et intégrer toutes ces solutions aux problèmes actuels. Et je pense que ce sera Ethereum, par simple effet de réseau.

Une question un peu plus technique : au sujet d'Ethereum, il y a beaucoup de réflexion en ce qui concerne le débat preuve d'existence *versus* preuve de travail, ainsi que sur le statut des mineurs. Peux-tu nous en dire un peu plus ?

La preuve de travail, on s'est toujours accordé pour dire que c'était un mal nécessaire pour décourager les mineurs de créer des ASICs[51] et aboutir de fait à la centralisation du réseau.

Le choix qui a été fait dans l'écriture du code Ethereum, a été de fonctionner avec une organisation en modules : le mode de minage est un module, l'encodage est un autre module, la machine virtuelle c'est un autre module, etc. C'est un *design* qui a clairement empêché les mineurs de créer des ASICs, parce qu'ils savaient qu'on était en mesure de changer le module minage à tout moment [et donc de rendre leur matériel caduque]. Il y a aussi une autre raison d'ailleurs, c'est qu'on a toujours eu dans l'idée de passer à la Preuve d'Existence.

Pour forcer ce passage, il y a d'ailleurs dans le premier patch de Geth[52] une espèce de "bombe" qui devrait rendre le minage inutile d'ici fin 2016, et forcer une "hard fork" vers la preuve de travail. L'idée est que la difficulté du minage de la Preuve de Travail va augmenter de manière exponentielle à partir d'octobre, ce qui fait que vers fin décembre il n'y aura plus de possibilité de trouver un bloc. C'est un impératif qui a été mis en place parce que dans les débuts d'Ethereum, on n'était pas sûr que ce serait facile de faire les hard fork ; après tout sur la blockchain bitcoin on les assimile un peu à la fin du monde...

Mais en réalité le changement pour Homestead[53] a prouvé de façon très empirique qu'un fork sur Ethereum est non seulement possible mais même assez facile. La bombe est moins importante désormais, et il s'agit juste de

[51] Un ASIC est un circuit intégré dédié à une application précise. En l'occurrence les ASICs développés pour le Bitcoin ont conduit de fait à une course au matériel que seuls les plus gros acteurs du monde des mineurs ont pu suivre et donc, *in fine*, à une centralisation du réseau.
[52] Geth est un des clients développés pour Ethereum, c'est-à-dire un des langages dédiés au développement des applications sur Ethereum.
[53] Homestead est la seconde des 4 étapes de déploiement d'Ethereum, et a été officiellement lancée en mars 2016.

demander aux mineurs de changer leurs logiciels quand il le faudra, ce qui n'est pas la fin du monde quand on est un gros pôle de minage.

Maintenant, si je peux m'essayer à une petite prédiction à la Nostradamus, je pense qu'on va assister à une hard fork pour délayer cet "ère glaciaire", pour la rendre effective plus tard, en 2017 ou même en 2018, parce que la Preuve d'Existence n'est tout simplement pas au point. Je m'y suis beaucoup intéressé sur le plan théorique, notamment parce que je suis bien copain avec Vlad Zamfir, qui travaille sur Casper, le modèle de Preuve d'Existence d'Ethereum. Il y a encore des questions qui ne sont pas résolues : par exemple comment est-ce qu'on va amorcer le lancement du système de Preuve d'Existence ? Avec une information toute bête quelque part sur un site web, c'est-à-dire sur un système centralisé ? Il y a certainement mieux à faire mais c'est encore un peu tôt pour savoir.

Il y a dans la blockchain une sorte d'impératif de la transparence… Une société où toutes les données seraient inscrites en clair, ça te semble plutôt souhaitable ? Ou dangereux ?

Il est très facile pour une technologie d'être corrompue. Comme toutes les révolutions dans monde réel, d'ailleurs : ça commence avec des slogans du genre "le pouvoir au peuple" et en réalité on finit trop souvent avec un dictateur…

Avec des technologies aussi compliquées, avec le Bitcoin et Ethereum qui sont tout sauf simples à appréhender, et des avancées qui les suivront et qui le seront encore moins, il y a un risque énorme. Il est tout à fait possible que demain on se retrouve dans un monde où un géant comme Google arrive en annonçant: "j'ai implémenté la blockchain dans mon moteur de recherche, il y a désormais 300 millions de nœuds qui font tourner la Google Chain". Et si le modèle de la Google Chain est un modèle où ils peuvent à loisir inverser les transactions, ou bien transmettre toute l'information vers la NSA, eh bien ce sera tout simplement la fin de cette technologie et de ses promesses.

Comment éviter ce danger ?

C'est dur ! [rires] On ne l'a pas évité avec internet par exemple : je me souviens des débuts, quand tout le monde parlait de cyberpunks, de la fin des frontières, du règne du cyberespace… Et on voit où on en est. Donc le danger existe.

Alors comment l'éviter ? On fait au mieux pour monter en capacité le plus vite possible la technologie qu'on pense être valide aujourd'hui, et qu'on pense être pure, et on fait en sorte que tous les protocoles soient open source ; on parle à des industriels, aux grosses entreprises, on fait du lobbying auprès des gouvernements pour encourager la mise en places de choses qui soient pures, et on fait au mieux avec les moyens du bord...

Quelle vision as-tu des acteurs économiques traditionnels, des grandes entreprises… Est-ce que la blockchain est la "disruption" qui va laisser les anciens grands gagnants du système sur le carreau ?

Non, je ne pense pas que ça va les tuer. C'est plus compliqué que ça.

Par exemple, prenons BitTorrent. A l'époque où c'est sorti, tout le monde pensait que c'était la fin des CD, de la musique, que désormais tout passerait sur MP3. On avait d'ailleurs assisté du même coup à des valorisations de sociétés comme Napster pour des sommes absolument délirantes. Tout cela parce qu'on avait une mauvaise compréhension de la technologie et qu'on pensait que désormais plus personne n'achèterait rien et que tout le monde partagerait tout. En 2016, on voit pourtant que le marché a été complètement repris en main, notamment par iTunes. Parce que les gens de chez Apple ont vu arriver la vague, et ils ont été suffisamment malins pour se dire que si les gens en avaient marre de payer 10 € pour un album, on pourrait tout à fait les faire payer plutôt 79 centimes par chanson, en emballant le tout dans le machin digital qui va bien et qui fonctionne avec le nouvel iPhone... Le tout sur une plateforme, avec un service un peu sexy... et voilà le travail !

Je pense que la blockchain en général, et que Bitcoin en particulier, ressemblent assez à BitTorrent. On va créer un futur potentiel qui va faire peur à certaines personnes, mais qui va donner des idées à d'autres personnes. Et c'est tout à fait possible que les applications qui vont bousculer ou tuer les acteurs dominants d'aujourd'hui soient en fait mises en place par des sociétés qui ont rien à voir avec la blockchain, mais qui se seront parfaitement positionnées pour profiter du mouvement. C'est quelque chose qui risque d'arriver.

Après, est-ce que les grandes entreprises ont plus à gagner qu'à perdre ? Moi je pense qu'elles ont plus à gagner, mais ça dépend dans quel secteur. Par exemple, l'idée que Bitcoin va tuer les banques, c'est une vieille rengaine, mais je vois bien dans mon entourage que les gens ne sont pas tous prêts à ça.

Tu soulèves un sujet clef qui est l'adoption généralisée de la blockchain, et de façon générale l'expérience utilisateur. C'est le prochain défi à relever à ton sens ?

Ce que je peux dire, c'est que pour l'instant il y a une friction énorme.

Regarde Bitcoin, qui existe pourtant depuis 7 ans, et qui vise à remplacer l'argent: aujourd'hui encore il y a des gros traders bitcoin qui dans leur vie de tous les jours payent avec leur carte bleue, parce que le processus est trop lourd !

C'est la même chose pour Ethereum. Un exemple tout bête : supposons que l'on soit dans le métro, et que mon voisin joue à Angry Birds, ou Candy Cruch sur son téléphone. Si je veux y jouer aussi parce que ça a l'air bien, je sors mon téléphone, peu importe le système d'exploitation, et je vais sur le catalogue d'application : en trois clic je trouve ce que je cherche et je me mets

à y jouer. Maintenant supposons qu'au lieu d'Angry Birds, c'est Mist, le moteur de recherche d'Ethereum, que le gars a sur son téléphone. Pour y jouer, c'est très simple aussi: il faut télécharger tel software, ensuite aller sur telle place de marché, puis entrer ses coordonnées bancaires, attendre trois jours pour avoir des bitcoins, puis aller sur ShapeShift pour avoir des éthers, avant de pouvoir enfin utiliser l'application. Simple effectivement.

Il y a donc un énorme problème de friction. Je pense qu'il va falloir que des banques s'y mettent ou bien que des services financiers de certaines boîtes s'y mettent, pour faire l'interface entre le public et la crypto-monnaie.

Par exemple Slock.it travaille avec RWE sur un projet qui concerne la construction de bornes de chargement d'électricité, de manière à pouvoir faciliter la facturation et la comptabilité. Il y a plusieurs avantages au système, notamment les importantes économies d'argent grâce aux simplifications de l'organisation du travail et des processus, sans compter la résilience accrue et un dialogue plus facile avec les autres bases de données... Bref, ils font une grosse économie d'argent, mais ils comprennent bien aussi que l'utilisateur ne va pas sortir son portefeuille numérique à chaque utilisation. Donc leurs services financiers réfléchissent à la possibilité de convertir des euros en ether. C'est la seule façon de procéder, mais elle va prendre du temps parce qu'il y a notamment des problèmes de régulation. Ceci dit, les gens comme RWE, qui sont des sociétés qui valent des milliards et des milliards, sont bien placés pour résoudre ce genre de problèmes. Les petites start-up ne vont pas voir les pouvoirs publics pour faire du lobbying, alors que les grosses sociétés échangent tous les jours avec le régulateur.

A quand la conversion ether/euros alors ?

Pour des gens comme moi c'est déjà possible, mais pour des gens comme ma maman, disons que c'est du long terme…

A quand le déploiement de Slock.it dans ce cas ?

En son temps. Ce projet, il vient quand même de deux années de réflexions. En deux ans, j'ai créé une énorme liste de cas d'usage en fait, qui me viennent depuis mes débuts à Ethereum. Dans la liste, il y avait des idées tirées par les cheveux, mais aussi des choses plus réalistes, et j'avais en gros 200 à 300 cas d'usage qui correspondaient finalement à autant de boîtes que je voulais créer par la suite. Et le top de la liste, c'était l'Internet des Objets et la communication machine-machine.

C'est un domaine immense mais particulier… quand on a deux machines qui veulent se parler aujourd'hui, ça passe par un serveur centralisé, ça coûte de l'argent, alors que si elles se parlent sur une blockchain, elles vont pouvoir se parler entre elles directement, ou plutôt je devrais dire se synchroniser autour de l'état de blockchain. Et ce qui est clef c'est que, peu importe ce qu'elles utilisent, de l'ether ou des coquillages, en fait tout le monde s'en moquera, précisément parce que ce sont des machines.

En somme, la blockchain est une nécessité parce qu'avec la montée en puissance de l'Internet des Objets, on ne pourra plus tout faire passer par des serveurs centralisés ?

> Exactement. C'est un peu la vision de Paul Brody dans le papier d'Adept, "device democracy".

Que penses-tu d'IPFS ?

> C'est un de nos partenaires. Une de nos idées est de rendre disponible la location par IPFS de l'espace de stockage disque des Ethereum Computer contre par exemple des ether. On travaille pas mal sur ces idées de revenu passif, mais comme tout le reste il nous faudra beaucoup de nœuds pour réaliser ces idées, donc *a priori* ce serait plutôt pour bien plus tard.
>
> Le seul problème que j'ai avec IPFS, et dont j'ai d'ailleurs discuté avec Juan Benet, qui en est le créateur, c'est le système d'incitation et la procédure de motivation des utilisateurs qui vont fournir cet espace disque. Là-dessus, pour l'instant, il n'y a pas grand-chose. En revanche le système de stockage décentralisé marche très bien.
>
> Par contre chez Swarm, le projet que développe Viktor Tron à la Fondation Ethereum, les procédés d'incitation sont déjà beaucoup plus riches. Au fond, j'aimerais voir un amalgame des deux, ce serait un système intéressant.

