- Présentation Henri d'Agrain, DG CHECy
- Quelle est la question ?

Est-il judicieux d'établir un lien entre l'Internet des objets et la sécurité des objets connectés d'une part, et le phénomène blockchain d'autre part ? Difficile à ce stade d'apporter une réponse claire, mais quand même, on peut apporter quelques éléments de réponse. Cependant, pour analyser ces éléments, je vais me permettre de faire un peu d'histoire.

- Rappel sur le rapport Théry :

En 1994, était publié un rapport, resté fameux par son titre, « Les autoroutes de l'information ». Il fut écrit par Gérard Théry et remis au Premier Ministre de l'époque, Edouard Balladur. Avec une vingtaine d'année de recul, sa lecture est particulièrement éclairante de ce que nous vivons aujourd'hui. Elle nous révèle comment trois hauts fonctionnaires reconnus pour leurs grandes compétences, voyaient l'avenir des réseaux numériques et le rôle qu'Internet allait y jouer. On lit en effet dans ce rapport que « son mode de fonctionnement coopératif n'est pas conçu pour offrir des services commerciaux. Sa large ouverture à tous types d'utilisateurs et de services fait apparaître ses limites, notamment son inaptitude à offrir des services de qualité en temps réel de voix ou d'images. » On lit plus loin, après une liste des limites de l'Internet de l'époque pointées par les rédacteurs du rapport : « Ce réseau est donc mal adapté à la fourniture de services commerciaux. »

Pour mesurer la saveur de cette histoire, dont les conséquences sur notre économie numérique se font sentir aujourd'hui encore, il faut rappeler qu'en juillet 1994, au moment même où ce rapport était publié, Jeff Bezos créait à Seattle Amazon qui allait devenir en moins de 15 ans le leader mondial de la fourniture de services commerciaux grâce à l'Internet.

Quels enseignements tirer de cette épisode malheureux ? Ils sont multiples. Nous en retenons un pour la question que nous nous posons aujourd'hui : il n'est pas possible de penser le futur numérique sans une compréhension approfondie des phénomènes à l'œuvre. Une projection linéaire sur la base des leçons du passé est inopérante.

- Les phénomènes à l'œuvre :

Le contexte : Une numérisation croissante, massive et profonde de tous les secteurs d'activité et leur mise en réseau. ***Tout s'accélère, et nous n'avons encore rien vu !***

Pour bien comprendre la puissance de ces transformations numériques, je vous propose de retenir trois lois :

La loi de Metcalfe

La valeur d'un réseau est proportionnelle au carré du nombre de pôles connectés. La valeur d'un réseau de 10 machines est proportionnel à 10^2 soit 100. Si une onzième machine rejoint le réseau, la valeur du réseau élargi d'une unité est proportionnelle à 11^2, soit 121. La valeur du réseau croit de 21% par la croissance de 10% du nombre de pôle dans le réseau !

La loi de Moore

À prix égal, la capacité de calcul d'un microprocesseur (matérialisée par la densité de transistors sur une puce) double tous les 18. La loi de Moore a été étendue à la bande passante (le transport des données) et aux mémoires de stockage de données. Par exemple, sur les 15 dernières années, à prix égal, la puissance des machines a été multipliée par un peu plus de 1 000.

La loi de Grötschel

La vitesse de calcul des machines, grâce à la croissance de l'efficacité des algorithmes (séquence d'instructions d'un programme informatique), progresse 43 fois plus vite que la loi de Moore. Si donc, en 15 ans, la capacité des machines a été multipliée par un ordre de grandeur 1 000, celle des algorithmes a été multipliée par 43 000.

Le cumul de ces trois lois crée une situation inédite, singulière. Il n'existe pas dans l'histoire de l'humanité, un progrès dont le taux de croissance soit constant. Il n'existe pas d'innovation dont l'efficacité s'amplifie à une telle vitesse, en accélérant sans cesse. La courbe formée par ce type de développement est bien connue : c'est une fonction exponentielle.

Bien entendu, les menaces qui se déploient dans le cyberespace sont soumises à ces mêmes lois du numérique. Elles connaissent une croissance exponentielle. Le problème, c'est que notre intelligence à les plus grandes difficultés à appréhender les transformations exponentielles. Nous avons une tendance naturelle à prolonger de manière linéaire le fruit de nos observations et de notre expérience.

