Année universitaire 2018-2019

DUMEZ Jérémy

Cybercriminalité et crypto-actifs

Mémoire rédigé sous la direction de M. Luc-Michel Nivôse

Conseiller à la Cour de cassation

L'Université Paris II – Panthéon Assas n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à leur auteur.

REMERCIEMENTS

Je tiens d'abord à remercier le Magistère, ainsi que ses Directeurs, MM. Dominique Bureau et Louis d'Avout, de permettre aux étudiants du Magistère de se confronter pour la première fois à un véritable travail de recherche, avec la très grande liberté qui nous est accordée, tant s'agissant du sujet de notre étude, que de la personne de notre Directeur.

Je tiens ensuite à remercier tout particulièrement mon Directeur de mémoire, Monsieur Nivôse, pour la confiance qu'il m'a accordée, la bienveillance dont il a fait preuve à mon égard ainsi que les conseils avisés qu'il m'a prodigué dans la manière d'aborder le sujet.

SOMMAIRE

INTRODUCTION

> *«- Depuis quelque temps, des pièces de fausse monnaie circulent. J'en suis averti. Je n'ai pas encore réussi à découvrir leur provenance. Mais je sais que le jeune Georges - tout naïvement je veux le croire - est un de ceux qui s'en servent et les mettent en circulation. Ils sont quelques-uns, de l'âge de votre neveu, qui se prêtent à ce honteux trafic. Je ne mets pas en doute qu'on abuse de leur innocence et que ces enfants sans discernement ne jouent le rôle de dupes entre les mains de quelques coupables aînés.»*[1]

En 1972, le doyen Carbonnier affirmait déjà que « l'évolution des mœurs et des techniques donne naissance à de nouvelles formes de délinquance ».[2]

1.- Actualité. En décembre 2018, le CEO (PDG) d'un *exchange*[3] canadien, QuadrigaCX est décédé en demeurant l'unique personne à détenir les *clés*[4] des *cold wallets*[5] contenant l'équivalent de 125 millions d'euros en cryptomonnaie appartenant à plus de 100 000 clients. Depuis lors les fonds sont inaccessibles. La société, désormais en faillite, est placée sous protection de la loi face aux demandes de retrait de fonds de ses créanciers.

Des transactions postérieures à ce décès ont suscitées le doute et entraîné des enquêtes et analyses de *wallets* liés à *l'exchange* qui ont révélé, d'abord que les portefeuilles étaient vides et ensuite des liens entre la plateforme et des activités criminelles : fonds d'origines douteuses, fonds « *mixés* »[6] afin d'en dissimuler la provenance, fonds liés aux hacks retentissants de plateformes comme Bitfinex, ou encore provenant de places de marché illégales (*black markets*) sur le *dark web*, comme Silk Road.

---

[1] André Gide, *Les faux-monnayeurs.*

[2] CARBONNIER (J.), *Sociologie juridique*, éd. A. Colin, [1972], éd. PUF, coll. Thémis, Paris, [1978], Refondue coll. Quadrige, [1994] et [2004], cité in *La lutte contre la cybercriminalité au regard de l'action des états*, R. Boos, Thèse de doctorat .

[3] Une plateforme d'échange en crypto-actifs.

[4] La clé privée est l'équivalent du mot de passe pour avoir accès aux portefeuilles.

[5] Portefeuilles (*wallets*) froids (*cold*), est une technique de stockage de la cryptomonnaie non connectée à internet, plus sécurisée.

[6] On parle de *mixing*, *tumbling* ou *blending* pour désigner la pratique qui consiste littéralement à mélanger les cryptomonnaies de différentes provenances pour en diminuer la traçabilité.

Des fonds provenant d'autres exchanges postérieurement à la banqueroute de ces derniers auraient également transité par QuadrigaCX (comme Cryptsy ou encore Mt.Gox, sur lesquels nous reviendrons).[7]

Ce cas, le plus actuel illustre à lui seul la majeure partie du sujet, à savoir la confusion faite *a priori* entre la cybercriminalité et les crypto-actfs, l'opacité de ce secteur et les risques pour les investisseurs du stockage de crypto-actifs sur un *exchange*.

2.- **La cybercriminalité**. Il n'existe pas de définition de la cybercriminalité. A la suite de la doctrine, l'on peut approcher la notion comme « *utilisé généralement pour décrire l'activité criminelle dans laquelle le système ou le réseau informatique est une partie essentielle du crime, (ce terme) est également employé pour décrire des activités criminelles traditionnelles dans lesquelles les ordinateurs ou les réseaux sont utilisés pour réaliser une activité illicite. Dans le premier cas, les technologies sont la cible de l'attaque et, dans le second, elles en sont le vecteur*[8] ».

Sur le plan criminologique, la cybercriminalité est caractérisée par une motivation à la fois financière et technique, selon les personnalités, se rapprochant ainsi d'une certaine forme de « criminalité en col blanc » (*white-collar crime*). La *summa divisio* en la matière réside dans la distinction des *hackers*[9]. D'une part, des *hackers* dits *white hat* (« chapeau blanc »), expert en sécurité informatique, discipline parfaitement légitime, agissant de manière éthique en avertissant notamment des vulnérabilités qu'ils découvrent. D'autre part, des *hackers* dits *black hat* (« chapeau noir »), exploitant les vulnérabilités qu'ils découvrent pour en tirer un profit, notamment financier, de manière illégale.
Seule cette dernière catégorie relève de la cybercriminalité, étant précisé que la fontière entre les deux est très souvent poreuse et qu'un hacker peut passer d'un côté et de l'autre au cours de sa « carrière ».[10]

---

[7] « *QuadrigaCX : analyse des 5 wallets liés au "crypto grand banditisme"* », Journal du Coin.com, 23 février 2019 ; « *Reports Shows QuadrigaCX "Cold Wallets" Actively Involved in Significant Criminal Acivity: Ties to Silk Road, Hacked Funds, Identity Theft and Drug/Human Trafficking* », blog Zerononcense.com, 16 février 2019.
[8] QUEMENER (M.), *Criminalité économique et financière à l'ère numérique*, Economica, p.34.
[9] Hacker étant ici un terme générique, qu'il convient de distinguer du piratage informatique et de la cybercriminalité.
[10] D'anciens hackers black hats peuvent ainsi se reconvertir dans le consulting, comme Kevin Mitnick. Un hacker agissant de manière black hat peut également agir de manière éthique, comme c'est le cas de Marcus Hutchin, ayant reconnu avoir codé le malware bancaire Kronos et pourtant ayant contribué à

La cybercriminalité aurait augmenté de 23% en France en 2018, coûtant en moyenne 8,6 millions d'euros par entreprise française et devrait coûter 4,6 milliards d'euros dans le monde dans les cinq prochaines années.[11]

3.- Délimitation. La présente contribution n'adressera la question de la cybercriminalité qu'exclusivement en lien avec les crypto-actifs. Ainsi, ne seront pas évoquées les infractions se rapportant par exemple à la propriété intellectuelle et aux marques, les infractions telles que la diffamation, le racisme, l'espionnage industriel, la pédopornographie, le harcèlement ou encore les infractions bancaires et financières comme les faux ordres de virements.

4.- **Crypto-actifs.** En novembre 2018, plus de 2000 crypto-actifs étaient échangés, 900 n'existeraient déjà plus.[12] A titre préliminaire, il convient de présenter la technologie au fondement des crypto-actifs, la blockchain, encore appelée chaîne de blocs. [13]

5.- **Origines**. Bien que faisant l'objet d'un récent attrait, la blockchain, dans son concept, remonte au début des années 1990. Conçue dans un but d'horodatage de documents numériques[14], c'est en 2009 qu'elle gagne en intérêt avec Bitcoin. Le protocole Bitcoin (avec une majuscule, pour le distinguer du jeton numérique et monétaire *" bitcoin"*).

6.- **Définition**. La blockchain est une technologie de stockage et de transmission de l'information opérant de façon transparente, sécurisée et décentralisée (*i.e.* sans organe central de contrôle). La blockchain enregistre ces informations sous forme de blocs (d'où la chaîne de blocs) et constitue donc une base de données infalsifiable.

Transparente. Chacun peut consulter l'ensemble des échanges inscrits sur une blockchain depuis sa création.

---

arrêté la diffusion du ransomware WannaCry, ce sur quoi nous reviendrons. On parle de hackers grey-hats.

[11] « Le cybercrime en 2019 : impact et opportunités », rapport Accenture, 6 mars 2019.

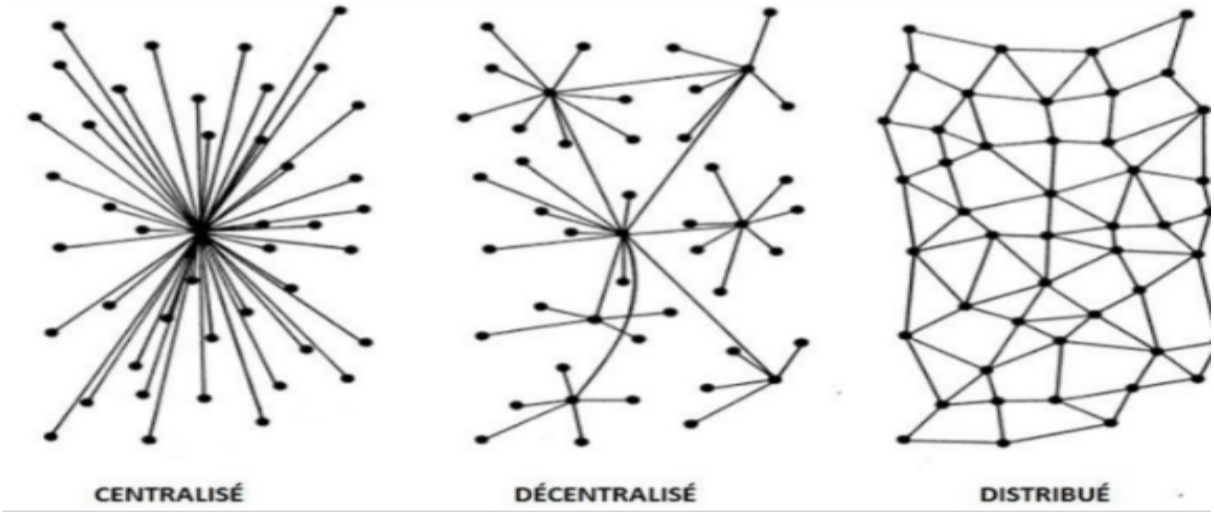
[12] C. Le Moign, ICO françaises : un nouveau mode de financement ? AMF, novembre 2018.
Basé sur CoinMarketCap et DeadCoins

[13] L'essentiel des développements à ce sujet sont issus de l'ouvrage « *La Blockchain décryptée, Les clefs d'une révolution* », Netexplo, Mai 2016, par Blockchain France

[14] « *How to Time-Stamp a Digital Document* », S. Haber, W. Scott Stornetta, https://www.anf.es/pdf/Haber_Stornetta.pdf

Sécurisée. Tout d'abord, un niveau de sécurité est permis par le couple *clé publique*[15]*/clé privée*[16], reposant sur la cryptographie dite « asymétrique ». La comparaison d'usage est celle avec le monde bancaire opérant sur le modèle du RIB/PIN. Le RIB peut en effet être communiqué au public, il est destiné exclusivement à recevoir des fonds, il correspond à la clé publique. Le PIN au contraire sert à retirer des fonds, il doit être conservé de manière confidentielle, il correspond à la clé privée.

Décentralisée. La blockchain présente une caractéristique essentielle : son caractère décentralisé, en ce qu'elle est distribuée, on parle de *distributed ledger technology* (DLT). C'est à dire que différents exemplaires de ce registre transparent existent simultanément sur différents ordinateurs qui sont autant de noeuds du réseau (*nodes*).



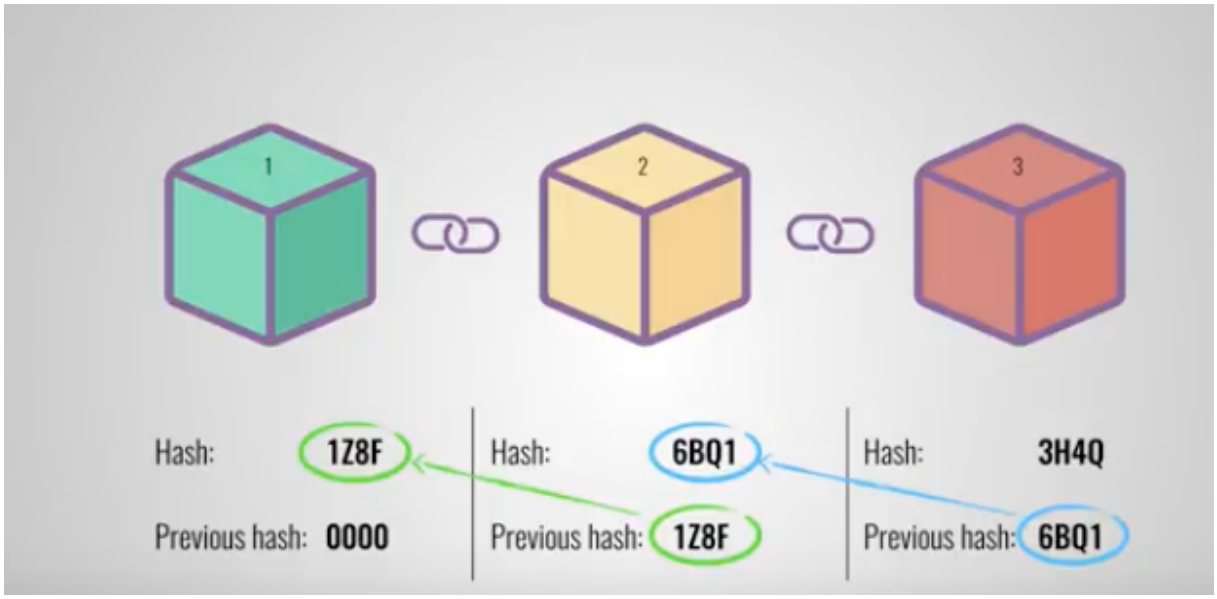
Enfin, un niveau supérieur de sécurité repose sur le mécanisme de validation des blocs appelé preuve de travail, *Proof of Work* (PoW) qui permet, par la résolution de problèmes mathématiques, la confiance.

7.- **Fonctionnement**. Un bloc stocke donc : des informations, un *hash* et le hash du bloc précédent. Les informations stockées dépendent de la blockchain en question, pour Bitcoin, il s'agit de l'émetteur, du destinataire et du montant.

---

[15] Par exemple : 02f5e25778dcee9539b25799831277eb8e731ffcbdcd9e68f79f8ca43c570b94ba
[16] Par exemple : Kzczf8E4oq8MLakhRS479gpZpSe2e6u2xErKHQNqpeFMPEK4irtc
Exemples provenant de https://cryptoast.fr/cles-privees-cles-publiques-et-adresses-dans-bitcoin/

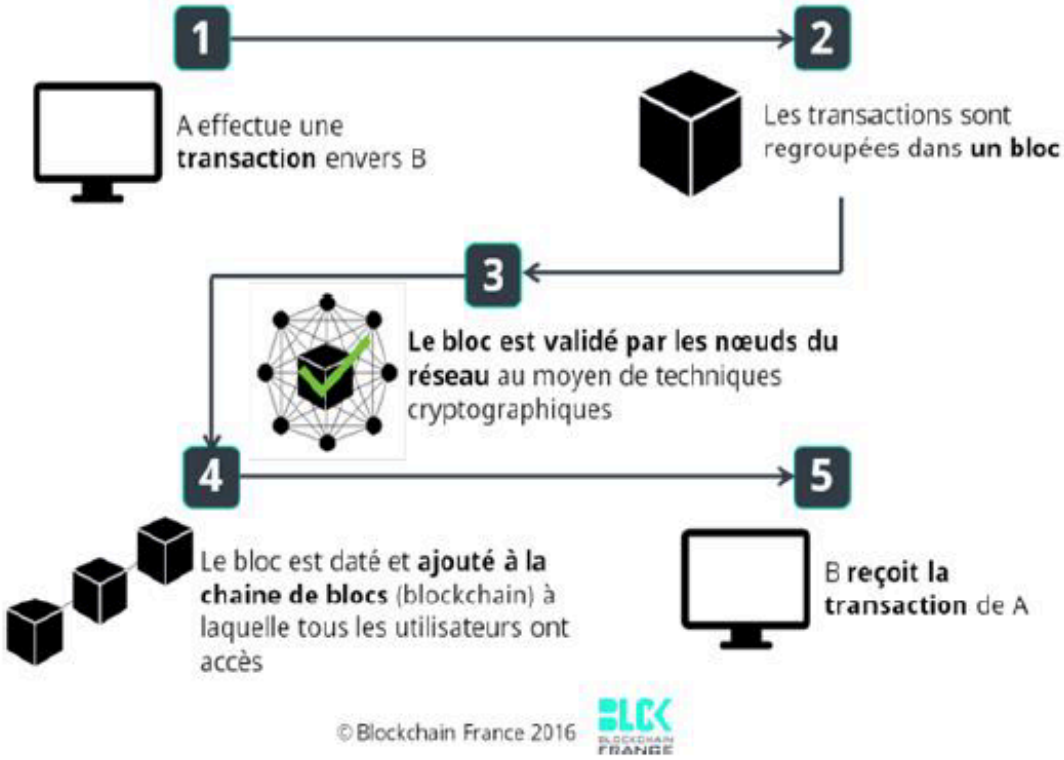
Le *hash* est une suite de caractères, assimilable à une empreinte numérique unique, modifier un bloc revient à modifier le hash, ce qui rend toute altération détectable. Chaque bloc contient également le hash du précédent bloc afin de former une chaine de blocs et retracer les transations.



How does blockchain work – simply explained (YouTube)

Puisque chaque bloc contient le hash du bloc précédent, en modifier un revient à modifier la chaine et la rendre invalide. Modifier un bloc est tout de même possible, néanmoins il faudrait qu'il recalcule l'ensemble de la chaine de blocs pour la rendre de nouveau valide.
Afin d'empêcher cela, le mécanisme du « *Proof of Work* » empêche la création de nouveaux blocs, ainsi pour Bitcoin, cela prend 10 minutes pour ajouter un nouveau bloc à la chaine.
En raison de son caractère distribué, chaque utilisateur, chaque nœud reçoit une copie du registre, puis lorsqu'un nouveau bloc est créé il est envoyé à chaque nœud, qui le vérifie et l'ajoute ensuite à sa chaine de blocs, ceux qui sont altérés sont rejetés car ils n'ont pas requis le consensus de la majorité du réseau. Pour altérer la blockchain, la modifier il faut donc modifier chaque bloc, procéder de nouveau à la preuve de travail et prendre contrôle de plus de 51% du réseau distribué. Cela est donc peu vraisemblable.

Pour illustrer le fonctionnement de la blockchain, il conviendra de prendre pour exemple son cas d'usage le plus emblématique, Bitcoin. Les informations nécessaires sont donc : qui donne, quoi, à qui ?



Ainsi, si A souhaite donner deux bitcoins à B : la transaction entre les utilisateurs est d'abord regroupée dans un bloc. Pour vérifier que A détient bien les deux bitcoins qu'il prétend transférer à B, une vérification est opérée par les utilisateurs du réseau (les *mineurs*), qui remonteront la chaîne de blocs et l'historique des transactions de A pour vérifier que les deux bitcoins qu'il a reçu antérieurement n'ont pas été réutilisés. Ce mécanisme de vérification est appelé *Unspent Transaction Output* (UXTO) pour transaction non dépensée. Bitcoin résoud donc le problème de la double dépense.

Le bloc est donc vérifié, selon une technique cryptographique qui dépend du type de blockchain, la plus commune étant la Proof-of-Work (preuve de travail). Une fois le consensus distribué entre les nœuds du réseau atteint, le bloc est validé. Il est ensuite horodaté et ajouté à la chaîne de bloc, B reçoit désormais les deux bitcoins. Il sera considéré propriétaire de ces bitcoins s'il dispose de la clé privée permettant de les dépenser.
Les mineurs, pour avoir effectué ce travail de validation sont rétribués, en bitcoins, cela constitue l'incitation économique de sécurisation du réseau. La transaction aura pris un certain temps, une dizaine de minutes pour Bitcoin, 15 secondes pour la blockchain Ethereum, cette durée étant prévue dans le code source du protocole.

8.- **Distinction**. L'on distingue en la matière les blockchains publiques (comme c'est le cas de Bitcoin) et les blockchain privées.

Les blockchains publiques sont apparues les premières, leurs registres sont accessibles à tout un chacun, qui peut envoyer des transactions et participer au processus d'approbation, la règle de la majorité s'impose.

Les blockchains dites de *consortium* sont d'un type hybride, le processus d'approbation est contrôlé par un nombre restreint et choisi de nœuds. Le nombre de participant est donc limité et sélectionné et ce n'est plus la règle de la majorité qui s'impose.

Les blockchains privées, quant à elles, sont contrôlées par un unique acteur.

9.- Médiatisation et enjeu de compétitivité. Paris a accueilli les 16 et 17 avril 2019 le *Blockchain Week Summit*, au cours duquel le Ministre de l'Economie et des Finances, Bruno Le Maire a déclaré que « *le développement de l'écosystème blockchain est une priorité pour le Gouvernement* », affirmant avoir recensé plus de 200 projets blockchain en France et confirmant la place ambitieuse que comptait prendre la France[17]. La blockchain trouverait en effet des cas d'usages dans de nombreux secteurs[18] : banque, finance, assurance ; énergie ; santé ; luxe… Le juriste a par exemple connaissance du dispositif d'enregistrement électronique partagé (DEEP) pour la représentation et la transmission des titres financiers qui ne sont pas admis aux opérations d'un dépositaire central de titres.[19]

10.- Enjeux du mémoire. Bruno Le Maire résumait parfaitement le dilemme, le point de tension entre innovation et protection : « *Nous ne devons pas entraver l'innovation car ces nouvelles technologies sont susceptibles d'apporter demain des services nouveaux, plus efficaces et plus adaptés aux consommateurs. Mais nous ne devons pas non plus nous montrer*

---

[17] « Bruno Le Maire : ''Le développement de l'écosystème blockchain est une priorité pour le Gouvernement'' », Gregory Raymond, Capital, 15 avril 2019.

[18] « *Les mystères de la blockchain »,* M. Mekki, D. 2017, p.2160

[19] Ordonnance n°2017-1624 du 8 décembre 2017

naïfs vis-à-vis des risques associés à l'usage de cette technologie complexe et des crypto-actifs ».[20]

La présente contribution se propose d'abord de revenir en profondeur sur les notions en cause afin d'en cerner précisément tant la nature que le fonctionnement et la portée, préalable indispensable à l'analyse. L'analyse, quant à elle consistera à s'interroger, en toute humilité et le plus sincèrement possible. Il importera d'exposer la distinction centrale entre les infractions commises sur la technologie nouvelle elle-même et les infractions plus classiques, commises au moyen de la technologie, voire même simplement liées à celle-ci et sans nouveauté ni complexité spécifique, conformément à la définition rappelée de la cybercriminalité. La présente contribution, au croisement des disciplines, du droit, notamment des affaires, du droit pénal, mais également de la cybersécurité s'efforcera de mettre fin à une confusion répandue en démontrant que les crypto-actifs sont des non-sujets d'infractions, en ce sens qu'ils ne sont pas, en soi, intrinsèquement, délictueux, mais servent des buts légitimes et ne sont liées que de manière contingente tantôt comme objet, tantôt comme support, à des infractions. Au travers des développements, l'on s'interrogera sur le devenir de cette cybercriminalité spécifiquement liée aux crypto-actifs (crypto-criminalité) en prenant en compte l'impact de la réglementation récente issue de la loi Pacte, ainsi que l'indispensable dépassement de la nécessaire et classique répression pénale - consacrant au demeurant désormais, dans une certaine mesure, une forme de crypto-criminalité - qui passera par des moyens nouveaux de lutte, une sensibilisation accrue et une coopération étendue des acteurs, tant publics que privés, l'autorégulation étant une force vive en cette matière.

[20] « Bruno Le Maire : ''Le développement de l'écosystème blockchain est une priorité pour le à'' », Gregory Raymond, Capital, 15 avril 2019.

TITRE 1 : LES CRYPTO-ACTIFS : (NON)-SUJETS D'INFRACTIONS

Les crypto-actifs en eux-mêmes sont-ils fondamentalement constitutifs d'infractions ?

L'objet du Titre 1 sera d'envisager les crypto-actifs comme potentiels sujets d'infractions, à la manière d'une enquête, en examinant les reproches qui peuvent leur être le plus pertinemment adressés. Le lecteur sera amené à s'interroger sur leur nature intrinsèque, leurs variantes, ainsi que leur fonctionnement afin de déterminer si les crypto-actifs sont fondamentalement constitutifs d'infractions.

Un chapitre premier, sera consacré aux cryptomonnaies, tandis qu'un second chapitre sera consacré aux financements en crypto-actifs.

Chapitre 1: Les cryptomonnaies ou « monnaies virtuelles »

S'agissant d'abord des cryptomonnaies, dont l'on préférera la dénomination à celle de « monnaies virtuelles » utilisée pour décrédibiliser leurs fondements, il conviendra d'abord de s'interroger sur leur qualité même de monnaie (section 1) avant d'adresser les reproches qui leurs sont le plus couramment adressés ayant trait à leur(s) vulnérabilité(s) intrinsèque(s) (section 2).

Section 1 : Les cryptomonnaies, fausses monnaies ?

Si l'une des premières interrogations s'agissant des cryptomonnaies a précisément porté sur leur évenuelle nature de monnaie véritable, et, certes plus rarement le cas échéant, leur caractère de « fausse monnaie » (§1), leurs connexions avec la sphère de l'économie dite, elle, « réelle » suscite des questionnement ayant trait à la stabilité financière (§2).

§1. Caractère délictueux des cryptomonnaies : le délit de fausse monnaie

L'une des premières infractions que l'on pourrait imputer aux cryptomonnaies, faisant d'elles une forme, en soi, de cybercriminalité est le délit de fausse monnaie.

Si certaines, notamment le bitcoin, viennent sérieusement concurrencer les monnaies traditionnelles (A), elles ne forment pas un ensemble monolithique et des cryptomonnaies alternatives (*altcoins*) méritant davantage le qualificatif de fausse monnaie se livrent une concurrence entre elles (B).

A – Les monnaies traditionnelles face au bitcoin

11.- Phénomène monétaire. L'apparition de la monnaie fait encore à l'heure actuelle l'objet de débats académiques, qui, bien que passionnants intéressent peu le juriste. Il ne sera donc pas question de revenir sur la question de la non-coincidence des besoins et les origines du troc. L'existence de la monnaie sera prise pour acquise. Les formes de la monnaie, en revanche, attireront l'attention. L'on distingue traditionnellement trois formes de monnaies : fiduciaire, scripturale et électronique. La monnaie fiduciaire (*fides*, la confiance) est la monnaie corporelle (billets et pièces). La monnaie scripturale désigne les écritures dans les livres de compte des établissements de crédit. La monnaie électronique fait l'objet d'une définition légale, il s'agit d'une « *valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne pysique ou morale autre que l'émetteur de monnaie électronique* ».[21] Il importe donc d'emblée de distinguer la monnaie électronique, telle qu'ainsi définie, des cryptomonnaies.

12.- Notion de monnaie. La monnaie, telle que définie par Aristote, est classiquement définie de manière fonctionnelle en ce qu'elle remplit trois buts : unité de compte, réserve de valeur et intermédiaire des échanges.

Unité de compte. C'est-à-dire la capacité de mesurer la valeur des flux et stocks de biens, de services ou d'actifs.

Réserve de valeur. C'est-à-dire la capacité de transférer du pouvoir d'achat dans le temps et qui est réduite par l'inflation.

Intermédiaire des échanges. C'est-à-dire la capacité d'éteindre les obligations, l'on parle de pouvoir libératoire de la monnaie.

13.- Création monétaire et souveraineté. « *Montrez-moi la monnaie de l'impôt (…) rendez à César ce qui appartient à César, et à Dieu ce qui appartient à Dieu* » répondit Jésus aux pharisiens qui lui demandaient s'il était conforme à la loi de payer les impôts romains[22].

---

[21] Art. L.315-1 du Code monétaire et financier

[22] Mc 12,13-17 ; Mt 22,15-22 ; Lc 20,20-26

Les liens entre la souveraineté, exprimée par la perception de l'impôt et la monnaie ne sont pas nouveaux. Les Etats se sont progressivement arrogés le monopole de l'émission des billets et des pièces et exercent un contrôle sur la création monétaire par les banques commerciales afin de défendre ce monopole.

14.- Cours forcé. Désigné également par le terme d'inconvertibilité, le cours forcé supprime le droit de pouvoir exiger l'échange de papier-monnaie contre du métal précieux, comme l'or. C'est donc l'Etat, qui par son autorité proclame l'inconvertibilité, qui va de paire avec le cours légal, condition nécessaire de son acceptabilité.

15.- Cours légal. L'article L.111-1 du Code monétaire et financier dispose que « *la monnaie de la France est l'euro* », l'article R642-3 du Code pénal en assure l'effectivité en prescrivant : « *Le fait de refuser de recevoir des pièces de monnaie ou des billets de banque ayant cours légal en France selon la valeur pour laquelle ils ont cours est puni de l'amende prévue pour les contraventions de la 2e classe.* »

Une monnaie ayant cours légal ne peut être refusée en règlement d'une dette : tout créancier ou commerçant a le devoir de l'accepter. C'est le pouvoir libératoire universel de la monnaie.[23]

16.- Arsenal pénal protecteur. L'article L.442-1 du Code pénal protège ce monopole et dispose que : « *La contrefaçon ou la falsification des pièces de monnaie ou des billets de banque ayant cours légal en France ou émis par les institutions étrangères ou internationales habilitées à cette fin est punie de trente ans de réclusion criminelle et de 450 000 euros d'amende.* »

Il est à mettre en paralèle de l'article qui le suit immédiatement et qui élargit le champ d'application de l'infraction : « *Le transport, la mise en circulation ou la détention en vue de la mise en circulation des signes monétaires contrefaisants ou falsifiés mentionnés au premier alinéa de l'article 442-1 ou des signes monétaires irrégulièrement fabriqués mentionnés au deuxième alinéa de cet article sont punis de dix ans d'emprisonnement et de 150 000 euros d'amende*. » (art. 442-2 C. pén.).

---

[23] « La monnaie », Banque de France, Publications, 17 décembre 2018

Même la monnaie n'ayant plus cours légal est protégée de la contrefaçon et de la falsification, avec une peine deux fois moins importante (art. 442-3 C. pén.). Si ces incriminations ne portent que très peu, s'agissant des cryptomonnaies, puisque leurs éléments matériels ne visent que « les pièces de monnaie ou billets de banque ayant cours légal en France », or on ne peut pas sérieusement soutenir qu'une cryptomonnaie comme le bitcoin soit une falsification ou contrefaçon d'une pièce ou d'un billet de banque, en dépit des représentations illustratives - souvent journalistiques - du bitcoin.

En revanche, une disposition porte davantage, il s'agit de l'article 442-4 du Code pénal qui dispose que : « *La mise en circulation de tout signe monétaire non autorisé ayant pour objet de remplacer les pièces de monnaie ou les billets de banque ayant cours légal en France est punie de cinq ans d'emprisonnement et de 75 000 euros d'amende.* ». Selon nous, cette incrimination est parfaitement applicable aux cryptomonnaies, telles que le bitcoin. La mise en circulation pourrait être effectuée par le procédé du minage, l'objet de « remplacer les pièces de monnaie ou les billets de banque ayant cours légal » est en théorie rempli, il s'agit en tout les cas de l'objet de Bitcoin, présenté comme un système de paiement de pair à pair. A notre connaissance, aucune application de ce texte n'a été faite, selon certains avis, cela proviendrait du fait que le texte vise les « signes monétaires » ce qui ferait référence à une monnaie physique et non dématérialisée. La réponse se trouverait peut être dans la mention « non autorisé », a contrario les cryptomonnaies seraient donc autorisées ? Selon nous, même si l'article était en théorie applicable, il est en pratique impossible d'interdire les cryptomonnaies.

Ces incriminations se retrouvent d'ailleurs dans le Livre IV intitulé : « des crimes et délits contre la nation, l'Etat et la paix publique » au sein d'un titre IV intitulé : « des atteintes à la confiance publique ».

La confiance joue un rôle indispensable dans l'adoption et la pérennité d'une monnaie. La confiance du public dans la monnaie est fondamentale, la Banque de France y veille, notamment en « proposant des technologies d'émission des billets les plus sécurisées possibles afin d'empêcher la contrefaçon »[24].

[24] « La monnaie », Banque de France, Publications, 17 décembre 2018

17.- Valeur intrinsèque de la monnaie. A l'origine, la monnaie était matériellement représentée par des métaux précieux, comme l'or, connus pour leur solidité, transportabilité, rareté, ce qui constitue leur valeur. Puis il a été question, de corréler d'une façon ou d'une autre les monnaies aux métaux précieux et particulièrement à l'or.