D'autres projets te semblent prometteurs ou t'intéressent à part ces deux-là ?

> Swarm et IPFS ont un potentiel énorme.
>
> A part eux, dans la Fondation, il y a Mist, le moteur de recherche sur Ethereum, qui est complètement sous-estimé. Pour comprendre un peu de son potentiel, il suffit d'imaginer par exemple un système avec des publicités, stockées dans un serveur centralisé de la fondation, qui récompenseraient en ether les gens qui les regardent. Ça permettrait ensuite d'utiliser le réseau sans avoir besoin de miner et sans avoir besoin de d'aller acheter de l'éther; et ce serait un excellent procédé d'embarquement pour la fondation et son projet. .
>
> Sinon, il y a bien sûr Augur et Gnosis, les oracles[54]. Ujo Music[55], aussi. Il y a également plein de projets chez Consensys, BoardRoom par exemple. Comme il y a là-bas plein de compétences et d'excellents développeurs, Nick Dodson par exemple, il est intéressant de regarder ce qu'ils vont faire. Pour l'instant je n'ai encore rien vu qui soit en production, mais une fois que ça sera lancé, on en saura plus...
> Mobotiq[56] a un prototype qui marche, mais il y aura probablement de la friction notamment du point de vue culturel, et particulièrement aux Etats-Unis où les

[54] Voir la partie consacrée aux cas d'usage.
[55] Voir la partie consacrée aux cas d'usage.
[56] Mobotiq développe un nouveau type de véhicules fondés sur un fonctionnement de Pair à Pair.

gens ont un rapport spécial à leur voiture. Mais en Europe ? A Paris, vu les soucis de circulation que l'on a, ce ne serait pas du luxe.

Est-ce que pour toi on se dirige avec tous ces projets vers une société vraiment décentralisée ?

La question est dure, je n'ai pas ma boule de cristal sur moi [rires]. Plus sérieusement, aujourd'hui, personne ne le sait.

Les DAO sont un excellent exemple. Est-ce que des gens se diront que c'est possible de prendre des décisions dans une organisation de 3000 personnes, ou est-ce qu'en dernière analyse ils préfèreront des modèles avec des dictateurs, façon Steve Jobs ? Est-ce qu'il n'y a pas une tendance générale de l'humanité à tout ramener à une forme de centralisation, et est-ce qu'une vraie décentralisation est possible au fond au vu de la nature humaine ? Je ne sais pas.

Honnêtement, moi, j'aimerais croire qu'on arrivera à une véritable décentralisation, parce que si on continue à tout centraliser on va se retrouver avec des systèmes abominables à la Orwell, et il n'en faudra pas beaucoup pour ça. Les gens qui ont vécu des guerres ou des changements politiques assez brutaux, par exemple au Venezuela, sont les premiers à le dire : tout allait bien, c'était un pays très bien, tout ça, et du jour au lendemain la dictature et la famine... Ce genre de choses horrible peut arriver, et plus on tarde à trouver un modèle de décentralisation qui permette aux gens de s'auto-organiser, plus on fait courir un risque à l'humanité en général.

Dans la vision de société que porte la blockchain, il y a aussi quelque chose qui relève du remplacement de l'homme par la technologie non ? Les programmes autonomes par exemple…

J'en avais beaucoup parlé avec Gavin Wood, et il était convaincu qu'il n'y avait aucun danger de scénario dans le genre Skynet[57], parce que ces programmes autonomes sont par nature déterminés. Ils n'ont pas de place pour les chiffres aléatoires, et en fait tout ce qui pourrait remplacer les humains dans le monde réel sont des choses qui se fondent sur des critères aléatoires. De ce point de vue-là, je pense qu'il n'y a pas de danger.

Je pense qu'on va voir beaucoup de DAO, si ça fonctionne bien, qui utiliseront des humains comme un peu une sorte d'intermédiaire, pour aller faire des choses dans le monde réel. Par exemple dans le monde de l'assurance, il faut bien que quelqu'un aille faire le constat. Si on dit "voilà j'ai cassé ma voiture" il faudra bien quelqu'un pour aller prendre la photo pour être sûr qu'il ou elle n'a pas menti.

J'aimerais bien voir une décentralisation du travail, où les gens puissent travailler de la maison ou d'où ils veulent d'ailleurs, n'importe où dans le monde, contre des ethers ou autre chose, d'une façon appropriée pour trente sociétés

[57] Dans la série Terminator, l'intelligence artificielle Skynet devenue incontrôlable s'oppose aux humains pour la domination de la planète.

à la fois. Aujourd'hui il y a un modèle qui est coercitif. On signe un contrat exclusif avec une société on travaille plus de quarante heure par semaine, et puis c'est tout, on a peur de poser des questions pendant les entretiens d'embauche, parce qu'on se dit que si on pose trop de questions on n'aura pas le job… En réalité on est à la merci des employeurs. J'aime bien cette idée de DAO où les humains sont remplacés par des ordinateurs qui ne mentent pas, qui ne sont pas partie prenante, ou émotionnels, ou racistes, et à qui on pourra dire "aujourd'hui je vais faire ci, aujourd'hui je vais faire ça". Un peu comme Task Rabbit en fait, mais sans l'exploitation.

Je pense qu'il y a plus d'espoir que de peur sur ce sujet, en tout cas pour moi.

Une phrase de conclusion ?

Personne n'a de boule de cristal. Ceux qui le prétendent sont des menteurs ; c'est un peu comme l'internet dans les années 1990, la blockchain est devenue *mainstream*, et les gens commencent à se poser les questions de "comment je fais pour". Moi j'étais dans la Silicon Valley de 1995 à 1999, et j'ai beaucoup vu d'arnaques, de *scams*, des gens avec de bonnes idées qui n'étaient pas du tout commerciaux, des gens avec de bonnes idées qui étaient très commerciaux, des gens qui étaient complètement cinglés et puis des investisseurs qui ne comprenaient rien à la technologie mais qui se disaient que c'était le futur et qu'ils allaient se faire plein d'argent en le dépensant à tort et à travers.

Je pense que ça va se répéter. Ça se répète déjà un petit peu, et ça va vraiment s'accélérer. Il faut faire attention, et garder son calme, parce que la blockchain ce n'est pas la fin du monde, c'est juste un outil qui peut permettre de faire des choses utiles. Si on l'utilise intelligemment.

Interview de Richard Caetano, Cofondateur de Stratumn

Stratumn est devenue en mars la première start-up blockchain à lever des fonds en France (600.000 € auprès d'Otium Ventures et de plusieurs business angels). Son cofondateur, Richard Caetano, nous présente ici sa vision de la blockchain et du bitcoin.

A qui s'adresse Stratumn ?

> Nos clients, ce sont les développeurs de tous types : indépendants, petites et grandes entreprises, *think tanks*, banques… A long terme, nous voulons construire des *templates*, des modèles, qui seront très faciles d'accès et d'utilisation, même pour les développeurs qui découvrent la blockchain.
> Ce que nous voulons donc, c'est enlever toutes les barrières à l'entrée de la blockchain, c'est-à-dire premièrement la "scalability", la capacité à croître de manière exponentielle limitée par la taille des blocs, deuxièmement les ressources et le maintien de l'infrastructure, et enfin l'appréhension du sujet, qui évolue à une vitesse inimaginable.
>
> Pour ce faire, nous créons notre propre environnement privé, avec notre propre protocole Chainscript, auquel les développeurs se connecteront, dans une approche "plug & play", ce qui leur permettra d'accéder à la puissance de la blockchain sans avoir besoin de la maîtriser complètement.
> Notre grille tarifaire sera établie dans le même idéal d'accessibilité, avec des premiers prix autour de 10 €/mois pour une petite application. Nous espérons vraiment démocratiser l'accès à la blockchain.

Penses-tu que le bitcoin puisse être remplacé par une autre crypto-monnaie ?

> Bitcoin est une technologie. La crypto-monnaie et la blockchain sont inséparables en tant que tel.
>
> En fait, l'existence même du bitcoin résulte d'un équilibre très complexe entre trois éléments : un facteur technologique, un facteur économique et un facteur social.
>
> Le facteur technologique représente la blockchain en elle-même : son protocole, la puissance de calcul nécessaire et disponible, la capacité de stockage, etc. Le facteur économique fait référence aux incitations à miner [le minage est le processus qui permet la validation des blocs] : miner rapporte de l'argent, c'est pour cela que les mineurs existent. Enfin le facteur social représente le phénomène social qu'est Bitcoin : il y a un effet de réseau. Plus il y a de personnes qui utilisent le bitcoin, plus la valeur du bitcoin augmente.
> On comprend très rapidement qu'enlever l'un de ces trois aspects ferait tout s'écrouler : sans technologie, pas de blockchain. Sans incitation à miner, pas de vérification. Sans utilisateurs, pas de valeur. L'équilibre trouvé par Bitcoin n'est pas sous le contrôle de quelqu'un. Il n'est pas réplicable à volonté. En ce sens, il est vraiment unique et exceptionnel.

Par conséquent, on ne peut pas savoir si quelque chose pourra remplacer Bitcoin. C'est possible, mais cela prendrait un temps considérable de reconstruire cet équilibre.

Chez Stratumn, on parie sur les deux possibilités : que Bitcoin soit la crypto-monnaie unique ou à défaut dominante, ou bien que de multiples autres apparaissent et se développent.

Tu paries donc aussi sur les blockchains privées ?

En fait, sur une blockchain, il existe ce que j'appelle le "Decentralized Dilemma" (dilemme de décentralisation). Il faut un réseau et un seuil critique d'utilisateurs pour qu'une blockchain fonctionne. Tant que ce seuil n'est pas atteint, il s'agit simplement d'une multiplication d'acteurs auxquels il faut faire confiance. Et on ne peut pas "forcer" une décentralisation. Elle doit émerger.

Mais les entreprises n'ont besoin que de "semi-confiance" afin d'amorcer ce changement de paradigme de pensée, afin d'abandonner cette posture défensive que nous adoptons instinctivement dans tous nos échanges et qui fait naître ce besoin d'intermédiaires.

Nous pouvons donc nous appuyer sur un réseau d'intermédiaires de confiance qui aurait accès à la blockchain et à la validation des transactions, et chacun des nœuds de ce réseau pourrait être contrôlé par des nœuds d'audit. L'avantage majeur, bien que l'on garde une part d'intermédiation, serait que personne ne contrôle vos données.

De quel côté te situes-tu dans le débat sur la levée des obstacles techniques du Bitcoin, notamment la question de la taille des blocs ?

Je compare souvent le réseau Bitcoin à la ville de Carcassonne. C'est une ville de toute petite taille, avec de grands murs épais qui la protègent. Le coût de la protection est très élevé, de la même façon que dans le réseau Bitcoin.
Si l'on considère une ville de taille gigantesque, par exemple Los Angeles, et que l'on essaie de construire autant de remparts, ce serait beaucoup, beaucoup plus coûteux d'offrir le même niveau de protection. C'est la même chose pour la blockchain : si sa taille augmente très fortement, le coût de protection deviendrait hors de prix, ou bien il en résulterait une moins grande fiabilité si l'on souhaite conserver la même puissance de réseau.
C'est pour cela que je soutiens la position conservatrice des mineurs, qui ne souhaitent pas faire augmenter la taille des blocs. En revanche, je peux tout à fait imaginer un futur où

> d'un côté le Bitcoin servira de "trust network", qui constitue sa grande force grâce à son processus de proof-of-work sur lequel repose sa fiabilité (volume de transaction limité ; temps de dix minutes avant qu'une transaction soit validée ; grande puissance de calcul).
> de l'autre, des sides chains[58], ou des off chains, serviront de réseaux de paiement, puisque le Bitcoin n'est pas actuellement optimisé pour cette

[58] Une side chain est une blockchain secondaire qui se développe parallèlement à une blockchain principale, mais qui y est rattachée afin de pouvoir en connaître toutes les informations. Les sides chains permettent

utilisation (qui nécessite de grands volumes de transaction et des temps de confirmation très rapides).