- Revenons donc à l'Internet des objets :

Dans un tel contexte, bien sûr, avec des prévisions de connexion de 50 à 250 milliards d'objets dans les 15 prochaines années, nous n'avons plus affaire au même réseau, aux même volumes de données, et non plus donc aux mêmes menaces. Il est nécessaire de mettre en place une infrastructure de confiance afin de sécuriser les échanges de données entre ces milliards d'objets.

- Le protocole blockchain, vers une infrastructure de confiance décentralisée :

Depuis quelques mois, nous entendons parler presque quotidiennement de la blockchain. Que recouvre ce terme abscons, inconnu de la plupart d'entre-nous il y a un an encore ? Début 2015, presque aucune publication n'était disponible sur un sujet essentiellement réservé à des geeks ou des individus appâtés par des perspectives de gains faciles. Depuis le mois de juillet dernier, l'actualité de la blockchain est explosive ! Le sujet n'a cessé de prendre de l'ampleur. La blockchain a même reçu la consécration de The Economist, qui en a fait sa une du 31 octobre 2015 sous le titre « The Trust Machine ».

En 2008, un mystérieux développeur, ou peut-être un collectif, se faisant appeler Satoshi Nakamoto, publie sous licence libre MIT le protocole de la blockchain dans un logiciel écrit en C++. Ce protocole propose une solution particulièrement élégante et habile pour résoudre le problème du modèle de confiance dans un environnement numérique entre personnes qui ne se connaissent pas et ne peuvent se faire confiance a priori. En 2009, le même Satoshi Nakamoto lance la première application basée sur le protocole blockchain pour créer une crypto-monnaie, le Bitcoin. Alors même que le protocole qui le sous-tend est paré de nombreuses vertus, le pauvre Bitcoin pâtit, lui, d'une réputation sulfureuse, injustement méritée à notre avis. Qu'il puisse être utilisé dans des activités

illégales n'invalide pas la pertinence du modèle, ou alors ce devrait être le cas pour toutes les monnaies fiat. De fait, le Bitcoin est la première expérience réussie de développement d'une structure de consensus décentralisé, dont il faut analyser la remarquable robustesse depuis sept ans, en l'absence de toute autorité de régulation. L'algorithme du Bitcoin intègre sa propre régulation. Publié en 2000, l'article fameux « Code Is Law » de Lawrence Lessig – le code fait loi – trouve un archétype dans la blockchain du Bitcoin. D'ailleurs, un professeur de finance de l'université de Californie, sollicité par la Banque de Suède pour lui suggérer des nominations au prix Nobel d'économie, ne s'y est pas trompé en proposant, peut-être en forme de clin-d'œil, le nom de Satoshi Nakamoto pour la promotion 2016 des candidats à la prestigieuse distinction.

Une Blockchain peut être définie comme l'historique décentralisé et exhaustif de toutes les transactions effectuées depuis sa création et qui y sont consignés par blocs consécutifs comme dans un registre ou un grand livre de compte. La sécurité de la transaction est assurée par un réseau pair à pair d'ordinateurs qui valident et certifient la transaction avant de l'inscrire de manière définitive dans un bloc. Une fois enregistrée, cette dernière devient infalsifiable et facilement vérifiable. Le protocole blockchain conjugue les éléments de deux théories, celle de la théorie informatique et celle de la théorie des jeux. De la théorie informatique, il met en œuvre de manière extrêmement habile les technologies de réseaux de pair à pair et de la cryptologie. A la théorie des jeux, il emprunte la notion « d'équilibre de Nash en stratégie dominante ». C'est d'ailleurs au titre de la théorie des jeux que ce situe la principale innovation du protocole blockchain, en proposant une solution radicale au problème de la confiance entre deux parties prenantes qui ne se connaissent pas.

