ÉCOLE DE GUERRE

LA TECHNOLOGIE BLOCKCHAIN ET SON CÔTÉ DISRUPTIF POUR DE MULTIPLES APPLICATIONS FUTURES

Par le chef d'escadron Cécile Lambert,
Officier stagiaire de la 26ème promotion
de l'École de Guerre

« L'innovation distingue clairement le leader du suiveur »

Steve JOBS

Sommaire

Table des abréviations

ACPR	Autorité de Contrôle Prudentiel et de Résolution
AFNOR	Association française de normalisation
AMF	Autorité des Marchés Financiers
API	Application
Art.	Article
BART	Blockchain Advanced Research & Technologies
CMF	Code Monétaire et Financier
CNAM	Conservatoire Nationale des Arts et Métiers
CNIL	Commission Nationale de l'Informatique et des Libertés
CRJ	Centre de Recherches Juridiques
CUERPI	Centre Universitaire d'Enseignement et de Recherche en Propriété Intellectuelle
C3N	Centre de lutte contre les criminalités numériques
DAG	Directed Acylic Graphs
DARPA	Defense Advanced Research Projects Agency
DdoS attack	Distributed Denial of Service attack (attaque de déni de service)
DNS	Domain Name System (système de noms de domaine)
Ed.	Édition
EUROPOL	Office Européen de Police

FATF	Financial Action Task Force (ou GAFI)
GAFA	Google, Apple, Facebook et Amazon
GAFI	Groupe d'Action Financière
Ibid.	Ibidem (au même endroit)
Id.	Idem
IoT	Internet of Things (Internet des objets)
IRCGN	Institut de Recherches Criminelles de la Gendarmerie Nationale
ISO	Organisation internationale de normalisation
JO	Jeux Olympiques
KYC	know your cutomer (connaissance client)
KSI	Keyless Signature Infrastructure
N°	Numéro
Obs.	Observations
ONG	Organisation Non Gouvernementale
ONU	Organisation des Nations Unies
Op. Cit.	Opus Citatum (ouvrage cité)
OTAN	Organisation du Traité de l'Atlantique Nord
P.	Page
PIB	Produit Intérieur Brut
PJGN	Pôle Judiciaire de la Gendarmerie Nationale.
PKI	Public Key Infrastructure (Infrastructure à clés publiques, ICP)
PME	Petites et Moyennes Entreprises
POS	Proof Of Stake

POW	Proof Of Work
Préc.	Précité
R&D	Recherche et Développement
RGPD	Règlement Européen sur la Protection des Données Personnelles
SACEM	Société des Auteurs, Compositeurs et Éditeurs de Musique
TIC	Techniciens en Identification Criminelle
TCP/IP	Transmission Control Protocol/Internet Protocol (protocoles Internet)
UE	Union européenne
V.	Voir
WORO	Write Once, Read Only

Résumé

En 2008, suite à la récession économique caractérisée par la crise des « subprimes », Satoshi Nakamoto publiait un article sur le fonctionnement d'une monnaie électronique décentralisée, non soumise à une autorité centrale de régulation (le Bitcoin) et dont le support technologique est la blockchain ou chaîne de bloc en français. La blockchain s'est donc fait tout d'abord connaître de par le développement du bitcoin. Cependant, si le bitcoin est indissociable de la blockchain il n'est pas vrai de l'inverse. Il s'agit avant tout d'un registre ouvert, décentralisé et réputé infalsifiable. Ce sont donc des technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers. La chaîne de bloc permet donc d'obtenir un consensus entre des acteurs qui ne se font *a priori* pas confiance.

Mais on ne peut pas parler d'une blockchain mais de blockchains au pluriel. Nous pouvons distinguer des blockchains publiques où tout le monde peut lire et écrire, des blockchains privées où le registre est fermé et l'accès permissionné, et enfin des chaînes intermédiaires semi-publiques ou de consortium avec des restrictions pour lire ou écrire. Des « smart contracts », c'est à dire des logiciels d'assistance à la préparation, à l'exécution automatique et à la supervision de contrats, peuvent également être ajoutés à la chaîne. Les avantages de la blockchain sont principalement sa décentralisation, son immuabilité, sa résilience et sa traçabilité pouvant conduire à une baisse

des coûts de structure et à l'amélioration du service dans de nombreux domaines.

Face à la multiplication d'annonces de création de blockchains dans tous les secteurs d'activité, la question qui se pose alors est de savoir quels sont les réels enjeux de la technologie, présentée comme une promesse d'avenir, et comment accompagner son passage de l'expérimentation à la maturité, en combinant régulation et soutien à l'innovation ?

La blockchain constituerait donc une nouvelle promesse d'innovation et de disruption des modèles économiques dominants. En effet, ses caractéristiques semblent intéressantes pour un certain nombre d'applications futures dans des domaines aussi variés que l'administration (accès simplifié et sécurisé aux services), la chaîne logistique (traçabilité et lutte contre la contrefaçon), la gestion de données (données médicales, de KYC, procédures judiciaires) et la certification (cadastre, état civil, droit de la propriété intellectuelle).

Les perspectives ouvertes par les blockchains sont donc considérables et ne doivent pas être ignorées.

Cependant, en l'état de la technologie, des défis restent à relever pour un déploiement plus vaste de celle-ci. À l'heure actuelle, elle présente un certain nombre de risques auquel il est nécessaire d'apporter des solutions en vue de son implémentation dans la durée. Elle se heurte entre autre à des limites techniques (scalabilité), sécuritaires, écologiques (consommation énergétique), géopolitiques ou encore juridiques.

Les possibilités d'applications sont donc variées et son potentiel disrupteur appelle une stratégie publique alliant régulation et soutien à l'innovation dès à présent.

Il convient d'instituer des régulations de base (règles fiscales et comptables, statut juridique dont le droit de la preuve) qui soient raisonnables et attractives, de promouvoir des travaux de recherche et de développement interdisciplinaire pour faire disparaître les freins de la technologie et de développer la formation sans se cantonner aux spécialistes. Dans ce cadre, la France et l'Union européenne doivent se saisir maintenant pleinement du sujet des blockchains en se plaçant à l'avant-garde de leur développement.

Introduction

J.P. BARLOW marquait les esprits en 1996 avec sa célèbre Déclaration d'Indépendance du cyberespace. « *Grâce à Internet, nous créerons une civilisation plus humaine et juste. Nous créerons un monde dans lequel chacun peut entrer, sans privilège ou préjudice dus à la race, à la puissance économique, à la force militaire, ou au lieu de naissance* ». Pourtant, cette belle déclaration reste du domaine idéologique car après un peu plus de vingt ans, les richesses et le pouvoir n'ont jamais été aussi concentrés entre les mains de puissants acteurs tels que les gouvernements, leurs services de renseignements et sur internet les GAFA[1]. L'arrivée des GAFA répondait peut-être au manque de confiance entre les individus. Or cette question de la confiance est toujours fondamentale. Comment avoir confiance en des organismes centralisés et tout puissants ? Comment avoir confiance dans l'information non vérifiée qui circule sur les réseaux sociaux ?

C'est cette notion de confiance qui est à l'origine de la réflexion de Satoshi Nakamoto et de la publication en 2008 d'un article[2] sur le fonctionnement d'une monnaie

1 L'acronyme **GAFA** désigne quatre des entreprises les plus puissantes du monde de l'internet à savoir Google, Apple, Facebook et Amazon.

2 Satoshi Nakamoto a désigné Gavin Andresen, directeur technique (CTO) de la Fondation Bitcoin, comme étant son successeur. Le fonctionnement de cette cryptomonnaie et de la blockchain est décrit dans un article fondateur publié sur internet en 2008 : « Bitcoin: A Peer to Peer Electronic Cash System », cf. le lien suivant :

électronique décentralisée, le bitcoin. La création du bitcoin en 2008 est probablement liée à la crise financière de la même année, caractérisée par la crise des « subprimes »[3]. La question de la confiance dans les banques et les monnaies classiques étaient alors au cœur des préoccupations. En réalité, derrière le pseudonyme de Satoshi Nakamoto se cache probablement un collectif. Son article décrit le fonctionnement d'un protocole permettant la production d'un registre infalsifiable, utilisant un réseau informatique pair à pair, la blockchain, ou chaîne de blocs en français, comme support technologique à la toute première cryptomonnaie[4], le bitcoin.

La blockchain s'est donc faite tout d'abord connaître de part le développement du bitcoin puis d'autres cryptomonnaies. Cependant, si le bitcoin est indissociable de la blockchain, l'inverse n'est pas vrai.

En effet, elle n'est pas seulement un outil dédié aux cryptomonnaies et aux échanges financiers. Il s'agit avant tout d'un registre ouvert, décentralisé et réputé infalsifiable. Il s'agit donc d'une nouvelle façon de stoker des données, de les préserver de toute modification, d'y accéder et d'intégrer de nouvelles informations qui deviennent infalsifiables. Ces nouvelles données, inscrites sur un grand registre distribué partagé par l'ensemble des membres du réseau, peuvent résulter de l'exécution d'une

---

https://bitcoin.org/bitcoin.pdf et sa traduction en langue française sur le présent lien.

3 FAURE-MUNTIAN (Valéria), GANAY (Claude) et LE GLEUT (Ronan), Rapport n°1092 au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, *« les enjeux technologiques des blockchains (chaînes de blocs) »*, site internet www.assemblee-nationale.fr, 20 juin 2018, p. 18.

4 Monnaie virtuelle en français.

opération, d'une transaction, ou de l'exécution automatique d'un programme informatique dénommé smart contract.

Dans un souci de simplification et de compréhension, la blockchain peut être comparée à un grand livre de compte (base de données publiques) dont les lignes de compte sont des données informatiques et les pages du livre sont des « blocs » reliés les uns aux autres par la cryptographie, d'où l'idée de chaînes de blocs.

Ce sont donc des technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers. La chaîne de bloc permet d'obtenir un consensus entre des acteurs qui ne se font *a priori* pas confiance.

En France, l'Ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse a donné un début de définition légale à la blockchain même si celle-ci reste limitée. Selon l'article L223-12 du CMF[5], il s'agit d'un dispositif d'enregistrement électroniquement partagé permettant l'authentification d'opérations sur titres spécifiques, destinés à être échangés sur les plateformes de financement participatif.

La blockchain ou chaîne de blocs est un terme très à la mode aujourd'hui que l'on retrouve dans les médias grand public, la classe politique, les dirigeants etc. Tout comme

5 Selon l'article L223-12 du CMF « sans préjudice des dispositions de l'article L223-4, l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État ».

pour les promoteurs de logiciels open source à la fin des années 1990, elle dispose aujourd'hui de partisans zélés. Cependant, si leurs applications dépassent le cadre strict des cryptomonnaies et sont potentiellement nombreuses, peu conjuguent à ce jour maturité technologique suffisante et pertinence d'usage. Devant un certain phénomène de mode, un regard plus distancié paraît donc nécessaire.

Face à la multiplication d'annonces de création de blockchain dans tous les secteurs, la question qui se pose est alors de savoir quels sont les réels enjeux de la technologie blockchain, présentée comme une promesse d'avenir, et comment accompagner son passage de l'expérimentation à la maturité, en combinant régulation et soutien à l'innovation.
Le but est d'essayer de prendre du recul, d'expliquer de manière pédagogique un objet complexe et protéiforme et de caractériser les enjeux qu'il soulève aux niveaux économique, juridique et sociétal. Permettra-t-elle une société plus juste, ou renforcera-t-elle l'écart entre ceux qui ont le pouvoir et ceux qui ne l'ont pas ?

La technologie blockchain a fait son irruption dans un paysage déjà bien fourni en terme d'innovations comme l'intelligence artificielle ou l'internet des objets.
Tel le protocole « TCP/IP », technologie sous-jacente d'internet que nous utilisons inconsciemment pour aller sur Google ou Facebook, nous pourrons utiliser demain de nouveaux services fondés sur la technologie blockchain sans même avoir conscience de l'utiliser. La blockchain constituerait donc une nouvelle promesse d'innovation et de disruption des modèles économiques dominants. Cette

disruption repose sur la désintermédiation sécurisée, distribuée, en mode « pair à pair ».
On parle même de blockchains au pluriel. Il existe à ce titre trois types d'applications : les transferts d'actifs numériques (par exemple le bitcoin), les registres distribués (par exemple Everledge) et les smarts contracts (par exemple Ethereum).
Considérée comme très prometteuse, cette technologie pourrait permettre d'enrayer les inégalités, en permettant à la moitié de la population mondiale non bancarisée d'accéder à des services financiers, d'améliorer la transition d'énergie locale sur des réseaux micro-grids *via* des échanges directs entre producteurs et consommateurs, de créer un moyen de communication de machine à machine sans intermédiaire ni capture des données pour les objets connectés, de garantir l'authenticité et une traçabilité des produits de manière irréfutable etc.
Les possibilités d'applications sont donc variées et son potentiel disrupteur appelle donc une stratégie publique alliant régulation et soutien à l'innovation dès aujourd'hui.
En France, les pouvoirs publics s'intéressent d'ailleurs à cette technologie et un rapport parlementaire a été présenté aux Chambres le 20 juin 2018 dans le cadre de la mission d'information commune sur « les usages des blockchains et autres technologies de certification des registres »[6].

6 FAURE-MUNTIAN (Valéria), GANAY (Claude) et LE GLEUT (Ronan), Rapport n°1092 au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, *« les enjeux technologiques des blockchains (chaînes de blocs) »*, site internet www.assemblee-nationale.fr, 20 juin 2018, 209p.

Après avoir expliqué le fonctionnement des blockchains (I), il est essentiel d'identifier les typologies d'usage répondant à un réel besoin et non à un effet de mode (II), pour enfin identifier les limites techniques et les risques associés à cette technologie (III) afin d'encourager la recherche de solutions pertinentes et pérennes.

Chapitre I : Le fonctionnement des blockchains

Section I : Fonctionnement et typologies des blockchains

I. Le fonctionnement d'une blockchain

La blockchain constitue la première solution au problème des généraux byzantins[7]. Ce système informatique décentralisé peut ainsi gérer les défaillances de certains de ses composants en utilisant un algorithme cryptographique fondé sur un système décentralisé de preuves. Une transaction n'est donc pas le fait d'une entité centrale mais elle émerge de multi-décisions provenant de diverses entités. Et plus le nombre d'entités est grand, plus la structure est fiable.
Pour simplifier, la blockchain peut être comparée à une énorme base de données publiques ou à un registre des comptes ouvert et dans lequel chaque transaction ou donnée est enregistrée de façon définitive et immuable. Ce registre informatique est constitué de plusieurs blocs reliés les uns aux autres par la cryptographie d'où le terme de

7 LELOUP (Laurent), « *Blockchain : la révolution de la confiance* », Eyrolles, 2017, p. 46.

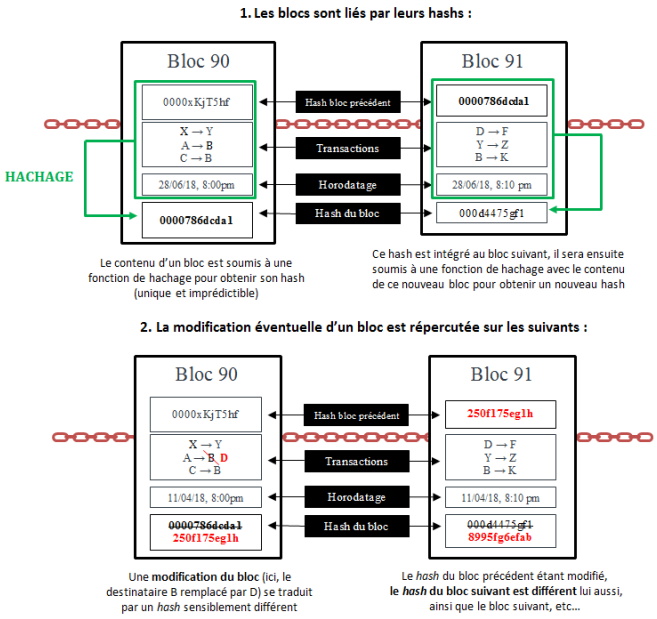
chaîne de blocs ou blockchains, les blocs étant composés de plusieurs enregistrements ou transactions. Ce registre est distribué entre des utilisateurs, qui l'utilisent en tant qu'autorité de confiance garantissant la validité des différents enregistrements.
Pour enregistrer et intégrer des données dans un bloc, des personnes appelées « mineurs » doivent résoudre des puzzles algorithmiques. Il s'agit de calculs de hash, très complexes nécessitant de grosses puissances de calcul. Les « mineurs » vérifient, enregistrent et sécurisent les transactions. Elles sont regroupées dans des blocs, qui sont ensuite enchaînés les uns aux autres pour former la blockchain. Le premier qui réussit à résoudre le problème cryptographique difficile appelé « Proof of Work » (Pow) ou « preuve de travail » en français est rémunéré par la création d'un certain nombre de bitcoins (12,5 bitcoins par bloc miné actuellement[8]). Les mineurs sont donc appelés ainsi car ils sont un peu les nouveaux chercheurs d'or.

Les blocs constitués de plusieurs transactions ou données « signées » par clés publiques sont ensuite « horodatés » par leur auteur. Chaque bloc, outre les transactions et l'horodatage, possède un identifiant (case à fond noir du bloc 90 dans le schéma ci-après), qui prend la forme d'un « hash » c'est-à-dire d'une suite binaire, permettant de relier les blocs les uns aux autres. Ce hash est toujours le résultat du « hachage » du bloc précédent[9].
Le dernier bloc en date est ajouté au précédent (celui-ci étant dit « miné ») par le premier « mineur » ayant réussi à résoudre le problème cryptographique.

8 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 36.
9 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 26.

La fonction de hachage a pour avantage de rendre chaque ensemble de données unique puisque qu'elle est constituée de telle sorte qu'il existe 2^{256} combinaisons possibles soit l'estimation du nombre d'atomes dans l'univers connu. Le hash a également l'avantage d'être imprédictible.