De manière plus générale, quels seront selon toi les secteurs impactés par la blockchain ?

Le premier à être impacté sera le secteur bancaire et de la finance. Non seulement il sera le premier mais je pense qu'il sera aussi le secteur le plus impacté sur le long terme. La blockchain permet de réduire 80 % de l'inefficacité du système bancaire actuel. Grâce à cette technologie, la banque ne sera plus jamais la même. On observera prochainement une obsolescence massive du travail des intermédiaires dans ce secteur.

Mais deux autres secteurs me viennent à l'esprit principalement : la santé et les gouvernements. Je pense pour les gouvernements notamment à la capacité de la blockchain à révolutionner la démocratie, les titres, la propriété, le cadre légal …

Quelle application de la blockchain te fascine le plus ?

Toujours le bitcoin, qui a des applications globales. 3,5 milliards de personnes n'ont pas accès au système bancaire par exemple. Le bitcoin est une solution pour eux. De manière générale, le bitcoin représente le libre-commerce, qui lui-même apporte la paix. Je croix que ce serait un euphémisme de dire que le pouvoir des citoyens émane de leur argent. Aujourd'hui, ils peuvent décider d'un monde plus transparent, où l'information ne serait plus asymétrique. Le bitcoin peut disrupter n'importe quelle industrie.

L'intérêt du Bitcoin réside dans son mécanisme public de vérification de transactions, qui rend le réseau extrêmement fiable. N'importe quelle autre crypto-monnaie ou blockchain peut certes agir comme réseau de confiance, mais ce qui rend le Bitcoin exceptionnel est la quantité de puissance de calcul dans le réseau qui protège cette confiance. Mon point ici, c'est qu'il est très rare de construire un réseau aussi fiable, car il faut pour cela la réunion de trois éléments, ceux que je citais au début, qu'on ne retrouve dans aucune autre crypto-monnaie, peut-être à l'exception de celle d'Ethereum qui est en train de progresser sur ces trois aspects.

En temps qu'Américain installé en France, que penses-tu de l'écosystème blockchain français ? Comment pourrait-il être développé ?

Mon expérience chez Paymium en 2011- 2013 me fait immédiatement penser à une chose : il est très difficile de travailler avec une banque lorsque l'on parle de bitcoin et de blockchain. Il y a un rejet initial automatique.

Quand je parle de bitcoin en France, la première chose que j'entends c'est "C'est la drogue, l'argent sale, le terrorisme …". Il y a beaucoup de rééducation à mener. La technologie est neutre, c'est les gens qui s'en servent qui sont

d'accroître le volume d'informations pouvant être traitées au sein d'une blockchain (volume normalement limité), tout en restant sur une même blockchain principale.

parfois critiquables. Le dollar finance tout aussi bien, même mieux, la drogue et le terrorisme. Dit-on pourtant que le dollar est mauvais intrinsèquement ?
Il faut faire prendre conscience au public que le bitcoin et la blockchain ne sont pas le problème, mais bien la solution. Il est en effet facile de suivre les traces de transactions effectuées sur une blockchain. De ce fait, et contrairement aux idées reçues, le bitcoin peut contribuer à lutter contre le terrorisme.

Nous avons besoin du soutien du gouvernement car les start-up du secteur sont coopératives et conscientes des risques. Elles veulent et demandent un cadre légal, une régulation précise et claire. Cela serait un signal positif à tout l'écosystème.

Les pouvoirs publics doivent aussi prendre conscience de la nécessité d'éduquer sur le sujet. Nous avons besoin d'une approche raisonnable de la blockchain, et non braquée, anarchiste ou conservatrice.

Que dirais-tu à ceux qui découvrent la blockchain et veulent se renseigner ?

Faites bien la distinction entre la "hype" et le réel, au risque de faire face à une désillusion. Creusez et cherchez à comprendre ce qu'est vraiment la blockchain. Il n'y a qu'ainsi que vous vous rendrez compte de son extraordinaire potentiel et que vous pourrez construire les nouveaux paradigmes de société de demain.

Interview de Nadia Filali et Philippe Dewost, Co-pilotes de LabChain, initiative de place lancée en 2015 par la Caisse des Dépôts et Consignations.

Comment la blockchain est-elle venue à la Caisse des Dépôts et à chacun d'entre vous ?

Nadia : Pour moi, tout commence lors d'un dîner, où un jeune adolescent me parle du Bitcoin. Comme ce garçon est souvent très bon observateur des évolutions technologiques et sociétales, je m'y suis intéressée et j'ai trouvé ça fascinant... Ce sont d'ailleurs les adolescents qui ont les premiers adopté le bitcoin comme monnaie d'échange de composants de jeux en ligne.

Philippe : De mon côté, j'avais lu çà et là divers articles sans y prêter grande attention. C'était pour la plupart des "papiers" sur les crypto-monnaies qui m'intéressent peu et je n'ai pas creusé le sujet. Mais par la suite une connaissance professionnelle de longue date m'a suggéré de lire le livre blanc d'IBM intitulé "Device Democracy"[59].

Ce document m'a bluffé : non seulement très bien construit et documenté, il s'agissait du premier rapport que je lisais qui plaçait la blockchain dans un cadre beaucoup plus large que simplement celui des crypto- monnaies. Immédiatement, ça a résonné avec une conviction que je porte depuis longtemps : avec la multiplication de la puissance de calcul (loi de Moore) dans des terminaux de plus en plus nombreux (1milliard de smartphones vendus par an), l'Edge Computing allait être une réalité à mesure que les calculs seraient de plus en plus réalisables et réalisés à la "bordure" des réseaux comme Snips[60] est en train de le démontrer par exemple.

Voir IBM faire le lien entre l'Internet des Objets et la blockchain était éclairant, mais en découvrant à l'été 2015 la déclaration de Marc Andreessen[61] [qui comparait début 2015 Bitcoin/Blockchain à TCP/IP lorsqu'Internet avait 5 ans], j'ai compris que ceux qui étaient au coeur du sujet (en tant que développeurs ou investisseurs) semblaient avoir entrevu un potentiel considérable, même si aucune application grand public n'était encore tangible... J'ai commencé à creuser plus intensément le sujet de mon côté, puis Nadia et moi nous sommes croisés au mois de mars et avons partagé nos intuitions et intentions tout en réalisant que nous constituions un binôme extrêmement complémentaire.

Nous avions la conviction que ce ne devait pas rester qu'une affaire de geeks, et avons enclenché le long processus de maturation du projet au sein de la CDC.

Nadia : De par mon profil financier, j'ai dans mes contacts des gens qui travaillent dans des banques ou des assurances et j'ai commencé à échanger

[59] Le lien du livre blanc d'IBM : http://ibm.co/1LbcEAt
[60] La start-up, fondée par trois chercheurs français, est spécialisée dans l'intelligence artificielle.
[61] Marc Andreessen est un des pionniers du web, notamment fondateur de navigateur Netscape

avec eux sur ce qu'il se faisait sur le sujet blockchain dans leurs structures. A la Caisse des dépôts, une table ronde sur les fintech et les banques a été l'occasion d'échanger avec d'autres sur ces sujets.

Nous avons pu organiser avant la fin de l'été une première présentation du sujet qui a permis d'initier et d'emporter la conviction de la Directrice Générale Adjointe de la CDC et d'une partie du Comité de Direction qu'il était important de s'intéresser au sujet.

Philippe : On peut dire qu'il y a eu ensuite deux dates importantes : d'abord la Une de *The Economist* en octobre 2015 (The Trust Machine), qui a subitement rendu le sujet "sérieux", puis en interne, pendant un séminaire sur la transformation numérique, organisé fin novembre 2015, tous les intervenants extérieurs ont successivement affirmé que la blockchain était la prochaine disruption majeure à surveiller. Cela a fait réfléchir les présents : peut-être Nadia et moi n'avions pas tout à fait tort d'insister sur le sujet depuis quelques mois....

Nadia : Ce qui est intéressant, c'est que lors des ateliers qui ont suivis, la blockchain est ressortie en premier dans la liste des sujets sur lesquels on devrait travailler à la Caisse. Au-delà de l'intérêt réel pour une technologie qui promet de transformer le quotidien de chacun avec une forte dose d'inconnue, je pense que la tendance actuelle dans les grandes entreprises à favoriser l'innovation, notamment dans le domaine numérique dans des modes de gestion ouverts et transverses autour et avec les collaborateurs, peut expliquer une partie du succès de l'initiative.

Philippe : Je dirais même que c'est le fait de s'autoriser à regarder et explorer l'inconnu qui intéresse. On redécouvre qu'il peut se passer des choses intéressantes dans une conférence qui n'a pas de programme, qu'il peut sortir du bien de l'inattendu, ce qui n'est pas forcément dans la culture de nos grandes organisations. S'autoriser à faire, à expérimenter et à apprendre par soi-même et avec d'autres nous donne l'opportunité de travailler en direct avec les acteurs de l'innovation.

Cette dimension d'avancée dans l'inconnu, on l'a retrouvée par la suite : le projet a beaucoup muri depuis le feu vert de la Direction générale.

Notre première action concrète a été de prendre le sujet à l'envers, et de commencer par écrire le communiqué de presse. Ça nous a obligé à penser dans des mots extrêmement clairs ce que devrait être l'initiative de place et comment nous souhaitions qu'elle soit comprise. Cette ébauche de communiqué, où figurent les logos des premiers partenaires, nous a permis d'en attirer d'autres, qui désiraient eux aussi figurer sur cette annonce d'initiative.

Nous avons choisi cette démarche car nous savions que même si le travail se ferait sur 2016, la fenêtre d'opportunité, elle, était à ce moment-là, en décembre 2015, et notamment pour ne pas laisser l'enthousiasme de *The Economist* retomber. Nous avons pu communiquer avant la trêve hivernale, juste à temps.

Puis au mois de janvier - et c'est là que nos boîtes mails ont viré au cauchemar [rire] – une foule d'autres acteurs de toute taille se sont rapprochés de nous : nous avions bien précisé dans le communiqué que la porte restait ouverte à d'autres potentiels partenaires.

Nous avons eu de nombreux retours qui nous ont surpris de manière positive. Globalement, les gens nous disaient "c'est super ce que vous faites là, personne à part la Caisse aurait eu la légitimité de le faire". Il est vrai que si un acteur privé était sorti du bois en disant "je vais coordonner la filière", tous ses concurrents l'auraient regardé avec suspicion. La Caisse redécouvre aujourd'hui sa capacité à rassembler en tant qu'acteur neutre et institutionnel, y compris dans un domaine assez inconnu.

Nadia : D'ailleurs, nous avions d'abord seulement proposé l'initiative, mais les choses avançant, on nous a demandé de la coordonner et de la gérer. Bien entendu ça a un côté pratique pour les participants, mquelque part, et c'est un peu l'ironie du sujet blockchain, c'est notre position de tiers de confiance qui nous donne la légitimité de mener ce travail. A cela s'ajoute que la Caisse couvre un périmètre assez large, donc quand il faut faire travailler des banquiers, des assureurs, des mutualistes, qui couvrent toute la palette et tous les métiers, la CDC apporte un certain consensus.

Il faut bien comprendre aussi qu'on a souhaité que cette initiative parle aux collaborateurs et les implique. Concrètement, on a fait le tour de chaque direction pour présenter le projet et on a demandé de le proposer à des collaborateurs qui soient motivés, qui connaissent pourquoi pas un peu de code, mais qui surtout aient envie de bosser de manière collaborative avec d'autres boîtes pour traiter des cas d'usages.

Notre volonté n'était pas d'aller puiser dans un vivier de "techniciens" en leur donnant une feuille de route. On souhaitait faire participer des collaborateurs métiers afin de les faire collaborer avec les développeurs des start'up et qu'ils construisent les processus et les services de demain. Naturellement l'équipe côté Caisse des Dépôts s'est formée autour de nombreux métiers incluant des financiers, des juristes, des collaborateurs des back offices, des contrôleurs de gestion, des architectes IT, des contrôleurs de risques, et ce de 22 à 60 ans… Ces personnes vont construire les offres de demain, et on propose de les confronter à cette nouvelle technologie : c'est ça qui a plu. Ça correspond d'ailleurs à un processus de transformation voulu par la Caisse, vers le numérique, avec une organisation plus horizontale et agile.