Depuis 1971 le système étalon-or établi par les accords de Bretton Woods (1944) ne vaut plus, c'est la fin de la convertibilité du dollar en or, les monnaies nationales n'ont dès lors plus de réel sous-jacent, de valeur intrinsèque. L'on peut même avancer qu'elles ne reposent sur rien à part la contrainte (cours « forcé »), et depuis 2008 la confiance dans les instiutions, notamment les banques centrales et les politiques monétaires se dégrade.[25]

La dématérialisation diminue d'autant la valeur intrinsèque de la monnaie et la confiance des agents économiques, elle ne représente que des chiffres sur des comptes, immatériels, impalpables. L'on parle ainsi de monnaie-*fiat* pour désigner une monnaie fiduciaire contrôlée par les états et émise par une Banque Centrale, comme l'Euro ou le Dollar. *Fiat,* en latin « qu'il soit fait » relevant quasiment de l'acceptation divine de l'autorité, sans plus de justification.

18.- Bitcoin est-il une monnaie? En 1984, Friedrich Hayek, économiste et philosophe, Prix Nobel d'économie en 1974 pour ses travaux sur la théorie de la monnaie déclarait : *« je ne crois pas au retour d'une monnaie saine tant que nous n'aurons pas retiré la monnaie des mains de l'État ; nous ne pouvons pas le faire violemment ; tout ce que nous pouvons faire, c'est, par quelque moyen indirect et rusé, introduire quelque chose qu'il ne peut pas stopper. »* [26]

D'un point de vue fonctionnel, économique, le bitcoin répond aux trois fonctions assignées à la monnaies : unité de compte c'est à dire un étalon, un instrument de mesure de la valeur ; un instrument d'échange, en ce qu'il est disponible à tous, sans frais, c'est un actif liquide, qui est de plus en plus accepté (plus de 100 000 sites internet dans le monde) [27] ; enfin et c'est comme on le verra sa fonction la plus connue, réserve de valeur, c'est à dire la capacité à transférer du pouvoir d'achat, l'on peut utiliser le bitcoin immédiatement ou bien le

---

[25] Bitcoin, totem & tabou, que présage l'essor des cryptomonnaies ? Rapport de l'Institut Sapiens, Février 2018.

[26] Bitcoin, totem & tabou, que présage l'essor des cryptomonnaies ? Rapport de l'Institut Sapiens, Février 2018.

[27] Le site useBitcoins.info recense les endroits acceptant le bitcoin.

thésauriser et l'utiliser dans le futur (bien que la volatilité au moins partiellement causé par spéculation peut aller en sens inverse).

En revanche, d'un point de vue juridique, le bitcoin n'a pas cours légal en France, l'on ne peut obliger un créancier à le recevoir comme mode de paiement, bitcoin n'est donc pas une monnaie (absence de pouvoir libératoire universel). On le considérera donc comme un bien meuble incorporel, ce que l'analyse fiscale a confirmé.[28]

20.- Origines de Bitcoin. Le premier bitcoin a été créé le 3 janvier 2009, Bitcoin a donc récemment fêté ses dix ans. Bitcoin est né dans un contexte très particulier, à savoir une crise financière mondiale sans précédent comparable depuis 1929. A cet instant, la confiance envers des entreprises perçues comme les plus solides (ex. Lehman Brothers) ainsi que celle de l'ensemble du système financier est remise en question. Une défiance s'installe à l'égard des banques et de la finance et ses excès. Le rôle même des gouvernements et des banques centrales est en question.

Satoshi Nakamoto[29] a inséré, dans le premier bloc de la blockchain Bitcoin, un message faisant référence à un nouveau sauvetage des banques par l'État : le titre d'un article du *Times* daté du jour " *Chancellor on brink of second bailout for banks* ". L'objectif de ce message était avant tout de prouver que la blockchain Bitcoin avait véritablement démarrée le 3 janvier 2009, mais la concordance de la naissance de cette technologie avec la crise financière a souvent servi d'explication sur l'idéologie portée par Bitcoin.[30] Jusqu'ici, la monnaie a nécessité un intermédiaire, un tiers de confiance, une banque centrale, pour garantir que la monnaie émise est véritable et une banque commerciale pour vérifier le solde disponible des opérateurs et ainsi maintenir la confiance. Bitcoin se présente comme une alternative aux monnaies nationales en ce qu'il est un moyen de transférer directement de la valeur, par le réseau Bitcoin (pair à pair), en se passant d'intermédiaire-tiers de confiance.

---

[28] Conseil d'Etat, 8ème et 3ème chambres réunies, 26 avril 2018, N°417809

[29] Auteur du livre blanc (white paper) *Bitcoin : A Peer-to-Peer Electronic Cash System* https://bitcoin.org/bitcoin.pdf

[30] Bitcoin, totem & tabou, Que présage l'essor des cryptomonnaies ? Rapport de l'Institut Sapiens, Février 2018.

Il constitue un moyen d'échanger librement de la valeur, à faible coût, de manière anonyme (ou à tous le moins pseudonyme)[31] et sécurisée. C'est une véritable révolution et l'auteur doit bien admettre que chaque fois qu'il s'y penche une nouvelle fois depuis la première fois en 2011, il connaît le même étonnement. La genèse de Bitcoin et des crypto-monnaies subséquentes est à rechercher à la croisée de diverses disciplines, courants idéologiques et mêmes de certaines personnalités qui ont façonné la réalité qu'il nous est donné d'observer aujourd'hui.

21.- Cypherpunks. La contribution la plus importante à la création de Bitcoin provient asurément du mouvement *cypherpunk*. Dans les années 1990, l'apparition de l'internet grand public attire des passionnés, des hackers au sens noble du terme[32] qui, sensibles aux considérations relatives à la vie privée (et l'on sait l'importance que ces questions ont désormais prise) s'initient la cryptographie. L'idéologie cypherpunk, sans vouloir la dénaturer, apparaît comme fondamentalement soucieuse de la liberté individuelle et de la vie privée, s'opposant à toute forme de contrôle, ce qui passe, entre autre par le chiffrement des communications et l'échange de monnaie, sans contrôle ni censure[33]. L'anonymat ou à tous le moins la pseudonymisation en ligne apparaît au fondement de la démocratie et de l'exercice des autres libertés[34]. Il faut avoir à l'esprit que Bitcoin est davantage un aboutissement qu'une découverte fulgurante et soudaine, il est le fruit de plus d'une quinzaine d'années de travaux divers, de littérature et d'échanges entre des communautés (la liste de diffusion cypherpunk et les forums notamment).

Nick Szabo, juriste et informaticien est une personne clée dans l'émergence de Bitcoin. Il a pour sa part travaillé sur Bit gold[35], qu'il fait ressurgir en 2005. Bit Gold, est un projet de monnaie numérique décentralisée dont le fonctionnement est extrêmement proche de Bitcoin, mais qui n'a pas réussi à résoudre parfaitement le classique problème de la *double dépense.* [36]

---

[31] Par nature, Bitcoin est fondée sur une blockchain publique, transparente, les adresses ainsi que l'émetteur, le montant et le destinataire sont connus, néanmoins, il faut encore passer de l'adresse à l'identité de son détenteur.

[32] *The Hacker Manifesto*, Phrack http://phrack.org/issues/7/3.html

[33] Eric Hugues, *A Cypherpunk's Manifesto*, https://www.activism.net/cypherpunk/manifesto.html

[34] Voir en ce sens les débats récents à propos d'un projet de loi de lutte contre la haine sur internet, une proposition de loi a finalement été déposée le 20 mars 2019 .

[35] Pour le *white-paper*, v. https://nakamotoinstitute.org/bit-gold/

[36] Bitcoin, totem & tabou, que présage l'essor des cryptomonnaies ? Rapport de l'Institut Sapiens, Février 2018. **Double dépense** :Si un utilisateur essaie de dépenser ses bitcoins auprès de deux destinataires

Hal Finney, Adam Back (Hashcash) Wei Dai (b-money[37]) sont des personnalités ayant travaillé de leur côté et ayant développé leur propre système.

Bitcoin, dont le *white-paper*, comportant seulement neuf pages, et daté du 31 octobre 2008, reprend à son compte ces technologies pour les faire fonctionner ensemble. Il faut bien avoir à l'esprit que ces technologies se sont succédées en s'inspirant souvent l'une de l'autre, leurs concepteurs ayant à l'esprit la même littérature.

22.- Satoshi Nakamoto. L'auteur de ce document demeure toujours inconnu, des recherches, notamment récentes, poussées par la médiatisation dont le bitcoin a fait l'objet n'ont pas abouties, certaines personnes proclamant être Satoshi[38], d'autres, perçues comme les personnalités les plus susceptible d'être Nakamoto, le réfutant farouchement.

Il pourrait s'agir selon toute vraisemblance d'un groupe de personnes plutôt que d'un individu. Une certitude est que Satoshi Nakamoto, a confirmé s'être retiré du projet en mai 2011, période qui coincide avec une réunion à laquelle la *Central Intelligence Agency* (CIA) américaine a convié les porteurs du projet, il confie alors la succession du projet à Gavin Andresen. Il est clair que Nakamoto a pris soin de dissimuler son identité, fidèle à l'idée qui fonde le projet à savoir l'absence d'organe central ou de « gourou » auquel se rattacher et de dogmes sur les orientations stratégiques que devraient prendre Bitcoin.

L'absence de contrôle, une gouvernance fondée sur le consensus, l'absence de censure, de restriction ou d'embargo, c'est en cela que Bitcoin représente idéal anarcho-capitaliste.

23.- Prouesse technique indéniable. Bitcoin est une cryptomonnaie, mais également et avant tout un protocole, un système de paiement, pair à pair (*peer-to-peer*) utilisant la cryptographie, un registre distribué, la blockchain, fonctionnant par un système de consensus où les utilisateurs du réseau (les nœuds) participent à sa gestion (vérification des transaction, validation ou rejet et actualisation) et y sont incités en étant rétribués en bitcoins pour avoir apporté leur puissance de calcul, supprimant ainsi le besoin de confiance en une tierce partie.

---

différents au même moment, l'on parle de double dépense, la blockchain et la preuve de travail des mineurs permettent de l'éviter et créer un consensus pour décider laquelle sera rejetée et validée.

[37] https://nakamotoinstitute.org/b-money/

[38] Craig Wright, un entrepreneur australien, sur lequel nous reviendrons, prétend notamment l'être et mène des actions en justice pour que ses allégations soient reconnues, n'hésitant pas à menacer les personnes qui le contredisent publiquement, notamment sur les réseaux sociaux comme ce fut le cas sur Twitter le 11 avril 2019. Wright a alors offert 5000 dollars à la personne qui fournirait des informations personnelles sur @hodlonaut, s'attirant les critiques de la majorité de la communauté crypto.

Cette incitation est l'équivalent du processus de création monétaire puisque c'est de cette façon que les bitcoins sont créés.

Bitcoin est du point de vue pratique un logiciel pour ordinateur ou une appli mobile, qui fournit à l'utisateur un portefeuille permettant d'envoyer et recevoir des bitcoins. Ce logiciel est Bitcoin Core[39], un logiciel dit libre (*open source*) sous la licence MIT, son code source est librement consultable et téléchargeable et modifiable [40] les nombreux audits dont il a pu faire l'objet témoignent de sa sécurité. Comme nous l'avons précédemment exposé, le caractère distribué du registre constitue l'identité intrinsèque de Bitcoin et des autres cryptomonnaies et est un point esentiel à sa sécurité. En effet, contrairement à un système centralisé, par exemple une banque, le registre distribué est moins vulnérable aux attaques, à la fraude, à la suppression pure et simple provoquée par une attaque informatique ou une erreur.

24.- Quelques chiffres sur le Bitcoin. Le nombre maximal de bitcoins pouvant être émis est déterminé *a priori*, ce nombre est fixé à 21 millions, ce qui pourrait s'avérer dirimant pour une utilisation massive. Néanmoins, chaque bitcoin est divisable en cent millions d'unités appelées satoshi. Au 15 avril 2019, 17 647 625 bitcoins étaient en circulation, représentant une capitalisation de $ 90 265 028 263, ce jour là plus de 156 000 bitcoins se sont échangés, la blockchain de Bitcoin pesait plus de 212 GO.[41]

25.- Anonymat. Si le bitcoin est souvent présenté dans la presse généraliste comme une source d'opacité, d'anonymat et est associé à des activités criminelles, il est pourtant fondamentalement transparent puisque chaque transaction y est enregistrée de manière permanente. Cette contribution se propose, on le rappelle, de distinguer autant que faire se peut, à la manière cartésienne, afin d'éviter la confusion. Il est vrai que Bitcoin permet l'anonymat, ou plutôt le pseudonymat, en effet chaque utilisateur du réseau est identifié par une adresse, qui a l'apparence suivante : 3FkenCiXpSLqD8L79intRNXUgjRoH9sjXa[42]

Néanmoins, il est possible de connaitre, en analysant le registre, l'historique de chaque bitcoin, et ainsi de savoir quel montant a transité par quelles adresses, à quel moment

[39] https://bitcoin.org/fr/telecharger
[40] https://github.com/bitcoin/bitcoin
[41] https://bitcoin.fr/divers-graphiques-sur-bitcoin/
[42] Cette adresse est celle de Bitcoin.org

26.-L'évangélisation de Bitcoin. Bitcoin s'est propagé, d'abord dans le petit monde des cryptographes, développeurs, hackers, puis dans le monde plus large de la *tech* et des business angels de la silicon-valley (dont les désormais célèbres frères Winklevoss), ce qui créa une première communauté *d'early-adopters* et un effet de réseau mais Bitcoin demeura encore assez confidentiel. L'on assiste dans un second temps à l'émergence des premiers *exchanges* c'est à dire de plateforme d'achat et vente de cryptomonnaies, et au premier chef, de bitcoins. Nécessaires à la démocratisation, ces plateformes vont pourtant à l'encontre du fondement même de Bitcoin à savoir la décentralisation.

La popularité et l'usage grandissant de Bitcoin est à mettre en parallèle avec la création puis l'accès du grand public aux réseaux informatiques décentralisés, dont le plus connu est Tor (*The onion router*), un logiciel initialement développé dans les années 1990 par et pour l'amée américaine, désormais libre et s'inscrivant dans la même volonté que Bitcoin : protéger la vie privée en ligne, éviter le contrôle et la censure. Puisque décentralisé et permettant un traçage si ce n'est impossible au moins plus difficile, des sites internet proposant des biens ou services illicites se sont développés : drogues, armes, monnaie contrefaite, service de tueurs à gage, cartes bancaires volées… ces *black markets* sont désormais connu du grand public et feront l'objet de plus amples développements *infra*.

De véritables places de marché ont vu le jour, dont le plus populaire historiquement est Silk Road (littéralement, route de la soie, en référence au réseau de routes commerciales) mettant en relation acheteurs et vendeurs, principalement de produits stupéfiants. Les relations entre cryptomonnaies et en premier lieu le bitcoin sont indéniables : Silk Road n'acceptait que cette cryptomonnaie comme mode de paiement (la Section 1, du Chapitre 2 du Titre 2 précisera ces liens). Néanmoins il apparaît d'ores et déjà opportun de relever l'importance qu'ont joué Bitcoin et Silk Road dans l'histoire de leurs développement respectifs. Tor, combiné avec Bitcoin et Silk Road réalise l'utopie libertaire. Il faut souligner que la version originelle de Silk Road, telle que fondée par Ross Ulbricht (« Dread Pirate Roberts ») fut fermée par le FBI en octobre 2013, pour autant, chacun perçoit le destin que Bitcoin a connu jusqu'à présent. C'est donc que le destin de Bitcoin n'est pas (entièrement) consubstantiel aux activités menées sur le *dark web*, il est également, au moins en partie, autre chose. En France, l'écosystème s'est également développé pour devenir une industrie, d'abord autour d'une comunauté, et l'on doit beaucoup, s'agissant de la perception de Bitcoin, à des acteurs privés, notamment la Maison du Bitcoin, devenue CoinHouse qui promeut le développement de ces

technologies, par l'éducation sur la blockchain et les crypto-actifs, ainsi que la prévention et fournit certains services de conseil.

27.- Avantages et inconvénients du bitcoin par rapport aux monnaies fiat[43].

Avantages	Inconvénients
• **Paiement sans limite de montant, de frontière, à faible coût et dans un temps réduit, à tout moment**	• **Faible acceptation et utilisation comme moyen de paiement, l'effet de réseau est toujours en cours**
• **Irréversibilité des transactions, accroît la sécurité juridique pour les échanges**	• **Irréversibilité des transactions est dommageable en cas de vol**
• **Valeur refuge face à des monnaies subissant une hyperinflation en raison des politiques monétaires nationales**	• **Volatilité : car déflationniste et flottante**
• **Transparence transactionnelle et neutralité en raison du caractère décentralisé**	• **Taille de la blockchain importante, technologie énergivore en raison de la puissance de calcul**

[43] **https://bitcoin.org/fr/faq#quels-sont-les-avantages-du-bitcoin**

B- Concurence des cryptomonnaies, les *altcoins*.

D'une certaine façon, toutes les cryptomonnaies sont des monnaies alternatives en soi puisqu'elles n'ont pas cours légal. Les *altcoins* (*alternative coins*) désignent toutes les cryptomonnaies alternatives, distinctes du bitcoin, postérieures à celui-ci et plus ou moins conçues à partir de son protocole (Bitcoin). Bitcoin domine néanmoins le marché avec plus de 55%. Il existerait plus de 2100 cryptomonnaies, représentant une capitalisation d'environ 180 milliards de dollars[44].

Parmi les altcoins plus connues, nous porterons notre attention sur Ethereum (ETH), Ripple (XRP), EOS (EOS), Monero (XMR) et ZCash (ZEC).

28.- Ethereum. Ethereum a été créé en 2013 par Vitalik Buterin[45]. Ethereum désigne le protocole (de même que Bitcoin), tandis que la cryptomonnaie *stricto sensu* est l'Ether (comme le bitcoin), la plus petite unité de cette cryptomonnaie étant le gwei (comme le satoshi). Ethereum est, de manière simple, comparable à un ordinateur mondial décentralisé, une plateforme basée sur une blockchain (Ethereum Virtual Machine) permettant de déployer des applications décentralisées (DApps, i.e. *decentralized applications*) sa fonction initiale n'est donc pas de transférer de la valeur comme Bitcoin mais de faire fonctionner des programmes. L'on reviendra plus en détail sur Ethereum puisqu'elle a été créé en se financant par le moyen d'une *Initial Coin Offering* (ICO) et a fait l'objet d'une scission suite à une attaque impliquant un important volume de cryptomonnaies (*hard fork*) entre Ethereum (ETH) et Ethereum Classic (ETC).

Si Bitcoin représente la première génération de cryptomonnaies, Ethereum est présenté comme la deuxième génération du genre, apportant l'innovation majeure que constituent les contrats dits intelligents (*smart contracts*)[46] et permettant donc de créer des applications décentralisées sur la blockchain, exécutant des smart contracts et d'y implémenter une cryptomonnaie *ad hoc* à partir du jeton ERC 20.

---

[44] Selon coinmarketcap.com, au 1er juin 2019.
[45] v. le *whte-paper* **https://github.com/ethereum**

[46] Lesquels n'intéressent que de façon marginale la présente contribution mais soulèvent des questions intéressantes pour le juriste, v. en ce sens M. Mekki, « *Blockchain : l'exemple des smart contracts entre innovation et précaution* ».

29.- EOS. Lancée le 14 juin 2018, EOS représente la troisième génération de cryptomonnaies, fondée sur les bases d'Ethereum, elle a également été financée via une ICO, la plus massive à l'heure actuelle en ce qu'elle équivaut à environ 4 milliards de dollars[47].
Il est assez remarquable que les projets successifs prennent appui sur les précédents, ce qui est permis par leur caractère libre (*open source*) et la culture de l'écosystème. L'ICO a ainsi été financée en ether, EOS étant par ailleurs fondée sur les bases d'Ethereum et permettant également la création d'applications décentralisées, de manière concurrente à Ethereum[48].

	Ethereum	**Ripple**	**EOS**	**Monero**	**Zcash**
Classement (selon la capitalisation)	2ème	3ème	6ème	12ème	23ème
Capitalisation (en milliards $)	18,39	13,87	4,96	1,1	0,44
Spécificité	Smart contracts	Utilisé par les institutions bancaires ; transactions plus rapides ; protocole de PoC (et non PoW ou PoS)	Transactions plus rapides et gratuites	Anonymat (montant, émetteur, destinataire)	Anonymat (montant, émetteur, destinataire) Protocole ZK-Snarks et zero-knowledge

Tableau non exhaustif de quelques une des principales altcoins

[47] « Investors Bet $4 Billion on a Cryptocurrency Startup », P. Vigna, The Wall Street Journal, 29 mai 2018
[48] « EOS, la blockchain qui veut remplacer Ethereum », C. Perreau, Le Journal du Net, 4 mars 2019

30.- Variabilité des altcoins. Les *altcoins* sont donc moins populaires, moin diffusées, il est notable que les cryptomonnaies les plus anonymes ne constituent pas la majorité du marché, contrairement à l'idée selon laquelle les cryptomonnaies favorisent l'opacité. Les *altcoins*, moins populaires, sont ainsi moins sécurisées, puisque la sécurité du réseau décentralisé repose sur les nœuds du réseau, et sont plus facilement manipulable. Elles ont par conséquent un cours ainsi qu'une capitalisation moindre et bénéficient d'une acceptation et d'une liquidité moins développée que le bitcoin, ainsi l'on peut davantage s'interroger sur leur capacité à remplir les fonctions traditionnelles de la monnaie.

En outre, la question de leur valeur intrinsèque se pose avec plus d'acuité encore. En effet, contrairement aux principales altcoins précitées, apportant une innovation et répondant à un véritable besoin, ou résolvant un véritable problème, la plupart des altcoins ne sont que des dérivés du bitcoin et présentent une plus-value quasi inexistante.

31.- Interdiction des cryptomonnaies. Les cryptomonnaies ont dans un premier temps fait l'objet d'une volonté d'interdiction par certains Etats, pour des raisons diverses. La Russie avait déclaré Bitcoin illicite et pénalisé son utilisation[49]. L'Inde irait également en ce sens, une proposition de loi prévoit d'en interdire l'utilisation, elle prohiberait également l'activité des plateformes d'échange sur son territoire. La Chine a interdit les plateformes d'échange de cryptomonnaies et envisage depuis très récemment d'interdire l'activité de minage de cryptomonnaies, pour des motifs qui tiendrait à la réduction de la pollution. Comme le relève un auteur[50], l'interdiction s'avère vaine, au mieux l'utilisation peut être déclarée illégale mais la mise en œuvre de cette interdiction se heurterait frontalement à la décentralisation au fondement même des cryptomonnaies. La meilleure attitude semble donc être celle de la régulation, qui passe par la réglementation.

---

[49] « *Russifna authorities say Bitcoin illegal* », G. Baczynska, Reuters, 9 février 2014.

[50] « *Le Bitcoin devient monnaie courante : les monnaies digitales entre transparence, régulation et innovation* », V. Charpiat, Revue des Juriste de Sciences Po, 2014, n°9 p.49.

32.- Régulation des cryptomonnaies et rôle des plateformes d'échange. Si la qualification juridique des cryptomonnaies fait encore l'objet de débats, l'activité des plateformes d'échanges s'analyse, dans un premier mouvement, en un service de paiement, par suite soumis à l'obtention d'un agrément de prestataire de service de paiement de l'Autorité de contrôle prudentiel et de résolution (ACPR)[51]. La cour d'appel de Paris l'affirme dans un arrêt du 26 septembre 2013[52], l'ACPR faisant sienne l'analyse dans une note du 29 janvier 2014.
En droit positif, depuis l'entrée en vigueur de la loi PACTE, les cryptomonnaies sont incluses dans la notion plus large d'actifs numériques et les plateformes d'échange ont désormais le statut de prestataire de service sur actifs numériques (PSAN), comme il sera exposé *infra*. ils sont par suite soumis à certaines obligations, afin de procéder à leur enregistrement obligatoire ou à leur agrément optionnel, puis dans le cadre de leur activité, notamment le respect des normes LCB/FT.

[51] Art. L.522-6 C.mon. fin. ; le fait d'exercer cette activité sans l'agrément étant passible de trois ans d'emprisonnemen et 375 000 euros d'amende (L.572-5 C.mon.fin.)
[52] « *Fintech et droit pénal : une répression entre régulation et dématérialisation* », N. Catelan, revue de droit bancaire et financier, janvier-février 2017.

§2. Risque du mélange entre sphère crypto et sphère traditionnelle « réelle »

La nature des cryptomonnaies et l'absence de position sur leur qualification juridique entretien la confusion, le mélange des genre avec la sphère traditionnelle

33.- Confusion. Le mélange des genres entre monnaies *fiat* et cryptomonnaies est à ce point recherché que des distributeurs, analogues aux distributeurs automatiques de billets (DAB) et suscitant la même convoitise (haine ?)[53] apparaissent pour convertir ses euros en bitcoins, y compris en France, des frais étant appliqués et des plafonds fixés.[54]
L'analogie avec le système bancaire ne s'arrête pas là puisque, outre les portefeuilles, (*wallets*) s'agissant désormais des moyens de paiement, c'est une véritable carte, comparable à une carte bancaire traditionnelle qui a vu le jour, via un partenariat entre Coinbase et un acteur majeur du marché,Visa[55] permettant de dépenser sa cryptomonnaie aussi facilement que de la monnaie scripturale *fiat* et d'effectuer des retraits d'espèces aux DAB. Ce partenariat promet d'accélérer l'acceptation des cryptomonnaies d'une manière inédite, de par le réseau de commerçant dont dispose Visa, ainsi que son infrastructure et sa sécurité.
Il est par ailleurs possible d'acheter des bitcoins auprès de buralistes[56], ce qui participe d'une démocratisation plus ou moins souhaitable et répondant d'abord à une curiosité éphémère et à satisfaire à moindre coût.[57]

---

[53] « *Stolen Bitcoin ATM Owners Suspect Memphis Robbery Was Inside Job* », P.H. Madore, CCN.com, 7 mars 2019

[54] « *Un distributeur de bitcoins à Montpellier* », Bitcoin.fr, 11 août 2016. L'article, mis à jour au 17 avril 2019 affirme désormais que le distributeur n'existe plus.

[55] « *Visa et Coinbase lancent une carte adossée à des cryptomonnaies* », L. Mearian (adaptation J. Elyan), Le Monde Informatique, 18 avril 2019.

[56] Service proposé par la société KeplerK. https://keplerk.com
[57] Pour un test, v. le client ne sachant pas ce qu'est un bitcoin, ni ne comprenant le fonctionnement de la blockchain, le buraliste se trouvant pris au dépourvu et avouant n'être qu'un intermédiaire : « *J'ai acheté des Bitcoins dans un tabac et je ne sais toujours pas à quoi ça sert* », D.-J. Rahmil, L'ADN, 22 janvier 2019.

34.-Les Etats. Les Etats, dont on a montré que l'intervention est proscrite par l'idée même des cryptomonnaies, et dont certains les ont interdites, songent désormais à créer leur propre cryptomonnaie, entre annonces : Tunisie, Turquie[58], Estonie, Emirats Arabes Unis et mise en application : Iles Marshall[59] et Venezuela[60], notamment qui est le premier à lancer sa cryptomonnaie, le petro, ancré sur le cours du pétrole, (dont le Venezuela est richement doté) sur lequel est adossé le nouveau bolivar, avec pour objectif de contourner les sanctions financières internationales et de pallier l'hyperinflation subie par le bolivar.

Une réflexion suggère que la France pourrait envisager une cryptomonnaie d'Etat, Messieurs les députés Woerth et Person l'évoquant dans leur rapport d'information sur les monnaies virtuelles[61]. Cette cryptomonnaie, qui prendrait la forme d'un *stable coin*, n'aurait pas les risques liés à la volatilité et pourrait notamment « *jouer un grand rôle dans le financement de l'innovation* » mais surtout créer un lien plus direct entre les déposants et la banque centrale, redonnant un impact plus direct à la politique monétaire [62](les politiques monétaires actuelles, dénoncées, étant à l'origine des cryptomonnaies et de Bitcoin en 2008). La boucle serait bouclée. La Banque Centrale de Suède et celle d'Angleterre [63] y réfléchissent. Néanmoins, un consensus se dégage pour affirmer qu'un tel projet est loin d'être prêt, pour des questions aussi bien techniques que juridiques. La volonté serait donc davantage géopolitique que technologique[64]. L'Iran pourrait également s'engager dans cette voie, ainsi que la Russie et la Chine[65].

---

[58] « *Turkcoin : Turkish Politician Endorses Launching a National Cryptocurrency* », S. Das, CCN.com, 23 février 2018.

[59] « *Marshall Islands to issue own sovereign cryptocurrency* », G. Chavez-Dreyfuss, Reuters.com, 28 février 2018.

[60] « *Le Venezuela dévalue sa monnaie de 96%* », Le Monde avec AFP, 21 août 2018.

[61] Rapport d'information en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles, M. Eric WOERTH, Président et M. Pierre PERSON, Rapporteur, 30 janvier 2019

[62] « *Et si la France lançais sa crypto-monnaie d'Etat* ? », J. Lausson, Numerama, 2 février 2019

[63] « *UK Central Bank Mulls Cryptocurrency Linked To Pounds Sterling* », S. Sundararajan, Coindesk, 2 janvier 2018

[64] « *Les crypto-monnaie d'Etat, une arme géopolitique* ? », V. Castro, Usbek & Rica, 4 juin 2018.

[65] « *An Inside Look At China's Government Controlled Cryptocurrency Project* », L. Coleman, CCN.com, 31 mars 2018 ; « *La première crypto-monnaie étatique sera-t-elle chinoise* ? » V. Lucchese, Usbek & Rica, 27 juin 2017.

Bien que ces sujets soient éloignés de la démonstration principale de la présente contribution, l'on pense qu'il est important de remarquer cette tendance, ce curieux détournement des cryptomonnaies, originellement et profondément anti-étatiste, anarcho-capitaliste et libertaire par des Etats historiquement opposés à l'économie de marché et la propriété privée et connus pour la surveillance, la censure et les atteintes aux libertés les plus fondamentales. Cela est peut être le signe d'un nouvel ordre financier, parallèle à la domination du dollars.

35.-*Stable coin*. Une autre des immixtions entre la sphère crypto et la sphère de l'économie réelleest celle réalisée par le *stable coin*. Présenté comme une solution au problème de la volatilité des cryptomonnaies, les *stable coins* sont des cryptomonnaies (*coins*) adossés à des monnaies *fiat* (euro, dollar[66]), le pétrole[67] ou encore l'or

36.- Les entreprises traditionnelles. La banque d'affaires JPMorgan, première au monde en terme de capitalisation boursière a finalement joué le rôle de pionnier et lancé sa propre cryptomonnaie, le JPM Coin basé sur une blockchain privée. [68] Il s'agit plus spécifiquement d'un *stable coin*, indexé sur le dollars, qui permettra le transfert instantanné de fonds entre clients dits *corporate* c'est à dire isntitutionnels de la banque (paiements, transferts, opérations boursières). En pratique, le client de la banque dépose des fonds sur un compte spécifique et reçoit leur équivalent en JPM Coin, qui seront utilisés pour des transactions entre clients et pourront être convertit de nouveau en dollars, avec une parité de un pour un.

37.- Facebook Coin : brouille la frontière entre entreprise et Etat. Facebook, la société du réseau social éponyme, lancée en 2004 compte aujourd'hui plus de 2 milliards de membres actifs et possède d'autres réseaux sociaux tels Instagram (rachetée pour 1 milliard de dollars) ou encore WhatsApp (rachetée pour 19 milliards de dollars). Désormais cotée sur le Nasdaq, elle a une capitalisation d'approximativement 500 milliards de dollars (l'équivalent du PIB d'un Etat comme l'Argentine ou l'Autriche). Il a été annoncé en février 2019[69] que Facebook

---

[66] C'est ce que prétend la cryptomonnaie Tether (USDT), bien que sa capacité à pouvoir supporter la convertibilité de tous les USDT en dollar américain avec une parité de 1 :1 demeure incertaine et que la société ne garantirait contractuellement pas le rachat. La plateforme aurait ensuite affirmé que la cryptomonnaie est en fait adossée à plusieurs supports (autres devises, créances, prêts émis par la société) mais que les adossements sont parfaitement garantis. On reviendra sur ce sujet *infra*.

[67] C'est ce que prétend la cryptomonnaie Bilur

[68] « *JP Morgan est la première banque à lancer sa cryptomonnaie* », R. Bloch, Les Echos, 14 février 2019.