Le rôle du hachage dans l'intégrité de la chaîne de blocs

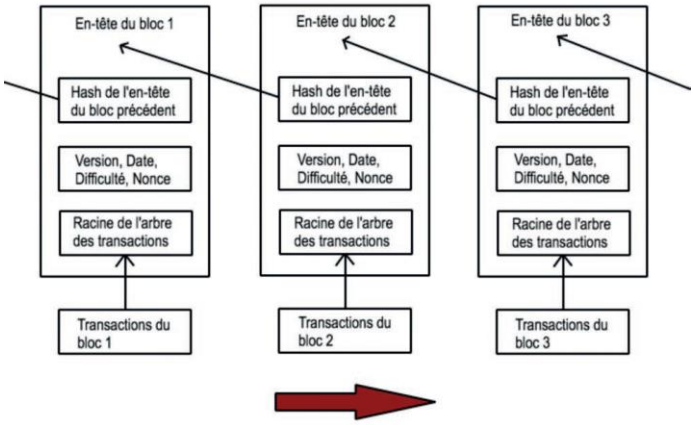


Source : OPECST

Quand un bloc est ainsi créé il est redistribué à l'ensemble des nœuds du réseau blockchain. Chacun possède alors une version de la blockchain de manière décentralisée, garantissant son immuabilité. Le concept de blockchain permet donc une gestion collaborative d'un registre

distribué et de s'abstraire ainsi de la nécessité d'une autorité centrale de confiance.

Fonctionnement simplifié de la blockchain



Source : Les annales des mines, « Blockchains et smart contracts : des technologies de la confiance ? », août 2017

Dès lors que les informations d'un bloc parent changent, le résultat du hachage n'est plus le même, ce qui a pour effet d'interrompre le processus de validation. En effet, tous les blocs étant liés cryptographiquement, modifier le contenu d'un bloc suppose recalculer les hashs de tous les blocs suivants[10]. La méthodologie de validation des blocs permet donc de se prémunir du risque d'attaque malveillante. De la même manière le fait que des centaines de copies du registre soient mises à jour simultanément et

10 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 31.

régulièrement vise à rendre les blockchains quasiment indestructibles[11].

Mais toutes les blockchains n'ont pas le même mode de validation des transactions. Le mode de validation associé à la première blockchain c'est à dire celle du bitcoin, est dénommée la preuve de travail ou « proof of work » (POW).

La preuve de travail est une compétition cryptographique entre les mineurs qui mettent à disposition leur puissance de calcul, et donc une ressource externe qu'est l'électricité consommée par l'ordinateur, pour participer au processus de validation des blocs. Le but pour les mineurs est de remporter le calcul mathématique pour créer et obtenir de nouveaux bitcoins. Nous l'avons vu préalablement, le bloc validé par le mineur qui sort victorieux des épreuves cryptographiques est alors transmis de pair à pair à chaque nœud du réseau qui ajoute à sa propre blockchain le bloc ainsi validé. Si deux blocs sont validés au même moment, les mineurs vont utiliser l'un ou l'autre pour intégrer son hash au bloc suivant. Dans ce cas deux chaînes parallèles se développent. Le protocole prévoit alors qu'après l'ajout de quelques blocs, seule la chaîne la plus longue subsiste, c'est-à-dire en pratique celle que la majorité des nœuds aura adoptée[12]. Cependant, ce mode de validation a l'inconvénient d'être particulièrement énergivore.

La principale alternative à la preuve de travail est appelée preuve d'enjeu ou proof of stake (POS) afin de pallier à l'inconvénient de la consommation excessive d'énergie. Dans ce mode de validation, le droit de valider les blocs est directement lié au montant de crypto-monnaie détenu.

---

11 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 34.
12 *Ibid*., pp. 36 et 37.

La POS recouvre en réalité deux preuves distinctes : la preuve de participation et la preuve d'enjeu.
La preuve de participation consiste à attribuer les blocs en fonction de la quantité de cryptomonnaies possédée par un nœud. La preuve d'enjeu va plus loin et exige de mettre en place des gages de ces monnaies qui seront détruits en cas de fraude.
Des dérivés de cette preuve d'enjeu existent et nous pouvons citer notamment la « preuve de possession » (*proof of hold*), fondée sur la durée de possession, la « preuve d'utilisation » (*proof of use*), en fonction du volume de transactions, la « preuve d'importance » (*proof of importance*), reposant sur la « réputation », ou encore la « preuve de destruction » (*proof of burn*) qui revient à détruire des cryptomonnaies, pour obtenir la confiance du réseau[13].

13 *Ibid.*, pp. 40-43.

Avantages et inconvénients de la preuve de travail (POW), de la preuve d'enjeu (POS) et d'une forme hybride des deux modes de preuve

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

Source : GIANG-TRUONG NGUYEN et KYUNGBAEK KIM, « A survey about consensus algorithms used in blockchain », Journal of Information processing systems, vol. 14, n° 1, février 2018.

La preuve de travail est donc une méthode fiable et sécurisée, mais lente et coûteuse en énergie. La preuve d'enjeu est une seconde méthode, plus rapide pour créer des blocs, plus économe tant en énergie qu'en matériel spécialisé, mais à la sécurité encore contestée. L'essentiel des critiques des détracteurs de la preuve d'enjeu concerne la sécurité d'une part et le risque de capitalisation excessive et de centralisation partielle d'autre part.

Au travers des divers modes de validation des transactions nous avons vu que la blockchain n'était pas uniforme. Outre, les modes de validation, une typologie des blockchains peut-être réalisée.

II. Typologie des blockchains

La blockchain n'est pas uniforme. Au lieu de « une blockchain » nous devrions dire « des blockchains ». En effet, différents types de blockchains peuvent être distingués selon le caractère ouvert ou fermé de celles-ci. Il existe donc des blockchains publiques, des blockchains privées et enfin des blockchains hybrides dites semi-publiques (ou blockchains consortium). Il ne faut surtout pas se méprendre sur la distinction entre blockchains publiques et blockchains privées. Elle ne repose pas sur une distinction entre blockchains de personnes publiques (États, collectivités…) et blockchains de personnes privées (entreprises, ONG…), mais bien sur le caractère ouvert ou fermé de la blockchain[14].

Les blockchains publiques, dont le meilleur exemple est celle support du bitcoin, sont ouvertes c'est à dire que tout le monde peut écrire et lire. Tous les participants ont accès à la base de données, peuvent en héberger une copie et la modifier en mettant à disposition leur puissance de calcul.

Les blockchains consortiums ou semi-publiques sont un intermédiaire entre les publiques et les privées. La blockchain est ouverte au public, mais toutes les informations ne sont pas accessibles. Dans ce type de chaîne, seuls les membres du consortium peuvent écrire mais tout le monde peut lire. Les règles de validation des blocs et les droits des utilisateurs sont définis au préalable. Ce type de blockchain n'est donc que partiellement décentralisé.

Les blockchains « consortium » permettent à plusieurs organisations indépendantes, voire concurrentes,

14 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 53.

d'archiver des données dans un registre décentralisé, voire même d'échanger des actes certifiés sans passer par un tiers de confiance. Dans le monde de la finance, ce type de chaîne peut particulièrement être utile en terme de KYC[15] et de lutte contre le blanchiment d'argent dont les mesures ont été étendues aux plateformes d'échange de devises virtuelles.

Ce type de blockchain semi-publique est en cours d'expérimentation par un consortium, dénommé R3 et regroupant plus de 80 établissements financiers du monde. Le consortium R3 a effectivement lancé une blockchain atypique dénommée « Corda » qui a été mise ensuite en open-source le 30 novembre 2016.

Enfin, les blockchains privées ont leur registre fermé et l'accès est permissionné. Seuls les membres de la chaîne peuvent lire et écrire. Dans ce cas une autorité régulatrice centralisée valide l'introduction de nouveaux membres et accorde les droits en écriture et en lecture. Le registre est distribué entre les membres de la chaîne mais les droits

15 Le KYC (Know Your Customer) est le processus par lequel les banques et les institutions financières vérifient l'identité de leurs clients et évaluent les risques potentiels pour établir une relation commerciale avec eux. Le but est d'empêcher le blanchiment d'argent et autres activités illégales *via* les institutions financières. En Europe le KYC a été développé par la Directive (UE) 2015/849 du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (« la quatrième directive »), le Règlement (UE) 2015/847 du 20 mai 2015 sur les informations accompagnant les transferts de fonds et enfin la Directive (UE) 2018/843 du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE.

restent centralisés. Malgré le caractère centralisé cette chaîne reste résistante aux attaques puisque le registre est distribué et les données restent immuables. Elle a en outre l'avantage indéniable d'être plus efficace en terme de rapidité d'accès aux données et de réduction des coûts pour les organisations. Elle peut donc permettre des approches distribuées à un coût réellement marginal.

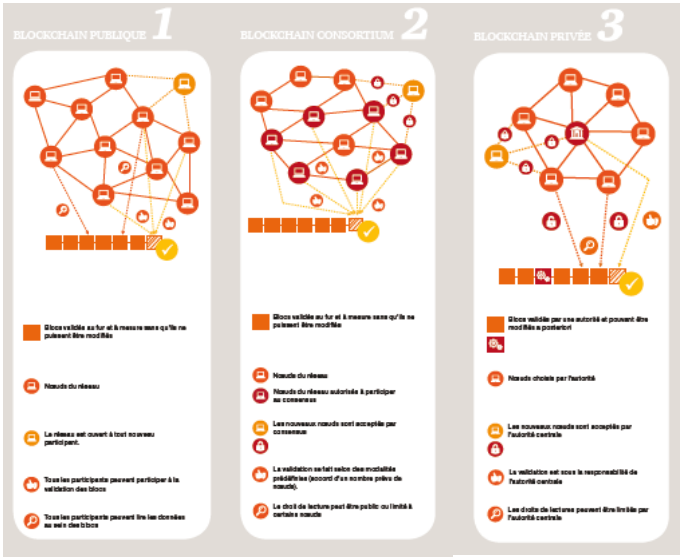
Ce type de chaîne semble particulièrement adapté pour les entreprises pour un usage interne ou avec leur écosystème de partenaires ou clients. En effet, cette configuration serait utile pour de grandes organisations à multiples acteurs où le partage de l'information est difficile mais où il doit rester du ressort des seuls membres.

À titre d'exemple, le Crédit Mutuel Arkéa a fait ce choix pour partager ses données clients entre ses différentes entités.

Les organisations militaires pourraient également être intéressées par le développement de ce type de chaîne pour le partage d'information de manière sécurisée.

Mais avant d'implémenter une blockchain privée, il faut avant tout se demander si une base de données ne serait pas plus pertinente.

Les 3 catégories de blockchains



Source : PWC

En parallèle des blockchains, des smart contracts peuvent être adossés à ces dernières. Il s'agit de logiciels d'assistance à la préparation, à l'exécution et à la supervision de contrats. Ils sont intégrés à la blockchain, électroniquement programmables et permettent l'exécution automatique *via* sa blockchain sous-jacente d'un contrat entre deux ou plusieurs parties selon la réalisation d'événements préalablement définis dans le contrat.
Ils permettent donc l'exécution du contrat, une fois les conditions préalablement définies remplies, sans possibilité de fraude, de mauvaise foi et sans interférence avec une partie tierce.

Les données, conditions d'exécution du contrat peuvent se trouver soit sur la blockchain elle-même soit à l'extérieur de celle-ci. Dans ce dernier cas apparaît un nouveau tiers de confiance dénommé « Oracle ». Celui-ci a pour rôle d'insérer les données nécessaires au sein de la blockchain à un moment précis pour l'exécution du contrat.
Ensuite, le smart contract lit les données insérées par l'oracle et s'exécute ou non selon les critères prédéfinis.
Cet oracle peut-être une personne physique, véritable tiers de confiance, ou automatisé *via* la connexion d'objets (IoT[16]). La transmission des informations *via* des objets connectés (IoT) autonomes se fait de pair à pair sous la forme de transactions sur la blockchain. Pour en garantir la sécurité un système de carte à puces est utilisé. L'intérêt de récupérer les données *via* les objets connectés est une automatisation et une autonomie de la gestion de la procédure, mais également l'enregistrement de l'ensemble de ces données sur la blockchain assure simplicité, transparence et sécurité.
L'association de l'intelligence artificielle aux smart contracts permettra peut-être à terme de pouvoir intégrer des notions à contenu variable (conséquences suffisamment graves, raisonnables, légitimes etc.) existantes dans le droit contractuel actuel et d'élargir les possibilités d'utilisation des smart contracts. L'intelligence artificielle permettra de gérer ces notions floues par une analyse prédictive[17].

16 Internet of Things ou internet des objets en français.
17 MEKKI (Mustapha), « *Le smart contract, objet du droit (partie 2)* », Dalloz IP/IT, droit de la propriété intellectuelle et du numérique, numéro 1, janvier 2019, p. 30.

Après avoir vu le fonctionnement des blockchains, il est intéressant de définir ses caractéristiques majeures.

Section II : Ses caractéristiques

La blockchain se caractérise principalement par sa décentralisation, son immuabilité, sa résilience et sa traçabilité.

La principale caractéristique de la blockchain est sa décentralisation et sa désintermédiation. Elle est conçue sans tiers de confiance, sans autorité centrale. Elle assume structurellement le compromis du réseau par les initiés et les étrangers. Selon L. LELOUP, « *le fait qu'une transaction soit acceptée ou rejetée est le fruit d'un consensus distribué et non d'une institution centralisée* »[18]. Une blockchain totalement décentralisée permet donc d'acheter ou d'offrir des microservices sans passer par plateforme dédiée comme par exemple Uber ou Blablacar, et d'économiser les coûts liés à son usage. Selon certains experts, la blockchain permettrait d' « ubériser » uber.
La blockchain est également définitive et immuable. Le registre est distribué sur l'ensemble des nœuds du réseau rendant infalsifiable l'historique des transactions. Il s'agit de multiples bases identiques actives simultanément et non pas seulement de simples copies ce qui offre une tolérance aux pannes (« fault tolerance ») et évite toute

18 LELOUP, *op. cit*., p. 15.

manipulation. Aucun membre ni même un administrateur ne peut venir corrompre le registre. Toute décision est donc indiscutable et irrévocable.
Ensuite, la blockchain représente une réponse sérieuse et efficace aux risques de cybercriminalité car elle offre une sécurité forte. Personne ne peut prétendre pirater le système puisque les données ne sont pas stockées sur un ordinateur unique. C'est la mise sur le réseau des données qui les protège des pirates. C'est un peu la différence entre un coffre-fort et une multitude de porte-monnaie disséminés aux quatre coins du globe : « *forcer le coffre-fort est difficile mais possible alors que forcer un porte-monnaie est trivial mais il est fastidieux de les attaquer tous un par un* »[19].
De plus, son architecture décentralisée évite que les prises de décision n'appartiennent qu'à une seule unité centrale. En effet, lorsque qu'un seul serveur décide de tout, l'altération ou le piratage de ce serveur rend les décisions caduques.
Grâce à l'utilisation de la cryptographie, la blockchain assure également la sécurité de ses transactions et rend la falsification difficile. La difficulté de minage, la fameuse preuve de travail, est suffisante pour éviter à une seule entité, ou à un groupe, de contrôler plus de 50 % de la puissance de calcul nécessaire (attaque dite à 51 %) pour prendre le pouvoir et donc contrôler la création ou le rejet de blocs. La corrélation difficulté de minage et résilience est extrêmement importante dans les protocoles PoW. Cependant, avec l'évolution rapide des techniques de

19 LOUBIERE (Paul), « *Quand Orange se prend pour Google et investit dans la start-up chain* », site internet https://www.challenges.fr, 10 septembre 2015.

crypto-minage, il devient plus aisé d'acquérir une importante puissance de calcul et donc de prendre potentiellement contrôle de la chaîne. Ainsi, si la blockchain bitcoin est sécurisée, ce n'est pas le cas pour la très grande majorité des autres blockchains[20].

Enfin, les réseaux blockchains sont tolérants aux pannes puisqu'ils mobilisent les efforts des nœuds valides pour rejeter ceux qui sont suspects.

La blockchain permet en outre de réaliser des économies d'échelle puisqu'elle permet d'abaisser le coût de chaque transaction. En fluidifiant les relations entre l'ensemble des intervenants (entreprise/clients, administration/citoyens etc.), elle permet d'améliorer la compétitivité en augmentant la rapidité des transactions.

Enfin, la blockchain est transparente et elle se caractérise particulièrement par sa traçabilité. Toute transaction ou donnée est inscrite de manière permanente et distribuée auprès de l'ensemble des nœuds de la chaîne.

Les principales qualités de la blockchain du bitcoin

20 V. le site www.crypto51.app qui évalue le coût d'une attaque 51 % en prenant en compte la difficulté de minage des blockchains PoW et le coût approximatif d'une heure de location de puissance de calcul pour réaliser une attaque.

Source : Blockchain France[21]

Section III : Première mise en œuvre, le bitcoin

L'application la plus connue à ce jour de la technologie blockchain est le bitcoin. C'est bien le bitcoin puis les autres cryptomonnaies qui ont popularisé dans un premier temps les blockchains.
En effet, la création de la première blockchain avait pour but de mettre en place un outil de paiement électronique, sous la forme de jetons, à l'aide d'un réseau décentralisé. Il s'agissait donc de créer une monnaie de l'internet, le bitcoin. La blockchain s'appuie sur les protocoles d'internet sans pouvoir y être assimilé. Monnaie électronique fondée sur un système pair à pair, la blockchain du bitcoin permet à deux personnes d'échanger des actifs sans passer par un tiers de confiance comme une banque.

21 Blockchain France accompagne les organisations dans la découverte, l'exploration et le déploiement des technologies blockchain, site internet https://blockchainfrance.net.

Selon L. LELOUP, il s'agit d'une chaîne de blocs ouverte « *fonctionnant par un réseau pair à pair, sans autorité centrale (et donc sans autorité financière [comme une banque centrale] tout en enregistrant chaque transaction dans un grand livre de compte (ledger) dans lequel toute modification est impossible* »[22].