Quelle est la maturité des acteurs, à la fois sur les aspects blockchain mais aussi dans leur travail avec les concurrents ?

Nadia : Les banquiers ont l'habitude de travailler avec des concurrents ; ils y sont obligés à cause de l'interopérabilité entre les systèmes. Ne serait-ce que sur les titres, ou les moyens de paiement... Ils travaillent régulièrement comme ça, mais d'habitude, c'est dans un mode de réflexion et sur le temps long. Ce qui change ici, c'est à la fois le mode de fonctionnement "agile" et la mise en place d'une

"sand box" opérationnelle très différente des réflexions de place habituelles. C'est aussi pour cela qu'une coordination agile est nécessaire, pour faire cohabiter des cultures assez différentes, depuis les banquiers jusqu'aux Start-up, en passant par les associations et les universitaires.

Sur le plan des méthodes de travail, certains sont plus avancés que d'autres face à ce type de collaboration. En ce moment, il existe un phénomène de création de directions de l'innovation, de mise en place de nouvelles méthodes d'organisation : ces méthodes de travail souples commencent à pousser un peu partout, et l'agilité dépendra des structures.
Par ailleurs, il est vrai qu'un certain nombre de participants à cette initiative sont concurrents sur certains de leurs métiers. Aujourd'hui, on a trouvé des cas d'usage qui rassemblent, comme l'identité numérique ou les KYC [identifiants virtuels] ; ces cas sont communs à tout le monde et où on sait qu'ailleurs certains avancent déjà sur le sujet, par exemple au Luxembourg.

On sait aussi que tout le monde n'en est pas au même niveau d'exploration du sujet. Certains ont des équipes qui travaillent en interne, d'autres apprennent avec la CDC au fur et à mesure… Les attentes sont donc assez différentes, et le jeu du collectif est évident pour certains, en apprentissage pour d'autres. C'est notre rôle de de mettre ça en musique, ce qui est complexe mais passionnant.

Philippe : Une autre nouveauté est que le domaine se déforme plus vite que la vitesse à laquelle on entre dedans. Depuis notre premier communiqué, il y a eu les annonces d'Hyperledger, des acteurs qui sont sortis du bois, une compréhension accrue des activités de R3… ça évolue très vite, avec des moyens très différents et pour l'instant, aucun acteur ne se démarque. Impossible de dire qu'il existe une voie claire qui se dessinerait, de laquelle on dirait : "bon, maintenant fini de jouer, la solution c'est par là..."

Nadia : A cela s'ajoutent beaucoup d'effets marketings d'ailleurs, ce qui rend assez difficile d'identifier le vrai du faux...

Philippe : D'autant que la presse ne nous aide pas toujours sur ces sujets, alors qu'elle devrait jouer ce rôle. L'enquête de *The Economist* était extrêmement bien faite, fouillée, claire, mais elle reste l'exception plutôt que la règle dans le traitement médiatique du sujet.

Pour compléter le propos de Nadia, je dirais qu'il y a deux phénomènes tout à fait nouveaux et très intéressants pour les organisations qui s'intéressent à la Blockchain.

D'abord, ce phénomène les invite à réfléchir à l'adéquation entre les rôles au sein de leurs organisations et les viviers de compétences internes à leur disposition. Blockchain reste un sujet où il est possible de monter en compétence par soi-même. Je suis personnellement convaincu que dans toutes les grandes organisations, et notamment chez nos partenaires de l'initiative de place, il y a environ une dizaine de collaborateurs qui auraient des choses à dire ou à faire sur le sujet. Ces personnes font ça sur leur temps libre,

en hobby, parfois même en dehors de leur cadre professionnel ; elles ne sont de ce fait pas encore valorisées pour leurs compétences sur le sujet, voire même pas du tout identifiées.

Et cette nouveauté explique qu'aujourd'hui les entreprises qui arrivent à maturité le plus rapidement sur ces thématiques numériques sont celles qui s'interrogent sur leurs capacités à identifier en interne les bonnes ressources, à les mobiliser sur les sujets qu'elles veulent développer, et à leur donner les moyens de le faire. Ce n'est souvent pas évident à conduire mais peut s'avérer très efficace et très mobilisateur.

Le second phénomène observé concerne les consultants. Nous avons été sollicités par de nombreux cabinets de consultants intéressés à rejoindre l'initiative, et les avons pour le moment éconduit poliment. Ce que nous avons compris, et qui nous a été confirmé officieusement par l'un d'entre eux, c'est que la blockchain est un des rares sujets sur lequel les cabinets de conseil apprennent en même temps que leurs clients... D'habitude, ils ont toujours 18 à 24 mois d'avance sur les tendances, leur permettant de développer les concepts et les offres de services nécessaires. C'est absolument révélateur, parce qu'à cette échelle, c'est une première.

Marc Andreessen vous a amené à la blockchain... maintenant que vous comprenez mieux la technologie, est-ce que la comparaison avec TCP/IP vous paraît toujours valable ?

Philippe : Oui et non. Marc Andreessen connait son sujet, puisqu'il a créé Netscape. Mais la comparaison n'est juste que jusqu'à un certain point
Le parallèle est juste dans la mesure où il s'agit d'un phénomène qui n'est pas encore perceptible du grand public, dont on ignore encore à quelle vitesse et jusqu'où il sera déployé, mais dont les gens au cœur du réacteur ont identifié deux caractéristiques :

La multiplicité des cas d'usages permise par la généricité de cette rupture technologique;
Le passage à l'échelle possible (scalabilité).

Nécessairement, une première limite est ce passage à l'échelle, qui sur la Blockchain de Bitcoin n'est pas encore résolue, et sur les autres blockchains reste théorique…

Une seconde différence fondamentale, de nature ontologique, entre les deux protocoles est que si internet est une formidable machine à copier et diffuser de l'information, la blockchain, elle, sert à transférer de la valeur et à tracer le déplacement d'actifs, ce qui a pour incidence dans le cas des blockchains publiques de créer de la rareté numérique (le jeton de valeur qui dès lors qu'il devient échangeable sur les marchés, devient une crypto-monnaie sujette aux mécanismes usuels de spéculation).

Je vois enfin une troisième différence : au début des années 1990, il n'y avait pas encore de presse spécialisée, ni d'appétence pour la Tech, et surtout pas

ce souci du buzz permanent qui caractérise les médias d'aujourd'hui. Il y a une accélération fondamentalement différente de celle d'il y a vingt ans.

Par exemple, lors des quatre ans que j'ai passés chez Wanadoo après sa fondation, entre le premier abonné et le moment où je suis parti pour une startup, nous avions atteint un million d'abonnés. Angry Birds, de mémoire, c'est 50 millions d'utilisateurs en 35 jours ; ce rapport au temps change, et il change aussi le discours.

A mon sens, ce dont la blockchain a le plus besoin aujourd'hui, c'est de pédagogie. Il y a un grand besoin de sagesse, et de beaucoup d'humilité face à ce qu'on ne comprend pas, et ce sous un déluge d'informations peu vérifiées. A l'époque, on disposait de beaucoup moins d'informations mais tout se construisait à une vitesse qu'on était encore à peu près capables d'assimiler culturellement.

Bictoin et Blockchain résistent à notre addiction bien française de réduction conceptuelle et échappe à toute formule, fut-elle élégante, qui tenterait de les emprisonner dans le confort d'une synthèse…

Nadia : Le rapport au temps est effectivement fondamentalement différent, que ce soit sur la presse ou même dans la R&D et le déploiement des technologies.

Une autre différence doit être soulignée : dans les années 1990, le protocole existait déjà, et il était à peu près stable. Avec la blockchain en revanche, le protocole n'est pas unique : divers protocoles potentiels coexistent, dont un en expérimentation depuis 7 ans mais dont le principal problème reste sa mise à l'échelle, problème dont les autres protocoles cherchent les solutions.

Pour revenir à la phrase de Marc Andreessen, on ne se trouve pas tout à fait à TCP/IP pour les 5 ans d'internet. On se situe à la fois un peu avant et un peu après : d'une part, davantage de gens ont entendu parler de la blockchain aujourd'hui que d'internet à l'époque, parce que le buzz a marché, et d'autre part, la technologie n'est pas exactement au même niveau de maturité technique, parce que la blockchain évolue moins vite que son buzz.

Philippe : Il y a un autre point de différence entre blockchain et TCP/IP, une autre différence fondamentale qui pour moi n'est pas assez soulignée.

TCP/IP est le fruit d'un long processus de maturation, parti d'une agence de défense américaine (la DARPA) qui voulait sécuriser les communications en cas d'attaque nucléaire, puis passé dans le civil, avec aujourd'hui encore une gouvernance qui reste largement américaine. C'était en fait une réponse, construite par des gens précis, à un problème précis. Or la blockchain, qui apparait avec bitcoin de façon très singulière, dans un moment très précis, sans que l'on sache qui, au singulier ou pluriel, a pensé cette architecture, a su faire preuve d'une capacité d'adaptation étonnante, et a peut-être même, sept ans après sa création, dépassé largement les desseins et les ambitions de son ou ses créateur(s).

C’est cette émergence de quelque chose de nouveau là où personne ne l’attendait qui constitue une vraie rupture. Bien sûr, il y avait eu des tentatives préalables d’établir des crypto-monnaies, mais sans succès; c’est bien cette combinaison brillante de briques technologiques préexistantes qui a réussi, à la surprise générale, à passer l’épreuve du temps. Et le plus incroyable, c’est que cet ovni technologique existe encore, sans avoir jamais demandé la permission à personne pour se lancer et se développer.

Pour conclure cette longue comparaison, le parallèle TCP/IP-blockchain est un excellent moyen de faire comprendre la situation : face à ce qu’on ne comprend pas, il faut simplement continuer à se poser des questions en toute humilité.

Nadia : Cette comparaison m’évoque aussi autre chose. Je pense que comme TCP/IP, la blockchain n’arrive pas tout à fait par hasard. Pour s’en rendre compte, il faut laisser de côté un instant le volet technologique et se pencher sur le volet social.

Dans le contexte actuel où les citoyens font le choix d’aller vers des partis politiques qu’on qualifie “d'extrême”, où d’autres choisissent l’opposition brutale, multiplient leurs engagements associatifs, vont dormir debout place de la République, on a le sentiment que la question politique de l'organisation des citoyens se pose de plus en plus. Or, les citoyens sont habitués depuis des décennies à l’amélioration constante de leur situation : santé, nourriture, emploi… Il est bien connu que la croissance n’existe que si on continue à accélérer, ce qui devient de plus en plus difficile avec nos ressources limitées. Que des individus se tournent vers le pair-à-pair, changent leurs modes de consommation avec le prêt ou la location plutôt que de l’achat, cela démontre une volonté de continuer cette progression sociale avec d’autres méthodes. La blockchain en participe peut-être.

Il me semble que quelque chose dans cette technologie est politique, quelque chose qui n’est probablement pas entièrement maitrisé, mais qui, je pense, intègre aussi l’intérêt collectif : ce projet touche directement les sujets qui nous préoccupent et interroge les modes de fonctionnement de notre société. C’est un projet perturbant, surtout pour les Français et leur mentalité jacobine ; il suffit de voir les questions qui nous viennent à l’esprit sur la blockchain sont toujours un peu les mêmes : comment va-t-on la contrôler, à qui appartient-elle, quelle est sa gouvernance…

Cette dimension-là ne doit pas être oubliée, parce qu’elle justifie aussi une partie de l’attention qu’on donne à la blockchain au-delà d’un phénomène de bulle. C’est un peu différent d’internet et de la promesse de diffusion de l’information, au fond maîtrisée par des acteurs gouvernementaux. La promesse de la blockchain est assez étonnante, même si nous en sommes pour l’instant bien protégés par nos règles, nos institutions, et par nous-mêmes: lorsqu’on entend que l’emploi demain risque d’être totalement différent de ce qu’il est aujourd’hui, cela ne simplifie pas son acceptation.