[69] « *Facebook and Telegram Are Hoping to Succeed Where Bitcoin Failed* », N. Popper et M. Isaac, The New York Times, 28 février 2019.

projette de lancer une cryptomonnaie, le Facebook Coin[70], au cours de l'année 2019, avec pour objectif de permetre aux 2,7 millliards de membres de s'échanger des fonds instantannément partout dans le monde. Le Facebook Coin serait un *stable coin*, déployé sur une blockchain qui selon toute vraisemblance serait privée (dite de consortium)[71]. Il serait d'abord déployé pour les utilisateurs de WhatsApp, adossé à un panier de cinq devises différentes, ce qui assurerait sa stabilité, sa neutralité ainsi qu'une relative indépendance vis à vis du Gouvernement des Etats-Unis. L'un de ses concurrents chinois, WeChat a lui pris l'exact contrepieds, en interdisant l'usage de cryptomonnaies sur sa plateforme.[72]

Ce projet suscite de vives réactions de la « communauté crypto » en ce qu'elle va à l'encontre de la décentralisation, au cœur de la philosophie, de la confiance et de la sécurité originelle, ainsi si Facebook garde la majorité du contrôle, l'intérêt est moindre. Facebook, en nombre d'utilisateurs équivaut à la Chine et à l'Inde réunies, les orientations stratégiques étant d'ailleurs au regroupement des plateformes Facebook, WhatsApp et Instagram[73]. Facebook rivalise par sa taille et ses moyens financiers aux Etats, par ailleurs, l'on sait que son fondateur Mark Zuckerberg est pressenti pour être candidat à la prochaine élection présidentielle américaine. « *Facebook aurait ainsi les moyens de devenir une sorte de banque centrale privée* », relèvent Clément Jeanneau et Alexandre Stachtchenko, co-fondateurs de Blockchain Partner, ce qui devrait justement être l'occasion pour les banques centrales de s'interroger sur les cryptomonnaies.

Cet attrait des Etats, des grandes entreprises et spécifiquement des banques et banques centrales, confirme d'abord que les cryptomonnaies ne relèvent pas en soi de la cybercriminalité et conduit néanmoins à s'interroger sur les risques de ces immixtions sur la stabilité financière.

---

[70] Initialement dénommé de la sorte par les commentateur, la cryptomonnaie prendrait finalement le nom de GlobalCoin, ce qui confirme les ambitions de Facebook à cet égard.
[71] « *Les questions étourdissantes que soulève le FacebookCoin* », C. Jeanneau et A. Stachtchenko, Blockchain Partner, 6 mars 2019.
[72] « *WeChat interdit les transactions en cryptomonnaies* », Journal du Coin, 8 mai 2019.
[73] « *Zuckerberg confirme la fusion des messageries Facebook, WhatsApp et Instagram* », JournalduGeek, 1er février 2019.

38.-La stabilité financière. Mario Draghi, le Président de la Banque centrale européenne, a récemment affirmé, lors d'une séance de questions-réponses, que le bitcoin ou les cryptomonnaies ne sont pas des monnaies, ce sont des actifs spéculatifs qui bien que très risqués ne représentent pas une menace au niveau macroéconomique, pour la stabilité financière, ce sujet relève à son avis davantage de la protection des consommateurs que de la Banque centrale européenne[74].

En outre les liens entre les crypto-actifs et le monde financiers restent encore limités. Néanmoins, un sujet très discuté, les produits dérivés sur cryptomonnaies, notamment bitcoins, pourrait remettre en cause cette analyse. Si la question des ETF (*Exchange Traded Fund*) fait l'objet d'hésitations, la *Securities and Exchange Commission* (SEC) ayant plusieurs fois repoussé des décisions à ce sujet, des *futures* existent d'ores et déjà, proposés notamment par le *Chicago Mercantile Exchange* (CME). Les volumes d'échange deviennent important, la seule journée du 13 mai 2019, plus de 33 000 contrats ont été vendus pour un montant de 1,15 milliard d'euros. Ce serait plus de 50 milliards de valeur notionnelle et 1,6 million de contrats négociés (équivalent de 8 millions de bitcoin) qui auraient été échangés depuis décembre 2017[75]. La possibilité d'être exposé aux cryptomonnaies, connaissant une forte volatilité, pour des montants importants pourrait, on le pense, constituer une menace pour la stabilité financière[76], outre les manipulations de cours que l'on exposera *infra*. La communauté Bitcoin est partagée s'agissant de ces produits dérivés, certains estimant que l'institutionnalisation est favorable à une diffusion plus large et une adoption des cryptomonnaies, d'autres estiment pour leur part que l'intérêt de Bitcoin est la détention en direct et l'absence de confiance dans une entité pour les conserver et les gérer[77].

Une autre immixtion des cryptomonnaies dans la sphère financière classique est la possibilité désormais pour les assurer de proposer des contrats d'assurance-vie exposés aux cryptomonnaies, via des fonds professionnels spécialisés[78].

---

74 v. également « *Virtual currencied and central banks monetary policy: challenges ahead* », ECON, Monetary Dialogue, juillet 2018 qui arrive au même constat.
75 « *CME Group Bitcoin Futures Hit $1.3 Billion Amid Parabolic Advance* », W. Suberg, CoinTelegraph, 14 mai 2019.
76 V. pour une étude détaillée « *Bitcoin Futures: From Self-Certification To Systemic Risk* », L. Reiners
77 « *Bitcoin et les ETF : un mariage de raison* ? » D. Fay-Manzo, Coin house Insights, 26 octobre 2018.
78 « *Le bitcoin a désormais sa place dans les contrats d'assurance-vie* », R. Bloch, Les Echos, 11 avril 2019.

Section 2 : Les cryptomonnaies, fondamentalement vulnérables ?

Il convient désormais d'examiner si les cryptomonnaies, le bitcoin pris comme référence, en tant qu'investissement n'est pas intrinsèquement vulnérable d'un point de vue financier (A) représentant consécutivement une potentielle fraude cybercriminelle, et s'il ne présente pas des vulnérabilités techniques, le rendant vulnérable à de telles attaques cybercriminelles (B).

§1. Une vulnérabilité financière

Il s'agira d'examiner si d'une part, Bitcoin est intrinsèquement assimilable à un système de Ponzi (A) et dans la négative, s'il représente une bulle spéculative car dépourvu de toute valeur intrinsèque (B).

A- Bitcoin et système de Ponzi

39.- Notion de système de Ponzi. Un tel schéma, aussi dénommé Pyramide de Ponzi (après Charles Ponzi, l'un des premiers instigateurs de ce type de fraude) est une opération d'investissement frauduleuse, qui consiste à recevoir des fonds de la part du public, pour en apparence l'investir, à ceci près que les fonds ne sont investis dans aucun actif. Les dépôts des investisseurs constituent la seule source de rémunération des nouveaux entrants dans le système. Lorsque les dépôts deviennent insuffisants face aux retraits, la pyramide s'effondre, au détriment surtout des derniers entrants. Pour exemple, la fraude mise en place par B. Madoff constituerait le plus important système de Ponzi (65 milliards de dollars américains), découvert par un analyste financier en 2005[79] il a été révélé par la crise de 2008. Il serait caucasse que la crise ait révélé un système de Ponzi pour contribuer à créer son successeur.
Bitcoin ne promet aucun retour sur investissement, il est à l'origine envisagé comme un système de paiement de pair-à- pair (*a peer to peer cash system*) et une monnaie. De plus, étant décentralisé, aucune autorité centrale ou entité spécifique ne pourrait faire de telles représentations frauduleuses de retour sur investissement ou profiter directement du profit de cette fraude.

---

[79] « *The World's Largest Hedge Fund is a Fraud* », 7 novembre 2005
http://static.reuters.com/resources/media/editorial/20090127/Markopolos_Memo_SEC.pdf

En revanche, il convient, à notre sens légitimement, de s'interroger sur la rétribution particulièrement élevée des premiers utilisateurs (*early adopters*) du protocole Bitcoin, à une époque où le minage nécessitait une puissance de calcul moindre. Des utilisateurs ont alors pu amasser une quantité massive de cryptomonnaie, avec des équipements grands public tandis qu'aujourd'hui le matériel est plus coûteux, plus énergivore et moins accessible. Il est vrai que le bitcoin est créé par le *mining*, néanmoins cette création monétaire étant de plus en plus difficile, le marché (achat/vente) sur les *exchanges* s'est développé et l'on pourrait d'une certaine façon dire que les nouveaux entrants du protocole Bitcoin, ou à tous le moins utilisateurs/possesseurs de bitcoins - étant donné qu'ils ne sont pas forcés d'en miner pour en acquérir – le payant à un prix élevé, rémunèrent les premiers entrants, les *early adopters*, qui n'auraient pas acheté directement leurs bitcoins mais les auraient produits à un coût moindre, réalisant une plus-value conséquente. Satoshi Nakamoto, créateur encore inconnu du Bitcoin, détiendrait selon certaines rumeurs plus d'un million de bitcoins[80].

La question est peu posée, et n'est qu'une humble réflexion, mais d'une part, l'on ne saurait affirmer que Bitcoin est, en soi, un système de Ponzi, l'investissement, si l'on peut le désigner ainsi, n'est pas fait envers une entité unique ou une personne mais un réseau/un marché, qui ne promet aucun investissement, sauf à prendre en compte l'espérance de l'acheteur dans une stratégie de spéculation, qui n'est a priori pas la fonction initialement envisagée de Bitcoin, et qui au demeurant, pourrait s'avérer rentable. L'on reviendra plus en avant sur la question des fondamentaux, de la valeur intrinsèque de Bitcoin, pour s'interroger sur son éventuel nature de système de Ponzi, en ce que l'investissement ne serait déployé sur aucun actif.

L'on ne saurait ainsi raisonnablement imputer au/aux créateur(s) de Bitcoin l'intention collective et peu louable d'avoir créé cette technologie à des fins de fraude et miné massivement en contribuant au développement de Bitcoin pour les revendre ensuite, réalisant une plus-value, et faisant chuter le cours voire empêchant par manque de liquidité, les nouveaux entrants de sortir du système.

---

[80] Selon un des développeurs du projet, il serait en réalité peu probable que ce soit le cas, il aurait pu ne pas en miner autant à ce moment, les avoir vendu ou perdu. La rumeur serait fondée sur le postulat que tout les bitcoins miné pendant la première année d'existence et non dépensés l'auraient été par Satoshi, ce qui peut ne pas être le cas : « Does Satoshi have 1 million BTC ? Core Dev explains why we cannot know », R. Allen, Chepicap, 13 mars 2019.
L'adresse ayant reçue la première transaction (Genesis block) détient 67 000 bitcoins environ (1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa), qui n'est pas celle de Satoshi.

De plus, une telle opération pourrait ne pas apparaître des plus profitable en considérant le fait que Bitcoin n'a que dix ans et que sa valeur a énormément fluctuée sur cette courte période, elle pourrait croître encore.

Il convient de rappeler que Bitcoin étant fondé sur la décentralisation, les nœuds (*nodes*) du réseau sont d'une importance capitale pour le bon fonctionnement et la sécurité de ce dernier. En cela, l'on peut estimer qu'en prenant des risques, en investissant du temps, des ressources et de l'espoir dans une technologie naissante, ces derniers méritent une rétribution en conséquence. Enfin, le fait que certains utilisateurs précoces aient dépensés des quantités importantes de bitcoins en échange de biens peu coûteux en équivalent monnaie fiat[81] peut révèler l'absence d'intention ab initio de thésauriser du bitcoin et de réaliser une plus value.
L'économiste Kaushk Basu a étudié les mécanismes derrière les systèmes de Ponzi. L'auteur distingue les Ponzi intentionnels (*deliberate*) dans lesquels les investisseurs sont invités à prendre part (avec un retour sur investissement promis), et les Ponzis non-intentionnels (*natural occuring Ponzis*) (expresson de Robert Shiller) sans créateur, simplement en ayant la les espérances des investisseurs se nourissant entre elles, les systèmes de Ponzi sont alors assimilables à des bulles financières. [82]

Dans un phénomène de bulle financière, les investisseurs acquièrent l'actif sans connaître ses fondamentaux, sa valeur intrinsèque, seulement car ils espèrent que d'autres feront de même, faisant monter le cours en spéculant, créant une sorte de cercle vicieux de prophétie autoréalisatrice.

Bitcoin ne serait donc pas un Ponzi intentionnel, ce qui semble le plus raionnable, comme montré *supra*, mais un Ponzi non-intentionnel ou naturel, assimilable à une bulle financière. Il faut admettre que même ce type de Ponzi non intentionnel, dont Bitoin relèverait, peuvent faire l'objet de manipulation (que nous étudierons *infra*) notamment de « *pump and dump* » qui est plus probable encore sur les *altcoins*.

---

[81] Le 22 mai 2010, 10 000 bitcoins étaient dépensés pour acheter des pizzas coûtant environ 25 dollars.

[82] Ponzis, The Science and Mystique of a Class of Financial Frauds, Kaushik Basu, Policy Research Working Paper, WPS6967, World Bank Group, Development Economic Vice Presidency, Office of the Chief Economit, July 2014

On ne pense pourtant pas que Bitcoin constitue fondamentalement une bulle spéculative, l'on croit comprendre que l'auteur juge la cause du mal au moment où les utilisateurs de Bitcoin ne l'ont plus vu comme système de paiement, et ont spéculé sur le fait que sa valeur pourrait monter :
« *One can buy Bitcoin the way one can buy euros and trade freely with others having euros.Trouble started when people began speculating that the value of Bitcoin would rise, thereby raising the demand for Bitcoin and making the value-rise a self-fulfilling prophesy* ».

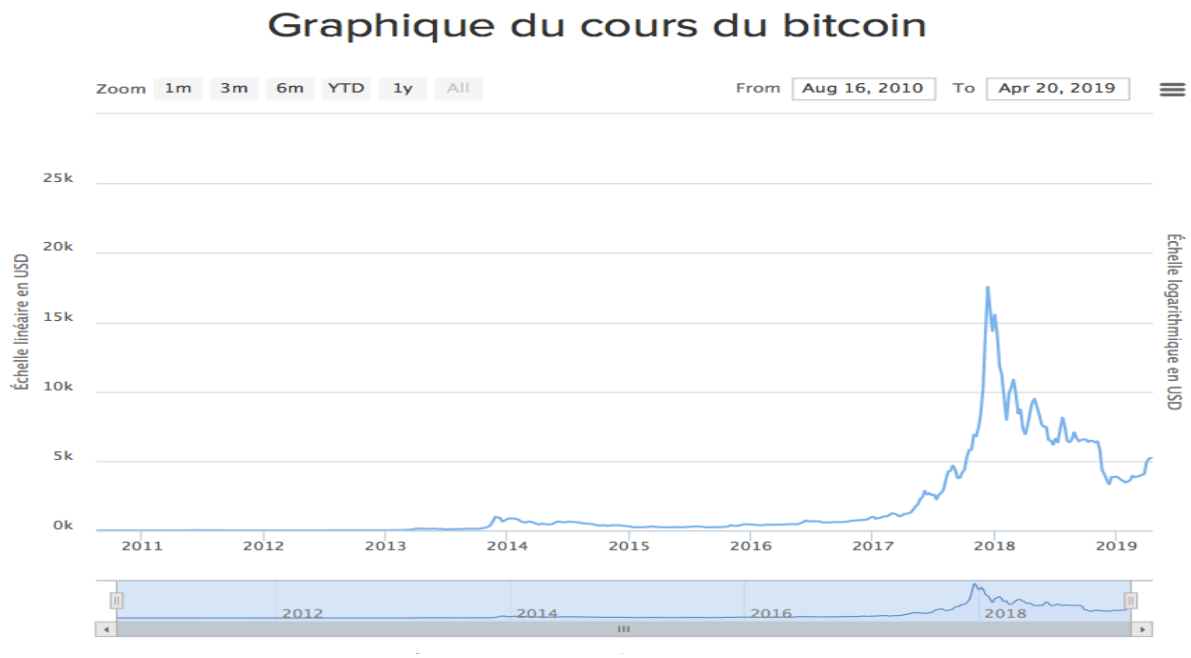
Néanmoins, les monnaies fiats sont elles aussi l'objet d'un marché, le marché des devises et sont aussi l'objet de spéculation voire d'hyperinflation et l'on ne parle pas de bulle spéculative pour autant. La spéculation n'est d'ailleurs pas un mal en soi, il a même été démontré qu'elle est nécessaire pour l'économie.

L'auteur admet, et l'on s'accordera avec lui, pour constater que l'essentiel de la valeur sur laquelle repose Bitcoin sont les leçons données aux banques centrales, et ce serait déjà beaucoup : « *The main value of Bitcoin may, in retrospect, turn out to be the lessons it offers to central banks on the prospects of electronic currency, and on how to enhance efficiency and cut transactions cost.* »

Bitcoin n'est donc pas en soi un Ponzi, il convient d'examiner en quoi Bitcoin n'est peut être pas même une bulle spéculative, en adressant la question de sa valeur intrinsèque.

B- Bitcoin : une hypothétique bulle spéculative

40.- Evolution du cours du bitcoin.



Le 17 décembre 2017, le bitoin atteint les 19 800 dollars.[83] Le 7 janvier 2018, les cryptomonnaies auraient atteint une capitalisation cumulée de 800 milliards de dollars. [84]

41.- Fixation du cours. Le prix du Bitcoin (et des autres crypto-actifs) est déterminé par confrontation de l'offre et de la demande. Les plateformes d'échange, formant le marché, reçoivent des ordres à l'achat et à la vente, répertoriés dans le carnet d'ordres. Le cours technique du crypto-actif correspondant en définitive au prix de la dernière transaction[85].
Néanmoins, il existe plusieurs dizaines de plateformes distinctes, avec leurs carnets d'ordres respectifs. L'on risquerait alors d'avoir plusieurs cours sur différentes plateformes, ce qui serait non transparent, non égalitaire, par conséquent peu souhaitable voire dangereux.

---

[83] « *17 décembre 2017 : le jour où… le bitcoin a flirté avec les 20 000 dollars* », B. Eschapasse, Le Point, 4 janvier 2018
[84] « *Comment est fixé le prix du Bitcoin* ? », J. Moretto, Coin House Insights, 13 décembre 2018.
[85] Ces facteurs dits techniques, pris en compte par le marché seraient seuls responsables de certaines variations importantes du cours, dont l'une des plus remarquable récemment, un « cap psychologique » des 4200 dollars ayant été franchi. « *Bitcoin : l'unique raison qui explique l'explosion des cours* », G. Raymond, Capital, 2 avril 2019. Au 27 mai 2019, le bitcoin a atteint les $ 8900 ayant donc doublé son cours en moins de 2 mois pour atteindre son plus haut depuis un an. L'avenir dira si ce cours est raisonnable.

Ce problème est résolu par la spéculation de certains investisseurs (arbitrages) plaçant des ordres d'achat sur une plateforme où le cours est bas et des ordres à la vente sur une plateforme d'échange où le cours est plus élevé. Les cours des différentes plateformes sont rééquilibrés par les mécanismes de marché et ces investisseurs rétribués, en ce sens la spéculation apparaît, dans cette mesure, indispensable.

42.- Bitcoin, bulle spéculative. Dennis Gartman, gourou de Wall Street spécialisé en *commodities* (matières premières) "*This is a market ... for criminals, this is a market for millennials (...) "There's no question blockchain has merit. It's going to change the manner in which we trade. It's going to change the manner in which we invest*[86]" **Warren Buffet**, le célèbre milliardaire, surnommé l'Oracle d'Omaha et dont la stratégie d'investissement remarquable, respectable et respectée, dans la valeur, a fait sa réputation, qualifie le bitcoin de « fantasme » et estime que "*You can't value bitcoin because it's not a value-producing asset*.[87] " **Paul Donovan**, Chief Economist des services financiers de la banque UBS compare Bitcoin à la tulipomanie de 1637, et estime qu'il est fondamentalement défectueux , vicié (*fatally flawed*)[88]. Gary Shilling, célèbre analyste financier qualifie le Bitcoin de « *black box* » dénonçant son manque de transparence et le comparant à la bulle des mers du Sud de 1720. [89]**Jamie Dimon**, le PDG de la banque JPMorgan avait dans un premier temps qualifié le bitcoin de « fraude » estimant qu'en acheter est « stupide » et qu'il licencierait un trader s'il en achetait.[90]

43.- Notion de bulle spéculative. Le cours, le prix d'un actif se fixe par la confrontation de l'offre et de la demande. S'agissant d'actifs plus traditionnels, tels des actions de sociétés, l'analyse financière est déterminante pour connaître les « fondamentaux » qui constituent la valeur dite intrinsèque d'une société. La valorisation de sociétés est une discipline complexe et il est utopique de vouloir la déterminer avec exactitude, néanmoins, plusieurs méthodes existent et leur combinaison permet d'approcher une valeur intrinsèque.

---

[86] « *Bitcoin is a market for criminals and millennials, Dennis Gartman says* », C. Aiello, CNBC, 13 novembre 2017

[87] « *Billionaire Warren Buffett Remains Clueless About Bitcoin, Calls It 'Delusiona*l' », B.Brown, CCN.com, 25 février 2019

[88] « *UBS Executive Paul Donovan Blasts Bitcoin Again, States Cryptos Are 'Fatally Flawed'* », W.Suberg, CoinTelegraph, 30 novembre 2018

[89] « *Gary Shilling : Bitcoin is a black-box* », Business Insider, 4 janvier 2019

[90] « *Jamie Dimon, le patron de JPMorgan, qualifie le bitcoin de "fraude"* », Les Echos, 12 septembre 2017.

Les difficultés proviennent d'un décalage entre la valeur réelle de l'actif en question et sa valeur de marché, autrement dit entre la valeur et le prix. « *Price is what you pay, value is what you get* » aurait résumé le remarquable Warren Buffett.

La spéculation est un pari sur l'évolution du prix d'un produit, elle peut toucher tout actif, peut contribuer à ce décalage et former une « bulle spéculative », une situation où le prix est surévalué comparé à la valeur. L'augmentation du cours est alors artificielle puisque essentiellement fondée sur les croyances des acheteurs que le prix sera « plus élevé demain » (prophétie auto-réalisatrice), parfois même en sachant le décalage entre le prix et la valeur de l'actif (théorie dite du plus grand fou). La finance comportementale (application de la psychologie à la finance) entre alors en jeu, les comportements moutonniers, de mimétisme euphoriques collectifs contribuent à alimenter la bulle, avec la crainte (FoMO). De plus, une image de facilité à gagner de l'argent rapidement (envie), la diffusion par les médias d'histoires de nouveaux millionnaires voire milliardaires du bitcoin (admiration), ainsi que certainement pour une part non négligeable, l'égo (fierté), la perception de comprendre une technologie nouvelle, de voir une opportunité d'investissement à ne pas rater (crainte) que d'autres, moins vifs n'auraient pas même encore perçu ni *a fortiori* comprise. Ces comportements ne peuvent être niés.

L'on pense que seule une partie des investisseurs sont exclusivement des spéculateurs, et que ce phénomène n'a lieu qu'à certains moments, ce qui explique que bitcoin a connu plusieurs bulles. Cela va dans le sens que le bitcoin est en phase de « product market fit » dans un langage de l'entrepreneuriat, c'est à dire qu'il cherche son marché, sa valeur réelle, les précédentes bulles n'ont pas explosé plusieurs fois.

La spéculation est nécessaire au bon fonctionnement du système économique et contribue à la fixation du prix d'un actif, en plus de rémunérer une anticipation correcte de l'évolution du cours et une prise de risque. L'on peut espérer qu'à force de pic et de chute, le bitcoin se démocratise et que les investissements fondés uniquement sur la spéculation disparaissent d'eux mêmes, en parallèle d'un mouvement de compréhension de la technologie et de ses fondamentaux.

44.- Bitcoin, hypothétique et périodique bulle spéculative. Il convient tout d'abord de rappeler qu'une augmentation rapide du prix d'un actif, en l'espèce du bitcoin, ne constitue pas nécessairement une bulle spéculative. Comme exposé, la bulle apparaît lors d'une surévaluation artificielle d'un actif suivie d'une correction brutale (éclatement de la bulle). Le cours du bitcoin a pu varier au gré de la confiance accordée au protocole, d'annonces médiatiques, de régulation/interdiction, de piratages, de liens avec des activités criminelles (souvent présentées sous cet unique angle au demeurant) etc. L'on sera d'avis que le bitcoin a pu connaître des périodes où l'appât du gain et la « peur de rater quelque chose » (FoMO, *Fear of missing out*) en l'espèce la peur de rater une opportunité d'investissement en apparence très rentable, ont fait que la spéculation, dans ces périodes contribue à l'essentiel de la formation du prix de la cryptomonnaie et que ce qui pourrait constituer les fondamentaux de la valeur du bitcoin ait été négligé.

L'argument principal des ceux défendant la bulle est qu'originellement présenté comme une monnaie, il ne remplit que très imparfaitement son rôle à l'heure actuelle, il est alors inutile socialement et économiquement, sa seule utilité serait une espérance de gain

45.- Comparaison entre Bitcoin et des bulles spéculatives avérées. Bitcoin a souvent été assimilé à des bulles spéculatives historiques.[91] Il est alors d'usage de rechercher les points communs entre l'intérêt pour les tulipes au XVIIe siècle, l'espoir dans la Compagnie des mers du Sud, la ruée vers l'Internet au début des années 2000, l'immobilier en 2008 ou encore les terres rares dans les années 2010. Bitcoin est même présenté comme la « mère de toutes les bulles » en ce que contrairement aux autres, il serait possible qu'un jour le prix du bitcoin tombe à zéro. Il est en effet possible que la valeur des bitcoins puisse tendre vers zero, comme toute monnaie (récemment le Zimbabwe ou le Venezuela), cela est moins probable pour le bitcoin puisque le protocle protège de l'hyperinflation (en tant que monnaie) et la demande (en tant qu'actif), la détention, par les *whales* ou l'industrie crypto semblent pérennes.

L'on attirera l'attention sur ce curieux mode de raisonnement, et l'on pense pour notre part que l'énumération de ces bulles se suffit à elle même pour montrer que tant les actifs en cause que les mécanismes à l'origine de l'éclatement des bulles sont très distincts.

---

[91] « *Quelques bulles, de la tulipe au bitcoin* », S. de Rivet et L. Kortobi, Libération, 13 février 2019

Il faut se garder de généralisation hâtive et de comparaisons peu pertinentes. L'un des arguments majeur de la thèse d'une bulle sur le Bitcoin étant la multiplication de son prix, comparable à ces bulles (x20 ou x17 respectivement pour la tulipomanie et les actions de la Compagnie des mers du Sud)[92] ce seul exemple suffisant alors apparemment pour qualifier Bitcoin de bulle, sans plus de démontration. Selon nous cette comparaison est tout à fait contingente et à employer le même raisonnement, il suffirait de prendre un exemple, disons Amazon. Amazon est créée par Jeff Bezos en 1994, qui a déclaré qu'il aurait regretté ne pas avoir profité de la ruée vers l'or des débuts d'internet, tant le secteur était en croissance. Introduite en bourse en 1997, le chiffre d'affaire se monte alors à 148 millions de dollars, pour une perte de 30 millions[93], la rentabilité interroge, rappelons que la période coincide avec les débuts de l'internet grand public et l'accès à un ordinateur personnel. Nombre de facteurs aujourd'hui évident n'étaient absolument pas acquis. En 2000, ce qu'il est convenu d'appeler la bulle internet éclate, pourtant Amazon, qui aurait perdu 98% de sa valeur entre 2000 et 2002[94] demeure et évolue pour croître. En 2018, la société pèse 1000 milliards de dollars et emploie 613 000 personnes dans le monde[95]. Warren Buffett lui même, qui avait une opinion défavorable pour Amazon s'est ravisé et avoue s'être trompé et n'y prendra jamais part pour cette raison « *I've probably got so many psychological problems with the fact that I didn't do it that it's very hard to do it* »[96].

---

92 « *Bitcoin : la bulle qui ridiculise toutes les autres* ! », N. Gallant, Capital, 18 décembre 2017.
93 « *En vingt ans, le fabuleux destin boursier d'Amazon* », P.Bertrand, Les Echos, 16 mai 2017
94 « *La bulle du Bitcoin explose pour la 4ème fois (et ça n'est pas la pire)* », J. Guillaume, Presse-Citron.net, 28 novembre 2018
95 « *Amazon posts record profits again, but stock drops as revenue of $56.8B falls short of expectations* », N. Levy, GeekWire, 25 octobre 2018.
96 « *Warren Buffett says he 'blew it' when he didn't invest in Amazon early, and the regret is what keeps him from investing today* », J. Bort, Business Insider, 15 mai 2018
Durant la rédaction de ce mémoire, Warren Buffett a radicalement changé d'avis et pris la décision d'investir pour la première fois dans la société Amazon. Tout le monde peut faire des erreurs (et les reconnaître). Pourrait-il prendre la même décision s'agissant des crypot-actifs ? L'avenir le dira.
« *Warren Buffett entre dans Amazon et fait son mea culpa sur Google* », H. Rousseau, Le Figaro Economie, 5 mai 2019.

46.- La spéculation, contre-intuitivement bénéfique pour Bitcoin. « *Les bulles ne sont toxiques que si elles contaminent le système bancaire, ce qui n'est pas le cas avec les cryptomonnaies* »[97] résume Nicolas Colin.

En effet, les cryptomonnaies étant une alternative au système bancaire, elles ne peuvent a priori l'affecter (sous réserve des interconnexions croissantes entre ces deux sphères, notamment via les dérivés sur cryptomonnaies). L'auteur développe « (…) *bien sûr, en cas de succès, l'emballement attire les spéculateurs, qui accompagnent le mouvement de façon opportuniste sans éprouver d'intérêt pour le protocole lui-même. Mais leur irruption n'est pas inutile : ils contribuent à attirer l'attention de nouvelles générations d'utilisateurs*. »

Plus encore, Bitcoin pourrait être considéré comme entité « antifragile » au sens de N. N. TALEB, c'est à dire que paradoxalement, plus il est attaqué, plus il se renforce.[98] Ainsi, si les ruées vers le bitcoin le font connaître, ses chutes, aussi retentissantes soient-elles, participent également de ce mouvement.

Le rapport de l'Institut Sapiens développe un raisonnement a priori contre-intuitif à ce propos, qui mérite selon nous l'approbation. Les auteurs postulent que la hausse du cours du bitcoin (par exemple par la pure spéculation) entraine une augmentation des moyens consacrés à sa production (*mining*), qui devient plus rémunératrice, de nouveaux utilisateurs affluent alors, c'est une véritable course à la ruée vers l'or. Pourtant, le minage ne crée pas plus de bitcoin puisque le protocole prévoit cette production à un rythme fixe et décroissant, néanmoins, le nombre croissant d'utilisateurs, de mineurs (nœuds du réseau) entraînera une augmentation de la sécurité du réseau. La spéculation contribue donc paradoxalement pour le bitcoin à un cercle vertueux : plus son cours augmente, plus le minage est lucratif et les utilisateurs nombreux, plus la sécurité du réseau augmente, plus le bitcoin est attractif, plus la demande augmente, plus la valeur (intrinsèque) augmente.

---

[97] « *Cryptomonnaies : un peu de cohérence* », N. Colin, L'Obs, 27 janvier 2018
Cité dans Bitcoin, totem & tabou, que présage l'essor des cryptomonnaies ? Rapport de l'Institut Sapiens, Février 2018.
[98] *Ibid*.

47.- La valeur intrinsèque de Bitcoin. Bitcoin est présenté comme dépourvu de sous-jacent, néanmoins, comme relevé par certains auteurs, cette terminologie est impropre, le terme de « sous-jacent » étant spécifique aux produits dérivés, à partir duquel la valeur d'un contrat financier dérive. L'on préférera l'expression de « valeur sous-jacente au système Bitcoin ».[99]

Même ses détracteurs, qui soutiennent que Bitcoin est dépourvu de valeur intrinsèque, admettent (et c'est une opinion courante) que la technologie sous-jacente à Bitcoin, la blockchain, elle, est tout à fait valable et valorisable pour sa part. Ainsi, la blockchain constitue-t-elle l'essentiel si ce n'est l'exclusive valeur de Bitcoin ? On ne le pense pas, d'abord, comme nous l'avons rappelé, elle n'est que l'une des technologies de Bitcoin, elle n'est que le registre distribué. Pour certain, c'est surtout cette dernière qui fait l'objet d'une bulle, qui est surmédiatisée[100] et la plupart du temps pas indispensable aux problème qu'elle prétend résoudre. Bitcoin a contribué à populariser la blockchain et il se pourrait désormais que l'on se trompe s'agissant de la hiérarchie du principal et de l'accessoire.[101]

Comme l'expose ce pertinent article de CoinHouse[102] il faut d'abord faire preuve d'une certaine forme d'humilité pour remettre en question nos conceptions les plus élémentaires sur l'argent, la valeur, la propriété numérique et faire preuve de recul pour se projeter plus en avant dans un monde où l'internet devient la forme principale de communication, où comme on le verra, les *tokens* prendront une place croissante.

D'abord, objectivement, la valeur de Bitcoin provient de sa rareté, « ce qui est rare est cher », le protocole Bitcoin prévoit un nombre limité de bitcoins (21 millions), émis de manière prévisible et décroissante (*halving*) divisée par deux tous les quatre ans (50 bitcoins par blocs en 2009, 25 en 2013) l'idée étant de lui conférer une rareté intrinsèque[103]. Un parallèle est souvent fait entre Bitcoin et l'or, l'on parle en effet de minage, tous deux ne sont pas altérable

---

[99] Bitcoin, totem & tabou, que présage l'essor des cryptomonnaies ? Rapport de l'Institut Sapiens, Février 2018.

[100] « *La grande escroquerie de la blockchain* », N. Roubini, Les Echos, 30 octobre 2018.

[101] Ibid.