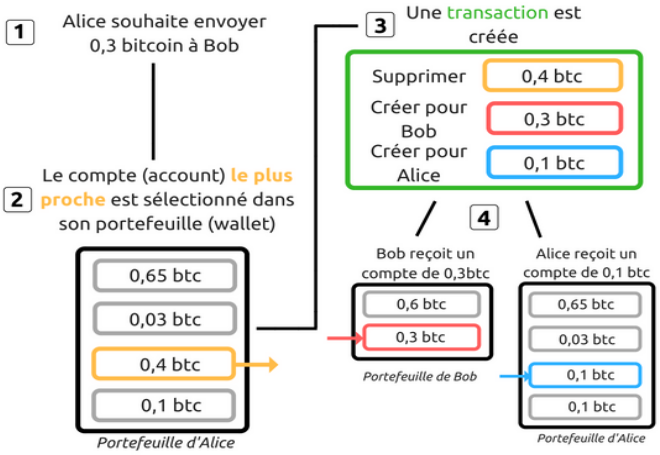
Une chaîne de blocs constitue ainsi une technologie WORO (write once, read only), la transaction ne pouvant être écrite qu'une seule fois. Chaque écriture est reliée à la précédente et ainsi de suite. Comme nous l'avons vu précédemment l'écriture n'est rendue possible que par la résolution d'un problème cryptographique, la preuve de travail (proof of work) qui est désignée sous le terme de minage et qui nécessite de très grosses capacités de calcul. Dans le cas du bitcoin, le mineur est rémunéré par de nouveaux bitcoins à chaque fois qu'il résout le problème cryptographique. Des consortiums se sont donc organisés en ferme de minage pour gagner un maximum de bitcoins. Le bitcoin est non périssable, identifiable puisque chaque bitcoin possède son propre numéro et est impossible à contrefaire. Il est fongible et divisible. Il se stocke sur un ordinateur, un smartphone ou un support amovible. Il est de plus en plus accepté comme moyen de paiement sur internet sur des sites de paiement comme Amazon ou Ebay.

Il est constitué d'une clé privée composée de 51 caractères alpha-numériques commençant par le chiffre 5 ou K et L dans des cas spécifiques, et d'une clé publique faite de 34 caractères alpha-numériques commençant par 1, 3 ou bc1 et qui fait office de portefeuille électronique.

---

22 LELOUP, *op. cit.*, p. 13 et 14.

Décomposition d'une transaction en bitcoin



Source : OPECST

Par la suite, d'autres cryptomonnaies ont vu le jour comme Litecoin ou Peercoin.
Si la blockchain a été popularisée par le développement des cryptomonnaies, sa réputation a pu être entachée par les utilisations illicites de ces monnaies virtuelles sur internet et a pu faire l'objet de polémiques. Pourtant, la blockchain est bien plus qu'un support pour les crypto-actifs[23]. Loin de ces polémiques, cette technologie du

23 « Virtual assets », ou crypto-actifs en français, est la nouvelle dénomination donnée aux monnaies virtuelles par le Groupe d'Action Financière (GAFI ou FATF) dans une déclaration publique (« *Public Statement - Mitigating Risks from Virtual Assets* ») du 22 février 2019, site internet du GAFI.

registre distribué peut présenter des usages potentiels multiples innovants voire disruptifs.

Chapitre II : Les typologies d'usage répondant à de vrais enjeux de société

Les possibilités de la blockchain, technologie qui se trouve derrière ces crypto-actifs, sont multiples et ne peuvent être intégralement présentées dans ce document (V. Annexe 1 : infographies des projets blockchains).
Il est à noter toutefois que les applications potentielles vont bien au-delà de la sphère financière. En proposant des bases de données décentralisées et partagées, la blockchain peut ainsi être une réelle force pour la sécurité, en particulier dans les 5 domaines suivants : la protection et la gestion des identités et des objets, la traçabilité des chaînes logistiques, l'intégrité des données et la désintermédiation.

Section I : La gestion des identités

La technologie blockchain peut faciliter la gestion des identités aussi bien des personnes physiques que des objets. Il devient ainsi possible de créer une identité numérique infalsifiable puisque stockée sur une blockchain pour les personnes physiques comme pour les objets.

I. La gestion des identités numériques des personnes physiques

La blockchain peut favoriser l'identification des personnes physiques dans le but de désintermédier et d'assurer une plus grande sécurité sur notre territoire ou lors d'événements prévisibles. Dans ce domaine, diverses applications sont envisageables.

Un service d'état civil ou un cadastre sur blockchain pourrait être envisageable afin de protéger l'identité et les biens des personnes autrement menacées par la corruption de leur gouvernement. Le cas de l'Estonie est un exemple particulièrement intéressant. En effet, un projet d'identité digitale est poursuivi afin de permettre aux citoyens estoniens d'avoir accès à leurs informations personnelles de manière plus efficace et rapide *via* la constitution de dossiers numériques aussi bien administratifs que médicaux[24]. Ce projet a démarré en 2002 par l'établissement d'une carte d'identité électronique, équipée d'une puce contenant des clés cryptographiques et permettant à son utilisateur de s'identifier pour accéder à l'ensemble des services administratifs en ligne comme pour voter ou acheter un ticket de transport. Cette carte est utilisée aujourd'hui par 94 % de la population.

La seconde étape a consisté en la numérisation de l'ensemble des actes de l'administration pour créer des

24 CHERIF (Anaïs) et MANIÈRE (Pierre), « *L'Estonie, royaume du tout-numérique* », La Tribune, 5 avril 2018. Disponible sur : https://www.latribune.fr/technos-medias/internet/l-estonie-royaume-du-tout-numerique-774138.html.

bases de données numériques des différents services de l'État et en l'interconnexion progressive entre cette base de données et les cartes d'identité numériques.
Enfin, en 2008, l'entreprise Guardtime a installé à la demande du gouvernement une infrastructure cryptographique équivalente à la blockchain dénommée KSI pour « Keyless Signature Infrastructure ». Ce registre public distribué permet de vérifier les données consultées ou changées de manière indépendante et sécurisée. Des droits de lecture différents en fonction de la situation ou de la personne peuvent être accordés, conciliant vérification d'identité et protection de la vie privée.
Les Estoniens peuvent donc, grâce à cette identité numérique, signer des contrats, payer leurs impôts, voter, accéder à leur dossier médical, intervenir en justice, réaliser des formalités etc. L'Estonie est donc particulièrement en avance en la matière et selon certains experts, la numérisation de ses services lui ferait économiser 2 % de son PIB par an[25].
Dans la lignée de l'Estonie, d'autres pays testent actuellement ou vont tester la blockchain dans leur administration publique. Par exemple, aux États-Unis, la start-up « oneName » utilise une blockchain pour générer des identités digitales qui peuvent être utilisées par l'usager pour l'ensemble des services web. Cette identité digitale évite la création de multiples comptes et de retenir d'innombrables mots de passe.
Toute cette architecture basée pour l'essentiel sur la technologie blockchain est aussi utilisée par d'autres institutions ou organisations que des États.

---

25 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 69.

Un projet pilote a été par exemple lancé par une ONG en Birmanie, pour distribuer des cartes d'identité numériques utilisant la technologie blockchain aux réfugiés Rohingya afin de leur permettre l'accès à un certain nombre de services[26].

De la même manière, à New York, la start-up «Blockchain for change » a lancé un projet de distribution de smartphones aux sans-abris en 2017 afin que ceux-ci puissent se créer une identité digitale sur une blockchain et avoir ainsi accès à divers services tels que la distribution de nourriture ou de vêtements ou encore l'accès à certains foyers[27]. En parallèle, ils peuvent recevoir de l'argent des organismes gouvernementaux et payer grâce à un crypto-actif, le « change coin ».

Dans le domaine migratoire, l'utilisation de la blockchain semble être particulièrement intéressante. Elle permettrait la création d'identités digitales pour les migrants afin d'assurer un meilleur suivi de ceux-ci au niveau international. Il existe à ce titre un projet, «ID 2020 », né d'un consortium international public-privé[28] qui se propose d'aider le milliard d'individus sans identité reconnue officiellement. L'objectif de ce consortium est de développer une identité numérique pour permettre à un sixième de la population ne détenant pas de preuve écrite de son identité d'enfin pouvoir avoir accès à un ensemble

26 https://www.challenges.fr/monde/une-carte-d-identite-blockchain-pour-les-rohingyas_555888.

27 https://lesclesdedemain.lemonde.fr/technologie/un-projet-blockchain-pour-donner-une-identité-digitale-aux-personnes-sans-domicile-fixe_a-88-6454.html.

28 Le consortium ID2020 regroupe des gouvernements, des ONG, des professionnels de la technologie et des experts issus des secteurs publics et privés.

d’activités et de services. À cette fin les sociétés Accenture et Microsoft travaillent ensemble sur un prototype de gestion des identités basé sur la technologie blockchain (privée ou permissionnée). Ce prototype est mis en œuvre sur la plateforme cloud Microsoft Azure et ne stocke aucune information personnellement identifiable, celles-ci étant stockées « hors chaîne ». L’accès à ces données nécessite l’autorisation de la personne concernée. Grâce à l’utilisation de la blockchain il n’y aura plus besoin d’un organe de contrôle centralisé.

Dans le domaine de la défense, la technologie blockchain pourrait offrir un registre distribué sécurisé entre les différentes unités, pour servir à stocker les identités numériques des combattants, valider leur présence sur les théâtres d’opérations et d’une manière plus générale remplacer les divers documents et journaux de marche. Elle permettrait également de gérer les niveaux de certifications pour l’accès aux bases opérationnelles.

Pour les forces de l’ordre, l’utilisation de la blockchain pourrait servir à stocker les identités numériques des personnels et surtout leur offrir un meilleur suivi professionnel et médical. En effet, le suivi des personnels (les Techniciens en Identification Criminelle par exemple) exposés aux produits dangereux pourrait être en partie automatisé *via* une blockchain et des smart contracts.

Enfin, lors d’événements de grande ampleur, la blockchain pourrait également favoriser l’identification de personnes physiques. Elle pourrait permettre la certification du statut et du niveau de sécurité des individus accédant à un événement comme pour les JO 2020 par exemple.

II. La gestion des identités numériques des objets

Comme pour les individus, la blockchain peut aussi faciliter la gestion des objets. En effet, elle permet de tracer et d'authentifier grâce à différentes techniques d'empreinte, de reconnaissance numérique, de capteurs etc.
L'intégrité des données, leur quasi immuabilité, est au cœur de la confiance garantie par le registre distribué permettant à la fois transparence, traçabilité et lutte contre toutes les formes de contrefaçon qui touchent toutes les industries. Il s'agit d'un enjeu global de santé et de sécurité publique.

A. La traçabilité

- Dans le domaine civil
L'enjeu majeur est l'assurance de la traçabilité des produits de leur fabrication jusqu'à leur remise entre les mains du consommateur.
Jusqu'à peu de temps, il n'existait dans pratiquement aucune industrie de connaissance consolidée et fiable du cycle de vie réel d'un produit c'est à dire ses conditions de transport, de sa localisation à un instant T, de son lieu de vente ou de reconditionnement. Or la technologie blockchain permet de certifier tout le cycle de vie d'un produit. Les chaînes logistiques vont plutôt utiliser des blockchains privées afin que seuls les intervenants accrédités puissent inscrire les informations les concernant sur la blockchain. Ainsi, chaque fournisseur ou intervenant

dans la vie du produit va détenir des accréditations spécifiques avec des accès différenciés aux données pour notamment éviter que les concurrents puissent avoir accès à des informations confidentielles.
Techniquement, il s'agit d'apposer un tag unique pour chaque produit dont les données (provenance, lieu de stockage, authenticité, certificat de propriété, historique) vont être stockées dans une blockchain. C'est à partir de cette identification unique que les différents acteurs (fournisseur, producteur, transporteur, vendeur etc.) vont déclarer leur intervention (provenance de la matière première, les conditions de fabrication ou de stockage, le transport en conteneur etc.) à chaque étape de la chaîne logistique (« chaîne logistique »). En bout de chaîne, l'identité numérique ainsi constituée peut être lue par un consommateur avec un smartphone en s'appuyant sur le marquage unique du produit.
L'utilisation de la blockchain et donc d'un registre numérique distribué et privé permet dans ce cas à la fois d'organiser un réseau de collecte d'informations et de prouver ultérieurement, grâce à celles-ci, l'origine et le contenu de chaque élément constituant l'identité numérique du produit. Ce registre est partagé entre les nœuds du réseau constitué par les intervenants de la chaîne logistique concernée. Ceux-ci sont connus et identifiés. Comme nous l'avons déjà évoqué, l'utilisation d'une blockchain privée ou à permission est donc la plus appropriée et un algorithme de consensus plus simple que dans le cas des blockchains publiques peut être utilisé.
De plus, grâce à cette immuabilité, des algorithmes d'analyse des cycles de vie des produits tels que déclarés par les intervenants de la chaîne logistique peuvent être utilisés afin de détecter des signaux faibles caractéristiques

d'anomalies, quelle qu'en soit la nature (dysfonctionnement, malveillance, irrégularité, non-qualité etc.). Cela permet ainsi de générer une boucle de rétroaction permettant de responsabiliser chaque intervenant et *in fine* de fiabiliser le fonctionnement des chaîne logistique[29].

Les industriels et les sociétés de service commencent à proposer des cas d'usage intéressants dont certains sont déjà déployés.

À titre d'exemple, l'application « Thingchain »[30] proposée par l'entreprise « Skuchain »[31], permet de tracer l'historique logistique (provenance, circuit de distribution, …) grâce à un code crypté et stocké sur la blockchain. La propriété de ce code peut être identifiée, tracée et transférée grâce à l'API Thingchain.

Depuis août 2017, Walmart[32], Kroger[33], Nestlé[34] et Unilever[35] se sont associés à IBM pour utiliser la technologie de la blockchain afin d'améliorer leur chaîne logistique.

Walmart expérimente la technologie blockchain pour augmenter la traçabilité de ses produits. Grâce à cette technologie elle peut avoir accès immédiatement et de

29 HUG (Matthieu), « *Un nouvel outil numérique pour la fiabilisation des chaînes logistiques : la blockchain* », dans les annales des mines, réalités industrielles, « *Blockchains et smart contracts : des technologies de la confiance ?* », Août 2017, p. 108.

30 http://www.thingchain.com.

31 Entreprise spécialisée dans l'implémentation de la blockchain pour les chaînes logistiques.

32 Chaîne de magasins américains.

33 Entreprise de grande distribution américaine.

34 Multinationale suisse.

35 Multinationale anglo-néerlandaise dans les produits de grande consommation.

manière certifiée aux informations de ses produits d'un bout à l'autre de la chaîne (production - distribution - commercialisation).
Nestlé expérimente une blockchain pour tracer ses produits et les faire rappeler plus facilement en cas de problèmes sanitaires. Selon Luca Comparini, responsable blockchain d'IBM, il faut aujourd'hui « *jusqu'à six jours pour remonter la chaîne logistique d'un produit, avec une plateforme intégrant la technologie blockchain cela pourrait prendre quelques secondes* »[36]. Lorsqu'il s'agit de rappeler des produits dangereux pour la santé publique, comme les laits infantiles de la marque Lactalis en 2018 puis début 2019, la rapidité de localisation de ces produits est fondamentale.
La société danoise de transport maritime de conteneurs Moller-Maersk a compris l'enjeu de la traçabilité dans son secteur puisque 9 marchandises sur 10 sont transportées dans le monde par voie maritime. Associée à IBM, la société de fret teste depuis 2018 une plateforme ouverte fondée sur la blockchain pour numériser la partie chaîne logistique du commerce maritime au niveau international. Le but est de supprimer à terme la paperasserie administrative, les retards, les pertes de denrées périssables et au final de réduire les coûts de transport d'au moins 20 %. Le port de Rotterdam, premier port d'Europe, effectue également un test en la matière.

36 Paroles prononcées lors de la conférence du salon « IoT World », le 22 mars 2018. V. PROTAIS (Marine), « *Les blockchains d'entreprise commencent à se déployer* », l'UsineNouvelle, 23 mars 2018, site internet http://www.usinenouvelle.com/editorial/les-blockchains-d-entreprise-commencent-a-se-deployer.N670439.

Toujours à Rotterdam, un laboratoire de recherche dans la blockchain « BlockLab » a été créé afin de développer des applications et des solutions concrètes. Ce laboratoire associe la municipalité de Rotterdam et le « Cambridge innovation Center », un incubateur et un centre d'innovation de Rotterdam.
En France, Carrefour a lancé, en 2018, sa blockchain pour son poulet d'Auvergne Filière Qualité Carrefour afin de garantir au consommateur la traçabilité de ses produits. Chaque acteur de la chaîne du poulet renseigne les informations de traçabilité qui le concerne sur la blockchain la plupart du temps *via* un smartphone. Au bout de la chaîne le consommateur a accès à des données précises (lieu et mode d'élevage, nom de l'éleveur, label, alimentation, etc.) *via* un Code QR[37] apposé sur l'étiquette de l'article. Carrefour devrait élargir prochainement ce test à huit autres produits.

- Dans le domaine militaire :
Les armées pourraient également utiliser des blockchains privées à des fins de logistique militaire dont le fonctionnement et les accès seraient contrôlés par le ministère des Armées. Elles pourraient également s'appuyer sur des blockchains de type semi-publiques (consortium) pour une gestion de données inter-services ou avec ses fournisseurs civils.
Via cette technologie, il serait par exemple possible d'améliorer la traçabilité des denrées, des pièces détachées et des divers produits transportés, d'accélérer les livraisons

37 Un QR code, ou code QR en français, est un type de code barre en deux dimensions constitué de modules noirs disposés dans un carré à fond blanc.

et de gérer les produits en flux tendu. Cela permettrait une traçabilité sécurisée tout au long du cycle de vie du produit et en cas de problème ou de dysfonctionnement, de retrouver rapidement la pièce défectueuse. La chaîne de blocs permettrait ainsi de mieux gérer les acheminements de matériels, de diminuer les coûts de gestion et d'assurance et de réduire les démarches administratives et les temps de transit. Au final, ce sont les opérations qui se trouveraient améliorées grâce à une logistique plus efficiente.

Courant 2018, Accenture[38] et Thales[39] ont présenté un prototype reposant sur la blockchain Hyperledger Fabric qui permet d'authentifier et de tracer les pièces utilisées dans l'aéronautique. Ce registre, où toutes les transactions sont inscrites de manière infalsifiables et immuables est partagé entre fournisseurs, fabricants et opérateurs.

Elle pourrait également être utilisée pour le suivi du matériel sensible comme les armes ou les substances toxiques. D'ailleurs, la « Defense Advanced Research Projects Agency »[40] américaine (DARPA) a cette volonté de garantir l'intégrité des données associées à des systèmes d'armes cruciaux comme les armes nucléaires ou les satellites *via* la technologie blockchain.