Quel devrait être le rôle de la puissance publique, à la fois dans son rôle d'impulsion (comme la Caisse des Dépôts) mais aussi en tant que régulateur?

Nadia : Nous avons souhaité associer les régulateurs, tout au moins dans les réflexions du think-tank, parce que cela nous semblait important qu'on comprenne le sujet en même temps. De cette manière, cela permettra d'être au même niveau de compréhension de la technologie si jamais venait le besoin de mettre en place de la régulation.

Notre conviction est claire : il est préférable de ne pas se précipiter sur la mise en place de la réglementation, et il est important de d'abord comprendre ce qu'est la blockchain avant de la réguler.

Philippe : Je crois que tout le monde connait la caricature un peu forcée des pouvoirs publics français face à un nouveau business : si ça bouge, je taxe, si ça bouge encore, je réglemente, et si ça ne bouge plus, je subventionne ! Cette vieille antienne, je souhaite qu'on l'évite sur le sujet blockchain. En France du moins, il me semble qu'on l'a assez bien compris.

Nadia : Il y a quelques initiatives en France, du gouvernement sur les bons de caisse (mini-bonds), de la Banque de France sur une expérimentation, qui sont de bons premiers pas. En revanche, pour être allés très récemment à Bruxelles pour ces sujets, nous avons compris qu'il y avait un très gros écart entre les pays à la fois en termes d'avancées techniques et de mentalités. Le réflexe naturel de certains organismes était de se demander comment contrôler, et arrêter le processus, tandis que d'autres institutions tentaient en revanche de montrer qu'il était trop tard pour arrêter ce projet, et qu'il fallait plutôt trouver des manières de travailler avec.

Les positions sont donc différentes, en fonction des pays et des organisations, parce que nous en sommes tous encore au stade de compréhension du sujet. Il y a aussi des difficultés inhérentes à la technologie. L'astuce marketing brillante qui a consisté à ne plus parler de bitcoin mais de blockchain a permis de lever un certain nombre de blocages (le fantasme du projet concurrençant le monopole des institutions sur la monnaie constituait un point de friction important), mais il reste des problématiques non négligeables sur le plan de la technologie, parce qu'elle est notamment porteuse de désintermédiation, et qu'il n'y a pas de plus gros tiers de confiance que la puissance publique…Malgré tout, l'avancée des Britanniques sur le sujet, qui ont présenté dans un rapport[62] des propositions d'utilisation de la blockchain pour réinventer le service public tout en le laissant au cœur du système, a permis de continuer à explorer le sujet. L'Estonie est aussi clairement en avance sur ces thématiques-là. Je suis assez confiante sur le fait qu'il y aura bientôt une bonne compréhension du sujet. Car un phénomène ne doit pas être sous-estimé : dans ces institutions, ceux qui se saisissent du sujet sont rarement opposés au

[62] Il s'agit d'un rapport de janvier 2016 du Government Office for Science, l'organe scientifique de conseil du premier ministre Britannique, qui s'intitulait : « Distributed ledger technology : beyond blockchain ». Plus d'informations : http://bit.ly/1TBMYr7

projet blockchain, et ils vont rapidement constituer des relais efficaces d'évangélisation en interne.

Philippe : Je suis tout à fait d'accord. A mon sens, la puissance publique a deux autres rôles à jouer, qui ne seront pas évidents. Le premier enjeu, c'est de comprendre le rôle transformationnel social, et de comprendre le besoin ou les attentes qui dont derrière cette technologie, pour savoir comment les écouter et les prendre en compte au plus vite, sans faire de promesses qu'on ne pourra pas tenir.

Et le second, plus immédiat et plus pragmatique, c'est de savoir comment transformer cette opportunité en avantage compétitif, soit à l'échelle d'une nation, soit à l'échelle d'un continent comme l'Europe. Il ne faut pas se leurrer: il est dans l'intérêt des Etats-Unis de s'assurer que les futurs experts mondiaux qui s'imposeront sur les sujets blockchain soient basés aux Etats-Unis, tout d'abord parce que s'ils sont sous leur juridiction, ils pourront les taxer et les contrôler.

Or je constate que blockchain est un domaine qui requiert des compétences aujourd'hui encore surabondantes en Europe, et particulièrement en France. Les Estoniens, les Roumains, les Slovènes, par exemple, ont des codeurs de très grand talent. L'Europe possède également une bonne maîtrise de l'algorithmie fondamentale, qui est au cœur de ces systèmes. Ce que nous avons voulu expliquer à Bruxelles, c'est que le plus grand service qu'on puisse rendre à l'Europe, c'est de lancer dès que possible des programmes de recherche sur ces sujets, de financer la blockchain, même si ce n'est à hauteur d'une fraction des montants qui alloués aux programmes spatiaux ou à la fusion nucléaire, mais de les financer tout de même.

Concrètement, il nous suffirait de par exemple s'aligner sur les Estoniens, qui sont aujourd'hui les plus rapides sur le sujet, pour démultiplier leurs projets, et faire de la blockchain un sujet politique et de souveraineté économique. Pour ça, il faut se préparer à investir massivement dans des entreprises ou des consortiums qui pourront, une fois le sujet à maturité, prendre la tête de la course mondiale. Cette compétition ne se passera peut-être pas uniquement par les technologies et les financements, mais aussi par le biais de cadres juridiques un peu "smart", puisqu'on constate que les plus beaux leviers de régulation et d'action ne se trouvent pas dans la blockchain elle-même mais sur le plan de ses interfaces (qu'est-ce qui a une valeur probante ou pas, quel statut pour les plateformes, etc.). C'est en jouant aux entrées-sorties qu'on pourra développer un écosystème favorable. C'est d'ailleurs l'intérêt absolu du régulateur, puisque comme le soulignait astucieusement le rapport britannique, la blockchain pourrait être l'occasion de changer la manière de faire de la régulation, en jouant sur la traçabilité des décisions par exemple.

En discutant avec Stephan Tual, de Slock.it, j'ai appris qu'ils rencontrent des problèmes opérationnels idiots, comme par exemple la nécessité de définir le lieu de résidence de la DAO, puisque les adresses sont obligatoires aujourd'hui pour éditer une facture en France…

Philippe : Si j'ai bien compris les raisons pour lesquelles Ethereum est en Suisse, ce n'est pas tant pour la fiscalité, c'est surtout pour des raisons de régimes juridiques et de législation qui permettent plus de choses qu'ailleurs. Les questions administratives telles que celle-ci, savoir pourquoi une facture doit mentionner une adresse, c'est aussi ce qui est intéressant dans ce sujet blockchain. La technologie va nous forcer à nous reposer des questions assez fondamentales qu'on ne se posait plus.

Nadia : Aujourd'hui, une facture s'adresse à une personne dans la mesure où elle habite à un endroit donné. Cela pose de vraies questions aujourd'hui, même sur le plan individuel. Le cœur du problème est bien sûr que la résidence est liée à la fiscalité et vice-versa.

Philippe : Tout cela nous oblige à dérouler un certain nombre de questions. Pour certaines, il faudra seulement mettre quelques grilles à jour. Mais pour d'autres, dont le fondement sera plus profond, il faudra peut- être apporter des réponses entièrement nouvelles.

Ma dernière question portera sur l'avenir, proche ou lointain : quelles urgences, et quels pronostiques pour la technologie selon vous ?

Nadia : Il y a bien sûr une urgence à s'y mettre, à ce que la France et l'Europe investissent. Nous faisons des expériences aujourd'hui à notre échelle, avec des budgets encore limités, mais si la volonté est d'approfondir les choses comme le font les Américains ou les Chinois, il faudra bien se mettre à investir. Bien sûr, il faudra garder en tête que cela peut se faire de façon intelligente, et pas en se contentant d'aligner des millions juste parce que les voisins l'ont fait.

Philippe : Ça me rappelle ce mantra du bon investisseur : "un investisseur n'investit jamais pour de mauvaises raisons". Investir pour investir, ou parce que les voisins ont investi, ou pour des raisons fiscales par exemple, ce sont de mauvaises raisons. Il faut se méfier dès lors que la raison de l'investissement n'a plus rien à voir avec l'objet de l'investissement...

Donc il faut investir intelligemment, et au sens global de la mobilisation. Nous savons que nous allons rester encore 12 à 18 mois au stade expérimental ; il ne faut pas être focalisé sur le court terme, et se dire que la clef sera d'abord la compétence et le génie des équipes, parce qu'on constate aujourd'hui ceux qui peuvent travailler sur ces sujets sont très peu nombreux. Et nous devons garder en tête le cas des États-Unis, où l'énorme déficit de talents crée une bulle indécente de salaires à la Silicon Valley.

Cette bulle n'existe pas encore en Europe : c'est une formidable fenêtre d'opportunité car nous avons notre chance si on se positionne ensemble. C'est un sujet que pourrait par exemple porter le tandem franco-allemand, même si

culturellement, nous avons encore peu de liens scientifiques. Serait-il par exemple pertinent d'envisager une blockchain multi-Etat pour répondre à un besoin de communication transfrontalier, pour accomplir quelques tâches bien précises, avec un haut degré de certification ? Ce sont des questions auxquelles il serait passionnant de chercher une réponse.
Une dernière chose à observer dans les mois qui viennent, c'est que nous serons tous témoins mi-juillet de la division par 2 de la rémunération des mineurs bitcoin, et de l'évolution du cours de la monnaie et de la stabilité du réseau. C'est, à court terme, une échéance intéressante à garder en tête !

Interview **de Luca Comparini,** Blockchain leader chez IBM France

Comment IBM en est-elle arrivée à la blockchain ?

> Avant tout grâce à nos 3 000 chercheurs dans le monde et les 6 milliards de dollars que nous investissons chaque année en recherche et développement. Cela nous permet souvent de travailler en amont. Nous avons par exemple vu émerger le sujet bitcoin assez tôt, puis le sujet Ethereum, et avons mené dans ce cadre plusieurs expérimentations internes ou privées avec des clients, en phase initiale de test.
>
> En janvier 2015 nous avons dévoilé l'un des premiers prototypes publics utilisant la blockchain d'Ethereum. Il s'agissait d'une machine à laver intelligente, construite avec Samsung. Trois cas d'usage ont émergé suite à cette expérimentation : une machine capable de s'approvisionner en lessive lorsque le réservoir est presque vide ; une machine capable de déclencher l'intervention d'un technicien si une pièce tombe en panne et est couverte par une garantie ; et une machine capable de communiquer avec d'autres objets du même contexte pour négocier des plages d'utilisation horaire, afin de réduire la consommation énergétique du foyer.

Quelles leçons avez-vous tirées de cette expérimentation, au niveau de la blockchain ?

> Cette expérimentation nous a surtout permis de faire assez tôt un état de l'art des potentialités de la blockchain et surtout des "Smart Contracts". A partir de là, nous nous sommes rendus compte que la blockchain pouvait être intéressante à deux niveaux :
> - pour l'Internet des objets. Le nombre d'objets connectés étant amené à exploser, il sera envisageable de privilégier des échanges d'objet à objet (dans ce contexte la blockchain pourrait apporter sécurité et confiance) plutôt que de les orchestrer de façon centralisée[63]. Ce cas d'usage reste cependant assez futuriste ;
> - pour simplifier les échanges et les interactions au sein des différents écosystèmes des entreprises, à commencer par les métiers bancaires et les assurances.

Quelles pistes avez-vous alors suivies ?

> Après avoir mené des expérimentations avec plusieurs technologies blockchain existantes, nous avons constaté qu'aucune d'entre elles n'était capable de satisfaire l'ensemble des exigences de nos clients. Nous avons donc pris l'initiative de la développer *ex novo*. L'initiative a démarré durant la première moitié de l'année 2015, même si certaines briques avaient déjà été posées en interne par nos laboratoires de recherche. Le 17 décembre 2015,

[63] Pour approfondir, cf le white paper « Device democracy », écrit à l'issue du projet : http://www01.ibm.com/common/ssi/cgibin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF

nous avons annoncé la création du consortium Hyperledger. Selon IBM, c'est la convergence très rapide de la communauté sur le socle de base TCP/IP qui a fait le succès d'Internet à ses débuts. Ce que nous voulons faire, c'est donc éviter la divergence des solutions blockchain et fédérer les efforts de développement entre les acteurs majeurs de l'IT.