[102] « *Quelle est la vraie valeur du Bitcoin* ? », D. Fay-Manzo, Coin House Insights, 16 octobre 2018.

[103] « *Qu'est-ce qui empêche de dépasser les 21 millions de bitcoins* ? », J. Moretto, Coin House Insights, 26 octobre 2018.

et sont utilisés comme réserve de valeur, l'énergie nécessaire pour en créer est de plus en plus importante, donc la rareté augmente, leur valeur repose sur des mécanismes de marchés etc.

Ensuite, et toujours envisagé de manière objective, ce sont les nœuds, les utilisateurs, formant le réseau et assurant son bon fonctionnement (transfert de valeur équivalent à une monnaie, ce qui représente un service), sécurisé (immutabilité de la blockchain) et rétribué (donc incitatif et durable), fondé sur un système de gouvernane par consensus pour évoluer (donc stable).
Par ce réseau, c'est la confiance entre les utilisateurs, qui n'est plus nécessaire (confiance dans l'absence de confiance), et l'absence d'intermédiaire qui constituent le cœur de la valeur.
La valeur de Bitcoin est donc basée dans la technologie, dans le code informatique de son protocole et dans les mathématiques. Le fonctionnement de ce protocole nécessite par ailleurs comme on l'a montré une puissance de calcul importante, ce qui constitue au moins le minimum minimorum de valeur intrinsèque du bitcoin (la première cotation étant d'ailleurs faite sur la base exclusive de son coût en électricité).

Si Bitcoin est vu comme un actif dépourvu de valeur en ce qu'il manquerait pour l'essentiel à sa fonction originelle de monnaie, en raison du coût – de quelques centimes début 2017 à 55 dollars fin 2017[104] (aux plus hauts historiques) - de la lenteur, de l'acceptation.
La réponse est que la technologie est évolutive et des solutions sont en germes depuis un certain temps voire d'ores et déjà déployées. L'on peut présenter le lightning network[105] qui pallie le problème de l'engorgement du réseau Bitcoin et des frais de transaction et permettrait ainsi sa scalabilité (capacité à croître)[106].

C'est enfin un écosystème (entreprises de minage, plateforme d'échange, fabricant de *wallets*, cabinets de conseil) et une communauté humaine, dont l'on peut penser avec une assez grande certitude qu'elle est en bonne partie portée par des convictions philosophiques et sociétales authentiques, et une attitude à la conservation de principe du bitcoin[107] qui constituent ce qui

---

[104] « Lightning, la mise à jour du bitcoin qui pourrait tout changer », G. Raymond, Capital, 23 janvier 2018 ; « Introduction au Lightning Network », D. Fay-Manzo, Coin House Insights, 19 juin 2018

[105] v. le *white-paper* https://lightning.network/lightning-network-paper.pdf

[106] Bitcoin, totem & tabou, que présage l'essor des cryptomonnaies ? Rapport février 2018, Institut Sapiens

[107] Les détenteurs se dénomment « hodl », en référence au message « HOLD » (littéralement, détenir, tenir la position) pour signifier leur confiance

pourrait être le sous-jacent de Bitcoin.[108] Ainsi, c'est l'appréciation subjective par les agents économiques et les comparaisons qu'ils effectuent avec d'autres biens, voire d'autres monnaies, idéalement (comme le suggérait F. Hayek)[109] à ce titre, l'exemple du bolivar vénézuelien est topique.

En conclusion sur ce sujet, si dans l'opinion publique, le bitcoin – souvent alors qualifié de monnaie « virtuelle » - est présenté comme ayant traversé ou faisant l'objet d'une bulle spéculative, dépourvu de valeur intrinsèque[110], de sous-jacent, nous resterons pour notre part plus nuancé et nous garderons de toute affirmation, espérant avoir emporté la conviction de ce que la réalité est bien plus nuancée. Tout au plus pourrions nous constater qu'à certaines périodes, le bitcoin a fait l'objet de comportements spéculatifs, mais ils ne sont pas en soi dommageables et la « valeur réelle » de Bitcoin étant à notre sens en construction permanente, il est trop tôt pour se prononcer sur une surévaluation. En revanche, il faut admettre, et l'on y reviendra en détail, que certaines *Initial Coin Offerings* (ICO) et certains *altcoins* font l'objet d'une bulle, voire de véritables infractions. Mais les crypto-actifs, Bitcoin en tête, ne sont pas des sujets d'infraction.

48.- Perspectives. Bitcoin pourrait avoir une valeur encore plus élevée que celle atteinte à ses plus hauts historiques fin 2017. Bitcoin n'est peut être pas (encore) prêt pour le monde. Néanmoins, ses développements récents, dont l'un des plus prometteur est le Lightning Network qui permettra un nombre illimité de transactions par seconde sur le réseau, des transactions instantanées ainsi que des frais très faibles, ce qui pourra en faire le système de paiement originellement souhaité et par conséquent rendre incontestables ses fondamentaux. Le monde n'est peut être - également - pas (encore) prêt pour Bitcoin, son utilité en tant que monnaie est surtout pertinente, à l'heure actuelle dans les états connaissant une hyperinflation[111], ou bien dans les pays émergents où les travailleurs émigrés envoient de l'argent à leur famille par exemple (*remittances*).

---

[108] ibid.
[109] Pour une véritable concurrence entre les monnaies
[110] Pour se convaincre du contraire, une liste de 22 raisons pour penser le contraire : « *You Say Bitcoin Has No Intrinsic Value ? Twenty-two Reasons to Think Again*. », M. Rees, Bitcoin Magazine, 5 juillet 2014.
[111] « *Venezuela's Hyperinflation Sees Record Highs of Bitcoin Use* », R. Campbell, CCN.com, 10 août 2016.

§2. **Vulnérabilité technique**

49.- Sécurité de Bitcoin. Par vulnérabilité technique, il ne s'agira pas d'exposer les freins au développement de Bitcoin comme système de paiement (qui relèvent selon nous de sa valeur) et des évolutions technologiques. Il conviendra plutôt d'analyser la résilience de la technologie, en elle même, face aux attaques cybercriminelles. Si la valeur de Bitcoin repose, comme on a tenté de l'exposer, sur la sécurité du réseau et la confiance en ce dernier, justement car il permet l'absence d'intermédiaire de confiance, une vulnérabilité technologique remettrait l'intégralité du protocole en cause.

Il faut d'abord relever que par son caractère *open source*, Bitcoin et sa sécurité son auditable par tous, et a été audité à de nombreuses reprises en seulement dix ans. La technologie fonctionne toujours sur la base du même protocole et algorithme cryptographique, elle ne semble donc pas vulnérable. L'on peut lire ici et là que la technologie elle même n'a jamais été attaquée et que seuls les utilisateurs, par négligence, ont pu perdre leurs clés privées[112] , se voir pirater leurs *wallets*, liés ou non à des plateformes d'échange. Ceci est en grande partie exacte et l'on tient à le souligner, l'objet de la présente contribution reposant précisément sur cette distinction (attaque sur la techologie/au moyen de la technologie). Il importe donc bien de ne pas céder à cette confusion, la vulnérabilité n'est pas, dans bien des cas intrinsèque à la technologie Bitcoin, mais contingente à tel utilisateur, tel comportement ou telle attaque d'une plateforme d'échange.

Néanmoins, afin d'être plus nuancé et d'apporter en précision, Bitcoin a évidemment connu des failles de sécurité[113], comme tout logiciel, peu nombreuses, et qui ont contribué à sa solidité actuelle. Certaines ont été exploitées, on parlera d'attaque contre le protocole.[114][115]

---

[112] L'archétype restant l'histoire de J. Howells, un britannique ayant miné 7500 bitcoins en 2009, en une semaine, il arrête ensuite le mining, puis plus tard renverse accidentellement de la limonade sur l'ordinateur, il conserve le disque dur contenant les bitcoins. Au cours d'un rangement, il se déleste de son disque dur dans une décharge. A ce moment, il perd $ 600 000, au moment où il prend conscience de son erreur (à l'occasion d'un reportage à la télévision), $5 000 000, il ne les a jamais retrouvés.

[113] https://bitcoin.org/en/alerts

[114] « *Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies* », Rapport du Sénat, http://www.senat.fr/rap/r17-584/r17-58416.html

[115] Le 15 août 2010 est généré un bloc contenant une transaction créant 184 467 440 737 bitcoins pour trois adresses différentes. Cette faille est liée au fait que le code n'avait pas prévu le cas de création de quantités aussi grandes de bitcoins

50.- Notion d'attaque dite des 51% (de la majorité ou du consensus). Ce type d'attaque porte sur la technologie elle même, sur la chaîne de blocs, on parlera d'attaque utilisant le protocole[116]. Il s'agit de l'hypothèse où une entité parvient, seule, à contrôler la majorité de la puissance de calcul. L'attaquant peut alors annuler ou modifier l'ordre des transactions (forme de censure) ou encore revenir sur leurs transactions, contournant la limite de la double-dépense. Elle consiste donc à modifier l'histoire de la chaîne de blocs, dont l'objet est précisément d'être un registre en principe infalsifiable, la chaîne de blocs prend alors une fourche et se sépare entre deux versions. Si elle est un succès, ce type d'attaque ne permettra néanmoins pas d'empêcher les transactions ou d'annuler les transactions des autres utilisateurs sur le réseau, de même qu'elle ne permettrait pas de modifier la récompense d'un bloc, de créer de la cryptomonnaie ou de voler ces dernières qui n'ont jamais appartenu à l'attaquant.[117]

51.- Probabilité et cas d'attaques des 51%. La chaîne de blocs est sécurisée par un réseau distribué de nœuds où tous les participants participent, justement, à atteindre un consensus. En cela la blockchain est sécurisée, plus le réseau est développé, plus la protection est élevée. Une attaque des 51% est donc très peu probable et si elle survient, sa portée serait amoindrie (ne modifiant que certaines transactions sur les quelques blocs les plus récents pour une période limitée). Bitcoin est donc très sécurisé de par son réseau, le plus important, une récente étude suggère qu'une telle attaque sur le réseau Bitcoin coûteraut 1,4 milliards de dollars et consumerait autant d'élélectricité qu'un pays comme le Maroc[118]. Néanmoins, s'agissant de certaines *altcoins*, ayant une puissance de calcul moins élevée, la probabilité d'une telle attaque est plus importante. En juin 2018, ZenCash[119], notamment a été la cible d'une telle attaque, aboutissant à réorganiser la chaîne de blocs, pour dérober 18 600 ZEN, équivalent à 550 000 euros à ce moment là. D'autres comme la blockchain Verge[120] ($1,75 millions de préjudice), Bitcoin Gold ($18,6 millions de préjudice)[121], ou Ethereum Classic[122] ($1 million de préjudice) ont subi ce type d'attaque.

---

116 Rapport du Sénat précité.
117 « *What is a 51% Attack ?* », Binance, 28 novembre 2018
118 « *Analysis :Bitcoin Costs $1.4 Billion to 51% Attack, Consumes as Much Electricity as Morocco* », M. Moos, Cryptoslate.com, 29 novembre 2019.
119 « *ZenCash (ZEN) victime d'une attaque des 51%* », Cryptonaute, 4 juin 2018.
Communiqué de ZenCash :https://blog.zencash.com/zencash-statement-on-double-spend-attack/
120 « *Privacy Coin Verge Succumbs to 51% Attack (Again)* », J. Wilmoth, CCN.com, 22 mai 2018
121 « *Bitcoin Gold Hit By Double Spend Attack, Exchanged Lose Millions* », J. Wilmoth, CCN.com, 23 mai 2018
122 « *Attaque des 51% sur Ethereum Classic : 1,1 million de dollars dérobés* », Journal du Coin, 8 janvier 2019

52.- Correctifs. Dans une telle hypothèse, le protocole Bitcoin serait modifié et adapté pour répondre à l'attaque, opérant un retour en arrière de la chaîne de blocs au moment précédent cette dernière, il faudrait alors que les autres nœuds du réseau atteignent un consensus pour accepter ces changements (*hard fork*).

53.- Risques quantiques. Bitcoin et les cryptomonnaies reposant par nature sur la cryptographie, ces technologies sont potentiellement vulnérables face aux ordinateurs quantiques, bien que les spécialistes semblent s'accorder sur le fait qu'une telle technologie ne soit pas encore opérationnelle. Bitcoin serait notamment menacé relativement aux clés : la clé privée, passant par un algorithme de chiffrement (ECDSA) aboutit à une clé publique, qui elle même après être passée par un algorithme (SHA-256) donne une adresse, qui elle est connue et communiquée. La sécurité actuelle repose sur le fait que ce chemin est unilatéral, il apparaît, compte tenu de la puissance actuelle des ordinateurs, impossible de faire le chemin inverse et de trouver la clé privée à partir de l'adresse d'un portefeuille. Un ordinateur quantique en serait capable. Revenant à l'attaque des 51%, une telle machine pourrait prendre le contrôle de la majorité du réseau.
Bitcoin pourrait néanmoins une nouvelle fois s'adapter et utiliser des algorithmes post-quantique, adopté par un consensus du réseau[123] ou bien il est possible que l'on assiste à l'émergence d'une monnaie quantique, présentée comme infaillible[124]

[123] « *Bitcoin est-il vulnérable face aux ordinateurs quantiques* ? » Bitcoin.org
[124] « *Une monnaie quantique infaillible* », Ins2i.Cnrs.fr, 30 janvier 2018, https://arxiv.org/pdf/1705.01428v3.pdf

Chapitre 2 : Les financements en crypto-actifs

Les financements en crypto-actifs sont principalement les Initial Coin Offerings (ICO), qui sont des levées de fonds par émission de jetons, opération de marché primaire (A), permettant le développement d'un projet et la valorisation d'un jeton sur un marché secondaire (B)

Section 1 : La levée de fonds par émission de jetons (marché primaire)

§1. Des financements hybrides au crédit variable

A- Un mode de financement véritablement innovant

54.- Notion *d'Initial Coin Offering* (ICO) . *L'Initial Coin Offering* (ICO) ou *Initial Token Offering* (ITO) est une opération de levée de fonds par émission de jetons (*tokens*), au moyen de la technologie blockchain, destinée à financer le projet d'une entreprise, qui les émettra en contrepartie d'un investissement en crypto-actifs (le plus souvent bitcoin et/ou ether) ou en monnaie *fiat* (euro/dollar).

La nature de cette opération est donc hybride entre levée de fonds de capital-risque (*venture capital*), financement participatif (*crowdfunding*) et offre au public de titres (*Initial Public Offering*).

Proche du capital-risque d'abord, s'agissant de la nature technologique des projets, de l'avancement de ces derniers (souvent au stade de la simple idée[125]) et des rendements importants attendus. Proche, ensuite, du financement participatif, en raison de la volonté de créer une véritable communauté dès l'origine du projet, les investisseurs étant utilisateurs et les contreparties à l'investissement étant utilisables dans le cadre du projet. Enfin, assimilable a priori également à une offre au public de titres en ce que l'émission de jetons vise les investisseurs de la manière la plus large possible.

---

[125] Sur un échantillon de 110 ICO, 84% en étaient au stade de la simple idée selon Ernst & Young (2017) cité dans C. Le Moign, ICO françaises : un nouveau mode de financement ?, AMF, Novembre 2018

L'un des intérêts principaux de ces opérations a justement résidé dans ce caractère hybride, enjeu de la qualification juridique non précisée et par conséquent l'absence de soumission à un régime spécifique existant. La première ICO a eu lieu en 2013, pour financer le projet Mastercoin (devenu Omni), elle a permis de lever 500 000 dollars en bitcoin[126].
Mais l'essor des ICO s'est produit au cours de l'année 2016 et surtout 2017, popularisant ce mode de financement et suscitant la réflexion. Au niveau mondial, les opérations de ICO représentent environ 22 milliards de dollars au total, principalement entre 2017 et 2018. A l'inverse, en 2018, les 660 IPO à l'échelle mondiale ont permis de mobiliser environ 94 milliards de dollars.[127]

55.-Mécanisme. A l'origine de l'émission de jetons, un émetteur, dont la forme juridique était jusqu'ici assez libre, en pratique, le plus souvent sous forme sociétaire et plus spécifiquement de société par actions simplifiées (SAS) bien que les premières ICO auraient été réalisées sans structure sociétaire. Elles s'analyseraient en société créées de fait comme le relèvent les praticiens. [128]

L'émetteur a donc un projet d'activité, fondamentalement basé sur la technologie blockchain, qu'il expliquera dans un *white-paper*, ou livre blanc, constituant un document d'information destiné aux candidats à la souscription de jetons.

La nature des informations contenues dans ce document n'a été précisée que très récemment, comme on le verra (loi Pacte). Leurs qualité est donc variable, alors pourtant que, dans le secteur de la blobkchain la transparence est consubstantielle à la confiance[129]. Au fur et à mesure, la pratique a aboutit à un ensemble de bonnes pratiques[130] l'idée générale étant que le « bon » *white-paper* « *présente l'ensemble des caractéristiques générales du projet dans des termes compréhensibles par tous* ».

---

[126] J.R. Willett décrit le principe de l'ICO en janvier 2012 sur le forum Bitcoin Talk, son projet est d'ajouter une couche au protocole Bitcoin, de a même manière que l'email est par dessus le protocole TCP/IP « *Here's The Man Who Created ICOs And This Is The New Token He's Backing* », L. Shin, Forbes.com, 21 septembre 2017.
[127] « *660 introductions en Bourse ont eu lieu dans le monde au premier semestre – voici les 7 places boursières qui ont accueilli le plus d'IPO* », T. Chenel, Business Insider, 29 juin 2018.
[128] « *La mise en œuvre d'une ICO : les étapes en pratique* », P. LORENTZ, L. BENSOUSSAN, A. BARBET-MASSIN, Revue de droit bancaire et financier, n°1, janvier-février 2019
[129] « *ICO : l'impératif de la transparence »,* A. Stachtchenko, Medium, cité par : « *Regards sur une opération juridique non identifiée : les ICOs* », D. Legeais, Dalloz IP/IT 2018 p.113
[130] Issues de la Crypto-Valley Association ou encore de la FINMA, autorité fédérale de surveillance des marchés financiers suisses

Plus spécifiquement, cela implique que l'émetteur se présente, qu'il présente son projet sur le plan technologique, fonctionnel, humain (l'équipe), commercial, ainsi que les risques identifiés, le déroulement de l'émission (durée de l'offre, calendrier, plancher/plafond, cryptomonnaies ou monnaies fiat acceptées), ses caractéristiques (nature du jeton, norme technique, date et modalités de transmission du jeton au souscripteur, existence et modalité d'un marché secondaire) et objectifs (usage des fonds).

Bien que longtemps non exigées, les pratiques de *Know Your Customer* (KYC) dans le cadre de la lutte contre le blanchiment et le financement du terrorisme (LCB-FT) se sont développées, elles consistent par exemple en pratique : à vérifier l'identité des souscripteurs personne physiques par la prise de « selfie », à poser des questions relatives à la compréhension du projet et ses riques, à procéder à des déclarations sur l'origine des fonds…

Vient ensuite une phase de communication commerciale sur l'opération d'émission de jetons, celle-ci passe par des canaux divers, à la fois traditionnels (événements, conférences, site internet…), et innovants (réseaux sociaux, publicités, blogs, advisors, influenceurs…). La promotion de l'ICO est indispensable à son succès.

Souvent, une étape de vente privée (*private sale*) sera organisée, elle permet à un nombre restreint et choisi de candidats souscripteurs (le plus souvent des professionnels) de bénéficier, outre une priorité temporelle, d'un rabais sur le prix d'émission de jetons. Elle attire des investisseurs importants avec souvent un ticket minimum d'investissement.

Vient enfin l'opération de vente stricto sensu (vente publique) qui peut comporter plusieurs étapes, souvent une phase de prévente (*pre-sale*) sera organisée avec des rabais de l'ordre de 10 à 40%[131] puis la vente au grand public (*crowdsale*): les *tokens* sont émis de manière automatisée en contrepartie du versement de la souscription, au moyen d'un *smart contract*. Le *smart contract* est un programme informatique s'appuyant sur la technologie blockchain (le plus souvent Ethereum) pour y exécuter automatiquement des conditions préalablement inscrites.

---

[131] C. Le Moign, ICO françaises : un nouveau mode de financement ?, AMF, Novembre 2018

D'un point de vue juridique, le *smart contract* n'est pas un contrat, il est davantage perçu par la doctrine majoritaire comme une modalité d'exécution d'une relation contractuelle préexistante. En l'espèce, s'agissant d'une ICO, le *white-paper* et les conditions générales de ventes en tenant lieu[132]. L'opération pourra prévoir un montant minimum de souscription (*soft cap*) en deçà duquel le projet serait abandonné et un montant maximal de souscription (*hard c*ap) pour éviter la surcapitalisation.

Le financement étant réalisé car souscrit en totalité, il est alors mis fin à l'émission de manière prématurée. Le *token* est alors listé (*listed*) c'est à dire coté sur un marché, une plateforme, qui peut être centralisée ou décentralisée et qui fera office de marché secondaire.

56.- Taxonomie des tokens. Bien que certains tokens prennent des formes hybrides, l'on peut en distinguer trois types :

Les *coins*, c'est à dire les crypto-actifs représentant une monnaie d'échange, ce sont les cryptomonnaies étudiées précédemment.

Les *utility tokens* (jetons utilitaires) qui permettent d'accéder à des produits ou service proposés par l'émetteur.

Les *security tokens*, assimilables à des instruments financiers, ils donnent droit à des profits futurs de l'émetteur et/ou une participation à la gouvenance de ce dernier.

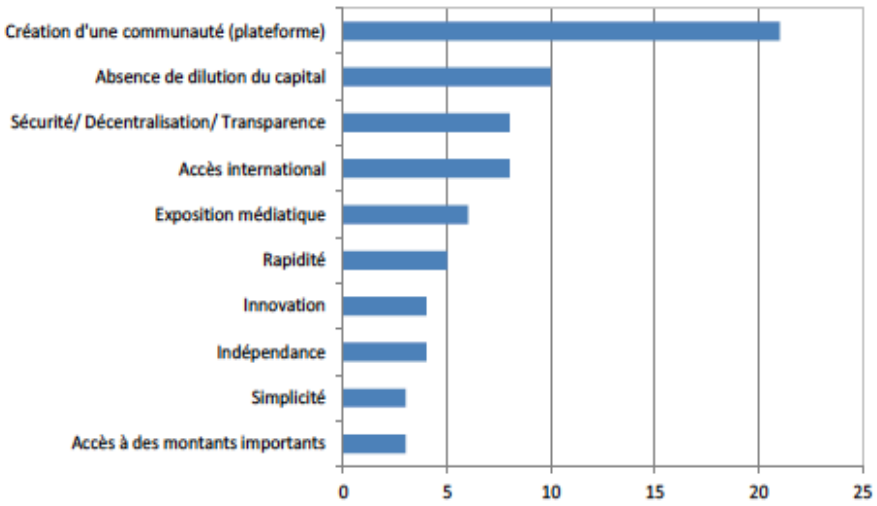
---

[132] « *La mise en œuvre d'une ICO : les étapes en pratique* », P. LORENTZ, L. BENSOUSSAN, A. BARBET-MASSIN, Revue de droit bancaire et financier, n°1, janvier-février 2019

Avantages/inconvénients.

	Emetteur	**Souscripteurs**
Avantages	• Créer une communauté d'investisseurs- utilisateurs engagée • Absence de dilution du capital social • Indépendance vis à vis des intermédiaires traditionnels et coûts moindres • Exposition internationale et communication • Accès rapide à des montants importants • Alternative aux financements traditionnels (capital/dette) • Permet une valorisation de l'émetteur	• Accès au capital risque • Rendements importants • Liquidité du token sur le marché secondaire
Inconvénients		• Méconnaissance des droits ou de l'absence de droits accordés par les crypto-actifs : souvent pas de part de capital • Manque de réglementation, de transparence, risques accrus d'échecs des projets, cyber-attaque, marketing trompeur, escroqueries

Graphique 7 : Raisons citées par les porteurs de projet pour lancer une ICO (en nombre de projets)



Source : AMF.
Lecture : plus de 20 projets ont cité la création d'une communauté comme une des raisons les ayant poussés à favoriser ce mode de financement. La question posée étant ouverte, les réponses obtenues sont libres et certains ont cité plusieurs raisons.

57.- Quelques exemples d'ICO. Le succès d'Ethereum. Pensé en 2013 par Vitalik Buterin alors âgé de 19 ans, rapidement rejoint par d'autres, Ethereum est un protocole qui permet la programmation[133] et l'exécution de smart contracts (par les nœuds du réseau).
Ethereum a été financé par une ICO, entre le 20 juillet et le 2 septembre 2014 (42 jours), n'acceptant que l'investissement en bitcoins (avec une parité initiale de 2000 ETH pour un bitcoin et finale de 1337ETH pour un bicoin), récoltant environ $18, 4 millions[134]. Lancé le 30 juillet 2015, son cours le plus bas était de $0,42 au 21 octobre 2015 et son plus haut de $1 432 au 13 janvier 2018, il est de $160 au 1er mai 2019.[135]

En pratique, il s'agit d'un ordinateur mondial décentralisé, on parle *d'Ethereum Virtual Machine* (EVM). Ethereum permet donc le développement d'applications décentralisées (DApps)[136].

---

[133] En langage Solidity
[134] « *Launching the Ether Sale* », V. Buterin, Blog Ethereum.org, 22 juillet 2014 ; « *15 insights on how Ethereum conducted its ICO in 2014* », CoinNounce.com,
[135] https://coinmarketcap.com/currencies/ethereum/
[136] « *Vitalik Buterin explains Ethereum* », Youtube, https://www.youtube.com/watch?v=TDGq4aeevgY

Pour un exemple d'application décentralisée parmi d'autres, l'on peut citer Augur, qui a pour finalité de devenir un « marché de prédiction décentralisé », basé sur la blockchain Ethereum. Les utilisateurs parient sur la probabilité qu'un événement arrive ou non et peuvent créer leur propre pari (performance d'une société, résultat d'une élection, sujets de partiels…). Les autres utilisateurs peuvent acheter et vendre des parts de probabilité qu'un événement de produise[137].

L'on assiste à l'émergence d'un phénomène de « décentralisation »[138] dont l'aboutissement est la DAO (*Decentralized Autonomous Organization*) qui est « *une organisation décentralisée dont les règles de gouvernance sont automatisées et inscrites de façon immuable et transparente dans la blockchain* »[139] pour fonctionner, elle a recours à des *smart contracts*. La première organisation du genre « TheDAO » a été créée en 2016 par l'équipe de l'entreprise Slock.it[140]. Pour illustrer ce phénomène, l'on peut décrire la proposition de Slock.it : lier les objets physiques (connectés) avec la blockchain Ethereum. Le slogan : « *louez, vendez ou partagez tout ce que vous voulez* ».
Par exemple, une serrure de porte connectée pourrait permettre la location d'appartement, si un locataire désire le louer, il paie le prix via une interface d'application mobile et le *smart contract* permet l'ouverture automatique de la porte. Les objets se « *louent eux mêmes* » résume l'un des cofondateurs[141].

TheDAO était une sorte de fonds d'investissement, s'appuyant sur Ethereum, financé via une ICO ayant permis de récolter 120 millions de dollars (150 millions selon certaines sources)[142]. L'organisation avait pour caractéristiques la transparence ainsi que la décentralisation, afin de permettre l'absence de confiance (*trustlessness*). Elle visait à financer des projets développés sur la blockchain Ethereum, les participants pouvant voter sur des projets (au moyen de leurs *tokens*) pour leur accorder un financement et en percevoir les produits via un *smart contract*.

---

137 v. Augur sur Coinmarketcap
138 « *Decentralizing Everything with Ethereum's Vitalik Buterin* », Disrupt SF 2017, TechCrunch https://www.youtube.com/watch?v=WSN5BaCzsbo ; « The Meaning of Decentralization », Vitalik Buterin, Medium, 6 février 2017
139 « *Qu'est-ce qu'une DAO* ? », Blockchain France, 12 mai 2016
140 v. le *white-paper* https://download.slock.it/public/DAO/WhitePaper.pdf
141 « *Slock.it : la promesse des objets connectés sur la blockchain* », S. Polrot, Ethereum France, 4 avril 2016
142 « *Automated company raises equivalent of $120M in digital currency* », R. Waters, CNBC, 17 mai 2016 ; « *A Venture Fund With Plenty of Virtual Capital, but No Capitalist* », N. Popper, The New York Times, 21 mai 2016

Le 17 juin 2016, TheDAO fait l'objet d'une attaque, en raison d'une faille dans le code source, causant un préjudice de 3 millions d'ethers (environ 50 millions de dollars à cette époque)[143] ce qui fait l'effet d'un séisme dans l'écosystème Ethereum et plus largement crypto et attire l'attention sur les problématiques de sécurité. Les séquelles de ce piratages sont d'ailleurs encore présente puisqu'il a aboutit à une scission résultant d'un désaccord au sein de la communauté Ethereum : poursuivre la chaîne de blocs Ethereum, fidèlement à la philosophie de la blockchain et son immutabilité ou bien opérer un retour en arrière dans la chaîne de blocs, antérieur à l'attaque pour en annuler les effets. Cela aboutit à un *hard fork*, une « fourche » dans la chaîne de blocs, entre Ethereum (ETH) et Ethereum Classic (ETC).
Ethereum est fondé sur le modèle de Bitcoin et, lui-même open-source, a inspiré des projets similaires et concurrents comme EOS, qui propose une alternative à Ethereum, et est à son tour devenu la plus grosse ICO de l'histoire, avec 4 milliards de dollars levés[144].

Exemple d'une entreprise française : Domraider. Domraider est une enteprise française qui propose deux service : la récupération et la revente de noms de domaines expirés (pratique du *dropcatching*) (Youdot) et un réseau d'enchères décentralisées sur la blockchain (Auctionity)[145]. Basée à Clermont-Ferrand, fondée en 2013, elle réalise en 2017 une ICO auprès de 3600 investisseurs, dans 117 pays pour une valeur de 6,9 milions d'euros sécurisés[146], avec un objectif annoncé à 35 millions d'euros et l'annonce d'avoir vendu l'intégralité des 560 millions de jetons prévus[147]. Le montant levé reste tout de même assez opaque, et cela probablement à dessein, comme l'ont remarqué certains observateurs[148] et qui tient à la l'absence de transparence de l'émission de jeton. En effet Domraider n'avait pas communiqué l'adresse du *smart contract* utilisé pour l'ICO, qui permet en temps normal à tout un chacun d'auditer et suivre le déroulement de l'opération (montants reçus, nombre d'investisseurs).

58.- Analyse bilan des premières ICO françaises. L'Autorité des marchés financiers (AMF) a eu à connaître de 83 ICO ou projets d'ICO, 74 se proposaient d'émettre des *tokens* conférant des droits d'usage ou de paiement, ayant donc les caractéristiques *d'utility token* ; 4 ayant le caractéristiques de *coins* ; 4 ayant les caractéristiques de *security tokens*.

---

143 « *The DAO : post mortem* », S. Polrot, Ethereum France, 24 janvier 2017.
144 « *EOS ou les dessous de la plus grosse ICO de l'histoire* », Les Echos, 28 juin 2018.
145 https://www.domraider.com
146 https://www.domraider.com/investisseurs/
147 « *DomRaider : une ICO sur le sol français, contre vents et marées* », L. Adam, ZDNet, 6 décembre 2017.
148 « *ICO : l'impératif de transparence* », A. Stachtchenko, Medium, 5 octobre 2017

Sur les 83 recensées, 15 ont été menées à leur terme fin octobre 2018. Selon L'AMF, 89 millions d'euros ont pu être levés en France depuis novembre 2016. Le capital risque (*venture capital)* a permis de lever 2,1 milliards d'euros en 2017, le financement participatif (*crowdfundin*g) 336 millions, et l'émission d'actions 2 milliards. Tous les *tokens* sont échangés sur un marché secondaire, 8 projets étant listés sur deux plateformes ou plus.

B- Un mode de financement sujet à carences et exubérances

Le nombre d'opérations réalisées, les montants levés, les succès retentissants, les rendements mirifiques promis[149], les pratiques bonnes ou mauvaises, ont contribué à des excès. Très vite, de nombreux projets ne respectent en effet plus les caractéristiques fondamentales de ces opérations.

Certains projets n'ont pas fondamentalement besoin d'une solution basée sur une blockchain et ne font que profiter d'un effet de mode, apportant peu d'innovation technologique. Les équipes sont parfois au mieux peu compétentes, au pire fausses. Les *advisors* ont des rôles et responsabilités opaques dans le développement du projet : dans quelle mesure conseillent-ils l'équipe, dans quelle mesure leurs conseils sont-ils appliqués, ne sont-ils rétribués que pour leur image ? Les jetons sont présentés de manière habile afin d'attirer l'investisseur et éviter le régulateur. De même que décrit *supra* s'agissant des cryptomonnaies et plus spécifiquemet du bitcoin, le grand public est sujet au *FoMO*, (*Fear of Missing Out*) encore plus depuis qu'il a manqué cette dernière opportunité.