38nAccenture est une entreprise internationale de conseil et de technologie. Elle offre des services dans les domaines de la stratégie, du conseil, du digital, des technologies et de la gestion déléguée d'opérations.

39 Thales est un groupe d'électronique spécialisé dans l'aérospatiale, la défense, la sécurité et le transport terrestre.

40 La « Defense Advanced Research Projects Agency » est une agence du département de la Défense des États-Unis chargée de la recherche et du développement de nouvelles technologies destinées à un usage militaire.

Pour les forces de l'ordre et notamment la gendarmerie nationale, la technologie des blockchains pourraient, comme pour les armées, permettre un meilleur suivi de son matériel, plus ou moins sensible (armement par exemple).

B. Lutte contre la contrefaçon

Nous l'avons vu, dans de nombreux domaines (agroalimentaire, pharmaceutique etc.), il est essentiel d'avoir une certitude quant à l'authenticité du produit puis une traçabilité de celui-ci. C'est en cela que la chaîne de bloc peut être un moyen de lutte contre toutes les formes de contrefaçons.

Actuellement, la société britannique « BlockVerify »[41] propose de lutter contre la contrefaçon qui touche divers secteurs tels que le luxe ou la pharmacie grâce à la technologie blockchain. Un tag unique est inséré pour chaque produit et l'ensemble des données le concernant est stocké sur la blockchain. À tout moment il est possible de vérifier les informations concernant le produit tels que sa provenance, son authenticité, son lieux de stockage, son certificat de propriété etc. Cela permet donc de découvrir les produits contrefaits, volés ou ceux détournés de leur utilisation première.

Dans le domaine de l'industrie pharmaceutique par exemple l'utilisation d'une telle technologie serait essentielle pour assurer l'authenticité des médicaments, leur traçabilité afin d'empêcher la contrefaçon et donc les risques sanitaires. Tracés par le biais de la technologie

41 http://www.blockverify.io.

blockchain, les médicaments pourraient tous être inscrits dans une base de données universelle, distribuée et accessible aux laboratoires pharmaceutiques comme aux particuliers, assurant transparence et sécurité[42].

Dans le domaine des produits de luxe, une start-up « EVERLEDGE », incubée dans le programme d'accélération de l'assureur Allianz France, utilise déjà l'association d'une blockchain publique et d'une blockchain privée pour certifier les produits de luxe et donc combattre la fraude et le vol de biens assurés. En l'espèce, il s'agit à terme de développer un registre des pierres précieuses et notamment de diamants. Chaque diamant se voit attribuer un numéro de série qui est micro-gravé sur la pierre précieuse et enregistré en parallèle dans la blockchain. L'ensemble des transactions diamantaires sont recensées sur la blockchain constituant un registre numérique immuable et inaltérable. À terme, quand la base de données sera suffisamment déployée, un vendeur de diamants pourra se voir obliger de donner la preuve cryptographique qu'il possède bien légalement ce diamant[43].

Section II : Gestion de données et certification

42 Cela suppose que l'écosystème entier et notamment l'ensemble des grands groupes pharmaceutiques s'y mettent, ce qui relève plus de l'idéologie que de la réalité à court ou moyen terme.
43 ROBERT (Arnaud), « *La chaîne du livre et les chaînes de blocs* », dans les annales des mines, réalités industrielles, « *Blockchains et smart contracts : des technologies de la confiance ?* », Août 2017, p. 55.

I. La gestion de données

Comme nous l'avons vu, utiliser la blockchain permet de passer d'un système centralisé et vertical à un système horizontal garant d'une meilleure résilience et surtout de l'immuabilité de l'information intégrée à la chaîne.

Dans cette optique la technologie blockchain peut être utilisée dans le secteur médical. L'ensemble des résultats (échographie, bilans sanguins, etc.) d'un patient pourraient être sécurisés sur une blockchain tout en permettant aux professionnels de la santé d'y avoir accès et de mieux se coordonner. La sécurisation des données personnelles médicales pourrait être réalisée par la distribution d'une clé privée au patient lui permettant d'avoir ou de donner accès aux données le concernant. Ainsi, l'information du patient est plus aisément transmise d'un professionnel à un autre, avec l'accord du patient. Mais pour que les données soient stockées au sein d'une blockchain encore faut-il une interopérabilité entre les systèmes et les logiciels utilisés par les professionnels de la santé et surtout convaincre l'ensemble de la chaîne de l'intérêt d'une telle implémentation.

En parallèle, la création d'un big data de données médicales anonymisées serait favorable à l'amélioration de la recherche scientifique et garantirait la fiabilité des études menées.

Dans le domaine de la finance, cette technologie pourrait également permettre une lutte accrue contre le blanchiment d'argent tout en diminuant les coûts de KYC par la mutualisation des données clients entre assureurs, banques et courtiers sur la blockchain. L'idée serait de stocker les données clients sur la chaîne de blocs et de pouvoir auditer toutes les personnes qui ont consulté ou apporté des modifications au dossier. Le client aurait quant à lui une clé cryptée que lui seul choisit de mettre à disposition des établissements financiers. L'institution aura alors accès à un certain nombre de documents de manière fiable et sécurisée. L'identité du client serait ainsi améliorée pour des coûts moindres. En parallèle cela réduira le processus administratif et la duplication inutile d'informations et de demandes conduisant à une plus grande efficacité. Cette mise en commun pourrait, dans un premier temps, être utilement réalisée entre les entités d'un même groupe.

Dans le domaine électoral, l'utilisation de la blockchain pourrait garantir la sécurité et la transparence des votes. À titre d'exemple, en France, le parti politique « Nous Citoyens », a récemment utilisé la blockchain pour garantir la sécurité et la transparence des votes en ligne pour une élection interne. L'Ukraine fait également partie des pays qui se sont lancés dans ce domaine. L'un des avantages potentiels est que les votants qui utilisent les chaînes de blocs peuvent vérifier à tout moment leur choix de vote au moyen de leur clé privée. La fraude électorale n'est plus possible car ni l'administrateur du vote, ni d'autres individus, ne peuvent modifier le vote *a posteriori*. Toutefois, des limites doivent être relevées telles que la vérification certaine de l'identité de l'électeur

qui suppose toujours la médiation d'un tiers[44] et l'accès aux clés privées que les pirates pourraient obtenir de différentes manières. Les votants pourraient aussi être tentés de louer ou vendre leurs clés privées pour des raisons pécuniaires.

Dans le domaine de la défense, les États-Unis s'intéressent à la technologie blockchain depuis 2015 et réalisent actuellement des recherches pour trouver des cas d'usage dans ce domaine. Ainsi, le président Trump a signé en décembre 2017 le programme d'investissement de défense d'un montant de 700 milliards de dollars qui fait explicitement référence à la blockchain pour protéger les données sensibles. Ce programme a également pour objectif d'évaluer l'état des recherches des autres puissances étrangères, des organisations extrémistes et des réseaux criminels en la matière[45].

Comme nous l'avons vu précédemment, la DARPA américaine aurait par exemple pour volonté de garantir l'intégrité des données associées à des systèmes d'armes cruciaux comme les armes nucléaires ou les satellites *via* la technologie blockchain. Elle a également lancé un appel d'offres en 2016 pour une « plateforme de messagerie sécurisée ». Celle-ci doit être capable de transférer des messages *via* un protocole décentralisé, sécurisé, sur plusieurs canaux, incluant le protocole de transport, le

44 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 70.
45 KEMPF (Olivier), « *La blockchain est-elle un tournant stratégique ?* », Revue de la Gendarmerie Nationale, 4e trimestre 2018, p.110.

cryptage des messages et la mise en œuvre de la blockchain personnalisée[46]. La clé de chiffrement utilisée ne rendrait les messages visibles que des destinataires finaux, mais la diffusion du message à l'ensemble du réseau garantirait la stabilité du système de messagerie. Dans ce type d'usage, la technologie pair à pair permet de ne pas avoir de serveurs entre les utilisateurs, rendant compliqué toute censure ou blocage comme l'a pu faire le Brésil ou la Chine avec la messagerie WhatsApp. Elle semble présenter un intérêt certain pour les échanges internes aux armées voire pour le partage d'informations critiques en opérations.

L'application civile « Status » fonctionne avec la blockchain Ethereum et se dit « privée, sécurisée et non censurable »[47].

D'autres pays semblent s'intéresser aux applications éventuelles de la blockchain dans le secteur de la défense. C'est le cas de la Russie, d'Israël ou encore de la Chine. La Chine souhaiterait par exemple développer la blockchain dans trois domaines que sont le renseignement, le cycle de vie des armes et la logistique militaire.

En France, le ministère des Armées s'est doté en juin 2018 d'une nouvelle direction, la Direction générale du numérique et des systèmes d'information et de communication (DGNUM), remplaçant l'ancienne Direction générale des systèmes d'information et de communication, et directement rattachée au ministre. Elle a notamment pour objectif d'orchestrer la transformation

46 *Ibid*., p. 109.

47 http://mybroadband.co.za/news/Software/268265-the-most-private-and-secure-messaging-platform-in-the-world-and-why-it-is-better-than-whatsapp.html.

numérique au profit des armées avec au cœur du dispositif la question des données.

Et pour les forces de l'ordre, quelles pourraient être les implications ?

Le premier avantage pourrait être l'interopérabilité. Les forces de l'ordre et la justice pourraient utiliser la technologie blockchain pour centraliser la collecte de preuves et des procédures judiciaires. La blockchain pourrait alors permettre à plusieurs utilisateurs d'accéder aux mêmes données avec des niveaux d'autorisation différents ou encore d'informer automatiquement les victimes chaque fois que l'affaire évolue.
De la même manière que pour les armées, une messagerie sécurisée fondée sur la technologie blockchain pourrait-être envisagées.
Le second avantage consiste dans le caractère immuable des données qui offre des pistes d'audit très intéressantes. En effet, l'anonymisation est techniquement difficile et la plupart des informations stockées sur les blockchains sont donc au mieux pseudo-anonymes. La technologie blockchain du bitcoin en particulier permet de suivre toutes les transactions impliquant une adresse bitcoin donnée jusqu'à la première transaction. Les forces de l'ordre peuvent à titre d'exemple reconstituer l'historique de transactions illicites lors de la saisie et de la perquisition d'ordinateurs dès lors qu'elles trouvent au préalable la clé de cryptage. Cela donne aux forces de l'ordre des moyens supplémentaires pour suivre les flux d'argent ce qui ne serait jamais possible avec de l'argent liquide. C'est un avantage considérable pour les magistrats, dans la mesure où elle constitue une preuve numérique des transactions

puisque la blockchain est publique, certifiée et non falsifiable. Les magistrats français n'ont d'ailleurs pas hésité à reconnaître le lien entre une infraction sur Internet et le possesseur de la clé privée de cryptage[48].

Le risque majeur est que les cybercriminels utilisent des techniques d'anonymisation ou d'offuscation[49] comme par exemple l'utilisation d'un service de mixage[50] ou un « darkmarket »[51]. Dans ce cas de figure, il n'est pas possible pour les forces de l'ordre de résoudre l'enquête à l'instant T, mais cela reste possible en cas de saisie d'un serveur illégal. Par exemple, la saisie des serveurs illégaux « AlphaBay »[52] ou « Hansa »[53] a permis aux autorités de remonter l'ensemble de ces transactions et de les analyser. Un dossier non solutionné aujourd'hui le sera peut-être demain grâce à l'immuabilité de la blockchain. Il s'agit alors de transformer les facteurs risques en opportunités.

48 V. ANONYME, « *La France démantèle un trafic de bitcoins, une première en Europe* », Challenges, site internet http://challenges.fr, le 07 juillet 2014.
49 Procédé par lequel un code est rendu impénétrable.
50 Plateformes proposant un mixage de crypto-actifs pour garantir sécurité, confidentialité et anonymat à ses clients.
51 Un « darkmarket » est un marché noir en ligne où l'on trouve des produits illicites.
52 « Alphabay Market » était un marché en ligne du darknet proposant de la drogue, des armes etc. Il a été fermé à la suite d'une action policière engagée aux États-Unis, au Canada et en Thaïlande en juillet 2017.
53 « Hansa Market » était un marché en ligne du darknet proposant de la drogue, des armes etc. Il a été fermé à la suite d'une action policière et judiciaire des Pays-Bas en juillet 2017.

La Gendarmerie Nationale investit en compétences et en ressources dans le domaine de la cybersécurité. La chaîne cybercriminalité s'appuie sur un réseau de proximité au niveau local (référents Cyber), des spécialistes au niveau départemental (Cyber N'tech[54]) et des experts au niveau national (PJGN[55]) réunissant les compétences de pointe du centre de lutte contre les criminalités numériques (C3N) et du département informatique, électronique de l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), constituant le réseau « CYBERGEND » composé de 3500 gendarmes spécialisés en technologie numérique[56]. Le C3N investit annuellement plusieurs centaines de milliers d'euros dans des outils pour lutter contre cette nouvelle forme de délinquance. Il a par exemple développé un logiciel de décryptage des rançongiciels.

- Le cas particulier de la gestion de données des objets connectés

En 2015, plus de 5 milliards d'objets connectés étaient déployés dans le monde. En 2020 ce chiffre devrait atteindre plus de 20 milliards alors que la population mondiale ne devrait pas dépasser les 8 milliards[57]. L'explosion de l'utilisation des objets connectés doit

54 N'Tech est un diminutif de nouvelles technologies.
55 PJGN : Pôle Judiciaire de la Gendarmerie Nationale.
56 V. site internet de la Gendarmerie Nationale : https://www.gendarmerie.interieur.gouv.fr/pjgn/SCRCGN/Le-centre-de-lutte-contre-les-criminalites-numeriques-C3N.
57 PWC France, « *Blockchain, catalyseur de nouvelle approches en assurance* », site internet *https://www.pwc.fr* p. 6.

conduire à une réflexion sur l'explosion parallèle des données générées par ces objets. Comment les gérer, les sécuriser, les exploiter voire les faire interagir ?
Le développement de la technologie blockchain en la matière pourrait faciliter la gestion de ces objets connectés. En effet, ces objets qui sont au cœur de l'écosystème informatique, font face à des risques de défaillance et de malveillance et souffrent donc souvent d'une faiblesse de sécurité.
La blockchain pourrait suivre ces objets connectés individuellement et augmenter la confiance, la transparence et la traçabilité dans leur déploiement d'une part et permettre de les faire interagir grâce à des smart contracts d'autre part.
La mise en relation des données de ces objets peut donner lieu à des solutions à haute valeur ajoutée économique. Néanmoins, la question de l'interopérabilité reste une question à résoudre. Il existe des centaines de standards de communication applicables à l'internet des objets. Pour permettre la remontée et la mise en commun des données générées par ces objets des plateformes de gestion émergent. Celles-ci seront à terme un élément clé de cette interopérabilité.
L'enjeu stratégique est donc pour la France de ne pas laisser passer le wagon et d'inciter les acteurs économiques français à développer leurs propres plateformes, à les imposer, en attirant concepteurs d'objets connectés et prestataires de services associés sous peine de voir des entreprises étrangères le faire et capter la valeur ajoutée associée[58].

58 V. la note scientifique de l'OPECST n°1 sur les objets connectés sur les sites du Sénat et de l'Assemblée nationale

Ces plateformes devront être particulièrement résistantes et résilientes pour faire face à la croissance exponentielle des IoT dans les années à venir. Seules les plateformes dotées de capacités de communication, de traitement de données et d'administration au plus près des objets répondront à ces enjeux. Or la blockchain apporte des solutions innovantes et adaptées pour réaliser ce type de plateformes. La blockchain offrira un registre distribué sécurisé qui permettra à l'utilisateur final de légitimer ses objets connectés, de les répudier ou de les bloquer selon les besoins. Le détenteur ou l'administrateur d'un objet pourra définir son statut (opérationnel, obsolète, en accès public…) d'une manière qui soit traçable et non contestable[59]. Comme nous l'avons vu pour les données médicales, la blockchain replacera le détenteur de ces objets au cœur du système en lui permettant le contrôle de ses données et de leur usage par des tiers *via* un système d'autorisations entre détenteur et plateformes.

II. Des services d'attestation et de certification grâce aux blockchains

(http://www.Senat.fr/fileadmin/Fichiers/Images/opecst/quatre pages/OPECST 2018 0013 note objets connectes.pdf).

59 GENESTIER (Philippe), LETONDEUR (Loïc), ZOUARHI (Sajida), PROLA (Alain) et TEMERSON (Jean-Marc), « *Blockchains et smart contracts : des perspectives pour l'Internet des objets (IoT) et pour l'e-santé* », dans les annales des mines, réalités industrielles, « *Blockchains et smart contracts : des technologies de la confiance ?* », Août 2017, p. 71 et 72.

La blockchain peut également offrir des services d'attestation et de certification de documents ou de droits pouvant concerner des domaines aussi variés que l'état civil, le cadastre, les contrats de type notariés ou encore les droits de propriété intellectuelle. De nombreuses start-up se développent dans ce secteur. Mais peu d'applications à ce jour ont une maturité technologique suffisante.

La start-up « Factom »[60] se propose par exemple d'utiliser la blockchain afin de certifier l'existence de documents et de ses versions suivantes. Les données sont enregistrées sur la blockchain de façon à créer une liste qui est envoyée sur tous les serveurs du réseau. Il est alors possible d'ajouter des éléments mais pas de modifier des données existantes. En France, la startup « KeeeX » propose un service similaire c'est à dire d'obtenir le preuve d'existence et d'authenticité d'un document.

Le canton de Genève a, par exemple, mis en place un projet pilote d'expérimentation de la blockchain Ethereum dans le domaine des services publics[61]. Ce projet a pour objet la livraison électronique d'extraits et autres documents officiels du registre du commerce[62].

La ville de Dubaï souhaite transférer l'intégralité de ses documents officiels sur la blockchain d'ici 2020.

Dans de nombreux pays en développement où l'administration est défaillante voire corrompue,

60 http://www.factom.org.

61 Site internet https://www.ge.ch>geneve-numerique.

62 République et canton de Genève, compte rendu de projet 2559, preuve de concept blockchain appliquée au registre du commerce, p. 6.

l'implémentation de blockchains pour pallier ces lacunes serait intéressante.