Quel sont les principes d'Hyperledger, et ses spécificités par rapport aux blockchains Bitcoin et Ethereum ?

Hyperledger est une blockchain privée, tandis que Bitcoin et Ethereum sont des blockchains publiques. Il faut d'abord souligner les différences entre ces deux grands types de blockchains, sans porter de jugement de valeur.

Les blockchains publiques reposent sur le principe de transparence : tout un chacun a accès à l'historique de tous les échanges. A l'inverse, dans les blockchains privées, c'est plutôt la confidentialité qui est mise en avant.

De plus, dans les blockchains publiques, il n'existe aucune barrière à l'entrée : nul ne peut empêcher l'autre d'effectuer des transactions. L'algorithme du "proof-of-work" sur lequel repose ces blockchains est techniquement génial, mais impose des contraintes d'architecture : en particulier, la validation des blocs est cadencée (elle n'intervient que toutes les dix minutes dans le cas de Bitcoin), et le nombre de transactions est très faible, trop pour concurrencer les infrastructures de marché existantes. Par exemple, VISA supporte en moyenne 2.000 transactions par seconde, et a été créé pour pouvoir en traiter jusqu'à 56.000 par seconde[64]. L'un de nos clients bancaire a même mesuré jusqu'à 150.000 transactions par seconde sur ses systèmes de back-end[65]. Avant qu'un réseau ouvert puisse atteindre de tels chiffres, il faudrait changer bien des choses.

Contrairement aux blockchains publiques, les blockchains privées imposent une barrière à l'entrée : le droit de participer au réseau d'échange. Ne peuvent faire partie du réseau que les membres qui en sont habilités. Les blockchains privées n'ont pas besoin du "proof-of-work". Elles se basent sur des algorithmes bien plus rapides pour accéder au consensus, élément crucial qui détermine le volume, la capacité de traitement, la vitesse, la performance…

Comment fonctionne la gouvernance d'Hyperledger ?

Le code est open source et la gouvernance est cadrée par la Linux Foundation. Nous sommes moteur de l'initiative Hyperledger, mais nous ne sommes pas le seul contributeur du projet. Notre proposition de code a été mise en open source sous le nom de Open Blockchain. Parmi les autres contributeurs on retrouve Digital Asset, Ripple, Blockstream et Intel[66]. L'ambition à terme est d'avoir une convergence des fonctionnalités vers une seule technologie "mainstream" : Hyperledger.

[64] Cf https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf
[65] Cf http://www-03.ibm.com/systems/z/resources/engines-of-progress/#citi
[66] Cf https://github.com/hyperledger/hyperledger

Nous raisonnons en écosystème : de notre point de vue, la vague blockchain est si importante qu'il n'est pas possible de coder dans son coin et d'imposer ses standards si l'on souhaite réussir. Plus nous sommes nombreux et agissons de façon accessible et méritocratique, plus nous avons de chances que les choses convergent.

Avez-vous déjà testé en interne la blockchain au niveau des processus d'IBM ?

Nous avons commencé avec notre banque interne, IBM Global Financing : nous avons "blockchainisé" fictivement les 6 derniers mois de transaction de l'année 2015.

Sur les 2,9 millions de transactions par an effectuées par cette banque, environ 25.000 litiges sont relevés (par exemple un client déclare ne pas avoir reçu de la marchandise alors que selon le transporteur, elle été livrée). Il faut en moyenne 44 jours pour résoudre un litige, pour un coût moyen de 31.000 $. Environ 100 millions $ de capital sont donc immobilisés en permanence uniquement pour se couvrir de ces problèmes[67].

Grâce à la blockchain, qui renforce la transparence et porte à la connaissance de tous les utilisateurs (dans ce cas les partenaires, les fournisseurs et les acteurs impliqués dans la chaîne de valeur) l'état d'avancement du processus, il devient possible de réduire le temps de résolution des problèmes à une moyenne de 10 jours. Cela permet donc de libérer une partie conséquente du capital bloqué, qui peut être employé ailleurs. Blockchain va ainsi permettre de compléter les systèmes existants, sans avoir à les remplacer.

Quels seront pour vous les premiers secteurs impactés par la blockchain ?

Je pense que les banques seront les premières à prendre le virage blockchain. Je crois aussi beaucoup au secteur de l'assurance, pour lequel je vois un intérêt à faire de la certification ("proof of existence") sur des blockchains publiques. Le secteur assurantiel est aujourd'hui entièrement déclaratif. Un cas d'usage facile à mettre en place pourrait être le suivant : aujourd'hui, quand l'assuré déclare parcourir 10.000 kilomètres par an, l'assurance n'a pas forcément les moyens de le vérifier. On peut donc imaginer qu'à chaque recharge d'essence, tous les 500 kilomètres par exemple, une notification soit envoyée vers une blockchain publique qui certifie le kilométrage, et que l'assureur puisse récupérer cette information.

Quels acteurs vous semblent les plus en avance sur le sujet ?

Le secteur des Banques et des Assurances est clairement en avance par rapport aux autres. Cela étant, certains de nos clients venant d'autres secteurs se montrent eux aussi intéressés.

[67] Cf https://www.youtube.com/watch?v=F0P7NM7d-ps

A mon sens, 2015 a été l'année de la découverte, 2016 est l'année de l'exploration, et 2017 ou plus sûrement 2018, sera l'année du déploiement (non plus de prototypes, mais de produits complets).

N'y a-t-il pas déjà des projets blockchain en cours de déploiement ?

Oui, des clients commencent à mener des explorations sur des cas d'usage qui impliquent peu de contraintes de réglementation. Pour voir des choses se développer sur des marchés hautement réglementés et complexes, il faudra attendre...

Quelle est votre vision d'Ethereum ?

C'est une très belle technologie, fascinante, encore plus que Bitcoin. Mais tout ne peut pas être résolu avec Ethereum, de la même façon que tout ne peut pas être résolu avec des blockchains privées.

Prenons un exemple très concret : quand vous allez au marché de fruits et légumes, le marchand n'a pas besoin de connaître votre identité. A l'inverse, quand un constructeur aéronautique achète des pièces à ses fournisseurs, il a besoin de connaître leur identité. C'est la même chose pour la blockchain : il y a deux types de marchés différents. Dans les marchés B2C ou C2C, certains paradigmes comme ceux pensés par Ethereum fonctionnent très bien. Dans les contextes B2B, Ethereum n'est à mon avis pas la meilleure solution.

Et votre vision de Bitcoin ?

En prenant ma casquette de technophile, je dirais que c'est une technologie passionnante : elle a résolu le problème du consensus pour la première fois.

Si la question porte sur le fait que Bitcoin puisse être utilisé partout, notamment dans des contextes règlementés, je reste mitigé. Je dirais que les aspects de "censorship-resistant" et surtout d'anonymat (au moins au sein du réseau Bitcoin) sont difficilement compatibles avec les enjeux de nos clients et les problématiques de "compliance" que la plupart d'entre eux doivent satisfaire.

Au-delà des choix d'architecture et des contraintes techniques qui peuvent limiter l'adoption du Bitcoin, la viabilité de ce protocole dépend de sa capacité à évoluer. Son modèle de gouvernance doit lui en donner les moyens.

Y a-t-il une bulle blockchain actuellement ?

Absolument. Les expérimentations se développent un peu partout, mais avant que la blockchain puisse remplacer tous les systèmes existants (il faudra attendre pour cela que les clients, les régulateurs, le marché et la technologie soient prêts), on assistera à une phase progressive où la blockchain commencera à compléter ces systèmes.

Où se place la France dans la blockchain ?

Il est évident que les anglo-saxons ont davantage de maturité technologique, de capacité à être rapide dans la prise de décisions et n'hésitent pas à investir financièrement sur le long terme.

Cela étant, la France me semble être tout à fait bien placée. L'initiative de la Caisse des Dépôts va dans la bonne direction, puisque "faire de la blockchain seul dans son coin" n'a aucun sens. La blockchain n'a d'intérêt que dans une logique d'écosystème, en interaction avec des acteurs appartenant aussi bien à un même marché qu'à des marchés différents, par exemple pour se partager des informations ou effectuer des transactions entre eux. Mon espoir est que l'initiative de la Caisse des Dépôts en fédère d'autres, qui ne soient plus simplement franco-françaises, car les frontières géographiques n'ont pas beaucoup de sens dans le monde de la blockchain.

Interview de Julien Maldonato, Directeur Conseil chez Deloitte**,** en charge de l'offre de transformation digitale auprès des institutions financières

Y a-t-il selon toi une bulle autour de la blockchain actuellement ?

La blockchain est sans conteste le "buzzword" de ces 6 derniers mois parmi les tendances technologiques, le bruit généré est énorme, l'imagination des commentateurs semble être sans limite, malgré une compréhension qui reste limitée. Un milliard de dollars a été investi dans les entreprises de la Blockchain et du Bitcoin avec néanmoins un ralentissement sur le 2ème semestre de l'année 2015. Les investisseurs restent prudents, je ne vois pas de bulle spéculative à l'horizon.

Puisque la comparaison est souvent faite entre la Blockchain et Internet, rappelons la séquence qui a précédée la bulle Internet :

- 1973 : Définition de la suite des protocoles TCP/IP à la base d'Internet
- 1983 : Adoption de la suite des protocoles TCP/IP par le réseau Arpanet comme son seul protocole officiel
- 1993 : Apparition du Navigateur web NCSA Mosaic
- 1996 : 1 million d'ordinateurs connectés au réseau Internet
- Mars 2000 : La bulle spéculative sur les valeurs du secteur de l'Internet atteint son apogée et finit par "éclater" (un krach s'étendant à l'ensemble des bourses et provoquant une récession sur le secteur technologique et l'économie en général)

J'ai assisté à l'explosion de cette bulle depuis les premières loges, je travaillais comme développeur dans une des nombreuses start-up californiennes de l'Internet en 2000, c'était la ruée vers l'or "Dot com" ! Aujourd'hui pour la blockchain nous sommes encore très loin d'une telle euphorie, il serait même prématuré de vouloir définir des standards, nous devons attendre d'avoir des premières expériences hors des labs, autres que Bitcoin.

À quelle échelle de temps vois-tu l'utilisation généralisée de blockchains pour les entreprises, et quels défis se posent à cet égard ?

Je partage le sentiment de Vitalik Buterin (fondateur d'Ethereum) pour qui il n'y aura pas de "Killer App" mais une "longue traîne" d'usages. S'il y a peu de doutes que les usages seront nombreux, l'horizon de temps de cette généralisation est plus difficile à prédire avec précision.

Certains commentateurs parlent d'une dizaine d'années, personnellement je pense qu'une généralisation pourrait prendre davantage de temps. Avant tout, de nombreux défis doivent être relevés pour permettre le développement de la blockchain :

- Le manque de connaissance et de compréhension par les entreprises ;
- L'approche de l'entreprise trop centrée sur elle-même : chaque entreprise développant sa propre chaîne avec ses propres standards ;

- Le choc culturel de placer confiance et autorité dans un réseau distribué plutôt que dans une institution centrale (avec un changement qui se fera à 80 % sur les processus métiers pour 20 % d'implémentation technologique);
- Les coûts d'un passage à l'échelle ;
- L'absence de gouvernance et de régulation ;
- L'absence de garantie du respect de la vie privée et de la sécurité.

Une fois tous ces défis relevés, certains imaginent la blockchain devenir un "ordinateur universel" à base de "Smart Contracts", mais il n'y a malheureusement pas de magie en informatique : il faudra écrire beaucoup de lignes de code pour rendre ces contrats "intelligents" (et sans bug) ! Les chantiers d'implémentation seront longs mais passionnants car ils pourraient structurer notre future société.