« *Peut-on qualifier une levée de fonds d'Initial Coin Offering alors même qu'elle ne repecte pas l'une des caractéristiques les plus fondamentales des technologie blockchain : la transparence* ? » s'interroge A. Stachtchenko[150]. Il semblerait que oui. Sans encore parler d'infractions (v. partie 2), des mauvaises pratiques ont été recensées afin qu'elles cessent, dans un mouvement d'autorégulation. Il s'agit de la technologie, d'abord, qui doit permettre d'auditer le déroulement de l'ICO (blockchain publique ou communication des adresses destinatrices) de s'assurer des montants levés (qui sont souvent communiqués pour inciter d'autres investisseurs) et de se tenir à ce déroulment : Gimli aurait par exemple changé les

---

[149] La performance moyenne pour le premier jour de listing d'une ICO serait ainsi de 920%, une sur deux gagnerait plus 25%. « *Comment le marché des ''ICO'' a pris sont essor* », N. Ait-Kacimi, Les Echos, 5 octobre 2017.

[150] « *ICO : l'impératif de transparence* », A. Stachtchenko, Medium, 5 octobre 2017

règles en cours de route et supprimé son *soft cap*, montant qui, s'il n'est pas atteint, met fin à l'émission et permet à l'investisseur de récupérer ses fonds.
Ces excès ont été en quelque sorte un « mal pour un bien » en ce qu'ils ont permis d'en prendre conscience et à terme d'assainir l'écosystème, conscient de l'importe de sa crédibilité auprès des régulateurs et du grand public.

60.- Notion de *Security token offering (STO).* Sur le modèle de l'ICO, l'on parle de STO pour designer l'émission de *token* prenant la forme de *security*, donc de titres financiers, qui sont dits "*tokenisés*", digitalisés sur une blockchain. Parfois presentées comme l'avenir des ICO, l'on sera d'avis de penser qu'elles adressent une problématique différente, spécifique au secteur de la finance[151]. A titre d'exemple, le 18 avril 2019 Société Générale a procédé à une *Secutity Token Offering* d'obligations sécurisées (*covered bonds*) d'un montant de 100 millions d'euro via sa filiale Société Générale SFH sur la blockchain publique Ethereum. Selon la banque, cette transaction permet notamment plus de transparence dans l'émisssion, l'automatisation des événements sur le titre, de réduire le coût ainsi que le nombre d'intermédiaires.[152]

Les *Security Token Offering* sont présentées comme un nouveau modèle, plus raisonnable que l'ICO. L'objet de la STO est d'émettre des *secutity tokens*, jetons représentant un instrument financier, un titre de capital, une part de la société et donnant des droits équivalents aux souscripteurs à ceux conférés par une action ou une créance[153].

Il n'est en réalité pas certain que les STO constituent l'avenir des ICO.[154] D'abord, il conviendra de développer des plateformes d'émission (marché primaire) et des plateforme d'échange (marché secondaire). Ensuite, bien que l'on parle de *security tokens*, il conviendra en principe de leur appliquer le régime des *securities* ou plus précisément, et selon une terminologie du droit français, des titres financiers, avec certainement des clarifications sur certains points spécifiques.

---

151 « *The Official Guide To Tokenized Securities* », A. Pompliano, Medium, 26 février 2018.
152 « *Société Générale émet la première obligation sécurisée sous forme de "security tokens" sur une blockchain publique* », Communiqué de presse
153 « *Les STOs peuvent-elles sauver le marché des cryptoactifs* ? », M. Zeller, Coin House Insights, 30 janvier 2019.
154 « *Pourquoi les Security Tokens intéressent plus les services marketing que les services juridiques ?* », W. O'Rorke, Medium, 11 avril 2019.

61.- Initial Exchange Offering (IEO). L'on parle d'IEO pour désigner une levée de fonds pratiquée directement sur une plateforme d'échange (*exchange*).[155] L'investisseur, qui possède un portefeuille lié à la plateforme (*wallet*) peut y participer directement. La plateforme d'échange apporte la simplicité, sa crédibilité, une base d'investisseurs. Vues comme une autre alternative aux ICO au cours de l'année 2019, les IEO reposent sur une plateforme d'échange centralisée, qui prendra une commission pour le service d'intermédiaire rendu. La centralisation est un avantage, les escroqueries y seront en principe inexistantes, la confiance sera plus importante de par la réputation des plateformes d'échanges, bien établies, le processus de *Know Your Customers* (KYC) de verification d'idenité sera pris en charge, ainsi que la cotation (*listing*) sur le marché secondaire… Néanmoins, la centralisation, contraire à la philosophie même de la technologie blockchain est davantage vulnérable aux attaques, comme on le verra par la suite.

62.- Tendances et perspectives. Il semblerait que les ICO connaissent une nouvelle phase, signant la fin de l'exubérance et des projets peu solides, décrédibilisant le secteur. Une nouvelle vague d'ICO s'apprêterait à émerger, plus saine, laissant moins de place à la spéculation inconsidérée et centrée sur *l'utility token*, qui retrouve sa vigueur comme par exemple le projet Foam : d'abord, un double test était proposé aux candidats investisseurs estimant leur connaissance du projet et leur intention de l'utiliser, 25% auraient échoué au test, ce qui est à la fois affligeant et surprenant mais doit être encouragé ; ensuite le montant de *tokens* pouvant être acquis, au-delà de 10 000 dollars nécessitait de préciser ses intentions ; enfin un mécanisme incitatif à l'utilisation et donc au développement du réseau, décourageant la spéculation a été instauré.

Un nouveau modèle émerge donc, d'abord issue d'une autorégulation, souhaitée et développée. Des bonnes pratiques, volontariste pour rendre le secteur responsable et se distinguer n'ont pas attendues la réglementation, aussi opportune soit-elle.[156]

---

[155] L'une des premières est Binance qui a lancé sa plateforme dédiée aux IEO Binance Launchpad.
[156] « *ICO : fin du buzz et retour à la raison* », Les Echos, 22 octobre 2018.

§2. Une réglementation souhaitée entre protection et attractivité

63.- Positions contrastées : interdiction, neutralité, réglementation. Certains états comme la Chine ont interdit les levées de fond en cryptomonnaies[157]. Aux Etats-Unis, les ICO se voient appliquer la même réglementation que l'offre au public de titres (les *tokens* sont assimilées à des *securities*) sous condition de remplir le *Howey Test*[158], afin de caractériser un contrat d'investissement, il importe que trois critères soient réunis : un investissement d'argent ; l'espérance de profits pour l'investisseur ; une entreprise « normale» (*common enterprise*), c'est à dire dont le succès ne dépend pas de l'investisseur mais d'un tiers. Ainsi, la SEC a récemment pu confirmer a contrario sa position en émettant une *no-action letter* (équivalent d'un rescrit) et en reconnaissant l'existence de jetons utilitaires (*utility tokens*) qui ne satisfont pas le test, s'agissant de la société TurnKey Jet[159].

64.- Opportunité de réglementer en France. S'agissant de l'opportunité de réglementer en France, il convient de rappeler la différence entre régulation et réglementation.[160] Bien que *regulation* se traduise par réglementation, il importe de ne pas confondre ces deux concepts.
Si la régulation paraît tout à fait opportune, souhaité et semble s'imposer avec la force de l'évidence, la réglementation, quant à elle ne va pas de soi. Il existe en effet une tension entre d'une part la protection des investisseurs et l'accompagment de l'innovation. L'on aurait en effet pu se passer de l'intervention du législateur et laisser les opérateurs se réguler d'eux-mêmes, définissant des bonnes pratiques et réprouvant les pratiques contestables comme cela se faisait déjà. C'est la proposition que défendent les tenants de la philosophie libertaire à l'origine de la technologie.
De plus, l'on pourrait se demander s'il est encore opportun de réglementer les ICO, leur nombre ayant fortement diminué. L'on peut tout de même penser qu'une réglementation est toujours nécessaire, comme l'indique Bruno Le Maire : « *la baisse du nombre d'ICO était prévisible et nécessaire à l'assainissement du marché* », mais cette dernière « *n'enlève rien*

---

157 « *La Chine interdit les levées de fonds en cryptomonnaies* », F. Schaeffer, Les Echos, 5 septembre 2017.
158 Utilisé par la Securities and Exchange Commission, *W.J. Howey Co.* (1946)
159 L'activité est celle de la location de jet privé, il est précisé que les fonds levés ne serviront pas à développer la plateforme, que les jetons seront utilisable immédiatement, qu'ils maintiennent une parité avec le dollar, ils ne seront pas présentés comme pouvant générer un profit, leur revente ne pourra se faire qu'à un prix inférieur. En empêchant la volatilité donc la spéculation, et excluant la source de profit, le jeton ne peut être considéré comme un titre financier. https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm
160 Bitcoin, totem & tabou, que présage l'essor des cryptomonnaies ? Rapport de l'Institut Sapiens, Février 2018.

au potentiel et aux avantages offerts par ce nouveau mode de financement », enfin cette baisse « *ne signifie pas que nos épargnants se trouvent moins exposés aux différents risques portés par les ICO* »[161].

La réglementation des opérations d'émissions de jetons pourrait en effet envoyer un signal que le « vide juridique » a été comblé en cette matière et qu'il n'est plus possible – ou en tous les cas qu'il sera plus difficile – de détourner ce mode de financement. Mis en parallèle avec l'autorégulation, l'identification des bonnes et mauvaises pratique par les acteurs de l'écosystème et les chartes de bonne conduite, les infractions liées aux crypto-actifs (partie 2) pourraient diminuer drastiquement, sous réserve de l'effectivité pratique de la réglementation. A la question « Pourquoi réguler ? » l'on peut répondre, à la suite de M. Guy Canivet[162] qu'il s'agit de « *prévenir le risque d'insécurité juridique* », en effet les opérateurs de ce secteur ont besoin de règles pour évoluer plus sereinement. Ainsi« *choisir la bonne régulation c'est réaliser des équilibres entre liberté des acteurs et protection des intérêts publics ou privés en cause* ».

65.- La position française. L'Autorité des marchés financiers (AMF) a lancé une consultation publique sur les ICO entre octobre et décembre 2017, dont les réponses recueillies viennent largement des bonnes pratiques adoptées et souhaitées par les acteurs et fournissent l'essentiel du droit positif. Le projet de loi « PACTE » (Plan d'Action pour la Croissance et la Transformation des Entreprises) a été adopté en lecture définitive à l'Assemblée nationale le 11 avril 2019. S'agissant des *Initial Coin Offerings* (ICO), c'est à dire des levées de fonds par émission de jetons, l'article prévoit un régime *ad hoc* de contrôle par l'AMF, résiduel et dont la principale mesure est l'octroi d'un visa optionnel.[163]

Un régime résiduel. L'article 85 du projet de loi (ancien article 26) prévoit (I, 7°) l'insertion dans le Code monétaire et financier (ci-après Comofi) d'un article L.552-1 disposant que les dispositions du chapitre II (« Emeteurs de jetons ») nouvellement créé s'appliquent à toute

---

161 « *Bruno Le Maire : "Le développement de l'écosystème blockchain est une priorité pour le Gouvernement"* », Gregory Raymond, Capital, 15 avril 2019.
162 G. Canivet, Blockchain et régulation, JCPE n°36 – Septembre 2017
163 « *ICO, Le législateur introduit des jetons dan le Code monétaire et financier* », F. Drummond, La semaine juridique édition générale n°52, 24 décembre 2018 (Le club des juristes)

offre de jetons « *qui n'est pas régie par les livres Ier à IV, le chapitre VIII du titre IV du présent livre ou le chapitre 1er du présent titre* ».
Autrement dit, ce régime s'applique à condition que ne sont pas en cause des instruments financiers ou autres réglementations spéciales.

En outre, un article L.552-2 nouveau définit le jeton[164] comme « *tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier directement ou indirectement, le propriétaire dudit bien* » l'article qui le suit immédiatement[165] définit alors l'opération d'émission de ces jetons : « *une offre au public de jetons consiste à proposer au public, sous quelque forme que ce soit, de souscrire à ces jetons*. »

Un visa optionnel. Le nouvel article L.552-4 du Code monétaire et financier dispose que « *préalablement à toute offre au public de jetons, les émetteurs peuvent solliciter un visa de l'Autorité des marchés financiers* ».
La délivrance de ce visa exige la réunions de plusieurs conditions prévues par le texte[166]: fourniture d'un document d'information (« *destiné à donner toute informations utiles au public sur l'offre proposée et sur l'émetteur* »), étant précisé que ce document et les communications à caractère promotionnel relatives à l'offre au public « *présentent un contenu exact, clair et non trompeur et permettent de comprendre les risques afférents à l'offre* ». Le *white-paper* se trouve donc soigneusement encadré, de manière similaire à celle du prospectus exigé lors de l'offre au public de titres.

Le législateur, avec l'article L.552-5 du même code, décrit les vérifications opérées par l'AMF : obligation pour l'émetteur d'être constitué sous la forme d'une personne morale établie ou immatriculée en France, présence d'un dispositif permettant le suivi et la sauvegarde des actifs recueillis à l'occasion de l'offre (information annuelle des souscripteurs

---

164 La notion de token, étant précisée désormais, c'est surtout sa qualification juridique qui mobilisé une partie de la doctrine et qui invite encore à l'heure actuelle à une appréciation au cas par cas : « *Réflexion sur la nature juridique des tokens* », L. Soleranski, Bulletin Joly Bourse – N°3, p.191, 1er mai 2018 ; Lachgar K. et Sutour J., « *Le token, un objet digital non identifié* ? », Option Finance n° 1437, 13 nov. 2017, p. 18. ; Bonneau T., « *Tokens, titres financiers ou biens divers* ? », RD bancaire et fin. janv. 2018, repère 1.
165 Art. L.552-3 nouveau du Code monétaire et financier
166 Qui renvoie pour les modalités de la demande au règlement général de l'AMF.

sur l'utilisation des actifs recueillis, art. L.552-4 Comofi), le repect des règles en vigueur en matière de lutte contre le blanchiment et le financement du terrorisme (LCB/FT).

La portée du visa. Le visa étant optionnel, un émetteur qui ne le demanderait pas ou ne l'obtiendrait pas ne serait pas pour autant interdit d'émettre des jetons. Néanmoins, les émetteurs l'auraient pas reçu ne pourront pas démarcher le public[167]. L'AMF publiera une liste des ICO ayant reçu son visa, ce qui permettra d'envoyer un signal aux investisseurs et drainer l'épargne dans des projets plus sûrs. « *Nous faisons le pari qu'il attirera les bons projets* » conclu Robert Ophèle, président de l'AMF. Il faut saluer la réactivité du régulateur qui a dans un premier temps annoncé être en mesure de délivrer les premiers visa en septembre 2019 puis en juin 2019. Précisons que le cas échéant, ce dernier pourrait être retiré, de manière temporaire ou définitive si l'AMF constate que « *l'offre proposée au public n'est plus conforme au contenu du document d'information ou ne présente plus les garanties prévues à l'article L.552-5* » aux termes de l'article L.552-6. L'AMF pourra également procéder à une déclaration publique si « *après ou non avoir sollicité un visa* » une personne diffuse des informations comportant des « *indications inexactes ou trompeuses concernant la délivrance du visa, sa portée ou ses conséquences* » (al.2).
Il n'est donc pas question pour un émetteur de bénéficier par le visa d'un blanc-seing ou d'en exiger la portée auprès des candidats investisseurs.

Ces dispositions permettent la reconnaissance, par le législateur de la pratique des levées de fonds par émission de jetons et l'implication du régulateur. Elle est nécessaire à la protection de l'épargne et adaptée à l'innovation. L'on peut espérer qu'à terme les infractions liées aux ICO et aux crypto-actifs (Partie 2) se tarissent.

66.-L'effectivité de la réglementation. De par son caractère global, « ambitieux » pour beaucoup, en réglementant également les prestataires de service sur actifs numériques (PSAN) ainsi que le droit au compte pour les émetteurs, crucial pour convertir les cryptomonanies recueillies en monnaies fiat et développer le projet. La loi PACTE renforce les pouvoirs de l'AMF, qui disposera du pouvoir de surveiller les ICO ayant reçu son visa et

[167] « *Vers un nouveau régime pour les crypto-actifs en France* », Dossiers thématiques, Fintech, AMF, 15 avril 2019.

superviser les prestataires agréés pour le cas échéant prononcer des sanctions à leur encontre. L'AMF pourra publier une liste noire, des ICO et PSAN qui ne respecteraient pas la réglementation et bloquer l'accès aux sites internet frauduleux proposant des services sur actifs numériques. Comme le résume Bruno Le Maire, ce cadre réglementaire ambitieux a été « *complété par des mesures relatives au traitement comptable et fiscal des crypto-actifs. L'ensemble de ces mesures forme un tout cohérent et sans équivalent dans le monde.* »

La nécessité d'une réglementation internationale est, en effet, un enjeu crucial de l'effectivité de cette réglementation, à commener par l'Union Européenne où l'on remarque qu'un règlement « Prospectus » entrera en application au 21 juillet 2019 applicable aux offres au public de « valeurs mobilières » au sens de MiFID 2 (catégories de titres négociables sur le marché des capitaux, à l'exception des instruments de paiement). La question de savoir si les jetons sont des « catégories de titres négociables », les qualifiant de « valeurs mobilières » se posera donc, et le cas échéant rendant applicable la réglementation prospectus. Un tel signe donnerait un signe de « fermeture de la place de Paris et de l'Union Européenne qui souhaitent au cotnraire favoriser le développement des fintech »[168]. La législation, tant souhaitée, réalisant œuvre compromission entre les désirs d'innovation et de protection, devrait alors être remise en cause.

[168] Intervention de Robert Ophèle, Président de l'AMF devant la Mission d'information sur les « Monnaies virtuelles » de la Commission des finances de l'Assemblée nationale, 5 avril 2018

Section 2 : Développement du projet et marché secondaire

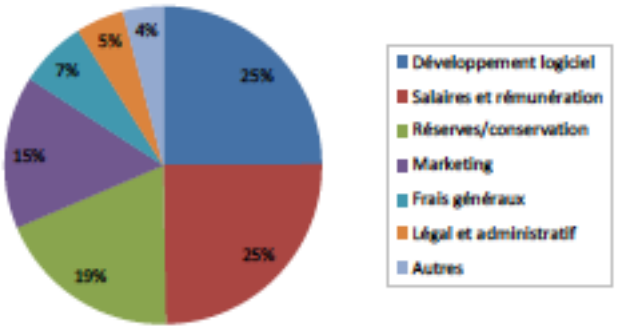
Le développement du projet, qui est l'objet du financement, peut rencontrer des obstacles, il est consubstantiel à la valorisation du token (§1) de même que l'existence d'un marché secondaire (§2).

§1. Développement du projet

Il est tout d'abord possible que des entreprises portant un projet sérieux, ne parviennent pas à lever des montants suffisants par l'émission de jetons, n'atteignant par leurs *soft cap*, pour diverses raisons, notamment de marché, en raison de la volatilité des cryptomonnaies, le timing peut parfois être mal choisi. Néanmoins, lorsqu'une ICO est un succès, son objet principal est de financer le développement du projet porté par l'entreprise.

67.- Objet du financement. L'utilisation concrète des fonds demandés doit en principe se faire conformément au document d'information (*white-paper*). La première étape est celle de la conversion des cryptomonnaies levées en monnaies fiat, afin de financer concrètement l'avancée du projet. A ce titre, le droit au compte bancaire opposable aux banques est une avancée importante qui permettra un développement facilité et rapide des projets (article L.312-23 nouveau du Code monétaire et financier). En effet, les cryptomonnaies n'ayant pas un pouvoir libératoire universel (elle ne sont pas acceptées par tous) elles ne permettent pas de payer les factures, les salaires, de plus leur conservation, soumise à la volatilité risque de précipiter l'entreprise voire de rendre le projet impossible à mener, sans pour autant qu'une infraction soit commise. L'article L.552-5 nouveau du Code monétaire et financier prévoyant que l'AMF vérifie que l'émetteur des jetons « *met en place tout moyen permettant le suivi et la sauvegarde des actifs recueillis dans le cadre de l'offre* » devrait contribuer à améliorer la transparence et la sécurité des fonds lors du développement du projet.

Graphique 10 : Répartition de l'utilisation des fonds levés
(en % de montants levés par l'émetteur)



Source : AMF

68.-L'exemple de Tezos. A l'origine de Tezos[169], Athur Breitman, un français (et son épouse Kathleen), qui en 2014 propose un nouveau protocole blockchain, dotée d'un fonctionnement différent de celui de Bitcoin, avec pour projet de développer un réseau décentralisé, similaire à Ethereum.

D'abord, une société est créée au Delaware, opère une levée de fonds (environ 600 000 dollars) pour préparer l'ICO. Une fondation est créée en Suisse (à Zoug, très attractive pour l'écosystème crypto au point qu'elle est baptisée « crypto-valley ») afin de mener l'émission et d'acquérir la société de l'Etat du Delaware ayant développé le projet (et détenant le code source). L'émission se déroule du 1er au 13 juillet 2017 et permet de lever environ 232 millions de dollars (en bitcoins et éthers)[170]. Un conflit entre les Breitman et le reste de l'équipe, notamment le Président de la fondation de droit suisse (détenant les fonds), s'est déclenché ainsi qu'une action de groupe (*class action*) aux Etats-Unis, sur le point de savoir si les jetons émis ont les caratéristiques de *securities* (titres financiers, avec le régime associé, notamment l'enregistrement auprès de la SEC). Le projet est encore actuellement en arrêt, le token n'est listé que sur une plateforme d'échange avec le statut de « prévente ».[171]

---

169 v. le *white-paper* https://tezos.com/static/position_paper-841a0a56b573afb28da16f6650152fb4.pdf
170 « *L'affaire Tezos : la « fièvre des ICO et ses risques* », F. G'sell, Frenchweb, 26 octobre 2017
171 « *Tezos : la cryptomonnaie à 400 millions de dollars victime d'un conflit juridique* », Journal du Coin, 20 octobre 2017.

Néanmoins, une intervention récente de son cofondateur[172] semble laisser penser que le projet n'est pas abandonné, Tezos a toujours pour ambition d'être « la dernière cryptomonnaie » en ce qu'elle pourra « se changer » en « adoptant les innovations des autres (cryptomonnaies)», les développeurs étant incités à améliorer Tezos (*Tezos : A Self-Amending Crypto-Ledger*, était intitulé le *white-paper*). Une version Beta a été lancée en juillet 2018, et le jeton (XTZ) est vendu chez Coinhouse.[173]

Ainsi, une opposition au sein de l'équipe peut empêcher ou retarder le développement du projet. Une attaque informatique peut également être une source de désagrément, comme ce fut le cas pour The DAO précédemment évoqué.

Face à ces diverses sources de risques, un nouveau modèle d'émission de jetons a émergé de la pratique, la DAICO (*Decentralized Autonomous ICO*)[174] afin de favoriser la transparence et le contrôle dans l'utilisation des fonds levés lors de l'ICO. Il s'agit d'allier une ICO traditionnelle à la DAO, pour mettre en place une sorte de robinet (*tap*) permettant à l'équipe ayant levé les fonds d'utiliser progressivement ces derniers, selon les votes des participants. Le débit peut être augmenté en fonction de l'avancement du projet ou auto-détruit pour restituer les *tokens*, et donc l'investissement en ethers, aux investisseurs proportionnellement à leur investissement. L'effectivité de ce modèle présente néanmoins des limites intrinsèques potentielles en ce que l'équipe développant le projet se réservera souvent une partie des jetons à l'issue de l'émission primaire et aura donc un poids dans l'issue du vote allouant le budget.
Ce mécanisme, issu de la pratique et de l'ingéniosité des membres de la communauté pourrait, additionné aux bonnes pratiques et à la réglementation nouvelle, diminuer d'autant les émissions de jetons peu sérieuses voire frauduleuses. Notons en outre qu'autant opportune et attractive qu'elle soit, la seule réglementation, voire la sanction pénale spéciale (v. partie 2) pourrait s'avérer moins effective en pratique que ces modèles plus mécaniques et technologiques.
La confiance dans les crypto-actifs et le développement de l'innovation passeront donc nécessairement par une coordination de l'autorégulation et de la réglementation.

---

[172] Podcast « 21 millions » par Grégory Raymond, Capital, 24 avril 2019
[173] « Tezo : la plateforme de smart-contract à la gouvernance décentralisée », D. Fay-Manzo, Coin House Insights, 27 juillet 2018.
[174] Mécanisme proposé par V. Buterin https://ethresear.ch/t/explanation-of-daicos/465

§2. Marché secondaire du *token*

69.- Intérêt du marché secondaire pour le *token*. L'intérêt du marché secondaire est, outre une porte de sortie, l'espoir d'une plus-value pour l'investisseur. Cet espoir sera d'autant plus grand que l'investisseur aura eu accès aux jetons en phase de vente privée (*private-sale*) ou de prévente (*pre-sale*) bien que la majorité des tokens soient émis lors de la *crowdsale*, qui est la plus publique. Certains peuvent ainsi être tentés de vendre leurs jetons acquis lors d'une phase prématurée dès l'ouverture du marché secondaire, attiré uniquement par la volatilité du jeton.
De plus, la capitalisation d'un jeton est souvent mal comprise, tous les jetons ne sont souvent pas émis lors de l'émission primaire. Une partie est souvent conservée par l'entreprise, voire attribuée à l'équipe technique (*bounty*). Il faut donc être vigilant face à ces mécanismes de réserve de *tokens* : vérifier le nombre de tokens émis lors de l'émission primaire et la possibilité d'en émettre dans le futur (et faire baisser le cours des jetons détenus, par le jeu de l'offre et la demande) ; sécuriser les tokens conservés ; s'assurer de l'émission progressive des tokens sur le marché par l'émetteur afin d'éviter les mouvements brutaux sur le cours.[175]
Sur les 15 projets français ayant terminé leur ICO, l'AMF relève qu'entre 6% et 80% des tokens sont conservés par l'émetteur (avec une moyenne de 25%), il convient donc d'être très vigilant et d'avoir une approche au cas par cas sur ce point. L'on remarque que ces risques ne sont pas prévus par la réglementation récente.

70.- Comparaison avec les marchés réglementés traditionnels. L'accès au marché secondaire, le trading passe traditionnellement par un prestataire de service d'investissement (PSI). S'agissant des *tokens*, tout un chacun peut accéder aux plateformes pour échanger, spéculer (une plus-value est également très souvent attendue en vendant ces tokens sur le marché secondaire). Si le marché secondaire ne se crée pas le *token* ne vaut rien ou presque.
L'échange sur une plateforme, un marché secondaire, assure la liquidité du token. La liquidité, c'est à dire la possibilité de trouver une contrepartie sur le marché, est essentielle, elle n'est néanmoins pas garantie. En analysant 1 009 tokens depuis 2015, Amsden et Schweizer (2018) observent que 42 % des tokens sont listés sur un marché secondaire après leur ICO.[176]

---

[175] C. Le Moign, ICO françaises : un nouveau mode de financement ?, AMF, Novembre 2018, p.7
[176] C. Le Moign, ICO françaises : un nouveau mode de financement ?, AMF, Novembre 2018

Sur les 15 projets d'ICO menés à leur terme dont l'AMF a eu à connaître, tous les *tokens* sont échangés sur un marché secondaire, 8 projets étant listés sur deux plateformes ou plus.

71.- Réglementation du marché secondaire. Le législateur s'est montré ambitieux et a réglementé le marché secondaire des crypto-actifs (dits « actifs numériques »). Un statut de prestataire de service sur actifs numériques (PSAN) est ainsi créé.

Les actifs numériques désignant les jetons émis ainsi que les cryptomonnaies[177] de ce que l'on croit comprendre de la périphrase « *toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange…* ».

Sont désormais listés les services sur actifs numériques[178] qui comprennent notamment « le service de conservation pour le compte de tiers d'actifs numériques ou d'accès à des actifs numériques » (1°) « le service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal » (2°) ou « contre d'autres actifs numériques » (3°) ainsi que « l'exploitation d'une plateforme de négociation d'actifs numérique (4°-».

Un enregistrement est obligatoire[179] pour les prestataires mentionnés aux 1° et 2°, sous condition d'honorabilité et de compétence des dirigeants et actionnaires ainsi que l'existence et la mise en place de procédure de lutte contre le blanchiment[180].

L'agrément est optionnel dans les autres cas, le prestataire doit alors disposer en permanence d'une assurance responsabilité civile professionnelle, d'un dispositif de sécurité et de contrôle interne adéquat, d'un système informatique résilient et sécurisé (au besoin l'AMF pourra solliciter l'avis de l'ANSSI), ainsi que d'un système de gestion des conflits d'intérêts.

---

[177] Article L.54-10-1 nouveau du Code monétaire et financier
[178] Article L.54-10-2 nouveau du Code monétaire et financier
[179] Article L.54-10-4 nouveau du Code monétaire et financier
[180] Article L.54-10-3 nouveau du Code monétaire et financier

Les prestataires sont soumis à des obligations[181] : conclure avec les clients une convention définissant leurs missions et responsabilité ; établir une politique de conservation ; ségréguer les détentions pour le compte de leurs clients de leurs propres détentions ; s'abstenir de faire usage des actifs numériques ou des clés cryptographiques conservés pour le compte de leurs clients, sauf consentement exprès et préalable de ces derniers. Les prestataires fournissant un service d'achat/revente d'actifs numériques (2° et 3°) sont soumis à des obligations spécifiques : publier un prix ferme des actifs numériques, ou une méthode de détermination ; publier les volumes et les prix des transactions effectuées ; exécuter les ordres des clients aux prix affichés au moment de leur réception.

[181] Article L.54-10-5 II- nouveau du Code monétaire et financier

TITRE 2 : Les infractions liées aux crypto-actifs

Si les crypto-actifs ne sont pas intrinsèquement constitutifs d'infractions, l'on peut, après avoir observé empiriquement l'ensemble des infraction impliquant des crypto-actifs, dresser une typologie pour constater que les crypto-actifs sont tantôt objets d'infractions en ce qu'ils sont la cible de la commission de telles infractions (Chapitre 1) et tantôt supports d'infractions en ce qu'ils les facilitent (Chapitre 2).

Chapitre I – Les crypto-actifs, objets d'infractions

Les crypto-actifs ont une valeur patrimoniale et suscitent ainsi la convoitise, l'appât du gain conduisant à la commission d'infractions - selon un mode opératoire renouvelé - telles que le vol (section 1), l'extorsion (section 2) et l'escroquerie (section 3).

Section 1 : Le vol

Le vol est une infraction de droit commun, « *la forme la plus fruste de l'appropriation du bien d'autrui* ».[182] Néanmoins, il suscite l'interrogation notamment s'agissant de l'objet sur lequel il porte, un bien meuble incorporel et du mode de commission selon lequel il s'opère.

72.- Elément légal. L'article 311-1 du Code pénal dispose que : « *Le vol est la soustraction frauduleuse de la chose d'autrui.* ».

73.- Soustraction frauduleuse. Initialement envisagée comme matérielle, c'est à dire comme une appréhension physique de la chose, la notion de soustraction s'est élargie pour prendre une conception plus juridique, c'est à dire le fait de se comporter à l'égard du bien comme le véritable propriétaire.[183]

---

[182] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.12

[183] *Ibid.*

La soustraction doit encore être frauduleuse, l'infraction est donc intentionnelle et les mobiles indifférents, étant précisé que le vol étant une infraction instantannée ces éléments doivent être réunis au même moment.[184]

74.- Chose d'autrui. Le vol doit porter sur une chose mobilière appartenant à autrui. La notion d'autrui ne pose guère de difficultés, précisons qu'il importe peu que la personne du propriétaire soit identifiée, il suffit que le bien n'appartienne pas à celui qui soustrait.[185]
S'agissant des crypto-actifs, donc de biens meubles incorporels, il faut distinguer.

Informations avec support. Tout d'abord, une distinction est faite entre le support et les informations[186] il est ainsi possible que le titulaire d'un portefeuille de crypto-actifs (*wallet*) soit victime d'un vol. Le portefeuille pourra prendre des supports divers : disque dur, clé USB ou encore un portefeuille physique dédié tels que ceux conçus par Ledger.

Par analogie avec une jurisprudence en matière de vol de disquettes informatiques[187] l'on peut estimer que la soustraction frauduleuse d'un support quelconque, contenant le portefeuille, c'est à dire la clé privée et stockant des crypto-actifs d'un détenteur constituera l'infraction de vol.

Informations sans support. S'agissant en revanche de cette branche de l'alternative, qui impliquerait une soustraction frauduleuse du seul contenu informationnel, donc de la clé privée permettant d'accéder aux crypto-actifs ou directement à ces derniers la solution est plus nuancée. En principe, une information ne saurait être susceptible de vol. Néanmoins, une jurisprudence récente de la Cour de cassation[188] ne trouve rien à redire à la qualification de vol par les juges du fond s'agissant de « *données utilisées sans le consentement de leur propriétaire* ». La doctrine relève que « *si une information peut faire l'objet d'une*

---

184 *Ibid. p.13*
185 Cass.crim., 11 mars 1942 : Bull. crim. 1942, n°23 ; Cass.crim., 23 octobre 1980 : Bull. crim. 1980, n°271.
186 (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.20
187 Cass.crim., 12 janv. 1989 : Bull. crim. 1989, n°14 ; Cass.crim., 24 avr. 2001 : Bull. crim. 2001, n°98.
188 Cass.crim., 20 mai 2015, n°14-81.336

appropriation frauduleuse, elle ne peut cependant résulter d'une soustraction puisque le propriétaire n'en est en rien dépossédé »[189].
Néanmoins, s'agissant de crypto-actifs, tant les clés privées, permettant l'accès au portefeuille et l'appropriation des crypto-actifs, que les crypto-actifs eux-mêmes, comme le bitcoin ne sont que des informations et l'on peut estimer que le propriétaire en est dépossédé lorsqu'un tiers transfert ces crypto-actifs, la transaction étant en principe irréversible car inscrite sur la chaîne de blocs.