Cette technologie pourrait être utilisée pour développer des cadastres dans les pays où il n'en n'existe pas, où certaines terres ne sont pas enregistrées dans une base officielle, où les risques de corruption et fraude sont grands. Ce pourrait être le cas de l'Afrique où 90 % des territoires ruraux ne sont pas inscrits dans un cadastre. Or, cette absence de sécurité foncière est un frein aux investissements étrangers pourtant nécessaires au développement économique de ces pays et la blockchain pourrait résoudre cette problématique.

Dans cette optique, le gouvernement du Honduras a conclu en 2015 une entente avec Factom, une jeune entreprise américaine pour l'utilisation de chaînes de blocs visant à gérer l'enregistrement des titres fonciers et à empêcher la fraude et la corruption. Toutefois quelques mois plus tard le projet a été abandonné pour des raisons inconnues. De la même manière le projet d'enregistrement des actes fonciers par la start-up Bitland au Ghana semble également ralenti[63]...

Concernant les droits de propriété intellectuelle ou droits d'auteur, la blockchain permettrait d'enregistrer et de certifier tout le parcours d'une œuvre d'art. Elle garantirait ainsi sa provenance, son authenticité et permettrait la gestion des interactions entre les parties concernées. Elle permettrait bien entendu d'empêcher toute reproduction illicite. Un registre mondial utilisant la blockchain pourrait être créé pour enregistrer tous les droits d'auteurs musicaux et autres. L'ensemble des transactions concernant l'œuvre serait enregistré sur la chaîne et

63 http://Bitlandglobal.com.

notamment les différentes cessions. Cela permettrait notamment de rémunérer l'auteur par un pourcentage des ventes conformément au droit de suite. En parallèle, des smart contracts pourraient être intégrés à la chaîne de bloc afin de rémunérer automatiquement les droits d'auteurs dès la diffusion ou l'achat d'un titre en suivant des conditions prédéfinies. Le lien entre l'auteur et son œuvre serait inscrit sur la chaîne et le nombre de droits non réclamés diminuerait[64].

À titre d'exemple, la société de gestion de droit « Allmade », qui opère surtout dans les pays africains, propose un système de boîtier à installer dans les lieux sonorisés pour l'identification des titres diffusés et aboutir au final à une répartition des droits plus juste. Ce processus est totalement géré par des blockchains alliant traçabilité et transparence[65].

De la même manière pour les livres, les droits d'auteurs pourraient être mieux respectés. L'utilisation de la technologie des blockchains garantirait aux ayants droits, lors de la vente d'un livre numérique d'occasion, que le même ouvrage n'est pas à la fois vendu et conservé par son premier propriétaire.

Enfin, lors d'un contentieux, apporter la preuve de l'inscription d'une œuvre sur la blockchain pourrait jouer un rôle probatoire substantiel. Mais cela pose la question

64 BARBET-MASSIN (Alice) et DAHAN (Véronique), « *Les apports de la blockchain en matière de droit d'auteur* », BRDA, 8/18, avril 2018, p. 22.

65 WAIGNIER (Christophe), « Blockchains et smart contracts : premiers retours d'expérience dans l'industrie musicale », dans les annales des mines, réalités industrielles, « Blockchains et smart contracts : des technologies de la confiance ? », Août 2017, p. 47.

de la position du législateur quant à la force probante de la blockchain (acte authentique, acte simple…).

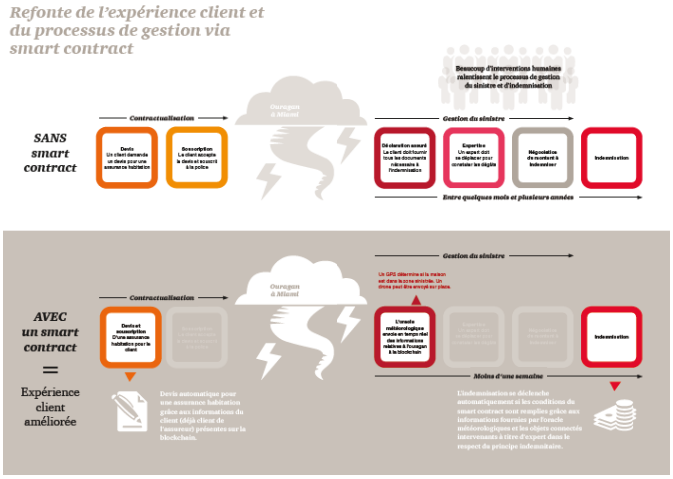
III. La désintermédiation

Le registre basé sur la technologie blockchain offre de par son caractère décentralisé ou distribué des possibilités multiples d'utilisation. Certains experts disent que la blockchain va « ubériser uber ». Trois domaines particuliers peuvent être évoqués : les assurances, l'énergie et la finance.

A. Les assurances

Concernant le domaine de l'assurance, les possibilités d'utilisation de la blockchain sont multiples.
Tout d'abord, pour les assureurs classiques, l'utilisation de la blockchain permettra un gain de temps dans la réalisation des devis d'assurance et dans la passation de contrats avec ses clients habituels grâce à l'accès simplifié aux données. Cela permettra une réduction des coûts de gestion et une meilleure satisfaction client.
Pour les assurances indicielles c'est à dire les assurances liées à un indice tels que la température ou l'hydrométrie, l'utilisation de la blockchain permettra à la fois de faire baisser les coûts de gestion et de transaction et d'indemniser plus rapidement et efficacement le client.

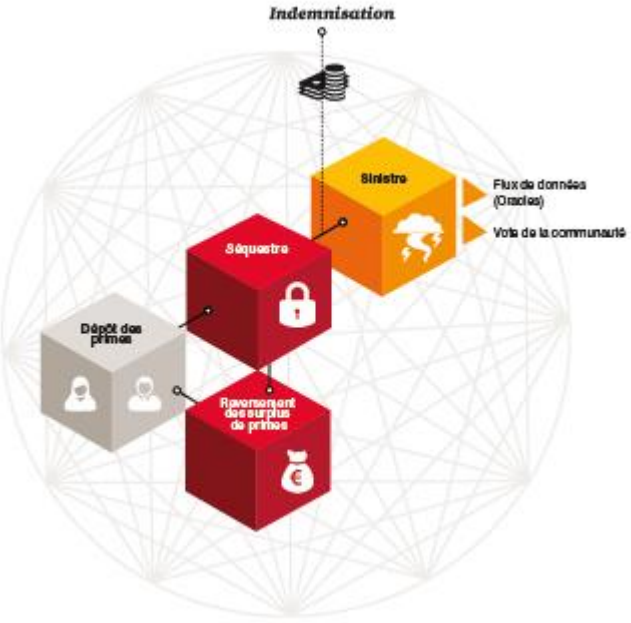
C’est par l’intégration de smart contracts à la chaîne qu’il sera possible d’automatiser l’indemnisation des assurés lorsqu’un événement survient. Le contrat sera alimenté par des données extérieures fiables (par exemple les données pluviométriques du service national de météorologie) fournies par des « oracles » ou par des objets connectés (IoT). Cela permettra de rendre beaucoup plus rapide le processus décisionnel et de diminuer les coûts de structure.
Ce type de contrat pourra par exemple être déployé dans le monde de l’agriculture ou des transports. Les agriculteurs pourront être indemnisés automatiquement après une certaine période de sécheresse prédéfinie dans le smart contract. Le voyageur (train-avion) pourra être indemnisé automatiquement en cas de retard du train ou de l’avion sans remplir de formulaire.
Sur ce modèle, l’assureur Allianz France expérimente, depuis 2016, l’indemnisation automatique de catastrophes naturelles *via* un smart contract.
AXA a quant à lui investit 55 millions de dollars dans un leader de la technologie blockchain, la société canadienne Blockstream.



Source : PWC

Ensuite, l'utilisation des blockchains pourrait faire émerger des assurances pair à pair permettant à chacun à la fois de participer au bassin d'assurés et aux gains d'investissement sans passer par un tiers (assureur).
La start-up française Wekeep propose déjà aux personnes, pour des assurances non obligatoires, de mutualiser leurs cotisations au sein d'un smart contract multi-signé. En cas de sinistre, si les conditions d'indemnisation sont remplies, l'ensemble des membres de l'assurance pair à pair vont donner leur accord par vote pour l'indemnisation.

Fonctionnement de l'assurance pair à pair



Source : PWC

B. L'énergie

Concernant la production d'énergie, le marché est actuellement unidirectionnel c'est à dire qu'il repose sur des producteurs centralisés. Pourtant, l'autoproduction se développe et le consommateur devient producteur. Dans ce contexte se pose la question de la revente de l'énergie

produite en surplus de sa consommation. À l'heure actuelle, le consommateur est obligé de passer par des producteurs centralisés pour revendre sa production locale. L'utilisation de la blockchain rendrait possible des projets locaux d'échange d'énergie pair à pair. Pour ce faire, des « smart grids » sont expérimentés localement afin d'équilibrer l'offre et la demande. À Brooklyn, aux États-Unis par exemple, grâce à un « microgrid », cinq maisons de President Street peuvent échanger de l'énergie en temps réel, sans intermédiaire, avec cinq autres habitations de l'autre côté de la rue[66].

C. La finance

Dans le monde de la finance, les établissements banquiers ont compris que la blockchain était plus une chance qu'une menace pour eux. En effet, son utilisation dans ce secteur est une opportunité pour limiter les coûts et rendre un meilleur service aux clients.
En France, l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) s'est dotée en juin 2016 d'un pôle dédié aux FinTech[67] et à l'innovation. Elle travaille étroitement avec l'Autorité des Marchés Financiers (AMF) et tous deux animent un forum FinTech qui regroupe banques, assurances, partenaires et pouvoirs publics. La Banque de France a également décidé de tester

66 LAURENT (Charlotte), « *7 applications possibles de la technologie blockchain* », site internet https://www.7x7.press/7-applications-possibles-de-la-technologie-blockchain, 22 février 2017, p. 3.
67 Expression associant les diminutifs de finance et de technologie. Elle désigne l'utilisation de la technologie pour repenser les services financiers et bancaires.

la blockchain afin d'être en mesure de juger par elle-même des potentialités de cette technologie.
Comme nous l'avons déjà vu, plus de 80 établissements financiers du monde se sont réunis au sein d'un consortium international pour expérimenter une blockchain *via* la start-up R3. Dans ce contexte, HSBC et ING ont utilisé la plateforme Corda mise au point par cette start-up pour réaliser une transaction dans le domaine du commerce international. HSBC était chargé d'une transaction pour le compte du géant du négoce de produits agricoles Cargill. Cette transaction portait sur une cargaison de soja transportée entre l'Argentine et la Malaisie. L'opération financière était constituée d'une lettre de crédit opérée entre HSBC et ING. En temps normal, au regard du nombre de documents à fournir par le vendeur, celle-ci aurait dû prendre entre 5 et 10 jours. Grâce à la technologie blockchain la transaction a été réalisée en 24 heures[68].
Des projets atypiques sont également en cours de développement comme par exemple les « non fungible tokens » (NFT) ou les « security tokens ». À l'heure actuelle, les entreprises peuvent émettre des actions pour leur activité puis organiser une introduction en Bourse pour vendre des titres aux investisseurs particuliers. La « tokenisation » fonctionne de manière similaire. Les actions de l'entreprise sont remplacées par des « security tokens » qui peuvent s'échanger au niveau mondial *via* des plateformes d'échange de crypto-actifs. Mais contrairement à l'introduction en Bourse d'une entreprise, un token n'a pas besoin de remplir tous les critères des

68 CUNY (Delphine), « *HSBC et ING réussissent la première lettre de crédit sur la blockchain* », site internet https://www.latribune.fr>banques-finance, 14 mai 2018.

autorités boursières et financières ni de suivre le long processus bancaire nécessaire pour être coté sur un indice comme le NASDAQ[69], par exemple.
Mais la blockchain est également et surtout une opportunité pour les populations n'ayant pas accès aux banques de pouvoir accéder à certains services.
Pour illustrer cette possibilité, le programme alimentaire mondial de l'ONU a développé un système de paiement des aliments achetés chez les fournisseurs locaux par les réfugiés syriens *via* une plateforme basée sur la technologie blockchain[70].
Des micro-crédits se développent également. Dans ce cas, la technologie blockchain permet d'effectuer des prêts entre particuliers de façon sécurisée, transparente et surtout sans autorité centrale. Cette décentralisation est une réelle opportunité pour les entrepreneurs des pays peu bancarisés, où les taux d'intérêt sont généralement très élevés. Les prêteurs ont davantage de possibilités d'investissement, et pour l'emprunteur il n'est pas nécessaire d'avoir un compte bancaire grâce à l'utilisation de crypto-actifs. Les transactions sont réalisées plus rapidement qu'avec le système bancaire traditionnel, offrant des taux d'intérêts plus compétitifs. Prêteur et emprunteur se mettent d'accord sur une prime de risque ou un taux d'intérêt, puis une fois l'accord validé, celui-ci devient un smart contrat auto exécutable *via* des lignes de code inviolables au sein de la blockchain. À titre d'exemple, l'application « ETHLend » permet le

69 Le **NASDAQ** (sigle de *National Association of Securities Dealers Automated Quotations*) est une bourse de valeurs ouverte en 1971.
70 https://www.crypto-france.com/blockchain-programme-alimentaire-mondial-onu-contournement-frais-bancaires.

développement de ces micro-crédits décentralisés *via* la blockchain de l'Ethereum. Pour sécuriser ces prêts, cette application utilise des tokens[71] qui peuvent représenter presque n'importe quelle valeur, entre autres l'or (DigixDAO), le pétrole (Bilur) ou des propriétés immobilières (REXmls).

Les possibilités et les implémentations ne manquent pas dans le secteur de la blockchain. Au regard du potentiel disruptif qu'offre la technologie blockchain, la France, et plus précisément le Ministère de l'Économie et des Finances, vient de lancer une consultation le 11 février 2019 destinée à recenser les projets et les expérimentations en cours dans l'écosystème français.

Le questionnaire a pour volonté de connaître la nature de la chaîne de blocs utilisée, le secteur d'activité, son degré de maturité, les modes de financements, les partenaires potentiels et leurs origines géographiques, les limites rencontrées et les améliorations souhaitées. Par cette enquête, Bercy souhaite identifier les obstacles au développement de cette technologie[72]. En effet, le développement et l'utilisation de nouvelles technologies nécessitent d'évaluer les risques inhérents à celles-ci, et ce, de manière approfondie.

---

71 Un token est un actif numérique émis et échangeable sur une blockchain.

72 LAUSSON (Julien), « *Le gouvernement voudrait connaître votre projet de blockchain* », Business, Numerama, site internet https://www.numerama.com/business/463714-le-gouvernement-voudrait-connaitre-votre-projet-de-lockchain.html, 12 février 2019.

Chapitre III : Les risques à anticiper...

Si la blockchain semble apporter des solutions disruptives à certaines problématiques (contrefaçon, suivi de matériel etc.), elle n'est cependant pas infaillible. Elle présente encore un certain nombre de risques auquel il est nécessaire d'apporter des solutions en vue de son implémentation dans la durée. Elle se heurte en autre à des limites techniques, sécuritaires, géopolitiques ou encore juridiques.

Section I : Freins techniques et failles sécuritaires

I. Les freins techniques

À l'heure actuelle, la technologie blockchain est confrontée à plusieurs freins techniques tels que sa complexité, sa capacité d'évolution (« scalabilité »[73]) ou encore son coût écologique.
La chaîne de blocs est tout d'abord très technique et est difficilement accessible pour le plus grand nombre. À partir du moment où elle ne fait pas partie de l'état d'esprit de l'entrepreneur (« mindset »), elle peut leur faire peur. L'acceptation de la technologie blockchain nécessite la

73 Passage à une vaste adoption impliquant de très nombreuses opérations chaque seconde.

multiplication de formations et d'expérimentations concrètes pour la rendre plus compréhensible et abordable et surtout pour éliminer les blocages, les peurs et autres excuses ou empêcheurs de passer à l'action.

La blockchain, surtout la publique, doit également faire face à une problématique de montée en puissance c'est à dire à l'augmentation du nombre de transactions. Ce frein est lié à son mécanisme de validation historique dont ses procédés cryptographiques sont source de lenteur. Il s'agit donc bien là de l'un des principaux défis pour les blockchains, à commencer par celle du bitcoin. Actuellement, 10 minutes en moyenne sont nécessaires pour l'ajout d'un bloc ce qui représente la réalisation de 7 transactions[74] par seconde au maximum. Nous sommes encore loin des 400 transactions par carte bancaire réalisées chaque seconde en France. Un changement d'échelle semble donc problématique et difficilement transposable pour la blockchain en l'état actuel de la technologie. Des start-up recherchent des options alternatives pour absorber un volume plus important de transactions (groupage de transactions, parallélisation de blockchain, etc.). Les innovations en la matière sont encore peu mâtures d'un point de vue technologique et les experts ne sont pas d'accord sur les options envisageables notamment pour des questions de sécurité de la chaîne.

La blockchain engendre également un certain nombre de risques écologiques liés à la technique du minage d'une part et au matériel utilisé pour ce minage d'autre part.

En effet, la technologie reposant sur la preuve de travail suppose d'effectuer des quantités très importantes de calcul. Pour miner des blocs et ainsi valider les

74 Chiffres de 2017.

transactions, les mineurs doivent résoudre des problèmes cryptographiques difficiles demandant de grands volumes de calcul. Ces calculs nécessitent une consommation considérable d'énergie électrique pour faire fonctionner les ordinateurs et les installations de refroidissement. Les blockchains ont donc des impacts énergétiques et environnementaux considérables.
Pour les mineurs, la rentabilité de leur activité dépend donc du prix de l'électricité converti en bitcoins. Une véritable compétition de puissance de calcul s'opère afin d'effectuer un maximum de fonctions de hachage. Comme nous l'avons vu en première partie, les mineurs se sont regroupés en pool et de véritables fermes de minage c'est à dire des usines de calcul, ont vu le jour. Ces fermes se situent dans des pays où l'énergie électrique est bon marché afin de rentabiliser au maximum l'activité de minage tels qu'en Chine.