Les grandes entreprises traditionnelles ont-elles selon toi plus à gagner (économies sur les coûts...) ou à perdre (nouveaux entrants très disruptifs) d'une arrivée massive de la blockchain ?

De potentielles économies sur les coûts sont à espérer pour les entreprises dont l'activité nécessite un fort volume d'échanges, c'est notamment le cas des banques. Santander a estimé en juin 2015 que la technologie de la blockchain pourrait permettre aux banques d'économiser de 15 à 20 milliards de dollars par an d'ici à 2022 en coûts d'infrastructures liés aux paiements internationaux, au *trading* et à la mise en conformité. Plus récemment, Morgan Stanley a estimé une baisse allant jusqu'à 50 % sur les coûts des transactions !

Il faut néanmoins tempérer ces chiffres car leur réalisation est conditionnée au cadre législatif et réglementaire. Si l'on prend le cas d'usage souvent discuté des opérations "post marché" (la phase de compensation et le règlement-livraison), plusieurs évolutions réglementaires seront à envisager : reconnaître la technologie Blockchain comme une preuve authentique au regard de la loi, amender la directive EMIR pour ne plus obliger la compensation, amender la directive MIF II pour ne pas qualifier la blockchain de système de négociation…

En outre, au-delà des contraintes réglementaires, quelle que soit l'industrie, de nombreuses inconnues subsistent encore dans l'équation du ROI (degré de mutualisation des infrastructures, coûts d'interfaçage des chaînes avec des services externes notamment le coût des "Oracles", coûts de dé-commissionnement des anciens systèmes, …)

La recherche d'économies sur les coûts n'est pas la première motivation des entreprises traditionnelles qui lancent des initiatives blockchain (pour cet objectif elles trouveront plus rapidement et plus facilement des gains *via* l'automatisation des processus), c'est davantage la peur de perdre son marché au profit de nouveaux entrants. Après la peur d'être "uberisé", on a maintenant la peur d'être "blockchainisé" !

Quels secteurs seront à ton avis les plus impactés ? Quels sont pour toi les cas d'usage les plus prometteurs ?

Les secteurs les plus impactés seront ceux où des échanges sont réalisés dans un contexte de confiance minimale. On cite souvent la possibilité que des blockchains remplacent les tiers de confiance traditionnels (banques, chambres de compensation, assureurs, notaires, …) mais également les plateformes de l'économie collaborative (Uber, AirBnB, Crowdfunding, …). Cette possibilité est prise au sérieux et tous ces acteurs se mettent progressivement en ordre de marche pour trouver une complémentarité future avec la blockchain.

Parmi les cas d'usage prometteurs, j'aime beaucoup celui de la coopérative TransActive Grid qui utilise la blockchain pour gérer de l'énergie renouvelable produite par des résidents d'un quartier de New York : de façon automatisée, sans intermédiaire, c'est la plateforme de blockchain Ethereum qui gère les flux énergétiques tout en conservant sur la chaîne l'historique de l'énergie produite et des transactions qui en découlent.

Un autre cas d'usage a retenu mon attention récemment, Deloitte au Pays-Bas a développé un prototype de "Warranty Bot" avec la nouvelle interface "Chatbot" de Facebook Messenger. Cette application permet à l'utilisateur de facilement tracer ses achats de biens (stockage des factures) et de souscrire puis gérer des garanties pour ses biens. La blockchain est utilisée dans ce cas pour permettre la traçabilité de l'achat du bien, de la garantie associée, de la revente du bien / changement de propriétaire, des extensions de garanties…

Comment Deloitte se prépare-t-il à la blockchain ? A partir de quand le cabinet a-t-il commencé à s'y intéresser ? A propos de Rubix : peux-tu nous expliquer ce que c'est ? Quel usage et quel avenir y vois-tu ?

Deloitte a formé il y a 3 ans une communauté d'experts (DC3 : Deloitte Cryptocurrency Community) qui regroupe aujourd'hui plus de 200 spécialistes des crypto-monnaies et de la blockchain dans 20 pays. Cette communauté interne a déjà collaboré avec le World Economic Forum, la Singularity University et la MIT Media Lab's Digital Currency Initiative pour étudier et définir des usages de la technologie blockchain.

En 2015, après une année de R&D, nous avons ouvert Rubix, une plateforme de "Blockchain as a Service" (BaaS) qui permet aux équipes et aux clients de Deloitte de créer, tester et déployer rapidement des "ĐApps" (decentralized applications) basées sur la technologie des contrats intelligents et de la blockchain pour n'importe quel usage, le tout dans un environnement privé.

En complément de notre plateforme Rubix, nous avons mis en place des partenariats avec 5 des start-up les plus en pointe dans le domaine de la blockchain : BlockCypher, Bloq, ConsenSys, Loyyal et Stellar Development Foundation.

A ce jour nous avons déjà réalisé pour nos clients 20 prototypes "ĐApps" incluant notamment : les paiements transfrontaliers, la banque digitale, la gestion des identités, la gestion des données de santé, la gestion des points de fidélité…

Avec Rubix, notre large communauté de développeurs et nos partenaires nous sommes aujourd'hui positionnés comme leader pour accompagner les entreprises dans les usages de la technologie blockchain.

Un dernier mot sur les pouvoirs publics, en France notamment : qu'attendre du législateur et/ou du régulateur sur ces sujets ?

Les pouvoirs publics ont la possibilité donner à la France un avantage compétitif fort en mettant en place un cadre législatif favorable, notamment en reconnaissant la technologie blockchain comme une preuve légale authentique. Cet avantage permettrait l'émergence d'un "écosystème blockchain français" propice au développement des futurs leaders mondiaux.

En outre, des investissements sont nécessaires dans les entreprises qui utilisent la blockchain, également dans l'enseignement et la recherche. Pour permettre ces investissements, la technologie blockchain pourrait être inscrite dans le Programme d'Investissements d'Avenir (PAI) de l'État français.

Neuf erreurs à ne pas faire en appliquant la blockchain à son business

John Rampton , Entrepreneur très curieux de blockchain, et gourou du marketing online. Il a notamment fondé la société de paiement en ligne Due. Après avoir tenté d'appliquer une solution blockchain à sa start-up, il revient dans ce texte sur les leçons qu'il a tirées de son expérience. Il met en garde en particulier contre 9 erreurs qu'il a commises, que voici :

1. Ne pas comprendre comment la blockchain fonctionne

> J'ai fait l'erreur de considérer que je pourrai comprendre sur le tas ce qu'il fallait savoir sur la technologie.
>
> Prendre le temps de lire la recherche disponible, faire le point sur l'état de l'art et consulter les tutoriels se serait avéré une bien meilleure idée. Une bonne idée également aurait été de chercher des informations du côté des entreprises compétentes qui travaillent dans l'écosystème blockchain et bitcoin, et de visiter les forums où l'on répond aux questions pour accéder à une compréhension un peu plus pratique de la technologie.
>
> Au lieu de ça, je me suis mal débrouillé, et j'ai perdu un temps et des efforts considérables qui auraient pu être évités, par exemple si j'avais compris plus tôt qu'il est possible d'héberger certains systèmes de donnée en dehors de la blockchain sans pour autant causer de doublons opérationnels.

2. Ne pas choisir les services blockchain qui correspondent à son besoin

> J'ai commis à l'origine l'erreur de me concentrer sur la blockchain bitcoin, sur des critères simples: 1- parce que j'en avais déjà entendu parler et 2- c'était celle dont la longévité offrait le plus de garanties en terme de stabilité.
> C'est ce qui me semblait à l'époque le choix le plus crédible, mais ce n'était pas nécessairement le plus adapté aux besoins de mon business, ce dont je me suis rendu compte quand j'ai commencé à me pencher sur les autres possibilités de blockchains.
> J'ai donc dû revoir ma copie et ai trouvé des services blockchains plus adaptés à mon besoin, quand bien même ils ne présentaient pas le même niveau de robustesse que la blockchain de Bitcoin.

3. Se montrer impatient au point de forcer la main à une adoption de la blockchain

> Il me semblait que tout le monde devait être aussi excité que je l'étais par le potentiel de la blockchain dans ses diverses applications.
> Pourtant, je me suis vite rendu compte qu'il fallait du temps pour gagner l'adhésion des autres organisations que je voulais inclure dans ma blockchain privée. Il fallait non seulement que je les convainque de la valeur ajoutée

apportée par la techno, mais qu'en plus on s'accorde sur le *software* à utiliser, ce qui était loin d'être le plus facile.
Depuis, j'ai dû apprendre à être patient. Mais j'ai également changé ma façon d'approcher ces organisations, en me fondant sur une approche proactive concentrée sur les bénéfices qu'elles retireraient de l'usage de la blockchain. Je suis convaincu qu'elles finiront par se rallier à cette idée, à terme.

4. Penser que chaque fonction de l'entreprise peut être améliorée grâce à la blockchain

La blockchain ne peut pas tout - du moins pas sous sa forme actuelle-.
La bonne nouvelle, c'est qu'étant donné que le réseau n'est accessible qu'à un nombre limité de personnes, tout ce qui ne fonctionnera pas au moment du test n'aura pas à impacter in fine votre activité ou votre image de marque.

5. Croire que le système est déjà protégé des erreurs des utilisateurs

Internet se sert de noms de domaines plutôt que des adresses IP pour identifier une adresse, tandis que la blockchain fait appel à des clefs publiques, ce qui rend plus facile l'erreur humaine.
C'est un exemple du genre d'erreur qui m'est arrivée, à moi et beaucoup d'autres. La mise en place d'une couche supplémentaire, à la façon des noms de domaine, permettrait de limiter ce genre d'erreurs d'utilisateur classique.

6. Ne pas limiter l'accès aux clefs privées

Il faut éviter d'accorder à tous les membres d'une organisation l'accès à la clef privée qui déverrouille l'accès à la blockchain.
C'est un point important, parce que l'ingérence de gens qui ne savent pas ce qu'ils font risque de corrompre le registre. J'ai donc dû déterminer qui devait avoir accès aux clefs privées, et quelles solutions d'accès étaient envisageables. Je continue de travailler à une solution d'urgence pour le cas où une clef privée se révélerait corrompue ou serait perdue.

7. Alourdir la blockchain

J'ai réalisé qu'en utilisant la blockchain pour des applications impliquant un grand volume d'informations, la quantité de données stockées dans la blockchain pouvait enfler à toute vitesse. Pour alléger la charge pesant sur la blockchain et donc revenir à un niveau de vitesse et d'efficacité acceptable, j'ai été contraint de relier la blockchain à une base de données extérieure.
Quand bien même la séparation des données peut affecter légèrement la fiabilité du système, cela reste toujours préférable à une blockchain plombée par la data.

8. Ne pas comprendre qu'il y a des limites à l'utilisation de la blockchain comme base de données

La blockchain est une excellente solution pour une base de donnée privée et sécurisée, mais ce n'est pas un fourre-tout destiné à absorber une quantité infinie de données. Tenter de s'en servir pour n'importe quelle application de base de données à grande échelle peut s'avérer une erreur.
Non seulement la blockchain sera incapable de contenir de façon fiable toutes les informations que vous souhaitez y stocker, mais cela pourrait également devenir très compliqué de prendre en charge en plus les outils d'analyse nécessaires au traitement de toute cette information.

9. Ne pas voir les défauts existants et potentiels

A cause de mon excitation pour cette technologie, j'ai considéré la blockchain comme la solution magique à mes problèmes - mais la réalité est qu'il existe bien des défauts inhérents à sa construction qui doivent encore être réglés.
C'est d'ailleurs un système qui continue d'évoluer, ce qui laisse la porte ouverte à d'autres défauts. Cela signifie aussi que j'ai dû agir avec plus de précautions avant d'intégrer complètement la technologie dans les applications dont je me servais pour mon entreprise.
Je suis donc resté à la phase de test et j'ai circonscrit les utilisations pour voir comment les défauts manifestes de la blockchain vont être résolus. C'est également pour cela que je suis convaincu de l'importance de la recherche, de la lecture, de l'engagement sur les forums et de se tenir au courant.