En cette matère particulière qui est celle des crypto-actifs, et en raison de l'environnement numérique dans lequel elle s'inscrit intrinsèquement, la qualification classique du vol est toutefois peu pertinente. En effet, la majorité des appropriations frauduleuses ne sont pas celles de supports physiques contenant des crypto-actifs, mais d'atteintes aux systèmes de traitement automatisés des données (ci-après « STAD »), des détenteurs, mais plus encore des plateformes d'échanges. Ce que l'on appelle donc communément « vol » dans le langage courant, pour désigner ces attaques sera juridiquement qualifié d'atteintes aux STAD, nous faisant entrer dans le domaine de la cybercriminalité

75.- Infractions contre les STAD. Un droit pénal spécial a donc émergé, avec une loi du 5 janvier 1988 (dite loi Godfrain) pour pallier les insuffisances du droit commun des atteintes contre les biens, étant précisé que leur cumul avec les infractions de droit commun est possible[190].

L'existence d'un système de traitement automatisé de données est donc une condition préalable à l'application de cette législation spécifique, aucune définition n'est pourtant prescrite. A titre indicatif, il est d'usage de se référer aux travaux préparatoires et notamment à la définition qu'en a donnée M. Thyrand, rapporteur au Sénat : « *Tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes entrées-sorties et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par un dispositif de sécurité* ». L'exigence d'un dispositif de sécurité restreignant le

[189] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.19
[190] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p. 269

champ de la notion, ainsi que le relève la doctrine, ne figure pas pas dans la loi, elle est par suite heureusement écartée en jurisprudence, qui en fait une interprétation large.

76.- Accès ou maintien frauduleux. L'article 323-1 du Code pénal prohibe : « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* ».

C'est l'infraction idoine pour lutter contre ce qu'il est convenu d'appeler piratage informatique ou *hack*. Elle vise l'atteinte à l'intégrité du système lui même, indépendamment de tout préjudice ou de tout résultat sur les données contenues dans ce STAD[191].
L'incrimination a un champ très large puisqu'elle vise des atteintes commises à l'égard de « *tout ou partie* » du STAD et qu'ainsi qu'il a été précédemment mentionné, les juges n'exigent pas que ce dernier soit sécurisé[192].

Accès. La jurisprudence interprète largement la notion pour inclure tous les modes de pénétrations irrégulières, directes ou indirectes, sur la machine même ou à distance[193].
Maintien. La distinction avec l'accès est opportune et permet d'appréhender une multitude de comportements, les deux qualifications étant indépendantes l'une de l'autre[194]. Ainsi, « *lorsque l'accès a été régulier, le maintien sur un STAD peut devenir frauduleux, lorsque, par une sorte d'interversion de titre, l'auteur du maintien se trouve privé de toute habilitation* »[195]. La doctrine est partagée s'agissant du cumul de l'accès et du maintien frauduleux ou de l'incompatibilité entre ces deux qualifications[196]. Il conviendrait de procéder à une analyse au cas par cas, selon que des faits distincts caractériseraient un

---

191 (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.271
192 CA Paris, 11e ch., 5 avr. 1994 : JurisData n°1994-021093, la jurisprudence est néanmoins parfois en sens inverse, par exemple, pour relaxer un prévenu d'accès frauduleux en ce que ce dernier « lui a en fait été permis en raison d'une défaillance technique concernant l'identification existant dans le système, défaillance reconnue par l'Agence nationale de sécurité sanitaire et de l'alimentation, de l'environnement et du travail » CA Paris, pôle 4, ch. 10, 5 févr. 2014. Néanmoins, dans cette affaire le prévenu a été déclaré coupable de maintien frauduleux. La succession de ces deux éléments, souvent indissociable se révélant alors très efficace.
193 CA Paris, 11e ch. corr. 5 avr. 1994
194 (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.275
195 CA Paris, 11e ch. corr. 5 avr. 1994
196 les juges du fond n'entreraient apparemment pas dans ces subtilités pour retenir le cumul v. CA Toulouse, 3e ch. corr. 21 janv. 1999 : JurisData n° 1999-040054 ; CA Paris, 9e ch., sect. A, 6 déc. 2000 : JurisData N°2000-134502.

comportement actif, « l'interversion de titre » nécessaire pour retenir le maintien, distincts du maintien « purement passif » (J. Devèze).

Frauduleux. Pour être constituée, l'infraction requiert que l'accès ou le maintien soit frauduleux, c'est à dire sans autorisation[197], le caractère irrégulier de l'accès ou du maintien découle alors du non respect des « règles du jeu » qu'elles procèdent de la loi, du contrat ou de la volonté du « maître du système »[198]. L'auteur de l'accès et/ou du maintien doit avoir conscience de cette irrégularité[199]. Une intéressante précision a été apportée, s'agissant des mobiles indifférents au caractère frauduleux, à l'accès ou au maintien opéré par goût du challenge technique, pratique fréquente dans le milieu de la sécurité informatique[200].
Le vol est désormais consacré, par au moins deux moyens, au travers de la législation réprimant les atteintes aux STAD : d'une part, l'accès ou le maintien frauduleux, lorsqu'il en est « *résulté soit la suppression ou la modification de données contenues dans le système* » est puni plus sévèrement (trois ans d'emprisonnement et 100 000 euros d'amende), d'autre part, l'article 323-3 du Code pénal réprime « *le fait d'extraire, détenir, reproduire, transmettre, supprimer ou modifier frauduleusement les données* » d'un STAD, qu'il réprime de cinq ans d'emprisonnement et de 150 000 euros d'amende. C'est donc, indirectement, le vol de données qui est désormais réprimé et plus sévèrement puni que le vol de droit commun.

77.- L'affaire Mt. Gox. Mt.Gox a été créé par Jed McCaleb de manière très rapide et insouciante, ce dernier, prenant conscience des risques réglementaires et du manque de réglementation à l'époque décide de vendre la plateforme à Mark (Robert) Karpelès (encore appelé Magical Tux). La croissance est au rapidement au rendez-vous au point que M. Karpelès est dénommé « baron du Bitcoin ».
M. Karpelès avait déjà été condamné pour piratage en France, il lui était reproché d'avoir détourné des données clients d'un précédent employeur en les redirigeant vers un nom de domaine qui lui appartenait. Il est présenté comme informaticien doué, mais peu doué relationnellement, autodidacte, intéressé par le code, la sécurité informatique, le piratage. Un jour l'un de ses clients propose de le rémunérer en bitcoins, Mark Karpelès a d'abord un intérêt apparent pour la technologie, il rachète en 2011 Mt Gox, qui est à ce moment une

---

197 CA Toulouse, 3e ch., 21 janv. 1999 : JurisData n° 1999-040054
198 CA Paris, 11e ch. corr. 5 avr. 1994
199 CA Paris, 15 déc. 1990 ; JurisData n°1999-106710
200 CA Paris, 12e ch., sect. B, 2 avr. 2004 : JurisData n°2004-252523

plateforme de vente de carte à collectionner, et la fait évoluer en une plateforme d'échange de bitcoins. Le fondateur, dirigeant est en même temps impliqué dans la sécurité du système et subi des attaques informatiques régulières, le 19 juin 2011, 400 000 bitcoins (9millions de dollars), sont détournés, la plateforme est bloquée et l'on reproche au dirigeant sa mauvaise communication.

Il modifie pourtant le code de la plateforme pour en corriger les bugs, et procède à un transfert en bitcoins pour prouver sa solvabilité, qui réalise à ce moment entre 70 et 80% des échanges mondiaux et compte 127 000 utilisateurs. Le 6 février 2014 la plateforme ferme, les dépôts et retraits sont gelés, aucune communication n'est fournie.
850 000 bitcoins disparaissent, équivalent de 500 millions de dollars de l'époque le fondateur est alors accusé d'avoir lui même subtilisé les crypto-actifs. Il aurait plus tard recouvré un quart des bitcoins.

Opérant depuis le Japon, M. Karpelès risquait 5 ans d'emprisonnement, pour avoir falsifié les données de la plateforme en 2013 pour y créer un million de dollars, puis pour avoir détourné les fonds de ses clients[201]. Il est d'abord laissé en liberté, il coopère puis est arrêté le 1er août 2015, il est libéré en juillet 2016 en échange d'une caution de 85.000 euros. L'affaire a récemment connu un premier dénouement lors du jugement du fondateur de Mt. Gox, condamné à deux ans et demi de prison, avec sursis, pour manipulation de données informatiques, ce qu'il aurait fait pour dissimuler les vols résultant d'attaques informatiques et abus de confiance, ayant détourné des fonds pour couvrir certains de ses frais personnels[202].
L'auteur plus probable du vol serait un cybercriminel d'origine russe, Alexander Vinnik, arrêté en Grèce en juillet 2017, il aurait blanchi 300 000 bitcoins issus de l'attaque de Mt.Gox[203] via sa plateforme (BTC-e), mais pourrait n'être qu'un blanchisseur, il devait être extradé en France pour être jugé[204] sur fond de tension politique avec la Russie et les Etats-Unis.

---

[201] « Bitcoin : le Français Mark Karpelès mis en examen au Japon pour détournement de fonds », Le Monde avec AFP, 11 septembre 2015.
[202] « Former Mt.Gox CEO Mark Karpeles Gets Suspended Jail Term », Bloomberg, Y. Furukawa, 15 mars 2019.
[203] « Bitcoin : le mystérieux Alexander Vinnik », N. Ait-Kacimi, Les Echos, 27 juillet 2018.
[204] « Bitcoin : les secrets d'Alexander Vinnik », A. Vidalie, L'Express, 11 décembre 2018.

78.- Attaques diverses et vulnérabilité des plateformes d'échange. Les vols de bitcoins sont le plus souvent la conséquence d'attaques de plateformes d'échange. NiceHash a ainsi vu 4700 bitcoins lui échapper en 2017,[205] de même que Bitfinex a perdu environ 120 000 bitcoins en 2016[206], il en est de même pour Bitstamp, où plus de 18 000 bitcoins ont été dérobés en 2015[207]. Très récemment, en mai 2019, c'est la plateforme d'échange Binance qui s'est faite dérober 7000 bitcoins[208]. Ces attaques témoignent de la régularité du phénomène et de l'ampleur des montants en jeu, bien que de moindre ampleur en comparaison avec l'attaque de Mt. Gox. Ces dernières, toutes postérieures, sont récurrentes et concernent des plateformes d'échange, ce qui n'est pas anodin.Une plateforme d'échange, Komodo, s'est auto-hackée, le 5 juin 2019, pour empêcher les pirates d'accéder aux fonds des utilisateurs, évitant un vol qui aurait pu se monter à 13 millions de dollars[209].

Comme exposé dans la première partie, l'idée même de la blockchain et des crypto-actifs est d'être fondée sur un réseau décentralisé, assurant la sécurité de la technologie. Or, en opérant le mouvement inverse, de centralisation entre les mains d'une plateforme, les risques sont accrus. La technologie blockchain n'est alors plus en cause et seules font l'objet d'attaques les plateformes, dont la sécurité est bien plus vulnérable.

79.- Recours des victimes. En principe, une transaction effectuée sur la blockchain est irrévocable, il s'agit de l'une des caractéristiques essentielles de cette technologie. Ainsi, les bitcoins volés, comme les bitcoins perdus (perte de la clé privée, comme le cas QuadrigaCX évoqué en introduction) sont perdus à tout jamais. Seul un *rollback*, une modification de la chaîne de blocs, afin de « revenir en arrière » litéralement, avant la transaction contestée comme ce fût le cas pour Ethereum après l'attaque de TheDao évoquée précédemment, peut permettre d'en annuler les effets. Une telle modification de la chaîne de blocs ne fait jamais l'unanimité, déjà pour Ethereum, la communauté s'est déchirée et la scission (*hard fork*) est encore visible aujourd'hui entre Ethereum Classic et Ethereum.

---

[205] « Hackers Steal More Than $70 Million in Bitcoin », S. Russolillo, The Wall Street Journal, 7 décembre 2017.
[206] « Bitcoin worth $72 mllion stolen from Bitfinex exchange in Honk Kong », C. Baldwin, Reuters, 3 août 2016.
[207] « Details of $5 Million Bitstamp Hack Revealed », S. Higgins, Coindesk, 1er juillet 2015.
[208] « Hackers Steal $40M Worth of Bitcoin From Binance Exchange », E. Lam, Bloomberg, 8 mai 2019.
[209] « *Komodo Hacks Itself and Saves Crypto Worth $13M After Learning of Security Vulnerability* », T. Simms, CoinTelegraph, 6 juin 2019.

Le dirigeant de la plateforme Binance avait laissé entendre qu'il envisageait un tel *rollback*[210] *en* procédant à une attaque des 51%, s'attirant les foudres de la communauté Bitcoin, car en contrariété avec la philosophie même de la technologie blockchain, de la décentralisation et du montant perdu ($ 40 millions) ne justifiant pas une telle manœuvre. En effet, que serait Bitcoin et la décentralisation si le dirigeant d'une plateforme d'échange pouvait, presque à sa guise, provoquer un retour en arrière de la blockchain, réorganisant ainsi les transactions ? Cela ruinerait la crédibilité de toute une technologie et aurait des effets désastreux en termes de sécurité pour les opérateurs.

De nombreuses plateformes ne survivent pas à des attaques d'une telle ampleur, Mt. Gox fait l'objet d'une procédure de liquidation depuis avril 2014. Récemment, Cryptopia une autre plateforme d'échange est placée en liquidation après avoir été l'objet d'une attaque lui substilisant l'équivalent de $ 16 millions en janvier 2019[211].

Dans le cas Mt. Gox, au 20 mars 2019, les fonds n'ont toujours pas été récupérés, une procédure de désintéressement des créanciers est en cours. En juin 2018, un tribunal de Tokyo a jugé que les clients devaient être remboursés du montant des crypto-actifs détenus et non de leur équivalent en monnaie fiat au jour de l'attaque. La plateforme détiendrait l'équivalent d'environ 630 millions de dollars, le *Rehabilitation Trustee*, chargé du désintéressement des créanciers ayant approuvé des demandes pour un équivalent d'environ 800 000 bitcoins, soit l'équivalent de plus de 3 milliards de dollars[212].
Binance, par l'intermédiaire de son dirigeant, Changpeng Zhao (« CZ ») a annoncé qu'aucun client ne subirait les pertes de cette attaque, dont les conséquences seraient prises en charge par un fonds, le SAFU (*Secure Asset Fund for Users*) auquel la plateforme dote 10% des frais qu'elle perçoit et les place dans un *cold wallet* pour fournir un système d'assurance en cas de crise. Les utilisateurs seront donc en quelque sorte indemnisés par la plateforme elle-même et ses fonds propres, plus prévoyant que Mt.Gox, qui a servi de leçon mythique à beaucoup et est encore présente dans les esprits. Les opérateurs peuvent donc se doter de mécanismes d'assurance indépendamment d'une législation les y obligeant a priori.

---

[210] « *Binance Considered Pushing for Bitcoin 'Rollback' Following $40 Million Hack* », W. Zhao, Coindesk, 8 mai 2019.
[211] « *RIP: Bitcoin Exchange Cryptopia Begins Liquidation After $15 Million Hacking* », M. Emem, CCN, 15 mai 2019.
[212] https://www.mtgox.com/img/pdf/20190320_report.pdf (en anglais à partir de la p.10)

80.- Atteinte au fonctionnement du système. L'article L.323-2 du Code pénal prohibe : « *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données* ».

Précisons que l'infraction d'atteinte au fonctionnement du système est indépendante de l'accès et/ou du maintien dans le système. Il est ici question non « *des atteintes physiques aux composantes matérielles du système, mais des atteintes logiques aux programmes et aux fichiers qui lui permettent de traiter l'information.*[213] ».

L'entrave suppose un acte positif[214] qui peut résulter de l'introduction d'un virus informatique dans le système,[215] pour que l'infraction soit constituée il faut que le fonctionnement du système soit empêché ou fortement ralenti[216]. Le délit d'entrave au fonctionnement du système est un délit intentionnel.

81.- Cryptojacking. Le cryptojacking consiste à utiliser la puissance d'un ordinateur, à l'insu de son propriétaire, pour miner des cryptomonnaies. Le plus souvent, il n'y a pas d'intrusion, donc d'accès ou du maintien dans le STAD. La création de cryptomonnaies, *ex nihilo* par le minage devient en effet de plus en plus difficile, notamment s'agissant du bitcoin et nécessite désormais des moyens professionnels, coûteux et énergivores. Le cybercriminel dispose de deux techniques courantes, il pourra ainsi injecter du code javascript permettant de faire fonctionner un programme minant des cryptomonnaies via le navigateur (*browser-based*) ou bien via un malware (*binary-based*) (accès et maintien frauduleux).
S'agissant de la première, il s'agit de miner des cryptomonnaies lors du lancement d'une page internet par l'exécution de code Javascript. Il est ainsi impossible de dire qu'une page web est compromise et difficile de remarquer un impact sur les performances de la machine, l'utilisateur ne remarquera donc rien la plupart du temps. Un service, Coinhive, permettant de miner des Monero en consultant des pages internet via un script intégré dans ces pages a même été lancé. Se présentant comme une solution alternative ingénieuse à la publicité pour financer des sociétés exploitant des sites internets (ex. The Pirate Bay, site de téléchargement de fichiers de pair-à-pair) lorsqu'il est injecté à l'insu des propriétaires de la page et exécuté à

---

213 Rapp. Hyest, Rapp. sur le Code pénal : Doc. AN n°2468, p. 112
214 CA Poitiers, ch. acc., 20 janvier 1988 : JurisData n°1988-049319
215 CA Paris, 15 mars 1994 : JurisData n°1994-020887
216 CA Paris, 5 avril 1994 : JurisData n°1994-021093

l'insu des utilisateurs, il présente un caractère frauduleux. Le service, bien que prélevant 30% des montants minés, a été fermé le 8 mars 2019, en raison notamment de la baisse des cours des cryptomonnaies, et du fork de Monero ayant conduit à la baisse du taux de hachage.

S'agissant de la seconde, il pourra par exemple s'agir d'un fichier (*malware*), se présentant sous forme de vidéo, reçue via les réseaux sociaux, qui une fois lancée, installera une extension sur le navigateur internet et propagera le fichier auprès des contacts de la cible, pour ensuite miner des cryptomonnaies, comme ce fut le cas pour Digmine, diffusé via Facebook[217]. Pour rendre l'attaque plus massive, le cybercriminel constituera un *botnet*, un réseau constitué d'un grand nombre d'ordinateurs infectés, sous son contrôle distant.
En 2017, le *malware* Adylkuzz, utilisant la même faille de sécurité Windows que WannaCry, développée *infra*. Il empêche que ce dernier vienne le concurrencer, pour exploiter la même vulnérabilité, de manière habile. Il a été utilisé pour miner des cryptomonnaies à l'insu des propriétaires, détecté par la start-up française Cyber-Detect, il aurait permis de créer l'équivalent d'un million de dollars en Monero au profit des cybercriminels en obtenant de ce que le réseau de machines infectées par eux travaillent à miner gratuitement pour leur compte.
Précisons que les deux techniques peuvent être combinées. Selon une étude de la société spécialisée dans les logiciels antivirus Symantec, un botnet regroupant 100 000 machines et procédant à du cryptojacking peut rapporter jusqu'à 30 000 dollars par mois en utilisant les navigateurs internet et jusqu'à 750 000 dollars sur la même période en utilisant des *malware*[218]. Le Monero (XMR) serait la cryptomonnaies la plus visée, elle présente des caractéristiques d'anonymat renforcées comme nous le verrons plus tard. Une étude démontre en effet que près de 4,3% des Monero en circulation auraient été miné par des cybercriminels[219] permettant d'engranger jusqu'à 56 millions de dollars.

La qualification juridique du cryptojacking est intéressante, elle relèverait dans le langage commun du vol de cryptomonnaies, avec la difficulté déjà mentionnée de la nature immatérielle de ces dernières, mais au demeurant, elle ne sont pas formellement volées puisqu'elles sont minées et donc créées à l'occasion de l'attaque elle même.

---

[217] « *Les malwares qui se propagent sur Facebook ont un nouveau jouet : les cryptomonnaies* », J. Cadot, Numerama, 30 décembre 2017.
[218] « *Beapy : Cryptojacking Worm Hits Enterprises in China* », Symantec, 24 avril 2019.
[219] « *A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth* » , S. Pastrana, G. Suarez-Tangil, https://arxiv.org/pdf/1901.00846.pdf

L'on songe au vol d'énergie, assimilé au vol par l'effet de la loi[220]. Néanmoins, une fois de plus, les qualifications pénales les plus pertinentes semblent être celles relatives au système de traitement automatisée de données. Plus particulièrement, s'agissant du procédé exploitant un script sur le navigateur internet de la cible, l'entrave au fonctionnement du STAD (article 323-2 du Code pénal) en ce que c'est non seulement, l'énergie, qui n'est au demeurant pas formellement soustraite, mais détournée, avec les programmes de l'ordinateur et la puissance de son processeur pour miner des cryptomonnaies, ralentissant à minima ses performances, voire dégradant à terme les composants.

L'atteinte au fonctionnement du système est punie de cinq ans d'emprisonnement et 150 000 euros d'amende[221]. La tentative, comme pour les autres délits d'atteintes aux STAD, est incriminée[222]. Le second alinéa prévoit une circonstance aggravante, lorsque l'infraction est : « *commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende* ». L'hypothèse, s'agissant par exemple du cryptojacking n'est pas théorique, qu'il s'agisse éventuellement d'agents minant des cryptomonnaies durant leur temps de travail[223] ou de manière plus large, de leur consultation de pages internet exécutant un script pour y parvenir.

S'agissant du procédé basé sur un programme malveillant (*malware*), l'accès et le maintien frauduleux (article 323-1 du Code pénal) pourrait également être appliqué, avec la circonstance aggravante, mentionnée à l'alinéa 2, prenant en compte le résultat « *altération du fonctionnement du système* » et portant la peine à trois ans (au lieu de deux ans) et 100 000 euros d'amende (au lieu de 60 000).
La technique du cryptojacking, populaire car peu coûteuse, relativement peu sophistiquée, discrète et offrant des retours sur investissement importants devrait prendre encore plus d'ampleur.

---

[220] C. pén. art. 311-2 disposant que la soustraction frauduleuse d'énergie au préjudice d'aurui est assimilée au vol.
[221] C. pén. art. 323-2 ; la sévérité des peines ayant été sensiblement renforcée, comme le note la doctrne d'abord par la loi n°2004-575 du 21 juin 2004 puis la loi n°2012-410 du 27 mars 2012 et en dernier lieu par la loi n°2015-912 du 24 juillet 2015.
[222] C.pén., art. 323-7
[223] « *Australian Government Employee Charged With Mining Crypto at Work* », Y. Khatri, Coindesk, 21 mai 2019.

82.- SIM swapping. Le « SIM swapping » ou « SIM hijacking » désigne une technique permettant de dérober des cryptomonnaies en contournant la double authentification. L'authentification à deux facteurs (2FA) est une méthode de sécurisation de plus en plus utilisée, il s'agit de demander, en plus du mot de passe principal, soit un mot de passe supplémentaire, soit un code temporaire, reçu sur le téléphone portable dont l'utilisateur a fourni le numéro lors de son inscription.

L'attaque consiste à obtenir au préalable les coordonnées téléphoniques de la victime puis demander à l'opérateur téléphonique de cette dernière, en se faisant passer pour elle (parfois via des complices en interne)[224], le transfert de la ligne vers une carte SIM que l'attaquant possède. L'attaquant peut dès lors avoir accès aux comptes divers de la victime, email, cloud, mais surtout ceux relatifs aux plateformes d'échanges de crypto-actifs.

En juin 2018, un cybercriminel, Joel Ortiz étudiant de 21 ans aurait ainsi dérobé, avec l'aide de complices, l'équivalent de 7,5 millions de dollars en crypto-actifs, à une quarantaine de victimes, profitant d'une conférence (Consensus) à New York, réunissant le milieu des crypto-actifs, en mai de la même année. Ortiz a été arrêté, notamment en raison du fait que, peu mature, il a trouvé bon d'envoyer des messages à la fille de l'une de ses victimes, pour s'amuser. Les enquêteurs ont demandé à l'opérateur téléphonique de dévoiler la liste des derniers appels, qui a montré que des téléphones de la marque Samsung étaient utilisés, la victime n'utilisant pas de Samsung, il s'agissait bien du pirate. Les télépones ont été identifiés par leur numéros IMEI. Les enquêteurs ont ensuite demandé à Google de rechercher les données liées à ces numéros IMEI, qui étaient associées avec des adresses emails dont une Gmail. Avec une autre demande à Google, les enquêteurs ont pu découvrir les emails, dont l'un contenant la carte d'identité de Ortiz, ainsi que des preuves montrant son intérêt pour le SIM swaping. Une demande aux plateformes d'échange de crypto-actifs (Coinbase, Bittrex, Binance) a montré qu'il a déplacé plus d'un millions de dollars de crypto-actifs sur une courte période.

---

[224] Dont la responsabilité est recherchée, par exemple contre AT&T et T-Mobile.
L'assignation de Michael Terpin résume le rôle joué par l'opérateur mobile dans ce type d'attaque ainsi : « cela revient à ce qu'un hôtel donne à un cambrioleur avec une fausse carte d'identité la clé d'une chambre et la clé d'une autre chambre protégée pour dérober la joaillerie du propriétaire » il réclame 224 millions de dollars ; « U.S. investor sues AT&T for $224 million over loss of cryptocurrency », G. Chavez-Dreyfuss, Reuters, 15 août 2018.

Il a finalement été condamné à 10 ans d'emprisonnement[225]. D'autres arrestations ont suivi, Xzavyez Narvaez, 19 ans en août 2018, ils auraient pour plusieurs, le point commun d'être membres actifs d'un forum (OGusers.com) une place de marché pour vendre des comptes Twitter et Instagram de personnalités connues piratés. En mai 2019, c'est un groupe de neufs cybercriminels connus sous le nom de « The Community » qui a été arrêté pour avoir commis des usurpations d'identité afin de dérober des crypto-actifs par septs attaques de ce type pour un montant de plus de 2,4 millions de dollars, certains membres, employés de l'opérateur téléphonqiue auraient ainsi participé à usurper l'identité des abonnés[226]. Cette attaque est de plus en plus répandue, l'une des victime de ce type d'attaque, Michael Terpin ayant perdu à lui seul l'équivalent de 24 millions de dollars en crypto-actifs en deux fois, en juin 2017 et janvier 2018. Au moment de la rédaction de la présente contribution, M. Terpin a gagné son procès devant la California Superior Court contre Nicholas Truglia, arrêté en novembre 2018, lui octroyant 75,8 millions de dollars en réparatione et dommages intérêts punitifs[227].

83.- Répression. La répression des infractions relatives aux STAD a déjà été précisée s'agissant de leurs applications respectives, précisons que l'article 323-7 du Code pénal dispose que « *La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peine* » et l'article 323-4 du Code pénal incrimine « *la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1* » la réprimant « *des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* » ce qui s'avère redoutablement efficace, la cybercriminalité liée aux crypto-actifs étant souvent le fait de groupement davantage que d'individus isolés.

---

225 « *'TELL YOUR DAD TO GIVE US BITCOIN:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers* », L. Franceschi-Bicchierai, Motherboard, 30 juillet 2018.
« *Cryptocurrency Thief Gets 10 Years in Prison* », Communiqué de presse, County of Santa Clara, Office of the District Attorney, 22 avril 2019. https://www.sccgov.org/sites/da/newsroom/newsreleases/Pages/NRA2019/Ortiz-Sentencing-.aspx

226 « *Nine Individuals Connected to a Hacking Group Charged With Online Identity Theft and Other Related Charges* », 9 mai 2019.

227 « *U.S. investor awarded $75 million in cryptocurrency crime case* », G. Chavez-Dreyfuss, Reuters, 10 mai 2019.

Des solution à ces attaques (cryptojacking) peuvent être trouvées dans des extensions pour les navigateurs interner comme NoCoin, MinerBlock, NoScript, ScripSafe, les bloqueurs de publicités comme AdBlock, installer un antivirus, être vigilant à l'activité de son processeur, et à sa nagivation, la prévention, la sensibilisation.

Par ailleurs, de manière générale, suivre des bonnes pratiques de sécurité telles que le chiffrement des portefeuilles, les portefeuilles hors-ligne, les portefeuilles matériels et les transactions multi-signatures.

Section 2 : L'extorsion

84.- Elément légal. L'article L.312-1 du Code pénal dispose que l'extorsion est « *le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque* ».

85.- Ransomware. Un *ransomware* (rançongiciel) est un programme malveillant procédant au chiffrement du contenu du disque dur d'un ordinateur (fichiers personnels, professionnels…) rendant ces fichiers inacessibles ou bien l'ordinateur inutilisable, sans avoir au préalable payé une rançon, souvent en bitcoins afin de recevoir la clé de déchiffrement. Un compte à rebours est parfois indiqué, menaçant de supprimer définitivement les fichiers, le montant peut le cas échéant augmenter. Les crypto-actifs sont donc l'objet de l'extorsion[228]. L'on peut même s'interroger, comme il a pu légitimement déjà être fait, sur l'existence même de ransomware avant l'apparition des cryptomonnaies et si ces dernières ne sont pas la condition déterminante de leur apparition[229].

L'auteur de l'extorsion fournit une adresse où la victime doit adresser le paiement, au travers le plus souvent d'un site internet hébergé sur le réseau Tor.

La technique du ransomware rentre donc dans la qualification d'extorsion, où l'attaquant obtient un résultat, « des fonds » ou « un bien quelconque » auquel peuvent être assimilés les bitcoins. Ce résultat étant obtenu par la mise en œuvre de moyens, en l'espèce, par une « contrainte », celle de l'indisponibilité du système et/ou des fichiers qui y sont contenus et la menace de ne jamais les récupérer. La contrainte, qui peut être physique ou morale, doit avoir été déterminante de la remise par la victime, cela s'appréciant in concreto[230].

Au surplus, l'extorsion opérée au moyen d'un ransomware sera susceptible de recevoir la qualification d'accès et de maintien dans un STAD, (cf supra) et d'entrave au fonctionnement d'un STAD. Parmi les cas les plus connus de ransomware, l'on peut citer Locky, ou plus récemment et ayant eu des conséquences beaucoup plus massives, Petya (2016), Wannacry, NotPetya ou encore Bad Rabbit (2017).

---

[228] Remarquons qu'outre le phénomène cybercriminel étudié ici, des comportements analogues se sont développés en marge, comme par exemple la demande de rançon de 300 000 euros en bitcoins faute de quoi les produits d'usines agroalimentaires belges (notamment Lavazza t Ferrerià seraient empoisonnées

[229] « *Is Cryptocurrency What Makes Ransomware Possible* ? », A.Levitin, 22 mai 2019

[230] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.33

86.- WannaCry. A titre illustratif, WannaCry aurait touché plus de 200 000 ordinateurs, dans 150 pays, en un week-end, se propageant grâce à une faille de sécurité dans le système d'exploitation Windows (EternalBlue) révélée au public par le groupe de hackers *The Shadow Brokers* visant notamment de nombreuses entreprises, dont des sociétés françaises comme Renault mais également des services gouvernemenaux ou encore des hôpitaux. La rançon est exigée en bitcoins, comprise entre $ 300 et $ 600 après quelques jours si l'utilisateur refuse de payer. Il semble qu'il soit au demeurant incertain qu'un utilisateur retrouve la pleine possession de ses fichiers une fois la rançon payée, c'est pourquoi il est recommandé de ne jamais payer, 174 personnes auraient tout de même payé, l'équivalent de 42 000 euros à ce moment[231]. Un compte twitter recense en temps réel les paiements faits vers les adresses des auteurs de Wannacry,[232] au total seulement 140 000 dollars auraient été extorqués, ce qui est dérisoire compte tenu de l'ampleur de l'attaque et de la criticité de la faille exploitée.

L'attaque WannaCry a impressionné par la vitesse à laquelle elle s'est propagée, mais également par la façon dont elle a été arrêtée. Il s'agit une nouvelle fois, comme souvent dans le milieu de la sécurité informatique, de l'intervention d'un *white hat*[233] bien que son exploit soit au départ, accidentel, comme il l'a lui même avoué[234]. La solution (*kill switch*) a été trouvée le jour même du début de l'attaque. WannaCry se connecte en effet à un nom de domaine (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.) le chercheur enregistre ce nom de domaine pour une dizaine d'euros afin de surveiller sa propagation, mais il s'avère qu'il l'a dans le même temps arrêté[235]. Des solutions sont ensuite trouvées pour déchiffrer le contenu des machines infectées[236]. D'autres ransomware ont ensuite vu le jour, sur le modèle de WannaCry, mais plus sophistiqués, ne comportant notamment plus de *kill switch*, d'interrupteur prévu dans le code pour arrêter la propagation, et plus fonctionnels s'agissant

---

231 « *Ransomware WannaCry : son impressionnant bilan en huit chiffres* », N. lellouche, 01net.com, 10 mai 2017.