L'extérieur et l'intérieur d'une « ferme » de minage

Source : Kncminer

L'ensemble des mineurs du réseau bitcoin effectuent en moyenne 4 millions de hash par seconde, représentant une consommation équivalente à la moitié de la puissance d'une central nucléaire[75] selon le site internet Digiconomist, ou encore équivalente à la production électrique annuelle de la Hongrie. Tous les experts ne sont pas d'accord sur la consommation énergétique de la blockchain du bitcoin, mais selon les estimations elle serait comprise entre 45 et 200 TWh par an[76]. Ces besoins sont, en outre, en augmentation exponentielle en raison de la méthode de validation utilisée et du nombre croissant de transactions. L'impact écologique est donc considérable en terme d'émissions de gaz à effet de serre. Cet impact est d'autant plus important que les fermes de minage sont surtout établies en Chine, pays qui présente pour sa production électrique l'intensité carbone la plus élevée au monde[77].

Cette consommation énergétique a déjà pu poser des difficultés d'approvisionnement au niveau local tels qu'aux États-Unis dans l'État de New York. En février 2018, du fait d'une augmentation excessive du prix de l'électricité pour les simples usagers, la ville de Plattsburg a dû interdire pendant 18 mois l'installation de nouvelles usines de minage[78].

D'ailleurs, certains cyberpirates font supporter le coût énergétique du minage à des victimes n'ayant pas suffisamment protégé leur ordinateur. Ce piratage

75 http://digiconomist.net/bitcoin-energy-consumption.
76 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, pp. 80-88.
77 Ibid., pp. 89 et 90.
78 V. « *Small towns try to tame the bitcoin boom* », Citylab.com, mars 2018, lien : http://www.citylab.com/life/2018/03/small-towns-try-to-tame-the-bitcoin-boom/556298.

dénommé le crypto-jacking consiste à contraindre un navigateur à miner des crypto-actifs à son insu. De nombreux sites, dont le propriétaire n'est pas forcément au courant de l'ajout d'un code de crypto-jacking, dissimulent *via* des annonces publicitaires ces processus de minage. Ensuite, les visiteurs de ces sites ne comprennent pas pourquoi leur appareil a subitement des performances ralenties. Cela est arrivé par exemple au site de partage de vidéos « Youtube ».

La preuve de travail n'est pas la seule méthode pour sécuriser une blockchain, la preuve d'enjeu étant une solution moins coûteuse et plus écologique à mettre en place. La preuve d'enjeu (POS) semble être la solution d'avenir à ce stade de la technologie même si sa sécurité doit être améliorée. D'autres méthodes de consensus pourraient être mises en œuvre pour répondre en urgence à ce défaut majeur et pour rendre la technologie blockchain viable à plus long terme. Pour se faire, la recherche doit relever le défi de la consommation énergétique.

Une initiative française (BART[79]) existe en la matière. Une trentaine de chercheurs mutualisent leurs compétences pour lever les verrous scientifiques liés aux blockchains, selon une feuille de route commune et définie pour six ans. Ce programme développe entre autre de nouvelles architectures assurant fiabilité et capacité de montée en charge du réseau. Cette initiative s'intéresse notamment à une méthode de validation des blocs moins

79 Blockchain Advanced Research & Technologies est un collectif de recherches académique français lancé par Inria, Télécom Paris Tech, Télécom SudParis et IRT SystemX qui travaille autour de 6 axes : les modèles théoriques, le passage à l'échelle et les outils de monitoring, la sécurité, les architectures, la confidentialité des données et les modèles économiques et de régulation.

énergivore, tout en utilisant des méthodes de consensus sécurisés par des moyens cryptographiques avancés.
De plus, outre la consommation énergétique, la technologie blockchain pose un problème environnemental de par l'utilisation d'appareils de hachage rapidement obsolètes et difficilement recyclables. Lorsqu'ils sont remplacés par de nouvelles versions plus puissantes, les anciens appareils ne peuvent être réutilisés à une autre fin, ce qui représente un gaspillage difficilement concevable au regard des problématiques environnementales actuelles[80].
Enfin, la blockchain fait un fort usage des technologies actuelles de hash et de chiffrement. Sachant que certains registres créés au travers de la blockchain sont conçus pour durer plusieurs dizaines d'années et que la fiabilité de cette technologie repose sur les techniques actuelles de cryptage, que se passera-t-il lorsque les algorithmes utilisés deviendront vulnérables du fait de l'avancée technologique ? Il se posera alors une véritable problématique de pérennité de la protection des informations stockées sur la chaîne. Si l'ordinateur quantique était conçu comme il est prévu d'ici 2030, les algorithmes actuels deviendraient particulièrement vulnérables. Ce type d'ordinateur aura en effet une puissance suffisante pour casser les protections actuelles.

80 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 91.

II. *Les failles sécuritaires*

D'une manière générale pour que les blockchains soient infaillibles, certaines conditions doivent être remplies, comme le nombre d'entités impliquées dans les transactions qui doit être en nombre suffisant, la répartition géographique des entités de calcul afin de ne pas mettre en péril le système par des enjeux géopolitiques, et enfin la fiabilité du protocole de communication et des algorithmes de calcul. Si d'une manière générale, la chaîne de blocs semble donc bien protégée, sa sécurité n'est cependant pas absolue. À ce titre, il faut distinguer les problèmes de sécurité liés à la chaîne elle-même et ceux liés à son environnement immédiat[81].

Les problèmes de sécurité liés à la chaîne elle-même peuvent concerner les lignes de code. En effet, au regard du nombre de lignes de codes créées lors de développement d'applications, des erreurs intentionnelles ou non peuvent être introduites. Les start-up et autres PME n'ont d'ailleurs pas forcément pour priorité la sécurité lors du développement de ce type d'applications. Des actions malveillantes peuvent intervenir ou des acteurs extérieurs peuvent développer une politique d'infiltration systématique des comités techniques internationaux à des fins stratégiques. Cependant, la majorité des blockchains publiques sont construites sur des protocoles open source qui sont accessibles en ligne. Tout le monde, dont la

81 McFARLAND (Charles), HUX (Tim), WUEHLER (Eric) et CAMPBELL (Sean), « *Rapport sur les menaces associées aux blockchain* », site internet McAfee, http://www.mcafee.com, juin 2018, 30p.

communauté des développeurs, peut vérifier ce code et proposer des améliorations de sécurité ou d'évolutivité. Le code peut également être audité par des sociétés spécialisées en sécurité. Des récompenses (« rewards » ou « bug bounty ») sont même proposées aux « ethical hackers » afin de découvrir des failles de sécurité dans les codes.

En outre, la destruction de l'infrastructure physique des chaînes est possible notamment pour des chaînes dont le nombre d'entités impliquées dans les transactions est insuffisant. En effet, pour que la blockchain soit sécurisée il faut que la contribution, c'est à dire le taux de hachage au réseau, soit distribuée de manière suffisante. Une entité ou un groupe collaboratif ne doit pas être en capacité de contrôler plus de 50 % de la puissance de calcul sous peine du risque d'une attaque dite des 51 %. En effet, une entité qui détiendrait une puissance de calcul supérieure à 51 % aurait la capacité de valider des blocs plus rapidement que les autres utilisateurs et pourraient par la même générer des blockchains à volonté ou déployer la technique de la double dépense[82].

La blockchain publique du bitcoin semble sécurisée en la matière puisque au regard du nombre de mineurs et de la quantité d'argent en jeu pour récompenser le minage, aucune double dépense ne semble suffisamment rentable pour compenser les moyens à investir dans une attaque des 51 %. Ce n'est en revanche pas le cas pour la très grande

82 La technique de la double dépense consiste à réaliser plusieurs transactions avec la même unité de cryptomonnaie et à ne payer qu'un seul destinataire.

majorité des autres blockchains publiques[83]. Il n'est d'ailleurs pas inconcevable qu'un acteur doté d'une forte puissance de calcul (un gouvernement, une multinationale par exemple) puisse utiliser cette attaque afin non pas de mettre en œuvre une double dépense mais pour simplement s'attaquer au réseau et créer un bouleversement économique à l'échelle mondiale à des fins politiques. Dans ce cas précis il s'agirait d'une attaque dite « Goldfinger »[84].

Il est à noter que les blockchains privées ou fermées, ne sont pas susceptibles de subir une attaque 51 % car les membres du réseau sont connus et un contrôle est donc possible. Elles ne sont tout de même pas à l'abri d'une erreur dans leur code source ou d'attaques de leur système par des cybercriminels à l'aide de technologies cloud, de botnets ou de pool de minage.

Enfin, les blockchains qui cherchent à dépasser le simple usage transactionnel en intégrant des programmes informatiques automatiques (des smart contracts), sont en contrepartie plus vulnérables. Ces programmes ajoutent de la complexité dans le protocole et, par voie de conséquence, de potentielles failles exploitables par des attaquants. Ce fut le cas pour la blockchain Ethereum en 2016 avec le vol de plusieurs dizaines de millions de crypto-actifs « Ether » lors d'une levée de fonds (Initial Coin Offering/ICO) dénommée « The DAO »[85]. La communauté Ethereum a alors décidé de réaliser un

---

83 V. le site www.crypto51.app qui évalue le coût d'une attaque 51 % en prenant en compte la difficulté de minage des blockchains PoW et le coût approximatif d'une heure de location de puissance de calcul pour réaliser une attaque.

84 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 64.

85« Decentralized Autonomous Organization ».

« Hard-Fork »[86] afin de priver l'auteur du hack des millions de crypto-actifs volés et de les retourner aux victimes. Contesté en interne, le « hard-fork » a conduit à la scission de la blockchain Ether en deux : Ethereum (ETH) avec les fonds reversés et Ethereum Classic (ETC). Cet événement était le premier de son genre. Le « Hard-Fork » permet donc d'apporter une solution et de modifier la blockchain en cas de faille de sécurité, de bug ou de piratage mais il peut également être source de problèmes. Le fait de modifier la blockchain est effectivement contraire à sa principale caractéristique qu'est l'immuabilité des transactions.

Si les problèmes de sécurité liés à la chaîne elle-même semblent restreints, l'environnement de la blockchain est quant à lui beaucoup plus fragile.
Comme nous l'avons vu, plus une blockchain possède un réseau étendu et distribué, plus il est difficile de modifier son code ou de créer une transaction frauduleuse. Ainsi, beaucoup de piratages recensés ne portent pas sur le protocole lui-même mais sur des interfaces avec celui-ci, tels que des sites internet de change.
En effet, les cybercriminels ont déjà pris pour cibles de nombreuses blockchains au moyen de techniques d'ingénierie sociale, de logiciels malveillants et d'exploits. Le phishing est le type d'attaque menée contre les blockchains le plus courant. À titre d'exemple, un

86 Les « forks » sont liés au fait que différentes parties doivent utiliser des règles communes pour conserver l'historique de la blockchain. Les « forks » sont utilisés pour ajouter de nouvelles fonctionnalités à une blockchain, pour inverser les effets d'un piratage ou de bugs catastrophiques.

cybercriminel a pu détourner l'équivalent de 4 millions de dollars en crypto-actif (IOTA) grâce à une porte dérobée au sein des porte-monnaie des utilisateurs. Pour disposer d'un porte-monnaie (« wallet ») en mesure de stocker les actifs numériques attachés à la blockchain IOTA, les utilisateurs devaient générer eux-mêmes la clé de cryptage pour le verrouillage de ce porte-monnaie. Ce protocole nécessitait l'utilisation d'un « SEED » c'est à dire une suite aléatoire de caractères pour générer cette clé privée utilisée pour chiffrer le porte-monnaie. Le cybercriminel a ainsi proposé aux utilisateurs un générateur automatique de « SEED » dénommé « Iotaseed ». Par ce biais, il a pu collecter et conserver l'ensemble des « SEED » et reconstituer facilement les clés privées. Au bout de six mois, il a eu assez de clés privées et a vidé tous les portefeuilles[87].

Les logiciels malveillants sont également une source d'insécurité. Le nombre de logiciels de rançon (ransomwares[88]) ont tout d'abord explosés à partir de 2016. Ces outils sont essentiellement utilisés par les cybercriminels pour se procurer des crypto-actifs qui offrent une facilité de transfert, sans contrôle central et de manière dissimulée. Mais, selon une étude de McAffee Global Threat Intelligence[89], ce type d'attaque a

87 V. ADAM (Louis), « *IOTA : le cryptobraquage a encore de beaux jours devant lui* », 1er février 2018, site internet http://www.zdnet.fr.

88 Un ransomware ou rançongiciel en français est un logiciel informatique malveillant qui chiffre et bloque les fichiers contenus sur un ordinateur et qui demande une rançon en échange d'une clé de déchiffrement.

89 McAffee Global Threat Intelligence est un service complet de cyberveille sur les menaces, délivré en temps réel.

commencé à diminuer à compter du 4ème trimestre 2017[90], alors qu'en parallèle les crypto-jackings ont augmenté[91]. Tous les types d'équipements sont d'ailleurs ciblés, ordinateurs, tablettes ou smartphones. Des téléphones Android ont d'ailleurs été infectés par un logiciel malveillant « ADB Miner » qui s'exécute comme un ver pour miner des crypto-actifs en Chine.

Les attaques contre les implémentations mêmes de la blockchain ou contre les outils sur lesquels elles s'appuient constituent également un autre type de menace.

Dans l'application financière de la blockchain, les utilisateurs des crypto-actifs utilisent des « portefeuilles électroniques », leur permettant de réaliser des transactions. Ces portefeuilles sont protégés par des clés privées de chiffrement.

Les cyberpirates peuvent voler les portefeuilles en remplaçant par exemple les adresses des portefeuilles par des adresses sous leur contrôle. Mais dans la plupart des cas, ces portefeuilles et plus précisément les clés privées, sont mal protégés soit par les propriétaires des portefeuilles soit par les plateformes d'échange. En effet, il existe souvent un problème de sécurité lié aux mots de passe du portefeuille. Certains utilisateurs incapables de mémoriser un mot de passe constitué d'une suite de 64 caractères, utilisent un « brain wallet » et ne retiennent qu'un mot de passe classique. Ils ont ensuite recours à un algorithme de hachage (SHA-256) chaque fois qu'ils ont

90 Le nombre de rançongiciels aurait diminué de 30 % entre le 4ème trimestre 2017 et le 1er trimestre 2018 selon McAffee Global Threat Intelligence.

91 Le nombre de crypto-jacking aurait augmenté de 1189 % entre le 4ème trimestre 2017 et le 1er trimestre 2018 selon McAffee Global Threat Intelligence.

besoin de leur clé privée. Ces utilisateurs créent des failles et les cybercriminels qui recherchent les portefeuilles cérébraux (brain wallet) sont en capacité de retrouver les mots de passes et de voler les crypto-actifs de ces portefeuilles.
Enfin, les plateformes d'échange des crypto-actifs sont les cibles privilégiées des cybercriminels aboutissant à des détournements conséquents de ces monnaies. À titre d'exemple, en janvier 2018, la plus importante plateforme d'échange de nationalité japonaise (Coincheck) a essuyé une perte de 532 millions de dollars en crypto-actif « NEM ».
Dans le cas de vol de crypto-actifs, il est difficile voire impossible de récupérer les sommes volées du fait du caractère décentralisé de la technologie blockchain. En effet, seul le cybercriminel, propriétaire du portefeuille ayant reçu les sommes dérobées est en mesure de restituer les sommes.

La blockchain est ainsi exploitée voire dévoyée par des opérateurs illicites, qui ont très rapidement perçu les innombrables avantages de cette technologie pour leurs activités illicites. En parallèle, les services répressifs peuvent se trouver en difficulté du fait d'une méconnaissance de cette technologie de la blockchain support des crypto-actifs et de son caractère international.

Section II : Sécurisation des données

La gestion des données est un autre élément clé de la blockchain. En effet, les blockchains publiques ne garantissent pas forcément la confidentialité des données stockées car si la cryptographie est utilisée pour lier les blocs entre eux, elle ne l'est pas obligatoirement pour l'inscription des données sur la chaîne. Il est donc essentiel de définir quelles données peuvent apparaître en clair sur la chaîne et celles qui ne pourront être stockées sur elle sans se retrouver en infraction avec les réglementations en vigueur. Pour ces données il convient de prévoir un mécanisme de cryptage permettant aux seules parties concernées de déchiffrer les données les concernant.

Les données peuvent être « on-chain », c'est à dire enregistrées directement sur la blockchain, ou « off-chain » c'est à dire en dehors de celle-ci. Dans ce cas, les blocs vont contenir un simple lien vers des données conservées à l'extérieur de la chaîne soit de manière dynamique soit sous forme de hash. Cette technique est plus rapide en termes de création de bloc mais a le défaut de réduire la protection offerte par la blockchain.

Le caractère international de la blockchain peut impliquer d'ailleurs des transferts de données internationaux et soumettre les participants à un régime spécifique. Figurant sur un registre partagé à travers le monde, les données inscrites sur la blockchain sont susceptibles d'être utilisées dans des pays qui ne garantissent pas le respect de la protection des données liées à la vie privée. Or comme le prévoit le Règlement Européen sur la Protection des Données Personnelles (RGPD)[92], le transfert de données personnelles vers des pays n'assurant pas un niveau de

92 Règlement Européen sur la Protection des Données Personnelles, UE n°2016/679 du 25 mai 2018.

protection adéquat est illicite et passible d'une amende administrative pouvant aller jusqu'à 20 millions d'euros ou dans le cas d'une entreprise, 4 % du chiffre d'affaire annuel mondial total de l'exercice précédent. Ce règlement vient en effet consacrer un certain nombre de principes tels que l'identification obligatoire d'un responsable de traitement, le droit à la rectification et le droit à l'oubli, exigences qui semblent par essence contradictoires avec un système de blockchain immuable et purement pair à pair.

De plus, l'article 5 du Règlement exige que les données soient conservées pendant « *une durée n'excédant pas le temps nécessaire au regard des finalités pour lesquelles elles sont traitées* ». Plusieurs solutions peuvent être envisagées. Tout d'abord, comme nous l'avons vu les données peuvent être stockées à l'extérieur de la chaîne, cette dernière ne comportant qu'une empreinte numérique. Une autre possibilité serait d'intégrer un smart contract qui aurait pour fonction non pas d'effacer les données personnelles mais de les anonymiser définitivement. Enfin, la mise en place d'un feedback pourrait également être envisagée. Celle-ci permettrait de « *créer une nouvelle ligne numérique et de rendre l'ancienne inaccessible* »[93]. Il s'agirait plutôt ici de faire évoluer la technologie que le cadre juridique.