Bilan

La leçon la plus importante : être curieux et ouvert d'esprit vis-à-vis du potentiel que la blockchain peut représenter pour nombre d'applications - et les mettre ensuite en place avec méthode, après un nécessaire travail de recherche et d'expérimentations.
Ce processus peut du reste être grandement facilité si les différentes entreprises cherchant à adopter ces potentielles applications collaborent entre elles.

CONCLUSION

Par Blockchain France

La blockchain n'est pas un sujet numérique de plus. Elle a le potentiel de transformer radicalement nos économies et nos sociétés. La France peut encore se placer à la pointe de la révolution qui s'annonce, à condition de suivre quelques principes de bon sens.

En janvier, le gouvernement britannique a publié un rapport sur la blockchain à destination du législateur et des pouvoirs publics. Il soulignait les dimensions essentielles devant permettre à la technologie de se déployer dans de bonnes conditions. Les propositions qui en ressortaient sont applicables aujourd'hui aussi bien à la France qu'au Royaume-Uni.

Le premier impératif est celui de l'investissement et de l'expérimentation. L'investissement devra se faire dans toutes ses dimensions et notamment dans la recherche. Nous avons en France des chercheuses et des chercheurs d'exception : il est important qu'ils s'approprient la blockchain comme terrain de recherche, et bénéficient pour ce faire des outils et des moyens à la hauteur des enjeux.

Investir, plus généralement, c'est identifier les nombreuses idées et les multiples talents que nous avons sur notre territoire, et s'assurer qu'ils peuvent se déployer où et quand il le faudra. A notre sens, la bonne démarche, que nous avons essayé de suivre en construisant ce livre, est d'aller sur le terrain et "mettre les mains dans le cambouis" pour dépasser le superficiel et les emballements. Allons regarder ce que la blockchain a vraiment sous le capot ! Ce n'est qu'en testant et en expérimentant que nous pourrons nous rendre compte de la réalité qui se cache derrière les promesses.

Le deuxième volet concerne le cadre de régulation. Brider une technologie à ses débuts serait une erreur ; d'autres écosystèmes comme celui de Londres avancent déjà à grande vitesse. Pourtant, il est essentiel pour les acteurs de la blockchain de pouvoir se projeter dans l'avenir, ce qui implique d'avoir une vision claire du cadre dans lequel ils évoluent, et de pouvoir *a minima* anticiper ses mutations. Il faut à tout prix éviter qu'une législation vienne soudainement, du jour au lendemain, détruire des entreprises qui auraient osé se lancer. Le flou juridique actuel ne doit pas constituer un frein pour que l'écosystème grandisse et change d'échelle.

Pour parvenir à ces objectifs, une méthode : cassons les silos ! L'innovation de chacun dans son domaine ne fonctionnera pas pour un sujet aussi complexe et transversal que la blockchain. Le défi qu'il faut au contraire assurer, c'est celui de la transversalité des compétences. Nous pouvons compter, en France, sur d'excellents spécialistes : expert(e)s du chiffre, des algorithmes, de l'Internet des Objets, de la data… mais aussi de savoir-faire industriels précieux venus de tous les domaines. Nous appelons ces spécialistes à se pencher sur la blockchain, et à rencontrer les juristes, les sociologues, les philosophes, les entrepreneurs et les développeurs pour donner à cette technologie toute sa plénitude.

La blockchain est un outil. Un outil ne peut être bon ou mauvais ; seule compte la façon dont il sera utilisé. L'important n'est donc pas de s'intéresser à la blockchain pour elle-même mais bien pour ce qu'elle rend possible, de la même façon que ce sont les applications internet créées par-dessus le protocole TCP/IP qui intéressent le plus grand nombre et non le protocole lui-même. De ce point de vue-là, ce qui sera construit dans les mois et années à venir sera essentiel dans le développement de cette technologie, d'autant que celle-ci renvoie à des enjeux politiques, de souveraineté, et plus fondamentalement de société. Plus que jamais, nous l'affirmons : la France ne doit pas rater la révolution blockchain. Au travail !

TABLE DES MATIERES

Annexe : Lexique

Altcoin : abréviation pour "Alternative Coin". Un altcoin est une crypto-monnaie autre que le bitcoin.

Bitcoin (BTC) : monnaie électronique décentralisée conçue en 2009 par un développeur (ou un groupe de développeurs) non identifié utilisant le pseudonyme Satoshi Nakamoto.

Blockchain : la blockchain est une technologie de stockage et de transmission d'informations à coût minime, sécurisée, transparente, et fonctionnant sans organe central de contrôle.
Par extension, une blockchain (littéralement une "chaîne de blocs") désigne une base de données sécurisée et distribuée (car partagée par ses différents utilisateurs), contenant un ensemble de transactions dont chacun peut vérifier la validité. Une blockchain peut donc être assimilée à un grand livre comptable public et infalsifiable.

Blockchains privées : par opposition aux blockchains publiques, les blockchains privées fonctionnent avec un processus d'approbation contrôlé par un nombre restreint et choisi de nœuds. Autrement dit, les participants au réseau sont limités et sélectionnés. Le droit de lire la blockchain, c'est-à-dire l'accès au registre, peut être lui soit public, soit réservé aux participants du réseau.

Clé privée : clé permettant à l'utilisateur d'une blockchain d'initier une transaction en signant cryptographiquement son message.

Clé publique : clé servant d'adresse sur une blockchain. Connue de tous, elle permet à un émetteur de désigner un destinataire.

Crypto-monnaie : monnaie électronique et peer-to-peer, se basant sur les principes de la cryptographie pour valider les transactions et la génération de la monnaie elle-même.

DAO (Decentralized Autonomous Organizations) : logiciel, programme, qui fournit des règles de fonctionnement transparentes et immuables à une communauté s'organisant autour d'un objectif commun. Elle a pour but, à la manière d'un fond d'investissement classique, d'évaluer des projets qui lui sont soumis, de décider collectivement avec les détenteurs de jetons de la DAO de financer ou non ces projets, et de distribuer les risques et récompenses qui y sont relatifs.

Devcon d'Ethereum : abréviation de "Developers Conference", un évènement annuel constitué de plusieurs jours de rencontres et conférences autour de la blockchain d'Ethereum.

Ether : cryptomonnaie d'Ethereum. Deuxième cryptomonnaie la plus utilisée derrière le bitcoin

Ethereum : blockchain permettant à son réseau d'utilisateurs de créer des smart contracts. Fondée par Vitalik Buterin et mise en place en 2015, elle connaît depuis une progression très importante. La blockchain d'Ethereum fonctionne avec la monnaie Ether. Contrairement à la blockchain du bitcoin, la blockchain d'Ethereum a vocation à accueillir des applications très diverses, qui sortent du cadre purement monétaire.
Fiat money : monnaie "classique", dont la valeur est donnée par la loi ou la régulation gouvernementale (euro, dollar…).

Microtransaction : transaction de quelques centimes. Dans un circuit "classique", *via* une banque par exemple, les microtransactions sont trop coûteuses à réaliser (les frais sont en effet supérieurs au montant des transactions). La blockchain apporte une solution à ce problème.

Minage : utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés.

Mineurs : personnes (particuliers ou sociétés) qui connectent sur le réseau une ou plusieurs machines équipées pour effectuer du minage. Chaque mineur est rémunéré au prorata de la puissance de calcul qu'il apporte au réseau.

Nœud : ordinateur relié au réseau et utilisant un programme relayant les transactions.

Proof of work : "preuve de travail" ou "preuve de calcul". Il s'agit du traitement cryptographique permettant la validation des blocs de transactions notamment sur Bitcoin. Afin d'éviter qu'une personne puisse valider plusieurs blocs de suites et ainsi autoriser une transaction frauduleuse, le système oblige tous les mineurs à travailler en compétition sur le prochain bloc. Pour valider un bloc, les mineurs doivent trouver le résultat d'une fonction de "hash" qui corresponde au bloc. Les mineurs vont, en utilisant la puissance de calcul de leur ordinateur, essayer toutes les combinaisons possibles jusqu'à trouver la bonne. La probabilité d'être celui qui puisse soumettre le bloc dépend ainsi uniquement du ratio entre sa puissance de calcul et celle de l'ensemble des mineurs. Le système POW (Proof of Work) permet donc d'avoir un validateur aléatoire parmi la masse de mineurs, tout en s'assurant que ce validateur est une machine, impartiale. Effectuer ce traitement requiert du temps de calcul : en général, un seul ordinateur du réseau y parvient en environ dix minutes (Bitcoin). La difficulté est régulièrement adaptée pour maintenir cet intervalle.

Proof of stake : Comme le proof of work, le proof of stake est une méthode utilisée pour atteindre le consensus distribué dans un réseau blockchain. A l'inverse du Proof of work, le Proof of stake ne demande pas aux utilisateurs d'utiliser leur puissance de calcul, mais plutôt de prouver la propriété d'un certain montant de crypto-monnaie. Ainsi si par exemple il y a 10 millions d'ether en circulation et que j'en détiens 1 million, j'ai 1 chance sur 10 de valider le prochain bloc de la chaîne. Cependant afin d'éviter que la concentration de capital ne permette de valider plusieurs blocs à la suite, si je suis désigné "validateur" du prochain bloc, je ne peux participer aux prochains "tirages au sort" pendant un certain temps.

Satoshi Nakamoto : pseudonyme de l'inventeur du bitcoin, dont la véritable identité est encore inconnue malgré de nombreuses spéculations.

Sidechain : blockchain secondaire qui se développe parallèlement à une blockchain principale, mais qui y est rattachée afin de pouvoir en connaitre toutes les informations. Les sidechains permettent d'accroitre le volume d'informations pouvant être traitées au sein d'une blockchain (volume normalement limité), tout en restant sur une même blockchain principale.

Smart contracts : programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarré

A propos de Blockchain France

Blockchain France, le "hub" de la blockchain en France, se donne pour but de démocratiser la blockchain auprès du grand public, des entreprises et des pouvoirs publics. Son ambition est de faire comprendre avec pédagogie le potentiel de la blockchain et ses enjeux aussi bien business que sociétaux, au travers d'exemples concrets, sans parti pris, et sans en occulter les limites.

Blockchain France est né à l'été 2015 d'une prise de conscience, celle de l'importance qu'allait prendre la technologie blockchain, et d'une constatation, celle de l'absence de contenu pertinent en langue française sur le sujet. Les quatre fondateurs, Claire Balva, Clément Jeanneau, Alexandre Stachtchenko et Antoine Yeretzian, créent alors le site blockchainfrance.net pour alimenter le débat avec du contenu francophone.

Une première tribune, publiée en octobre sur Médium, expose une conviction forte du projet : "La France ne doit pas rater la révolution blockchain". Elle est suivie en janvier de l'organisation de la première grande conférence publique en France sur le sujet, à laquelle s'inscrivent plus de 1500 personnes, témoignant ainsi de l'intérêt porté à cette technologie émergente.

Depuis, l'équipe de Blockchain France continue son travail de démocratisation, à travers des formations et missions de conseil aux entreprises, des meet-up et évènements co-organisés avec la communauté blockchain française, et des interventions publiques lors de divers événements.

Plus d'informations sur www.blockhainfrance.net

A propos de Netexplo

Seule 2% des entreprises dans le monde sont nativement digitales. Netexplo, l'Observatoire mondial de l'innovation digitale, s'intéresse aux 98% qui ne le sont pas encore, en leur fournissant une culture numérique internationale et ouverte afin d'appréhender les changements qui les attendent sur leurs marchés et dans leur organisation.

Netexplo, à travers ses publications, ses études tendancielles, et à travers une veille mondiale réalisée par son réseau de captation international composé d'une vingtaine d'université à travers le monde, met en lumière l'avenir des grandes entreprises, leurs futurs marchés et leurs prochains concurrents.

En révélant les usages émergents du numérique mondial et les grandes tendances qui vont impacter la société, Netexplo est une voie d'anticipation pour toutes les entreprises qui doivent faire face à leur révolution digitale.

Plus d'informations sur www.netexplo.org