232 @actual_ransom

233 Le chercheur opérant sous le pseudonyme MalwareTech, de son vrai nom Marcus Hutchins a plaidé coupable en avril 2019 d'avoir développé et distribué un malware bancaire, Kronos, il a été arrêté par le FBI lors d'une conférenceDef Con réunissant le milieu de la sécurité informatique à Las Vegas en 2017. Les hacker white hat héros d'un jour peuvent donc avoir été black hat à un moment de leur carrière, ce qui montre que tout n'est pas binaire, noir ou plan dans ce milieu, quoi qu'on puisse en penser et qui est fascinant sur le plan criminologique.

234 « *How to Accidentally stop a Global Cyber Attack*s », MalwareTech, 13 mai 2017.

235 « *WannaCry, un an après : un virus trop simple à désactiver* », V. Castro, Cyberguerre (Numerama), 18 décembre 2018.

236 Le français Adrien Guinet met au point Wannakey, deux autres français, Benjamin Delpy et Matthieur Suiche mettent au point WanaKiwi, respectivement applicables à Windows XP et 7, la faille exploitée sur Windows ayant ensuite été patchée, c'est à dire corrigée par Microsoft.

du paiement de la rançon. En effet, WannaCry ne permettait pas d'identifier qui avait payé la rançon, le déchiffrement devait être opéré de façon manuelle par les attaquants, cela revient à une situation où « *un groupe armé capture des otages et demande une rançon, mais tue les otages après que la rançon ait été reçue* »[237]. Ce qui conforte la position consistant à ne jamais payer. A titre indicatif, la société Altran aurait subi un préjudice estimé à 20 millions d'euros suite à une attaque par ransomware, cette dernière aurait pourtant versé plus de 300 bitcoins, sans recevoir la clé de déchiffrement en contrepartie. L'un de ses successeurs, NotPetya étant plus destructeur encore, en ce qu'il ne prévoit ni outil de déchiffrement, ni mécanisme d'arrêt, cette variante, visant purement et simplement la suppression des fichiers est dénommée *wiper*.

A titre de comparaison, le ransomware Ryuk aurait permis d'amasser plus de 700 bitcoins en seulement quelques mois au cours de l'année 2018, soit l'équivalent à ce moment de plus de 3 millions d'euros, en une cinquantaine de transactions seulement, ciblant les grandes entreprises, il s'avère beaucoup plus rentable que ses prédécesseurs[238].

Les ransomware sont une des menaces les plus importantes en termes de cybersécurité et cette tendance devrait se poursuivre. Au moment même de l'écriture de la présente contribution, la ville de Baltimore est victime, depuis plusieurs semaines déjà, d'un ransomware exploitant la même vulnérabilité que celle mise en lumière par WannaCry. La collectivité refusant de payer la rançon (100 000 dollars), une partie des systèmes de la ville est bloquée ; 10 000 ordinateurs auraient déjà été touchés. Ce nouveau cas rappelle que les cibles de cyberattaques peuvent être diverses : particuliers, entreprises, mais également collectivités et la nécessité d'investir en ce sens dans les infrastructures, des bonnes pratiques, la mise à jour des systèmes, l'hygiène informatique et la formation des agents[239]. L'ironie étant, en ce cas particulier que le ransomware se diffuse grâce à une vulnérabilité (EternalBlue) découverte par la NSA (qui se l'est vue dérober par un groupe de hackers, *the Shadow Brokers*), donc

---

237 « *WannaCry, un an après : un virus trop simple à désactiver* », V. Castro, Cyberguerre (Numerama), 18 décembre 2018.

238 « *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware* », A. Hanel, Crowdstrike Blog, 10 janvier 2019.

239 « *Paralysée par un puissant ransomware depuis trois semaines, Baltimore peine à relancer ses sytèmes* », G. huvelin, Cyberguerre (Numerama) ; « *Baltimore ransomware nightmare could last weeks more, with big consequences* », S. Gallagher, Ars Technica, 20 mai 2019.

développée avec des fonds publics et qui a des répercussions sur la vie courante des administrés[240].

Ce cas n'est pas le premier, des hôpitaux (en Angleterre), transporteurs (FedEx) laboratoires pharmaceutiques (Merck) notamment auraient également été touchés par des ransomwares. D'autres villes américaines ont été visées comme Allentown (causan un préjudice estimé à 1 million de dollars), San Antonio, les états et encore plus les villes disposant de moyens moindres, constituent une cible de choix.

87.- Répression. La tentative est incriminée[241], l'extorsion est passible de sept ans d'emprisonnement et de 100 000 euros d'amende[242], il existe des peines complémentaires et des circonstances aggravantes (violence notamment) pouvant le cas échéant changer la nature de l'infraction pour devenir délictuelle, néanmoins, elles nous semblent peu pertinente s'agissant des extorsions de nature cybercriminelles. L'extorsion, commise en bande organisée est punie de vingt ans de réclusion criminelle et de 150 000 euros d'amende[243] cette incrimination pourrait s'avérer pertinente, les ransomware étant rarement développés, distribués et maintenus par une seule personne.

La circonstance que l'infraction ait été commise en bande organisée est également prévue pour les infractions relative aux systèmes de traitements automatisés d'informations, l'article 323-4 du Code pénal disposant que : « *La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1* » et les reprime « *des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* »

88.- Ransomware as a service. Un phénomène est apparu, connu sous l'appellation générale de *Cybercrime As a Service* (CAAS) et plus particulièrement en la matière de *ransomware as a service*. Cette pratique consiste à vendre un *ransomware*, le plus souvent sur des forums spécialisés, notamment sur le *dark web*. Ainsi, la criminologie des cybercriminels change radicalement, ils ne sont plus les développeurs doués, découvrant les vulnérabilités et

---

[240] « *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc* », N. Perlroth et S.shane, The New York Times, 25 mai 2019.
[241] C. pén. art. 312-9
[242] C. pén. art. 312-9
[243] C. pén. art. 312-6

développant les programmes pour les exploiter. Ces derniers mettent leurs compétences à profit pour vendre les programmes, en l'espèce les ransomware ainsi développés, qui seront distribués, maintenu et rentabilisés par d'autres, le plus souvent incapables de les développer eux-mêmes.

A titre d'illustration l'on peut citer Tox, permettant de créer gratuitement un ransomware fonctionnant sur Tor à partir du logiciel, de définir le montant de la rançon, payable en bitcoins (dont le site prendra 20% à titre de commission)[244]. Ainsi, même une personne inexpérimentée peut devenir un cybercriminel, en diffusant un ransomware.

L'article 323-3-1 du Code pénal permet d'appréhender cette pratique prévoyant l'incrimination pour le fait « *sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3* »

Cette infraction est punie des peines prévues pour les infractions auxquelles il est renvoyé ou pour celle la plus sévèrement réprimée.

Un service de déchiffrement a été mis en place en collaboration entre Europol, la police néerlandaise et le service anti-viruse McAfee[245]. En mai 2019, une enquête menée par Propublica et appuyée sur une analyse de la blockchain Bitcoin par Chainalysis a révélé que des sociétés spécialisées dans la récupération de données à destination des entreprises (Monstercloud et Proven Data notamment), paient en réalité en secret les attaquants eux-mêmes, négociant directement avec les cybercriminels, et prenant au passage une commission ce qui encourage la cybercriminalité[246].

---

[244] « *Meet 'Tox' : Ransomware for the Rest of Us* », McAfee Labs, 23 mai 2015. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/
Plus récemment, c'est la plateforme de Ransomware as a Service Satan qui a démocratisé le phénomène

[245] https://www.nomoreransom.org/fr/index.html

[246] « *The Trade Secret Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers* », R. Dudley et J. Kao, 15 mai 2019.

Section 3 : L'escroquerie

89.- Elément légal. L'article 313-1 du Code pénal dispose que **: «** *L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge*. »

L'escroquerie est l'infraction qui relève le mieux de la délinquance astucieuse, « *le délinquant va provoquer la remise de la chose qu'il convoite, en utilisan la ruse, la tromperie, voire le mensonge*[247] ». Il sera par ailleurs, parfois, également question d'abus de confiance, la victime en ce cas remettant au préalable une chose que l'auteur de l'abus détourne à son profit.

L'escroquerie, infraction de commission, nécessite donc une tromperie, déterminant une remise par la victime, ainsi qu'une intention coupable.

S'agissant des escroqueries liées aux crypto-actifs, les moyens frauduleux constituant la tromperie reposeront prncipalement sur l'emploi de manœuvres frauduleuses, voire l'usage d'une fausse qualité. Ces moyens doivent déterminer la victime à remettre une chose, ils doivent donc lui être antérieurs et déterminant de cette remise[248].

S'agissant des manœuvres, elles impliquent un comportement actif de l'escroc. Le simple mensonge est inopérant, il doit être corroboré par des faits extérieurs, des éléments matériels de nature à lui donner force et crédit par exemple : l'élaboration d'une mise en scène, la production d'écrits voire une publicité[249]. La doctrine relève que la Cour de cassation semble retenir une conception de plus en plus minimaliste de ces faits extérieurs[250].

---

[247] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.41

[248] Cass.crim., 11 juill. 1990 : Bull. crim. 1990, n°284 – Cass.crim., 3 déc.1998 : Gaz Pal. 1999, 1, chron. 61.

[249] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.47

[250] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.48 ; cass.crim., 5 mars 2014 n°13-81.780 : JurisData n°2014-00820, 1ère esp. et cass. crim., 19

La doctrine estime encore que le recours à la publicité n'a pas pour effet en principe de donner au mensonge le caractère de manœuvre punissable[251]. Pour être qualifiée de manœuvre la publicité devrait atteindre un seuil d'intensité, permettant de rendre le mensonge crédible et d'abuser d'une victime normalement prudente, selon une appréciation in abstracto[252].

S'agissant désormais de la remise, à laquelles les manœuvres sont nécessairement antérieures puisqu'elles l'ont déterminé. L'objet de la remise (« *fonds, valeurs ou bien quelconque* ») peut ainsi concerner des biens meubles incorporels[253], les crypto-actifs sont donc susceptibles de constituer l'objet de cette remise autant que les monnaies fiats (euros), étant donné qu'ils ont une valeur patrimoniale et sont appropriés.

S'agissant désormais du préjudice, il est un élément constitutif de l'infraction, ce qui ne devrait poser de difficultés s'agissant de la remise de fonds ou de crypto-actifs, qui cause un préjudice patrimonial.

S'agissant enfin de l'intention coupable, conformément à l'article 121-3 du Code pénal disposant qu'il n'y a point de crime ou de délit sans intention de le commettre, l'escroquerie et une infraction intentionnelle, étant précisé que la preuve de cette intention sera souvent confondue avec l'emploi des moyens frauduleux[254].

90.- Plateforme frauduleuse d'investissement en crypto-actifs. Selon l'Autorité des marchés financiers (AMF), 55 millions d'euros de fraudes aux cryptomonnaies ont été déclarées par des particuliers en 2018[255].

---

mars 2014, n°13-82.416 : JurisData n°2014-005289, jugeant que l'infraction d'escroquerie est consomée par le seul fait de publier une annonce en vue d'une vente imaginaire sur internet en donnant des indications de paieement alors que les objets n'ont jamais existé.

[251] Tout au plus pourrait elle ainsi relever de la pratique commerciale trompeuse incriminée par ailleurs aux articles L.121-1 et suiv. C. cons.

[252] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.54

[253] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.56

[254] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.59

[255] Un premier bilan avait été de 31 millions d'euros et 200 sites internet frauduleux, touchant 700 victimes

Ce montant serait en réalité bien plus élevé, la Belgique comptant 5 fois moins d'habitants que la France estimant ce montant à 100 millions d'euros. Il n'y a qu'à se faire une idée en jugeant quelques cas individuels, un retraité marseillais escroqué de 810 000 euros[256], une clermontoise de 200 000 euros[257].

91.- Mode opératoire. La manière de procéder est récurrente : inscription sur une plateforme en apparence professionnelle mais en réalité fictive, l'utilisation d'un numéro de téléphone, des commerciaux décrivant leur activité prétendue de sociétés de courtage (avec parfois même l'argument d'un prétendu agrément).

Est alors demandé un premier investissement, de « test » qui s'avère très souvent en apparence fructueux, l'escroc n'hésite pas à employer de faux documents à l'appui (contrats d'investissement), promettant des rendements importants pour inciter à remettre au pot une somme plus importante.

Il faut par ailleurs signaler le rôle important de la publicité en ligne dans les escroqueries aux crypto-actifs, notamment sur les réseaux sociaux, Facebook ayant interdit les publicités relatives aux cryptomonnaies et *Initial Coin Offerings*, car fréquemment associées à des arnaques. Mark Zuckerberg disait alors vouloir « *étudier les aspects positifs et négatifs de ces technologies afin de les utiliser au mieux dans ses services* » semblant favorable à la décentralisation[258]. Depuis l'annonce de son projet de GlobalCoin, Facebook a décidé d'être plus souple et d'autoriser de nouveau les publicités en lien avec les monnaies virtuelles, mais non concernant les ICO, à condition toutefois de remplir au préalable un formulaire[259].

En France, l'Autorité des marchs financiers (AMF) a elle-même interpellé une influenceuse (Nabilla Benattia) ayant conseillé à ses abonnés sur Snapchat d'investir dans le bitcoin via une plateforme en ligne, promettant que « *même si vous n'y connaissez rien, ça permet de*

---

[256] « *Marseille : Un retraité arnaqué de 810 000 euros avec des Bitcoins* », 20 Minutes, 14 septembre 2018.
[257] « *Cryptomonnaies : une Auvergnate perd toutes ses économies sur un site frauduleux* », E. Trujillo, BFM Business, 4 septembre 2018.
[258] « *Cryptomonnaies : Facebook interdit leur pub pour éviter les arnaques* », A. Cherif, La Tribune, 31 janvier 2018.
« *New Ads Policy: Improving Integrity and Security of Financial Product and Services Ads* », R. Leathern, Product Management Director, Facebook.
[259] « *Demande d'ouverture de produits et services de cryptomonnaies* ». https://www.facebook.com/help/contact/532535307141067

gagner de l'argent sans investir beaucoup », assurant que ses fans peuvent « y aller les yeux fermés » que c'est « vraiment sûr » et « gratuit » et qu'il n'y a « rien à perdre »[260].
Les escrocs emploient des techniques de manipulations mentales (*social engineering*) ayant pour but de metre en confiance la victime par des échanges nombreux, lorsque cette dernière souhaite retirer son investissement, elle éprouvera la plus grande difficulté[261].

Les profils tant des escrocs que des victimes sont bien connus désormais.

D'une part, s'agissant du profil des victimes, il s'agit le plus souvent de personnes peu au fait de la technologie en général, et de la blockchain en particulier, ne connaissant que de loin, par l'entremise des médias généralistes, le fonctionnement et les potentialités, réelles ou prétendues des crypto-actifs, se trouvant dans la plus grande confusion, il s'agit souvent ce de personnes retraitées, vulnérables, ou des personnes cherchant un investissement et attirées par l'appât du gain facile, présenté sans risque.

D'autre part, du côté des auteurs, il s'agit de véritables réseaux, qui ont opéré par le passé des arnaques similaires, portant simplement sur un objet différent (diamants, Forex, terres rares, options binaires) [262] qui ont accumulé des moyens matériels et humains, prenant vraisemblablement la forme de véritables centres d'appels (souvent situés à l'étranger en particulière en Israel et à Chypre), une expérience, un discours commercial[263]. Certains escrocs n'hésitent pas à recontacter les victimes en se faisant passer pour la Banque de France ou l'ACPR en prétendant aider à recouvrer les pertes subies ou rapatrier les sommes escroquées, en demandant de verser au préalable des fonds supplémentaires.

Plus efficace que la répression, en matière d'investissement, et peu importe l'objet de ce dernier donc, la prévention est de mise : méfiance sur des rendements colossaux, compréhension du couple rendement/risque, méfiance s'agissant de profits rapides et garantis, connaissance du produit (le caractère atypique étant source de confusion).

---

[260] « *Bitcoin : le gendarme des marchés tacle Nabilla* », E. Goetz, Les Echos, 10 janvier 2018.
[261] « *Escroqueries liées aux bitcoins : réagissons* ! », S. Lebeau et W. O'Rorke, La Tribune, 17 octobre 2018.
[262] Forex, options binaires, arnaques financières en ligne : l'AMF, le Parquet de Paris, la DGCCRF et l'ACPR se mobilisent, 31mars 2016.
[263] v. M. Quéméner, « *Présentation d'une nouvelle dépêche sur les cyberfraudes par crypto-actifs* », Dalloz IP/IT 2019, p.55, témoignant de la persistance des procédés employés

92.- *Initial Coin Offerings* frauduleuses : Pyramides de Ponzi et *exit scam*. S'agissant des ICO frauduleuses, la publicité sur Internet joue également un rôle déterminant. C'est ainsi que le champion de boxe Floyd Mayweather aurait accepté de faire la promotion de l'ICO de la société Centra, qui a levé 32 millions de dollars en prétendant proposer une carte de débit soutenue par Visa et Mastercard, permettant de convertir les cryptomonnaies en dollars et les dépenser dans les commerces s'est avéré être une fraude[264]. Ce dernier a lui même été inquiété par la SEC ainsi que le producteur de musique DJ Khaled pour ne pas avoir dévoilé avoir été payé pour faire la promotion de l'investissement dans cette ICO (respectivement 100 000 et 50 000 dollars), se prétendant comme eux mêmes personnellement investisseurs F. Mayweather a accepté de restituer (*disgorgement*) 300 000 dollars, de payer 300 000 dollars de pénalités (*penalty*), et ne plus promouvoir de titre financier, digitaux ou non pendant trois ans et à coopérer[265]. Les ICO frauduleuses existent donc, elles ont pour trait commun de ne porter aucun projet, de ne développer aucune technologie. L'on peut les regrouper en deux catégories.

D'une part, l'on peut mentionner les *exit scams* qui consistent collecter l'investissement en monnaie fiat ou en cryptomonnaies et ne pas développer le projet, ou ne pas intégrer le token à la plateforme d'échange (marché secondaire), plus simplement, à « partir avec la caisse ».
D'autre part, l'on peut évoquer les pyramides de Ponzi, hypothèse déjà évoquée (et réfutée) s'agissant de Bitcoin. L'investissement, réservé à un cercle choisi d'investissement, cooptés par le bouche à oreille, sommés d'investir rapidement, mis en confiance par une promesse de rendement importants, et récurrent dont il s'avère qu'il est en réalité purement artificiel[266].

Au début de l'année 2018, à la suite nombreuses ICO qui ont échouées (la moitié mettent la clé sous la porte avant 4 mois) ou bien qui se sont avérées être des escroqueries (environ 20 % en avaient toutes les caractéristiques d'après une étude du Wall Street Journal), la *Securities and Exchange Commission* afin de protéger les investisseurs dans les ICO, a mis en ligne sa propre ICO du *Howeycoins* destiné à la prévention de ce type de pratiques[267] : compte à

---

[264] « Founders of a cryptocurrency backed by Floyd Mayweather charged with fraud by SEC », A. Kharpal, CNBC, 3 avril 2018.
[265] « *Two Celebrities Charged With Unlawfully Touting Coin Offerings* », Communiqué de presse, U.S. Securities and Exchange Commission, 29 novembre 2018.
[266] L'AMF met en garde contre ces arnaques dans le cadre de Epargne Info Service. Par exemple : « *Comment détecter et éviter les arnaques* », le 21 septembre 2017.
[267] Le site internet de l'ICO en question. https://www.howeycoins.com/index.html

rebours, rabais, garantie de rendements élevés, agrément prétendu de la SEC… chaque comportement est expliqué et prévenu.

93.- L'affaire OneCoin. OneCoin serait à l'heure actuelle la plus grande escroquerie liée aux crypto-actifs. Lancé en 2014 à Sofia en Bulgarie, la société, dirigée par Konstantin Ignatov (arrêté en mars 2019) promettait des rendements importants aux investisseurs, avec un risque minime mais s'avère être un système pyramidale où les investisseurs étaient incités à recruter de nouveaux membres. La société ne développant aucun projet blockchain aurait escroqué l'équivalent de 2 milliards d'euros à trois millions de membres dans le monde entier[268]. Comme l'indique Cyrus R. Vance, les accusés ont utilisé un système pyramidal classique (*old-school pyramid scheme*), sur une nouvelle plateforme (*new-school plateform*), rien de plus. Les seuls à bénéficier de l'existence de OneCoin sont les créateurs et complices.

Cela montre bien une fois de plus que les cryptomonnaies, de manière générale ne sont pas en soi une arnaque, mais qu'ils sont simplement un prétexte à la commission d'infractions classique, selon un mode opératoire renouvelé et contingent, qui change au gré de la tendance.

Le OneCoin avait un cours, prétendument basé sur l'offre et la demande, avec une évolution de 0.50 euros à 29,95 euros en janvier 2019, cette dernière étant en réalité fixée en interne, de manière totalement décorrelée du marché. Il ne s'agit pas même d'une cryptomonnaie qui serait minée comme le bitcoin, en utilisant la puissance de calcul, la cryptomonnaies n'étant même pas dotée d'une blockchain. Plus de 400 millions de dollars auraient été blanchis par le biais de compte détenus dans des fonds d'investissement en Irlande et aux Iles Caimans.

MyCoin (société Hong-Kongaise) aurait, quant à elle escroqué 400 millions de dollars à ses clients, sur des promesses de rendements exorbitant et un système de parrainnage[269]

Une autre affaire similaire de système de Ponzi, Bitconnect, lancé en 2016 et promettant des rendements importants, jusqu'à 10% garantis par mois, utilisant un système de parrainage incitatif qui a fermé s'est portes au début de l'année 2018 après des poursuites judiciaires et attaques informatiques par déni de service (DDoS) fait l'objet d'une enquête du FBI, qui procède au recensement des victimes[270].

Ainsi que les mises en garde de la SEC. https://www.investor.gov/howeycoins

[268] « *Manhattan U.S. Attorney Announces Charges Against Leaders Of "OneCoin," A Multibillion-Dollar Pyramid Scheme Involving The Sale Of A Fraudulent Cryptocurrency* », 8 mars 2019.

[269] « *Bitcoin : arnaque à 400 millions de dollars via une chaîne de Ponzi* », La Tribune, 10 février 2015.

[270] « *Seeking Potential Victims in Bitconnect Investigation* », Special Agent Vicki D. Anderson, 20 février 2019

Cette escroquerie porterait sur un montant de 2,5 milliards de dollars. Le 18 mai 2019, il a été annoncé une nouvelle version de BitConnect, qui devrait apparaître dès juillet 2019[271].

94.- Répression. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende, voire de dix ans d'emprisonnement et 1 000 000 d'euros d'amende lorsqu'elle est commise en bande organisée[272]. La tentative d'escroquerie est punissable[273].
L'autorégulation semble ici également pertinente, en complément nécessaire de la répression, par exemple le forum CryptoFR qui recense les faux sites d'investissements (373 à l'heure actuelle[274]), la liste noire des sites identifiée par l'AMF[275]est également pertinente.

La loi Pacte modifie l'article L.222-16-1 du Code de la consommation, avec trois nouveau alinéas : « *Est également interdite toute publicité, directe ou indirecte, diffusée par voie électronique ayant pour objet d'inviter une personne, par le biais d'un formulaire de réponse ou de contact, à demander ou à fournir des informations complémentaires, ou à établir une relation avec l'annonceur, en vue d'obtenir son accord pour la réalisation d'une opération relative à : « a) La fourniture de services sur actifs numériques au sens de l'article L. 54-10-2 du même code, à l'exception de ceux pour la fourniture desquels l'annonceur est agréé dans les conditions prévues à l'article L. 54-10-5 dudit code ; « b) Une offre au public de jetons au sens de l'article L. 552-3 du même code, sauf lorsque l'annonceur a obtenu le visa prévu à l'article L. 552-4 du même code.* »

Avec cette nouvelle disposition, les consommateurs se trouvent davantage protégés s'agissant de publicités pour des contrats conclus à distance portant sur des services financiers, auxquels sont désormais assimilés la fourniture de services sur actifs numérique et l'offre au public de jetons. La sanction, déjà prévue à l'article L.222-16-1du Code de la consommation est une amende administrative, dont le montant ne peut excéder 100 000 euros, a un champ d'application *rationae personae* très large puisqu'elle vise : l'annonceur, l'intermédiaire agissant pour son compte, l'acheteur ou le vendeur d'espace publicitaire et même toute personne diffusant une telle publicité, *in fine*.

---

271 « *BitConnect 2.0 : l'arnaque ultime aux crypto-monnaies renait de ses cendres* », Presse-Citron.net, 20 mai 2019.
272 C. pén. art. 313-2 5°
273 C. pén. art. 313-1
274 https://cryptofr.com/topic/9287/liste-de-sites-frauduleux
275 https://www.amf-france.org/Epargne-Info-Service/Proteger-son-epargne/Listes-noires

Cette interdiction nouvelle ménage une exception pour le PSAN agréé et l'émission de jetons visée par l'AMF,

De manière analogue, par contrecoup, bientôt, la liste des émissions de jetons ayant, elles, obtenu le visa, et des prestataires de services sur actifs numériques (PSAN) devrait renforcer la protection des investisseurs et réduire le nombre d'escroqueries. Une nouvelle infraction pénale spéciale est par ailleurs créée par la loi Pacte, qui insère au sein du Code monétaire et financier un nouvel article L.572-27 disposant qu' « *est puni de six mois d'emprisonnement et de 7 500 € d'amende le fait, pour toute personne procédant à une offre au public de jetons au sens de l'article L. 552-3, de diffuser des informations comportant des indications inexactes ou trompeuses ou d'utiliser une dénomination, une raison sociale, une publicité ou tout autre procédé laissant croire qu'elle a obtenu le visa prévu à l'article L. 552-4* ».
Un article L.572-26 nouveau du même Code vise les mêmes comportements et prévoit les mêmes peines s'agisant de l'agrément des PSAN.

Chapitre II – Les crypto-actifs, supports d'infractions

Les crypto-actifs, lorsqu'ils ne sont pas la cible d'infractions, en favorisent la commission via le dark web (section 1), peuvent contribuer au blanchiment de ces dernières (section 2), leurs cours pouvant en outre faire l'objet de manipulations encore mal appréhendées par la réglementation (section 3).

Section 1 : Crypto-actifs et marchés criminels sur le dark web

95.- Notion de *dark web*. Il est d'usage de distinguer différentes zones d'Internet, en fonction de leur degré d'indexation. L'on distingue ainsi le web traditionnel, le World Wide Web, ou l'Internet dit « en clair », accessible à tout à chacun via un moteur de recherche classique comme Google ; le *deepweb* ou web profond, est le web non indexé, tous les contenus ne peuvent ou ne souhaitent en effet être indexés, les sources sont globalement peu accssibles mais non dissimulées, elles obligent l'internaute à faire des recherches appuyées pour les identifier[276]; enfin le *dark web*, c'est l'internet volontairement dissimulé, accessible via un navigateur spécifique, il indexe du contenu supplémentaire. Par exemple, le navigateur *The Onion Router* (Tor), permet d'accéder à des sites internet dont l'adresse se termine en .onion (I2P, Freenet en sont d'autres).

Origines. Tor est un logiciel gratuit et open-source, à l'origine conçu par et pour l'armée américaine (la DARPA) en 1997.

Utilité. Il permet d'accéder à Internet en passant par un réseau décentralisé de milliers de relais différents, dissimulant la localisation véritable de l'utilisateur et son usge d'une éventuelle surveillance et notamment de l'analyse de traffic. La philosophie à l'origine de ce procédé est une nouvelle fois en grande partie héritée des cypherpunk. « *Bien entendu, l'État essaiera de ralentir ou d'arrêter la diffusion de cette technologie, en invoquant les préoccupations de sécurité nationale, l'utilisation de la technologie par les trafiquants de drogue et les fraudeurs fiscaux, et les craintes de désintégration de la société. Beaucoup de ces préoccupations seront valables; La crypto-anarchie permettra aux secrets nationaux d'être librement échangés et permettra le commerce de matériaux illicites et volés.*

---

[276] « *Darkweb : plongée en eaux troubles* », O. de Maison Rouge, Dalloz IP/IT 2017, p.74.

Un marché informatisé anonyme rendra même possibles des marchés odieux d'assassinats et d'extorsion. Divers éléments criminels et étrangers seront des utilisateurs actifs du CryptoNet. Mais cela n'arrêtera pas la propagation de la crypto-anarchie.[277] »

96.- La technique. Tor est un réseau « superposé » à internet (*overlay network*), c'est donc un réseau sur un réseau, il fonctionne sur l'infrastructure d'internet, sur le principe du « routage en oignon ». L'information sur Internet est représentée par des « paquets », Tor fait rebondir les échanges TCP au sein d'Internet afin de neutraliser les analyses de trafic (source/destinataire).

Le réeau est constitué de serveurs, appelés nœuds (*nodes*), c'est à dire d'ordinateurs d'utilisateurs volontaires, possédant le logiciel et connectés à Internet, qui vont dans un premier temps récupérer la liste des nœuds[278]. Il existe des nœuds d'entrée dans le réseau, des nœuds de sortie et des nœuds intermédiaires, chaque nœuds dispose par ailleurs d'une adresse IP.
Chaque client choisit alors automatiquement et aléatoirement un chemin composé de trois nœuds et construit un circuit. Au lieu de communiquer directement entre l'ordinateur de l'utilisateur et le serveur, les paquets de données suivent une trajectoire plus longue, car intermédiée et aléatoire.

Chaque nœud peut connaître le précédent et le suivant, ainsi le premier connaît l'adresse IP véritable, le second ne la connaît déjà plus, il ne connaît que celle du premier et du troisième qui sera ajouté

Tor fait appel à la cryptographie asymétrique, avec une clé privée et une clé publique dont dispose chaque nœud. L'utilisateur, qui a choisi les nœuds, récupéré leurs clés publiques et créé son paquet, chiffre le paquet avec la clé publique du nœud de sortie, puis du nœud intermédiaire et enfin du nœud d'entrée. Les paquets sont donc chiffrés successivement, à la manière d'un oignon et seront déchiffrés par les nœuds à l'aide de leur clé privée jusqu'à ce qu'ils arrivent au destinataire.

---

277 Timothy C. May, *Le manifeste crypto-anarchiste, 1989*

278 https://torstatus.blutmagie.de

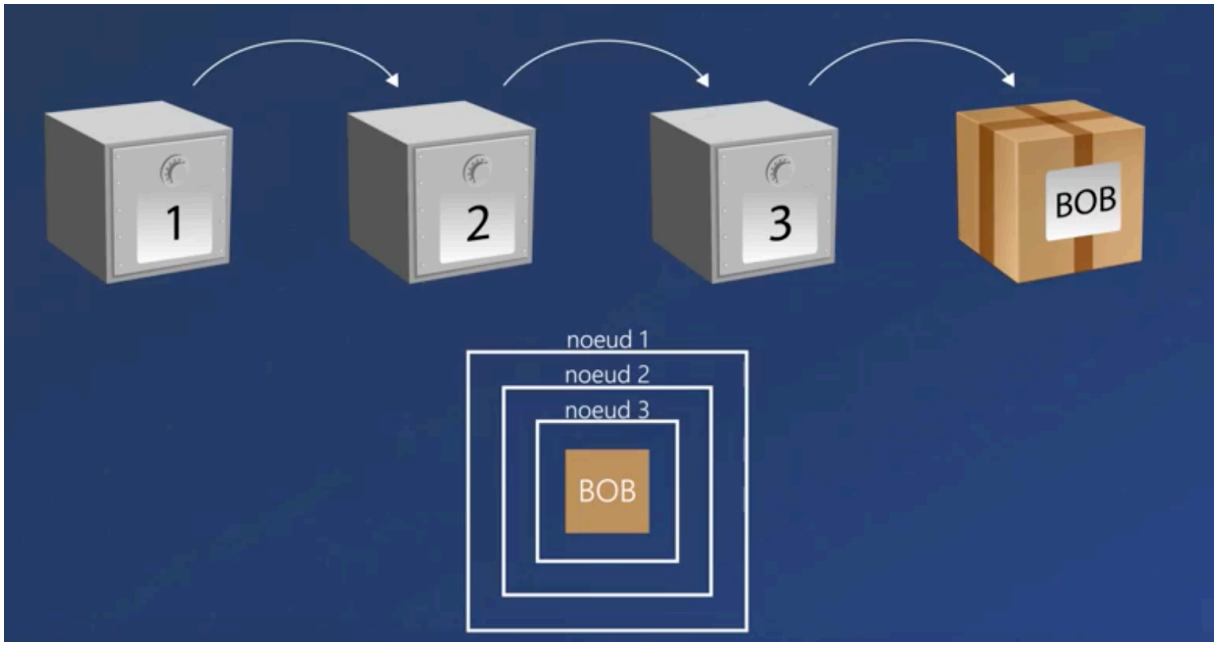


Image provenant de « TOR : the dark WEB – Monsieur Bidouille (YouTube)

Une des forces est que régulièrement, le circuit changera, le client empruntera un nœud d'entrée, intermédiaire et de sortie différent, avec une autre adresse IP. Tor permet donc en principe anonymat, résistance, performance, le grand nombre d'utilisateurs permettant de lutter contre d'éventuels nœuds de sortie espion. Comme pour Bitcoin, plus le réseau, décentralisé, est grand plus, plus il est fiable.