En outre, il ne faut pas non plus oublier de dire que la blockchain ne permet pas la vérification de l'authenticité des données enregistrées ou la vérification de la légitimité d'une opération non électronique. Il est en effet possible

93 MEKKI (Mustapha), « *Le smart contract, objet du droit (partie 2)* », Dalloz IP/IT, droit de la propriété intellectuelle et du numérique, numéro 1, janvier 2019, p. 31.

d'intégrer des données personnelles ou illicites dans des blockchains publiques. C'est le cas par exemple sur la blockchain bitcoin où l'on peut trouver des données à caractère pédopornographique. Le caractère immuable des données inscrites sur la blockchain peut alors être utilisé à des fins criminelles[94].

La Commission Nationale Informatique Libertés (CNIL) a réalisé une étude sur l'utilisation de la blockchain au regard des exigences du RGPD et a apporté les premiers éléments de réponse quant à la conformité de la blockchain à ce Règlement[95].

Depuis février 2018, un groupe de recherches sur les smart contracts a été créé par le Centre Universitaire d'Enseignement et de Recherche en Propriété Intellectuelle (CUERPI) rattaché au centre de recherche juridiques (CRJ) de l'Université de Grenoble-Alpes et soutenu par la Mission Droit et Justice, groupement d'intérêt public. Les recherches sont réalisées par une équipe pluridisciplinaire et internationale de 22 membres. L'objectif de cette équipe est de « déposer sur une plateforme en accès ouvert un « clausier », qui répertorie sur plusieurs occurrences la traduction informatique de

94 MATZUTT et HILLER « *A quantitative analysis of the impact of arbitrary blockchain content on bitcoin* », Financial Cryptography and Data Security International Conference, 2018, http://fc18.ifca.ai/preproceedings/6.pdf?utm_source=JeromeVosgienFR&utm_medium=SophosFranceLink.

95 Pour un état des lieux complet V. le rapport de la CNIL, « *Premiers éléments d'analyse de la CNIL, blockchain* », septembre 2018, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

clauses françaises et anglaises afin de les rendre auto-exécutables sur la blockchain »[96].

Section III : Les risques géopolitiques : les fermes de minage

Comme nous l'avons vu précédemment, les mineurs pour optimiser leurs capacités de calcul, leurs performances et donc leur rémunération, se regroupent pour former des pools appuyés ou non sur des « fermes de minage ». Ces phénomènes de concentration géographique s'expliquent surtout par les écarts de coût de l'électricité selon les États. À l'heure actuelle, quatre pools appuyés sur des « fermes de minage » assurent aujourd'hui plus de 60 % de la puissance de calcul nécessaire à la blockchain du bitcoin. Or parmi ces quatre pools, nous retrouvons trois pools chinois qui pourraient utiliser cette position dominante contre l'intérêt des autres utilisateurs[97]. En effet, plus de la moitié des serveurs se situeraient aujourd'hui en Chine du fait notamment du prix de son électricité. Avec une majorité des fermes de minage établies sur son sol, la Chine pourrait ainsi chercher à déstabiliser certains crypto-actifs, à commencer par le bitcoin.

---

96 FAVREAU (Amélie), « *Présentation du projet de recherche sur les smart contrats* », Dalloz IP/IT, droit de la propriété intellectuelle et du numérique, numéro 1, janvier 2019, p. 33.

97 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 39.

Ayant compris les enjeux stratégiques, la Russie a également choisi d'encourager l'implantation de pools de mineurs sur son territoire[98].

La technique du minage pose donc des questions d'ordre géopolitique. En effet, l'organisation des mineurs en groupement ou « pools »[99] induit le risque qu'une majorité organisée oriente la validation des blocs et rende caduc le principe même de la blockchain.

Il est donc fondamental que la France mais surtout l'Europe s'empare de cette problématique non seulement de manière technique mais également de manière stratégique afin de conserver une part de souveraineté et d'indépendance dans le domaine.

La France et l'Europe ne doivent absolument pas laisser passer leur chance d'être à la pointe de la technologie et d'obtenir un pouvoir d'influence sur les autres États par le développement de capacités de calcul et de blockchains européennes qui respecteraient les principes portés par l'Europe et afin de ne pas dépendre à terme des autres grandes puissances comme c'est déjà le cas avec internet et les GAFA. Il s'agit également d'une question de sécurité afin d'éviter qu'un seul État ne concentre sur son territoire la puissance de calcul nécessaire à l'altération de blockchains d'importance stratégique.

Dans cette optique, l'Union européenne a lancé en 2018 un observatoire de la blockchain qui a pour mission de constituer un cadre réglementaire proposable aux États membres, de réfléchir à des applications potentielles de la

98 *Ibid*., p. 100.

99 L'appartenance à un pool assure des revenus plus constants aux mineurs. Il existe trois pools d'envergure réduite en France : Big Block Data, Wizard Mining et Just Mining.

blockchain et enfin de proposer une approche pédagogique de la technologie au profit des citoyens. Cependant, en choisissant une entreprise américaine (Consensys) pour diriger les travaux, la Commission européenne a envoyé un très mauvais signal[100].

Section IV : Un cadre juridique à adopter

En raison de leurs caractéristiques, les blockchains publiques posent des questions inédites aux législateurs nationaux. Celles-ci portent notamment sur le cadre juridique, le régime fiscal ou sur la protection des données personnelles comme nous l'avons vu précédemment. Si l'absence de cadre juridique peut paraître *a priori* une opportunité, très rapidement cette liberté devient source d'incertitudes. En effet, quelle valeur juridique accorder à la chaîne de bloc et aux données enregistrées dessus ? Lors d'un contentieux, sera-t-il possible d'apporter la preuve de l'inscription d'une donnée comme une œuvre pour les droits d'auteur sur la blockchain ? Pourra-t-elle jouer un rôle probatoire substantiel ? Et en cas de réponse positive, quelle sera la force probante accordée à celle-ci ? Ces doutes méritent d'être levés par le législateur qui doit se positionner quant à la force probante de la blockchain (acte authentique, acte simple…).

À l'heure actuelle, il n'y a aucune reconnaissance de la blockchain en tant que registre. Le législateur français a apporté un début de réponse avec l'ordonnance du

100 FAURE-MUNTIAN, GANAY et LE GLEUT, *op. cit.*, p. 102.

28 avril 2016[101] relative aux minibons puis aux titres financiers, mais de manière très générale. Le législateur a voulu donner un poids juridique particulier à une inscription sur une blockchain, qui matérialiserait l'existence, le propriétaire ou le transfert de ces titres (actions, obligations, minibons). Mais ce début de cadre reste très limité. En absence de cadre juridique particulier, il faudra en cas de litige démontrer au juge la valeur juridique de l'enregistrement effectué sur la blockchain. Le cas ne s'est pas encore présenté en France.

Les smart contracts posent également des questions. En effet, quelle est la valeur juridique de ces contrats représentant la fonction d'automatisation décentralisée de la blockchain ?

Si le terme de smart contract fait légitimement penser à un contrat juridique conclu entre des parties, il s'agit en fait de protocoles informatiques qui permettent d'exécuter automatiquement des conditions contractuelles préalablement posées entre les parties. L'accord contenu dans les smart contracts pourrait tenir lieu de contrat écrit entre les parties à condition qu'il respecte le droit et notamment les conditions de formation des contrats[102]. En l'état actuel de la législation et de la technologie, un smart contract n'est qu'un mécanisme d'exécution pour un ensemble d'obligations déterminées au préalable dans un contrat principal. D'ailleurs, il ne faut pas confondre les clauses opérationnelles qui peuvent être automatisées, et les clauses non opérationnelles (clause de confidentialité

101 Ordonnance n°2016-520 du 28 avril 2016.

102 Article 1128 et suivants du code civil : une offre, une acceptation, le respect des conditions de validité (consentement, capacité, absence de dol, d'erreur etc.).

par exemple) qui ne peuvent l'être. Ainsi, le smart contract ne semble pas avoir pour vocation à remplacer le contrat juridique mais plutôt à se superposer à lui afin d'automatiser un certain nombres d'obligations[103].
Mais si lors de l'encodage du smart contract sur la chaîne une ou des erreurs étaient commises, que se passerait-il ? Qui serait légalement responsable de l'erreur ? Serait-il possible de contester la blockchain ou le smart contract devant un juge ? Et si oui, ce dernier aurait-il le pouvoir d'imposer des modifications au contenu de la blockchain ? Et dans ce cas, à quel moment ces décisions pourraient être retranscrites dans la blockchain[104] ?
Pour pallier à ces problématiques, différentes clauses doivent être intégrées comme des clauses de force majeure, clauses de transparence et de suivi, clauses relatives au droit applicable et désignant les juridictions compétentes etc[105]. Une clause d'arbitrage pourrait par exemple être intégrée dans les smart contracts *via* un code permettant à un tiers préalablement désigné de modifier la chaîne selon un processus arbitral. Cette action stopperait le fonctionnement du smart contract en attendant la résolution du litige.
À mesure que sa fonctionnalité s'élargira et que les freins techniques seront dissipés, les smart contracts commenceront à être utilisés de manière accrue dans le commerce international, ce qui conduira à une véritable révolution du droit contractuel. Les institutions d'arbitrage

103 GILLIOZ (Fabien), « *Du contrat intelligent au contrat juridique intelligent* », Dalloz IP/IT, droit de la propriété intellectuelle et du numérique, numéro 1, janvier 2019, p. 16.
104 Dès la première instance, après les délais légaux de recours, après appel ou la cassation ?
105 MEKKI, *op. cit.*, p. 28.

réputées qui anticipent une offre de résolution des différends sur mesure pour les smart contracts prendront un avantage concurrentiel important sur les autres institutions[106].

Nous avons déjà vu que pour s'exécuter le smart contract a besoin de données externes (météo, horaires de trains etc) fournies par de nouveaux tiers de confiance, les oracles. Ces oracles peuvent être des personnes physiques (notaires), des personnes morales (SACEM), ou ils peuvent être automatisés *via* des programmes etc. En tout état de cause, que se passe-t-il si l'oracle est défaillant ou malveillant ? Qui est responsable ? Un cadre juridique de l'oracle doit également être défini. En attendant, son intervention doit être minutieusement organisée dans un ensemble de stipulations contractuelles[107].

D'une manière générale, l'absence d'un cadre juridique clair est un frein au déploiement des utilisations innovantes de cette technologie. Une adaptation législative, qui ne peut d'ailleurs se limiter au seul territoire de la France, est fondamentale pour apporter une certaine sécurité juridique. Le caractère international de la blockchain nécessite une réflexion commune et une harmonisation internationale du cadre juridique garantissant à la fois sécurité, innovation et développement de nouveaux usages. Cette régulation ne doit pas être étudiée de manière simpliste et doit prendre en compte l'intégralité des avantages et des risques qu'elle peut apporter.

En effet, la question majeure est de savoir si la blockchain doit s'adapter à la régulation actuelle (au RGPD par

106 GILLIOZ, *op. cit*., p. 20.
107 MEKKI, *op. cit*., p. 29.

exemple), ou bien est-ce à la régulation de s'adapter aux technologies blockchains ? À titre d'exemple, pour être conforme avec le RGPD et la question des données personnelles, les blockchains publiques devront passer d'un format lisible et accessible à tous à un protocole rendant les informations détenues dans la blockchain illisibles et protégées[108]. Elles deviendront alors impossibles à tracer pour les forces de l'ordre rendant toute investigation impossible...

108 Et les rapprochant drastiquement des « privacy coins » comme Dash, Monero, Zcash etc.

Conclusion

Oscar Wilde[109], écrivait " *Le progrès n'est que l'accomplissement des utopies*.".
Si le désir de se passer d'une autorité centrale de contrôle comme en matière de monnaie est apparu dans un premier temps comme une utopie irréalisable, pourtant en 2008, suite à la crise financière et à la perte de confiance dans les institutions financières institutionnelles, Satoshi Nakamoto publie l'article fondateur de la blockchain et du bitcoin. Le bitcoin, monnaie électronique alternative, non soumise à une autorité centrale de régulation s'appuie sur un support technologique dénommé blockchain ou chaîne de bloc en français. La blockchain s'est donc fait tout d'abord connaître de par le développement du bitcoin. Cependant, si le bitcoin est indissociable de la blockchain il n'est pas vrai de l'inverse.
Il s'agit avant tout d'un registre ouvert, décentralisé et réputé infalsifiable. Il s'agit donc d'une technologie de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers. La chaîne de blocs permet d'obtenir un consensus entre des acteurs qui ne se font *a priori* pas confiance.
Mais on ne peut pas parler que d'une blockchain mais de blockchains au pluriel. Nous pouvons distinguer des

109 Oscar Wilde, écrivain irlandais, né à Dublin le 16 octobre 1854 et mort à Paris le 30 novembre 1900.

blockchains publiques où tout le monde peut lire et écrire, des blockchains privées où le registre est fermé et l'accès permissionné, et enfin des chaînes intermédiaires semi-publiques ou de consortium avec des restrictions pour lire ou écrire. Des smart contracts, c'est à dire des logiciels d'assistance à la préparation, à l'exécution automatique et à la supervision de contrats, peuvent également être intégrés à la chaîne.

Aujourd'hui, est appelée blockchain 1.0 tout ce qui concerne la monnaie électronique et ses opérations, blockchain 2.0 l'ensemble des applications financières et économiques autres que celles liées à la monnaie (« FINTECH ») et blockchain 3.0 les autres applications en dehors des sphères financières et économiques (administrations, santé, etc.).

Deux visions s'opposent alors entre ceux qui pensent que la technologie prendra des décennies pour se diffuser et se transformer dans le tissu industriel, et ceux qui pensent qu'elle est au contraire disruptive.

Les avantages de la blockchain sont principalement sa décentralisation, son immuabilité, sa résilience et sa traçabilité pouvant conduire à une baisse des coûts de structure et à l'amélioration du service dans de nombreux domaines. Les fonctionnalités de cette technologie paraissent séduisantes et les nombreuses applications potentielles de la blockchain alimentent aujourd'hui de vives discussions.

De nombreux pays se sont déjà positionnés. L'Estonie ou la Suisse expérimentent déjà la blockchain dans leur administration et d'autres pays comme les États-Unis, la Grande-Bretagne ou la Chine ont lancé des programmes de recherches en la matière. Des consortiums financiers ou divers grands groupes expérimentent également la

blockchain à leur niveau. Certaines applications de la chaîne de blocs examinées dans le présent document sont déjà déployées mais les données probantes actuelles indiquent que celles-ci sont encore à l'étape de la validation de principe et plutôt à petite échelle. Il n'est cependant pas facile de se tenir au courant des innovations et des progrès relatifs aux chaînes de blocs tant ce domaine change rapidement au niveau mondial.

Face à la multiplication d'annonces de création ou d'implémentation de blockchains dans tous les secteurs, la question qui se pose alors est de savoir quels sont les réels enjeux de la technologie, présentée comme une promesse d'avenir, et comment accompagner son passage de l'expérimentation à la maturité, en combinant régulation et soutien à l'innovation ?

En effet, la blockchain constituerait une nouvelle promesse d'innovation et de disruption des modèles économiques dominants *via* des applications prometteuses dans des domaines aussi variés que l'administration (accès simplifié et sécurisé aux services, identité numérique, vote etc.), la chaîne logistique (traçabilité et lutte contre la contrefaçon), la gestion de données (données médicales, de KYC, procédures judiciaires etc.), la certification (cadastre, état civil, droit de la propriété intellectuelle etc.) et la désintermédiation (assurances, énergie, finance etc.). Les perspectives ouvertes sont donc considérables et ne doivent pas être ignorées.

Même si de nombreuses applications paraissent prometteuses, des défis techniques (complexité, scalabilité), sécuritaires (lignes de code, diverses attaques), écologiques (consommation énergétique), géopolitiques (pool et fermes de minage, souveraineté, capacité d'influence etc.) et réglementaires (validité

juridique, compétence territoriale en cas de litige, clauses contractuelles, protection des données etc.) doivent être réglés avant toute implémentation plus vaste et dans la durée.

Les possibilités d'applications sont donc variées mais il est encore tôt pour tirer des conclusions définitives sur l'évolution de la technologie dans les 5 prochaines années ou plus. Pour l'instant, la technologie des chaînes de blocs suscite de l'engouement et son potentiel disrupteur appelle une stratégie publique alliant régulation et soutien à l'innovation dès à présent. Face à la concurrence internationale et au risque de se retrouver dépassé et dépendant dans un secteur prometteur, les pouvoirs publics doivent s'engager sans plus attendre sur la voie de la technologie blockchain.

Cependant, l'engouement généré par l'écosystème crypto-actifs/blockchain peut entraîner certaines dérives. Beaucoup de personnes développent une réflexion inversée c'est à dire qu'ils définissent un problème et qu'ils veulent trouver une solution *via* la technologie blockchain. Certains domaines ne sont pourtant pas adaptés à l'utilisation de la blockchain et notamment tout ce qui ne requiert pas un haut niveau de confiance ou de traçage. Il ne faut donc pas céder à un effet de mode mais plutôt proposer une stratégie concrète de développement de cette technologie ainsi que des projets pilotes se traduisant par des expérimentations au sein même des services publics centraux, là où une réelle plus-value a été définie au préalable.

Cela suppose en parallèle un soutien à la recherche pour être à l'avant-garde de leur développement, l'adoption d'une régulation de base raisonnable et attractive, des actions de formation et la veille des forces de l'ordre pour

contrer le dévoiement éventuel de la technologie par des criminels.