Au-delà du Bitcoin, il est fort probable que le protocole blockchain, et plus globalement les technologies de consensus décentralisé, provoquent, dans les mois et les années qui viennent, un véritable bouleversement de l'Internet. Ce protocole permet d'envisager une multitude d'applications dès lors qu'il s'agit d'enregistrer et de certifier une transaction, un échange ou une identification. Deux qualités de ce protocole lui confèrent son caractère exponentiel : d'une part il est extrêmement générique et neutre ; d'autre part il est perçu comme parfaitement scalable, c'est à dire fondée sur des bases de coûts principalement fixes permettant une montée en charge et une croissance des volumes d'activités rapide et économiquement viable. L'argument principal du protocole blockchain est de réduire de manière significative les coûts de transactions entre agents économiques en leur permettant de s'affranchir des tiers de confiance.

Les champs d'application de la blockchain sont multiples. Depuis plusieurs mois les expériences et les tentatives se développent dans de nombreuses directions. La technologie blockchain peut être utilisée pour des transactions qui vont au-delà d'une simple transaction de paiement ou d'enregistrement et qui contiennent des instructions beaucoup plus complexes, par exemple des instructions conditionnelles et programmables. On parle alors de contrats, un peu abusivement sans doute. Ces contrats sont publiés sur une blockchain pour qu'ils s'exécutent automatiquement sous certaines conditions, raison pour laquelle on utilise l'expression de « Smart Contract ». La société Ethereum, co-fondée par Vitalik Buterin, propose un framework destiné à générer des « Smart Contracts ». Pour prendre une comparaison simple, le code source Ethereum est un peu comme le système d'exploitation d'un smartphone. A partir de ce code, diverses applications, rédigées plus simplement, peuvent être développées par les utilisateurs pour élaborer des « Smart Contracts » sur la blockchain d'Ethereum. Et c'est essentiellement dans ce cadre que des expérimentations sont aujourd'hui menées autour de l'Internet des objets. Avec l'Internet des Objets, le protocole

blockchain pourrait trouver l'une de ses plus larges applications, compte tenu des problèmes colossaux de confiance qui ne manqueront pas de se poser. La confiance, la question de l'identité, du respect de la vie privée et de la confidentialité des données personnelles seront au cœur du développement du marché de l'Internet des objets.

En effet, et là je reprends une catégorisation que m'a soufflé mon ami Xavier dalloz, que certains d'entre vous connaissent peut-être, sur les apports de Blockchain pour établir la confiance de l'Internet des Objets, avec l'acronyme I.M.P.A.C.T

- ✓ Identification (je sais à qui je parle)
- ✓ Monétisation
- ✓ Preuve (consentement lu et approuvé – certifié)
- ✓ Autonomie (pas de manipulation)
- ✓ Contrat (ce qui manifeste notre accord par le code)
- ✓ Traçabilité (Mémoire distribuée non falsifiable) et Transparence

Plusieurs preuves de concept ont été lancées autour du mariage de l'Internet des Objets et de la blockchain. Citons par exemple les recherches exploratoires menées par Slock.It de Stephan Tual. La promesse de Slock.It est de permettre de louer, de vendre ou de partager n'importe quel objet sans intervention humaine, uniquement à partir d'une infrastructure blockchain Ethereum mettant en œuvre un smart contract. Exemple de la serrure connectée !

Plusieurs initiatives de cette nature sont engagées dans le domaine de la production décentralisée d'énergie et la consommation d'électricité. C'est le cas notamment d'un projet mené par SlockIt, encore eux, avec le géant allemand RWE pour la recharge autonome de véhicules électrique sur une prise ou une plaque d'induction. La transaction entre les 2 objets connectés véhicule et borne de charge se fait automatiquement et de manière sécurisée sur la blockchain Ethereum.

On peut également citer une initiative basée en Afrique du Sud, menée par une société active sur le bitcoin, Bankymoon. Elle a mis en place Usizo, une plateforme de crowdfunding pour l'alimentation en électricité. Les écoles sont équipées d'un compteur intelligent, et les donateurs sont invités à contribuer à l'approvisionnement en électricité de l'école en envoyant des bitcoins à l'adresse Bitcoin du compteur électrique de l'école.

- Conclusion

Je ne prétends pas que le mariage entre blockchain et IoT résout toutes les difficultés de la cybersécurité des objets connectés, loin de moi cette idée. Néanmoins, la construction d'infrastructure de confiance permettant de sécuriser les échanges entre les objets et leur environnement, de les tracer dans une structure décentralisée, est porteuse de sens.

Je vous remercie de votre attention.