Recherche et développement (R&D) :
La technologie blockchain n'est pas encore mûre. Ses failles techniques et sécuritaires, ses risques écologiques et ses limites juridiques doivent faire l'objet de R&D. Les principales priorités pour la recherche devraient être la réduction de la consommation énergétique, la capacité à monter en charge (scalabilité), la sécurité des systèmes et la fiabilité des applications. Il conviendrait également de résoudre la contradiction entre protection des données personnelles, qui suppose un certain anonymat, et lutte contre les fraudes, qui nécessite une forme de transparence des transactions sur le réseau.
Pour se faire, les pouvoirs publics doivent développer une politique de R&D cohérente et encourageant la coordination entre recherches publiques et privées. Ils doivent notamment :
- D'une manière générale, soutenir des secteurs d'excellence ou d'intérêt stratégique en France.
- Soutenir et aider la création d'un réseau d'innovateurs en technologies de chaînes de blocs et inciter ces derniers à soutenir les applications qui facilitent la fourniture des biens publics. Cette incitation pourrait prendre la forme d'une contribution financière à des projets d'infrastructure logicielle pour construire les blockchains de l'administration publiques de demain. L'enjeu sera alors de concevoir des expériences intelligentes et hautement personnalisées sur le moment.
- Promouvoir des travaux de recherche et de développement interdisciplinaires notamment dans les domaines de la formalisation (intégrité, confidentialité,

preuves, opposabilité), la sécurité, la qualité de service (bande passante, scalabilité, robustesse, fiabilité), et la gouvernance (évolution, neutralité) car la technologie blockchain touche les secteurs aussi bien scientifiques qu'économiques, juridiques, écologiques ou encore géopolitiques.
- Lier les travaux sur la blockchain avec ceux sur l'intelligence artificielle puisque cette dernière est introduite systématiquement dans la technologie et qu'elle pourrait apporter des solutions dans l'exécution automatique des smart contracts.
- Développer de nouveaux standards et protocoles.
Des technologies de registres distribués alternatives aux blockchains sont déjà en cours de développement dans des laboratoires de recherche. Ainsi, les « Directed Acylic Graphs » (DAG)[110], constitueraient la nouvelle génération de blockchain, plus rapide, plus efficace et moins chère. Il s'agit pour l'instant d'une expérimentation mais elle pourrait représenter une solution décentralisée à la gestion des objets connectés qui se multiplient.

Régulations de base raisonnables et attractives :
La technologie blockchain a besoin d'un statut juridique (droit de la preuve, statut du smart contract, clauses, compétence territoriale etc.) et d'harmonisation pour retirer l'insécurité juridique et donc susciter la confiance des utilisateurs et des investisseurs. À titre d'exemple, un

110 LEE (Sherman), « *Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0* », Forbes, 22 janvier 2018, disponible sur le site internet : https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/#3ed31a7180bc.

groupe d'experts de 16 pays travaillent ensemble depuis décembre 2016, sous l'égide de l'Organisation internationale de normalisation (ISO) pour la mise en place de normes volontaires afin de dessiner les contours de cette technologie qui souffre de ce besoin d'harmonisation. La France participe à ces travaux *via* l'Association Française de Normalisation (AFNOR).
De la même manière une politique fiscale claire, adaptée aux crypto-actifs et harmonisée est nécessaire. La mission d'information de la commission des finances de l'Assemblée Nationale, a publié le 30 janvier dernier un rapport sur les « crypto-actifs » comprenant 27 propositions dans l'optique de faire évoluer la législation française[111].

Formation :
Il est nécessaire de développer des formations sans se cantonner aux spécialistes. Une cellule d'agents publics ayant une expertise dans le domaine des blockchains pourrait être mise en place afin de pouvoir intervenir en appui des services de l'État.
En parallèle, des approches et des solutions novatrices pourraient être recherchées afin de faciliter l'accès à la technologie des chaînes de blocs à tous, en se concentrant par exemple sur l'accès aux outils cryptographiques et à leur utilisation.

111 WOERTH (Éric), PERSON (Pierre), (*et al*.), « *Rapport d'information déposé en application de l'article 145 du Règlement par la commission des finances, de l'économie générale et du contrôle budgétaire en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles* », Rapport n°1624, 30 janvier 2019, site internet http://www.assemblee-nationale.fr.

Blockchain et criminalité :

Comme toute innovation pouvant être positive pour la société, la blockchain peut être dévoyée de son usage originel par des organisations criminelles en recherche permanente de solutions rapides, anonymes et sécurisées. La technologie blockchain, transnationale par nature, répond parfaitement aux besoins des criminels. Elle offre donc des perspectives à la fois positives et négatives à travers ses nouveaux usages. De nouveaux contentieux vont nécessairement surgir et impliquer à la fois pour les forces de l'ordre et les autorités judiciaires une connaissance affinée des mésusages de cette technologie par les délinquants.

En conséquence, cette technologie doit s'inscrire durablement dans les enjeux de sécurité et d'ordre public socio-économique. Elle rend nécessaire le développement rapide de stratégies judiciaires accompagné d'une coopération policière et d'une entraide judiciaire internationales accrues. Cela suppose un investissement en terme de formation des différents acteurs de la chaîne (enquêteurs, magistrats) pour une meilleure prise en compte de la dimension technologique dans la lutte contre la criminalité organisée transnationale, mais également de développer des capacités d'investigation adaptées.

À ce titre, la Gendarmerie Nationale a toute sa place dans ce dispositif dans une logique partenariale avec les autres services régaliens (autorités de régulation et autres), les entreprises privées (opérateurs financiers et bancaires etc.), les chercheurs et les acteurs de la blockchain. Elle pourrait être associée, *via* ses experts, à la recherche publique/privée sur le sujet pour que l'aspect sécuritaire soit bien pris en compte.

Elle doit à la fois avoir un rôle de veille, réaliser des études de prospective et apporter si nécessaire des solutions en cas de dévoiement de la technologie à des fins criminelles comme elle a pu le faire dans le domaine des rançongiciels avec la création d'un logiciel de décryptage.
Forte de son expérience acquise depuis la première saisie nationale de bitcoins réalisée en 2014, la Gendarmerie Nationale dispose de toutes les armes nécessaires pour conserver sa prévalence tant au niveau national qu'international.

Remerciements

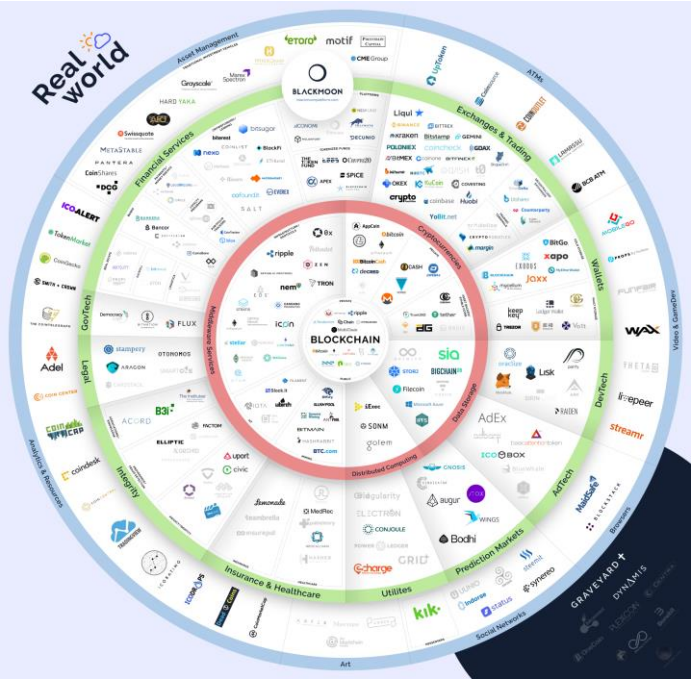
Je tiens à remercier l'ensemble des personnes qui ont contribué par leur soutien, leurs conseils avisés, leurs informations, à la rédaction de ce mémoire et notamment mon directeur de mémoire, l'adjudant-chef Patrice REVEILLAC, expert européen en monnaies virtuelles à EUROPOL.

Je tiens tout particulièrement à remercier mon époux, le chef d'escadron Sébastien NOCHEZ, pour son implication et son soutien.

Annexes :

Annexe 1 : Exemple de mapping des projets blockchain

Exemple n°1 : « *Real world* »



Exemple 2 : « *Blockchain startup Landscape* »

Exemple 3 : « *50+ blockchain real world uses cases* ».

Indications bibliographiques

1. Ouvrages généraux :

- COLLECTIF, réalités industrielles, « *Blockchains et smart contracts : des technologies de la confiance ?* », Les annales des mines, Août 2017, 128p.
- JEANNEAU (Clément), YERETZIAN (Antoine), STACHTCHENKO (Alexandre), BALVA (Claire), « *La blockchain décryptée, les clés d'une révolution* », 2016, 143p.
- LAMPORT (Leslie), SHOSTAK (Robert) et PEASE (Marshall), « *The Byzantine Generals Problem* », ACM Transactions on Programming Languages and Systems », Volume 4, n°3, juillet 1982.
- LELOUP (Laurent), « *La blockchain, la révolution de confiance* », Eyrolles, 2017, 224p.

2. Articles de journaux

- ADAM (Louis), « *IOTA : le cryptobraquage a encore de beaux jours devant lui* », 1er février 2018, site internet http://www.zdnet.fr.
- ANONYME, « *La France démantèle un trafic de bitcoins, une première en Europe* », Challenges, site internet http://challenges.fr, le 07 juillet 2014.
- ANONYME, « *Pourquoi la révolution blockchain est en marche* », Challenges, site internet https://www.challenges.fr, 12 novembre 2015.
- ANONYME, « *Comment HSBC a utilisé la blockchain dans le commerce international* », site internet https://www.challenges.fr, 14 mai 2018.
- AUFFRAY (Christophe), « *Big Data dans l'armée française : données, garde à vous !* », 14 mars 2019, site internet http://www.zdnet.fr.
- BALVA (Claire) et JEANNEAU (Clément), « *L'enjeu de la blockchain pour nos sociétés* », 15 septembre 2016 et *« Blockchain 5 applications concrètes (et révolutionnaires) »*, 24 mars 2017, site internet https://strart.lesechos.fr.

- BARBEZAT (Marc), « *Les 3 forces de la blockchain au secours de la cyber-sécurité* », site internet https://www.ledecodeur.ch, 14 février 2017.
- CHANTREL (Flavien), « *États des lieux de la blockchain en France : acteurs, régulation, formation...* », site internet https://www.blogdumoderateur.com, 27 novembre 2017.
- CHERIF (Anaïs), MANIÈRE (Pierre), « *L'Estonie, royaume du tout-numérique* », La Tribune, 5 avril 2018. Disponible sur : https://www.latribune.fr/technos-medias/internet/l-estonie-royaume-du-tout-numerique-774138.html.
- CUNY (Delphine), « *HSBC et ING réussissent la première lettre de crédit sur la blockchain* », site internet https://www.latribune.fr>banques-finance, 14 mai 2018.
- FONTAINE (Gilles), « *Blockchain, cette révolution qui secoue le monde de la finance* », site internet https://www.challenges.fr, 28 mars 2016.

- HOTTOT (Kévin), « *Un rapport remis au CSPLA suggère l'utilisation de la blockchain pour gérer les droits culturels* », site internet https://www.nextinpact.com, 1er février 2018.
- KAYE (Byron) et WAGSTAFF (Jeremy), « *For security agencies, blockchain goes from suspect to potential solution* », site internet https://www.reuters.com, 3 décembre 2017.
- LAUSSON (Julien), « *Le gouvernement voudrait connaître votre projet de blockchain* », Business, Numerama, site internet https://www.numerama.com/business/463714-le-gouvernement-voudrait-connaitre-votre-projet-de-lockchain.html, 12 février 2019.
- LOUBIERE (Paul), « *Quand Orange se prend pour Google et investit dans la start-up chain* », site internet https://www.challenges.fr, 10 septembre 2015 et « *Pourquoi Microsoft et JP Morgan viennent de s'allier dans le blockchain* », site internet https://www.challenges.fr, 1 mars 2017.

- MAREUGE (Céline), « *Blockchain : le potentiel de disruption est là* », site internet www.strategie.gouv.fr, 12 décembre 2017.
- MUIR (Rick), « *Policing and public services on blockchain* », site internet www.police-foundation.org.uk, 22 septembre 2017.
- PROTAIS (Marine), « *Les blockchains d'entreprise commencent à se déployer* », l'UsineNouvelle, 23 mars 2018, site internet http://www.usinenouvelle.com/editorial/les-blockchains-d-entreprise-commencent-a-se-deployer.N670439.
- SAAD (Clément), « *Blockchain : forces et faiblesses de la révolution de la cybersécurité* », site internet https://blog.pradeo.com, 8 mars 2018.
- WEINSTEIN (Jason), « *How can law enforcement leverage the blockchain in investigations ?* », site internet https://coincenter.org, 12 mai 2015.

3. Études :

- BLOCKCHAIN PARTNER, « *Chaîne logistique, traçabilité et blockchain* », site internet http://blockchainpartner.fr, 2017, 17p.
- BLOCKCHAIN PARTNER, « *Blockchain et santé* », site internet http://blockchainpartner.fr, 2017, 14p.
- BLOCKCHAIN PARTNER, « *Blockchain, cryptoactifs, ICO : panorama des enjeux juridiques* », site internet http://blockchainpartner.fr, 2018, 14p.
- CELLABZ, « *Blockchain & Beyond* », site internet www.cellabz.com, novembre 2015, 33p.
- CNIL, « *Premiers éléments d'analyse de la CNIL, blockchain* », site internet https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf, septembre 2018, 11p.
- COLLECTIF, rapport « *les enjeux des blokchains* », France stratégie, juin 2018, 150p.

- DYEVRE (Axel) et Mc NAMARA (Suzanne), « *Blockchain, enjeux, usages et contraintes pour la Défense* », CEIS, Les notes stratégiques, septembre 2018, 30p.
- FATF-GAFI, « *Public Statement - Mitigating Risks from Virtual Assets* », 22 février 2019, site internet http://www.fatf-gafi.org.
- FAURE-MUNTIAN (Valéria), GANAY (Claude) et LE GLEUT (Ronan), Rapport n°1092 au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques, *« les enjeux technologiques des blockchains (chaînes de blocs) »*, site internet www.assemblee-nationale.fr, 20 juin 2018, 209p.
- GIANG-TRUONG NGUYEN et KYUNGBAEK KIM, « A *survey about consensus algorithms used in blockchain »*, Journal of Information processing systems, vol. 14, n° 1, février 2018.
- McFARLAND (Charles), HUX (Tim), WUEHLER (Eric) et CAMPBELL (Sean), « *Rapport sur les menaces associées aux blockchain* », site internet McAfee, http://www.mcafee.com, juin 2018, 30p.

- PwC France, « *Blockchain, catalyseur de nouvelle approches en assurance* », site internet PwC https://www.pwc.fr, 36p.
- WOERTH (Éric), PERSON (Pierre), (*et al*.), « *Rapport d'information déposé en application de l'article 145 du Règlement par la commission des finances, de l'économie générale et du contrôle budgétaire en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles* », Rapport n°1624, 30 janvier 2019, site internet http://www.assemblee-nationale.fr.

4. **<u>Articles de doctrine :</u>**

- BARBET-MASSIN (Alice) et DAHAN (Véronique), « *Les apports de la blockchain en matière de droit d'auteur* », BRDA, 8/18, avril 2018, pp.21-25.
- BARLOW (John Perry), « *A Declaration of the Independence of Cyberspace* », site internet https://www.eff.org/cyberspace-independence, 8 février 1996.

- FAVREAU (Amélie), « Présentation du projet de recherche sur les smart contrats », Dalloz IP/IT, droit de la propriété intellectuelle et du numérique, numéro 1, janvier 2019, pp. 33-34.
- GILLIOZ (Fabien), « *Du contrat intelligent au contrat juridique intelligent* », Dalloz IP/IT, droit de la propriété intellectuelle et du numérique, numéro 1, janvier 2019, pp. 16-21.
- HILARY (Gilles), « *Blockchain : sécurité et confidentialité* », Revue de la Gendarmerie Nationale, 4e trimestre 2018, pp.98-103.
- KEMPF (Olivier), « *La blockchain est-elle un tournant stratégique ?* », Revue de la Gendarmerie Nationale, 4e trimestre 2018, pp.104-113.
- LAURENT (Charlotte), « *7 applications possibles de la technologie blockchain* », site internet https://www.7x7.press/7-applications-possibles-de-la-technologie-blockchain, 22 février 2017, 4p.

- LEFORT-LAVAUZELLE (Patrice), *« Comprendre la technologie du blockchain. Quelles applications dans la défense ? »*, Revue Défense n°187, Juillet-août 2017, pp.44-47.
- LEROUX (Maxime) et MASERATI (Frédéric), « *Blockchain : concepts et applications* », site internet www.keyrus.fr/fr, 23 mai 2017, 5p.
- MATZUTT (Roman), HILLER (Jens), HENZE (Martin), ZIEGELDORF (Jan Henrik), MULLMANN (Dirk), HOHLFELD (Oliver) et WEHRLE (Klaus), « *A quantitative analysis of the impact of arbitrary blockchain content on bitcoin* », The 22nd InternationalConference on Financial Cryptography and Data Security, février 2018, site internet http://www.springer.de/comp/Incs/index.html
- MEKKI (Mustapha), « *Le smart contract, objet du droit (partie 2)* », Dalloz IP/IT, droit de la propriété intellectuelle et du numérique, numéro 1, janvier 2019, pp. 27-32.

- NAKAMOTO (Satoshi), « *Bitcoin: A Peer to Peer Electronic Cash System* », site internet https://bitcoin.org/bitcoin.pdf, 2008.

5. Législations :

- Code monétaire et financier : article L223-12.
- Directive (UE) n°2018/843 du parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE.
- Ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse.
- Règlement Européen sur la Protection des Données Personnelles, UE n°2016/679 du 25 mai 2018.

6. Principaux sites Internet :

- Assemblée nationale : http://www.assemblee-nationale.fr

- BLOCKCHAIN FRANCE : https://blockchainfrance.net
- BLOCKCHAIN PARTNER : http://blockchainpartner.fr
- CELLABZ : www.cellabz.com
- CHALLENGES : https://www.challenges.fr
- CNIL : https://www.cnil.fr
- FRANCE STRATEGIE : https://www.strategie.gouv.fr
- GAFI : http://www.fatf-gafi.org
- KEYRUS : www.keyrus.fr/fr
- Les Échos : https://www.lesechos.fr
- Légifrance : http://www.legifrance.gouv.fr
- McAfee : https://www.mcafee.com
- Pwc : *https://www.pwc.fr*
- Sénat : http://www.senat.fr
- Wikipedia : http://www.wikipedia.fr