97.- Utilisation légitime. L'utilisation des outils d'accès au *dark web* ne constitue pas en soi une activité interdite. La loi pour la confiance dans l'économie numérique (LCEN) rappelant que l'utilisation de moyens de cryptologie permettant une navigation privée est libre sous réserve de sa déclaration[279]. Surtout depuis les révélations d'Edward Snowden, s'agissant des programmes de surveillance de masse opérés par les agences gouvernementales, et en particulier de la N.S.A. les individus ont pris conscience de l'importance de la protection de leur vie privée en ligne. Les intérêts sont nombreux à recourir à des solutions comme Tor, la navigation dite en « oignon » permet un degré d'anonymat plus important, bien que non absolu ; de plus, dans certains Etats, les journalistes, opposants au pouvoir en place, organisations non gouvernementales, lanceurs d'alertes, peuvent accéder à des sites soumis à des restreictions d'accès, évitent ainsi la censure et communiquent librement des informations et idées.

---

[279] art. 30 et 31 LCEN ; « *Le dark web ou l'internet clandestin et son encadrement juridique* », P.-X. Chomiac de Sas, Revue Lamy Droit de l'Immatériel, n°49, 1er juin 2018.

98.-Utilisation dévoyée. Tor peut être utilisé pour dissimuler des serveurs qui hébergent des sites internet dotés de l'extension .onion (extension réservée au réseau Tor). Le destinataire de la communication souhaite donc être protégé contre la surveillance du réseau.
Le serveur procédera de la même façon que le client, en sens inverse, il créera de son côté également un circuit, en choisissant des nœuds, de manière aléatoire, le client a fait de même les protagonistes se rejoignent au « RP » au point de rendez-vous en quelque sorte. Le RP est également un nœud du réseau, un intermédiaire, un service dit « caché » (*hidden service*) c'est cela qui est communément désigné *dark web*.

Image provenant de « TOR : the dark WEB – Monsieur Bidouille (YouTube)

Il existe donc a minima six nœuds, six adresses IP pour mettre en place une connexion. Tant le client que le serveur ne se connaissent pas mutuellement. La difficulté de localiser l'emplacement véritable du serveur et l'identité de ses administrateur est donc établie.

99.- Importance centrale des crypto-monnaies pour cette économie. Les cryptomonnaies jouent un primordial, indispensable pour les places de marchés du *dark web* (au point que l'on parle parfois de *crypto-markets*). L'intérêt d'utiliser des cryptomonnaies est d'abord, comme tout achat/vente à distance, la certitude de recevoir les fonds.
En effet, il peut être envisagé par l'acheteur l'éventualité d'une transaction en espèce et de le faire parvenir au vendeur par voie postale. Néanmoins, aucune certitude n'existe quant à sa bonne réception par le vendeur ou la mauvaise foi du vendeur. De plus, les transactions en monnaie scripturale, transitant par les établissements bancaires, laissent des traces et sont susceptibles d'éveiller les soupçons, ces établissements étant soumis à un processus de *Know*

Your Customer (KYC) poussé dans le cadre de la lutte contre le blanchiment et le financement du terrorisme (LCB/FT) ainsi que des obligations de vigilance et de déclaration auprès de Tracfin.

Les cryptomonnaies, qui ne peuvent être falsifiées et qui ne dépendent pas d'un organe central pallient donc ces deux risques, monnaies pseudonymes (bitcoin) ou annymes autant que faire se peut (Monero, ZCash…) assurent une plus grande discrétion des échanges.

Par ailleurs, les places de marché les plus importantes mettent en place un système de séquestre des cryptomonnaies (*escrow*) faisant la fonction d'intermédiaire et exécutant la transaction dès lors qu'aucune partie n'est lésée. De plus, les transactions en cryptomonnaies, une fois exécutées sont irréversibles, ce qui garantie la sécurité juridique.

100.- L'affaire Silk Road. Silk Road a été créé par Ross W. Ulbricht, opérant sous le pseudonyme Dread Pirate Roberts (DPR), entre 2011 et 2013. Il s'agit de l'un des premiers cryptomarché, l'on pouvait y trouver des produits stupédiants, des service de piratage, des faux papiers… Le site fait office d'intermédiaire entre acheteurs et vendeurs, moyennant une commission (*escrow*), la résolution des litiges étant confiée aux administrateurs du site.

En deux ans et demi d'existence, Silk Road a permis des transactions pour un volume d'environ 1 milliard de dollars, générant 80 millions de dollars en commissions, ce qui lui vaut le surnom de « e-bay de la drogue ».

Dread Pirate Roberts avait ainsi pour ambition de réaliser l'utopie crypto-archiste, inspiré par les travaux d'économistes libéraux, il est favorable aux échanges entre individus non soumis aux régulations et est hostile à la politique de guerre contre la drogue menée par le gouvernement. Il découvre Bitcoin, qui est également le fruit d'une utopie libertaire, ainsi que Tor, et réalise avec Silk Road cette utopie. Il lui est reproché de s'être engagé les incriminations de trafic de stupéfiants, de blanchiment d'argent, de piratage informatique et d'avoir tenté d'engagé un tueur un gage. L'enquête sur cette affaire est particulièrement intéressante, révélant le manque de coordination des autorités dans le recoupement des diverses failles ou erreurs de Ross Ulbricht. Pêle-mêle, l'infiltration du forum par des agents, notamment de la DEA et l'arrestation d'un administrateur (dont DPR a commandité l'assassinat) ; une vulnérabilité dans la page du site (codé par Ross Ulbricht lui même)

révélant l'adresse l'IP du serveur, exploitée par le FBI[280], ce qui a permis d'exploiter le contenu dudit serveur dont l'historique des connexions, qui a permis de localiser l'endroit d'où se connecte DPR, un café ; l'arrestation d'une administratrice suite à une enquête après l'interception de colis de médicaments à la douane ; la réception par Ross Ulbricht de fausses pièces d'identité et la visite subséquente des autorités à son domicile même ; des messages laissés sur des forums d'Internet en clair, sous un pseudonyme (altoid) faisant la promotion de Silk Road, d'autres sur des forums dédiés au développement et à l'utilisation de Tor, sur des forum spécialisés sur Bitcoin, avec son adresse gmail, dévoilant son nom et prénom… Une surveillance physique et l'infiltration préalable de la bibliothèque d'où se connecte DPR à ce moment aboutit finalement à son arrestation[281]. Le FBI aurait saisi 144 000 bitcoins (soit $ 28,5 millions au cours de l'époque, mais environ 1 milliards de dollars avec un cours approximatif de $ 7000 actuel) et au total, ce serait 174 000 bitcoins[282]. Des incertitudes demeurent, tant sur la réalité des méthodes employées par le FBI, que sur l'organisation de Silk Road, dont au moins une autre personne avait accès au compte administrateur[283].

L'affaire Silk Road est le premier cas de condamnation aux Etats-Unis pour la commission d'infractions sur le dark web. Ross Ulbricht est arrêté le 2 octobre 2013, il a été condamné à l'emprisonnement à vie, cette peine ayant été confirmée en appel[284] et la Cour Suprême des Etats-Unis ayant refusé d'en connaître de nouveau[285]. Très peu de temps après l'arrestation de Ross Ulbricht, Silk Road 2 voyait le jour, mis au point par DPR2 (Thomas White), qui fut arrêté ainsi que Blake Benthal (Defcon) en novembre 2014, et plaida coupable de traffic de drogues, blanchiment d'argent et fut condamné à 5 ans et 4 mois d'emprisonnement. Au cours de cette opération (Onymous) menée en coopération entre le FBI et Europol notamment, 17 personnes ont été arrêtées, les saisies s'élevant à l'équivalent d'un million de dollars en

---

280 Qui simula une connexion au site du côté admin, avec de mauvais identifiants, pour analyser le trafic réseau, observer les adresses qui s'y connectent et l'une attira l'attention, elle ne correspond à aucun nœud du réseau Tor. Le véritable serveur est donc localisé en Islande.

281 « *L'homme le plus connu du Dark Web* », Absol Vidéos, Youtube ; « *Une première condamnation aux USA pour la commission d'infractions sur le Dark Web* », E. Caprioli, communication- commerce électronique, LexisNexis, juillet-août 2017.

282 « *FBI Says It's Seized $28.5 Million In Bitcoin From Ross Ulbricht, Alleged Owner of Silk Road* », A. Greenberg, Forbes, 25 octobre 2013.

283 Six semaines après que Ross Ulbricht fut arrêté, une personne se serait connectée au compte de Dread Pirate Roberts, alors que ce dernier était en détention. « *Someone Accessed Silk Road Operator's Account While Ross Ulbricht Was in Jail* », J. Koebler, Motherboard, 2 décembre 2016.
Cela est probable, Ross Ulbricht lui même ayant laissé courir la théorie qu'il n'était pas le seul à administrer Silk Road.

284 United States of America v. Ulbricht, May 31, 2017, 15-1815-cr

285 « *U.S. Supreme Court turns away Silk Road website founder's appeal* », A. Chung, Reuters, 28 juin 2018.

cryptomonnaies[286]. Les agences ont communiqué sur le fait qu'à elle seule, l'opération aurait permis la fermeture de plus de 400 sites illiites sur le réseau Tor, bien que les chiffres soient contestés, la plupart étant des sites faux. Les méthodes employées par les agences, notamment le FBI, basées sur des travaux académiques de l'Université Carnegie Mellon sont également l'objet de contestation, exploitant une vulnérabilité du réseau Tor pour désanonymiser les utilisateurs en mettant en place des nœuds d'entrée (connaissant l'IP véritable de l'utilisateur) et de sortie du réseau (connaissant le destinataire) et en procédant par corrélation.[287]

101.- Successeurs et efficacité accrue: AlphaBay, Hansa. AlphaBay, lancé en 2014 et réunissant à son apogée 400 000 utilisateurs et 40 000 vendeurs ainsi que Hansa se présentaient comme successeurs de Silk Road. Opérant sur le réseau Tor, ils ont été fermés conjointement lors d'une opération en juillet 2017, menée par les polices néerlandaise, allemande ainsi que le FBI, la DEA et Europol. L'opération, surnommée Bayonet, avait pour objet de fermer dans un premier temps AlphaBay (le 4 juillet), dont le créateur et administrateur, un canadien, résidait en Thailande, où il a été arrêté.

Les clients allaient alors se déporter naturellement vers Hansa, qui était déjà sous la surveillance des autorités, faisant l'objet d'une procédure d'infiltration (*monitoring*) pour en prendre le contrôle de manière furtive jusqu'à ce qu'il soit fermé (le 20 juillet) des serveurs localisés aux Pays-Bas, ainsi qu'en Allemagne et en Lituanie ont été saisis et les administrateurs arrêtés en Allemagne. Durant cette période, entre 1000 et 8000 vendeurs apparaissaient sur Hansa et 27 000 transactions ont eu lieu.

L'enquête, pour ce cas particulier s'avère sophistiquée et redoutablement efficace. La police a dû en outre apporter des modifications au site lui même, pour recueillir les mots de passe (chiffrés) en clair, les communications PGP (chiffrées) en clair, recueillir les métadonnées, et faire télécharger aux clients un fichier permettant de mener à leur réelle adresse IP. C'est ainsi que plus de 10 000 adresses d'acheteurs (situés hors des Pays-Bas) ont été récoltées, ce qui permettra des centaines d'enquêtes partout en Europe[288]. Il s'agit de l'un des opérations les plus sohistiquées de lutte contre la cybercriminalité.

---

[286] « Operation Onymous », Europol, Communiqué de presse

[287] «*Court Docs Show a University Helped FBI Bust Silk Roa 2, Child Porn Suspects* », J. Cox Motherboard, 11 novembre 2015 ; « *Tor security advisory : "relay early" traffic confirmation attack* », Tor Blog, 30 juillet 2014.

[288] « *Massive Blow To Criminal Dark Web Activities After Globally Coordinated Operation* », Europol, Communiqué de presse, 20 juillet 2017.

102.- Non absolutisme de l'anonymat et non impunité. Bien que certaines agences de renseignement, NSA (et GCHQ, son homologue britannique) en tête se soient essayées à attaquer Tor, il apparaît qu'elles n'y soient pas encore parvenues[289]. Il semble qu'il soit impossible de désanonymiser l'ensemble des utilisateurs de Tor. Seule une analyse manuelle permet de désanonymiser une très petite fraction des utilisateurs, sans pouvoir être en mesure de viser des personnes spécifiques. Cela passe notamment par le contrôle d'un nombre significatif de « nœuds de sortie » au réseau Tor ou bien l'exploitation de vulnérabilités logicielles comme Firefox, le navigateur constituant la base de Tor Browser, le navigateur du réseau Tor[290]. Par ailleurs, si l'utilisation de Tor permet un certain anonymat, de nombreuses bonnes pratiques sont recommandées afin d'accroître son anonymat, autant de pratiques qui si elles ne sont pas respectées, constituent des failles qui pourront être exploitées par les enquêteurs, pêle-mêle et de manière non exhaustive : l'utilisation du plugin NoScript, pré-installé dans le TorBrowser afin de bloquer les scripts JavaScript permettant de tracer l'utilisateur, utilisation d'un VPN préalablement à l'usage de Tor, ne pas se connecter en parallèle au web en clair ou bien accéder à des services habituels (gmail, Facebook) via Tor, ne pas faire de lien (pseudonymes, adresse mail…) entre Tor et le web en clair, ne pas ouvrir de fichiers téléchargés, laisser la résolution de l'écran sur un format standard[291]…
La difficulté principale de la lutte contre les infractions commises sur le *dark web* réside dans l'enquête, la réunion de preuve et l'identification de l'auteur, les infractions étant par ailleurs constituées, indifféremment qu'elles soient réalisées sur l'Internet ou sur le *dark web*[292].

103.- En France. Le député Bernard Debré avait demandé, lors de questions au Gouvernement à l'Assemblée nationale, que l'on « interdise les bitcoins » constatant notamment qu'il est simple de « s*e procurer des drogues et se les faire envoyer par voie postale (…) pour payer il suffit de disposer de bitcoins, monnaies virtuelle qui s'achète auprès de banques en ligne* (sic) ». Le député faisait référence aux rédactions de certains journaux, qui en ont fait l'expérience avec succès.

---

289 Tor affirme que le logiciel ne contient aucun backdoor et qu'ils feront tout pour résister aux demandes qui leur seraient faites en ce sens. https://2019.www.torproject.org/docs/faq.html.en#Backdoor
290 « *NSA and GCHQ target Tor network that protects anonymity of web users* », J. Ball, B. Scheier et G. Greenwald, The Guardian, 4 octobre 2013. Pour plus de précision, voir « Technical and Legal Overview of the Tor Anonymity Network », E. Çalışkan, T.s Minárik, A.-M. Osula, CCDCOE.
291 Ces avertissements sont fournis par le projet Tor https://2019.www.torproject.org/download/download.html.en#Warning
292 « *Darkweb : plongée en eaux troubles* », O. de Maison Rouge, Dalloz IP/IT 2017, p.74.

Nous ne reviendrons pas sur les approximations relatives à Bitcoin que nous avons exposées lors de la première partie, ni sur la volonté d'interdire Bitcoin pour cette seule raison, contingente, qu'il peut servir à acheter des produits stupéfiants, comme les monnaies fiats[293]. En revanche, cela illustre la perception qu'en a l'opinion publique ainsi que le fait que les bitcoins, en tant que crypto-actifs sont un support d'infractions diverses.

Il existe également en France des individus administrant des plateformes sur le *dark web*, l'une d'elle dénommée Black Hand (la Main Noire) proposant classiquement drogues, armes et faux papiers a été démantelée en juin 2018, aboutissant à la saisie de 4000 euros en liquide, 25 000 euros en cryptomonnaies et à l'arrestation de quatre personnes, dont l'administratrice principale, une mère de famille lilloise de 28 ans, jusqu'alors sans casier judiciaire[294]. Le forum créé en 2015 comptait 3000 membres, l'administratrice et les moérateurs se rémunérant via des inscriptions ainsi que des commissions via le système de garantie des transactions, (*escrow*) sur le modèle de Silk Road.

104.- Moyens de lutte. Le droit français a des moyens procéduraux d'enquête pénale, classiques comme la sollicitation d'informations auprès des Fournisseurs d'Accès à Internet (FAI)[295] ; les interceptions de correspondances émises par voie de communications électroniques ainsi que le recueil des données de connexion sont possibles[296] Une autre mesure d'investigation, pouvant s'avérer davantage efficace est celle de la captation en temps réel des données exploitées par un matériel informtique prévu par l'article 706-102-1 du Code de procédure pénale, qui dispose : « *Si les nécessités de l'enquête relative à l'une des infractions entrant dans le champ d'application des articles 706-73*[297] *et 706-73-1 l'exigent, le juge des libertés et de la détention peut, à la requête du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire requis par le procureur de la République à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un*

---

[293] Une étude publiée en 2013 dans le Journal of Forensic Sciences, en coopération avec le FBI révèle que 97% des billets de banques en dollars en circulation aux Etats-Unis contiennent des traces de cocaine
[294] « *La Main noire, première plateforme du darknet démantelée en France* », S. Ghibaudo, France Inter, 16 juin 2018.
[295] CSI, art. L. 871-1 ; C. pén., art. 434-15-2.
[296] CSI, art. L. 852-1 et C. pr. pén., art. 706-95 et s
[297] Qui prévoit, notamment le trafic de stupéfiants (3°), blanchiment (14°)

système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ». Néanmoins, comme le relève l'auteur, l'anonymisation des utilisateurs du *dark web*, couplée entre autres, aux messageries chiffrées et à l'utilisation des cryptomonnaies constituent un « *obstacle presque insurmontable à l'efficacité du système répressif* » [298]. L'infiltration et l'enquête sous pseudonyme permettent aux enquêteurs l'observation des site, aux termes de l'article 706-87-1 du Code de procédure pénale. La doctrine remarque par ailleurs que contrairement à l'infiltration « physique », l'infiltration dans l'enquête immatérielle facilitée en ce qu'elle ne pose ni limite de temps ni autorisation de l'autorité judiciaire[299]. Il y aurait donc un effet dissuasif, préventif, les opérateurs sur le *dark web* étant au fait qu'un enquêteur peut le cas échéant infiltrer le site. Une procédure atypique, dite du « coup d'achat » est également mise en œuvre permettant aux forces de l'ordre (C. pr. pén., art. 706-106) et aux agents des douanes (C. douanes, art. 67 bis-1) d'acquérir des armes pour constater les infractions mentionnées au 12º de l'article 706-73 du même code[300].

105.- Actualité. Pour montrer l'acuité particulière de la répression des activités menées sur le dark web, l'on ne résiste pas à mentionner la saisie récente, en mai 2019, d'un autre marché criminel, baptisé Wall Street Market, comptant plus d'un million d'utilisateurs et 5000 vendeurs. Cette opération fut une nouvelle fois possible par la collaboration, notamment de la DEA, du FBI américain, ainsi que Europol et les autorités allemandes et néerlandaises[301]. Les administrateurs du site avaient peu avant tenté un *exit scam*, courant sur le *dark web* qui consiste purement et simplement pour ces opérateurs à fermer boutique et partir avec la caisse de cryptomonnaies, en l'espèce l'équivalent de 30 millions de dollars.

Un membre du support aurait menacé des clients de révéler leurs adresses. L'un des administrateurs aurait ainsi été démasqué par une connexion VPN instable (Virtual Private Network, permettant une connexion chiffrée) révélant sa véritable adresse IP. Un autre administrateur fut trahi par ses métadonnées, les connexions au serveur de Wall Street Market avec le VPN étaient faites à partir d'une adresse IP enregistré au nom de la mère du suspect.

---

[298] « *Le Darkweb : un nouveau défi pour le droit pénal contemporain* » L. Saenko, Dalloz IP/IT 2017, p.80

[299] « *Le dark web ou l'internet clandestin et son encadrement juridique* », P.-X. Chomiac de Sas, Revue Lamy Droit de l'Immatériel, n°49, 1er juin 2018.

[300] *Ibid*. v. également « *Enquêtes dans le Darkweb* », M. Quéméner, Dalloz IP/IT 2017, p.83.

[301] « *Double Blow to Dark Web Marketplaces* », Europol, Communiqué de presse, 3 mai 2019.

Le dernier administrateur avait utilisé sa clé publique PGP (méthode de communication chiffrée) sur un autre site (Hansa)[302]. Un autre site, DeepDotWeb a lui aussi été saisi au cours du mois de mai 2019, dédié au dark web, il proposait une interface recensant les places de marché du dark web, ainsi que des fiches, des notations, interviews. Le contenu de ce site était à ce point pertinent qu'il a nourri certains des développement du présent mémoire, il est regrettable que certaines ressources soient désormais inexploitables car rendues inaccessibles. Les administrateurs ont été arrêtés en Israel, d'autres personnes ont également été arrêtés en France, Allemagne et aux Pays-Bas ainsi qu'au Brésil. Le site aurait engrangé des milions de dollars en commission en proposant un service de recommandations vers des places de marché cybercriminelles[303]. En fermant cette plateforme, qui fait office de « porte d'entrée dans le dark web » c'est tout l'écosystème cybercriminel qui est perturbé.

En mars 2019, une opération de grande envergure (SaboTor) faisant collaborer des agences américaines, canadiennes et européennes a visé des acheteurs et vendeurs des places de marché du dark web, ce qui aboutit à la fermeture de 50 comptes et à l'arrestation de 61 personnes. Environ 300 kg de drogues diverses auraient été saisies, ainsi qu'une cinquantaine d'armes et plus de 6 millions d'euros (dont 4 millions de cryptomonnaies)[304]. Il s'agissait de la deuxième opération du genre, une première (Operation Disarray) avait été menée aux Etats-Unis par le J-CODE (Joint Criminal Opioid Darknet Enforcement) en avril 2018 pour montrer aux acheteurs de drogues, particulièrement les drogues de synthèse sur le dark web (causant de nombreux cas d'overdoses) qu'il n'étaient pas en sécurité [305].

Dans ce contexte, une place de marché du dark web, Dream, a récemment fermé d'elle-même, sans attendre une opération des autorités, faisant preuve d'une longévité remarquable de six ans[306].

---

302 «*How German and US authorities took down the owners of darknet drug emporium Wall Street Market* », D. Coldewey, TechCrunch

303 « *FBI has seized Deep Dot Web and arrested its administrators* », Z. Whittaker, TechCrunch

304 « *Global Law Enforcement Action Against Vendors and Buyers on the Dark Web* », Europol, Communiqué de presse, 26 mars 2019

305 « *Attorney General Jeff Sessions Announces Results of J-Code's First Law Enforcement Operation Targeting Opioid Trafficking on the Darknet* », 3 avril 2018

306 L'un de ses administrateurs et de surcroît vendeur, un français, Gal Vallerius (« OxyMonster ») avait de son côté été arrêté en août 2017, à Atlanta alors qu'il s'apprêtait, pour l'anecdote à participer au championnat du monde de barbe et moustache. Il a plaidé coupable de trafic de stupéfiants et blanchiment d'argent.

106.- Constat. « *Contrairement à un sentiment souvent exprimé dans l'opinion publique, le monde de l'internet n'est ni resté ni devenu un monde de non-droit*[307] ». Après avoir constaté ces nombreuses percées des autorités, il ne semble pas sérieusement possible d'affirmer que ces sites sont inatteignable, que l'anonymat y est absolu, que le *dark web* est une zone de non droit. La technologie est elle même faillible, peut le cas échéant être utilisée contre les cybercriminels (crypto-tracking), des erreurs humaines, de mauvaises habitudes subsisteront vraisemblablement toujours.

[307] « *Le Darkweb, un objet juridique parfaitement identifié* », Y. Charpenel, Dalloz IP/IT 2017, p.71.

Section 2 : Crypto-actifs et blanchiment

107.- Notion de blanchiment. Le blanchiment est une infraction de conséquence, elle se caractérise par une aide apportée *a posteriori* à l'auteur d'un crime ou d'un délit.
Le processus de blanchiment se déroule en trois étapes principales : d'abord, le placement (ou prélavage) qui consiste à transformer les sommes d'argent en espèce provenant d'une infraction en un autre instrument monétaire ou en un autre bien ; vient ensuite l'empilage (ou lavage), qui consiste à disperser les valeurs transformées au cours de la première étape en de multiples opérations, afin de brouiller les pistes et rendre plus difficiles les mesures d'enquêtes ; vient enfin l'intégration (recyclage) qui consiste à réinjecter dans l'activité économique des produits ayant acquis une apparence de légitimité, en procédant à des investissements ou des dépenses[308]. Nous tenons à préciser qu'il ne sera pas ici envisagé le financement du terrorisme (FT) via les crypto-actifs, la présente contribution ciblant la cybercriminalité financière et le financement avéré du terrorisme par ce biais n'ayant pas été démontré[309].

108.- Elément légal. L'article 324-1 du Code pénal dispose que **: «** *Le blanchiment est le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect. Constitue également un blanchiment le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit*. »

109.- Eléments constitutifs. Le blanchiment suppose une infraction préalable, qualifiée de crime ou de délit, tout crime ou délit, peu important qu'il soit ou non prescrit[310], peu important que l'auteur de l'infraction originaire soit poursuivi ou sanctionné.

---

[308] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.157.
[309] « *Changes in modus operandi of Islamic tate terrorist attacks* », The Hague, 18 janvier 2016, Europol, p.7 « Despite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement. »
[310] Cass.crim., 31 mai 2012, n°12-80.705

L'infraction de blanchiment est constituée dès lors que son auteur avait conscience de l'origine frauduleuse des fonds, sans que soit exigée de sa part une connaissance de la nature exacte des infractions d'origine.[311] Les éléments constitutifs du blanchiment proprement dit impliquent donc un élément matériel, qui peut prendre deux formes : l'aide à la justification mensongère de l'origine des biens et revenus et le concours apporté à une opération portant sur le produit d'un crime ou d'un délit.

La deuxième forme de blanchiment nous intéressera plus particulièrement, le blanchisseur permettra l'intégration dans les circuits économiques sains de flux financiers douteux, cela passe traditionnellement par des commerces recueillant de nombreuses liquidités, ou par des établissements financiers (soumis désormais à des obligations de vigilance et de déclaration), la dissimulation passant alors souvent en des montages juridiques, prête-noms, sociétés-écran, paradis fiscaux.

Le blanchiment étant une infraction intentionnelle, il faut que le prévenu connaisse dans la première forme de blanchiment l'existence de l'infraction d'origine dont l'auteur a tiré profit, dans la secone forme, le blanchisseur doit savoir que l'opération à laquelle il apporte son concours porte sur le produit direct ou indirect d'un crime ou d'un délit
La Cour de cassation reconnaît par ailleurs l'autoblanchiment, ce qui revient à un cumul de qualifications, contestable revenant à admettre, comme le relève la doctrine, la « *possibilité d'apporter son concours à soi même*[312] ». La Cour de cassation[313] applique donc le texte à l'auteur du blanchiment du produit d'une infraction qu'il a lui même commise [314]

Le blanchiment est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende. L'article 324-2 du Code pénal prévoyant une peine de dix ans d'emprisonnement et de 750 000 euros d'amende « *Lorsqu'il est commis de façon habituelle ou en utilisant les facilités que procure l'exercice d'une activité professionnelle* » ainsi que « *lorsqu'il est commis en bande organisée*. »

---

[311] Cass.crim., 18 janv. 2017n n°15-84.003
[312] (A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis, p.157.
[313] Confortée par une résolution du parlement européen du 25 oct. 2011
[314] Cass.crim., 14 janv. 2004 : Bull. crim. 2004 n°12 ; réservant toutefois l'application du principe ne bis in idem, un même fait ne pouvant fonder une condamnation pour blanchiment et recel Cass.crim., 26 oct. 2016 -, n°15-84.552

Tracfin (traitement du renseignement et action contre les circuits financiers clandestins), considère les risques élevés que présentent les crypto-actifs en termes de blanchiment de capitaux depuis 2016.[315] Ces risques, identifiés, sont désormais avérés et tiennent « *principalement à l'anonymat, en particulier pour les blockchains délibérément développées afin d'effacer la traçabilité des transactions* » ainsi qu'aux « *plateformes proposant des services d'échange de crypto-actifs contre d'autres crypto-actifs (services de change dits ''crypto to crypto'')* ». En 2017, Tracfin a reçu 250 déclarations de soupçon concernant directement l'usage de crypto-actifs, soit une hausse de 44% par rapport à 2016.

Les informations reçues provenant pour l'essentiel des établissements bancaires. Néanmoins, cela est à considérer au regard des quelques 68 661 déclarations de soupçons totales reçue la même année, les crypto-actifs ne représentant que 0,4% de ce total. Les montant d'origine criminelle blanchis via les cryptomonnaies serait estimés entre 3,4 et 4,5 milliards d'euros par ans (entre 3 et 4% des 112 milliards blanchis chaque année en Europe)[316].

Afin d'approfondir son expertise et d'améliorer ses capacités d'investigation, Tracfin a créé au mois de juin 2018 une nouvelle division d'enquête dédiée à la cybercriminalité financière, en spécialisant certains enquêteurs sur l'analyse de transactions en crypto-actifs.

Les risques, s'agissant des crypto-actifs consiste en l'échange de crypto-actifs issus d'activités illégales : blanchiment de fraude fiscale, escroqueries, produits issus du commerce de produits illicites sur le dark web, cyberattaques (*ransomware*, *cryptojacking*), étudiées *supra* d'être échangés contre des monnaies fiats pour être réinvestis dans l'économie. Egalement, à l'inverse, prévenir l'échange de monnaie fiat, issue d'activités criminelles non liées à la cybercriminalité ni aux crypto-actifs, contre des crypto-actifs, puis les convertir en monnaie fiat pour les réinvestir dans l'économie.

110.- Bitcoin et blanchiment. Si initialement Bitcoin était perçu comme un puissant outil d'anonymat des transactions, le registre public indique en réalité le montant de bitcoins associé à chaque adresse. Toutes les transactions enregistrées sur la chaîne de blocs sont également publiques. L'identité des propriétaires des adresses bitcoin n'est pas publique mais peut être déterminée, par exemple par le biais des plateformes d'échange qui enregistrent l'identité de leurs utilisateurs. Il reste néanmoins possible, pour accroître l'anonymat des transactions en bitcoins de suivre certaines pratiques : créer un nombre de portefeuilles, donc

---

315 « *Tendances et analyse des risques* 2016 », Tracfin

316 « *Criminals hide 'billions' in crypto-cash* », S. Silva, BBC, 12 février 2018, interview de M. Wainwright, directeur d'Europol.

d'adresses différentes et procéder à des transactions entre elles, revendre ses bitcoins sur une plateforme d'échange et en racheter immédiatement la même quantité, utiliser chaque adresse une seule fois, ne pas révéler son adresse…

111.- Plateformes d'échanges. L'une des premières affaires de blanchiment d'argent en lien avec les crypto-actifs implique Charlie Shrem, le dirigeant de BitInstant, une plateforme d'échange de crypto-actifs de l'Etat de New York. Il lui était reproché d'avoir vendu l'équivalent d'un million de dollars en bitcoins à des individus, désireux de s'approvisionner en drogues sur Silk Road où bitcoin était le seul moyen d'échange.

Coinhouse, principale plateforme d'échange en France recense ainsi plusieurs cas de blanchiment et une cinquantaine de tentative sur 18 mois. La plateforme a mis en place un système de vérification manuel des transactions pour les montants significatifs, tandis qu'il est automatisé pour les petites opérations, a interdit les paiements en numéraire dans sa boutique physique et limité à 10 000 euros le montant possible d'achats en cryptomonnaies sur le site internet[317].

Les cas de blanchiment existent pourtant, par exemple, en juillet 2018, Europol, en collaboration avec les autorités espagnoles a démantelé un réseau de blanchiment d'argent estimé à 2,5 millions d'euros en bitcoins via des plateformes d'échange[318]. En mai 2019, une nouvelle opération menée par Europol en coopération avec les autorités espagnoles a abouti à l'arrestation d'une organisation offrant des services de blanchiment (*laundering as a service*) gérant une plateforme d'échange de crypto-actifs, incluant deux distributeurs automatiques de crypto-actifs (ATM) les utilisant pour déposer du numéraire et le convertir en cryptomonnaie pour d'autres groupes criminels, 4 cold wallets et 20 hot wallets, par lesquels auraient transité 9 millions d'euros ont été saisis[319].

112.- ICO et blanchiment. Comme le relève Tracfin, des fonds d'origines illicites peuvent être investis dans les émissions en jetons, lesquels seront revendus à d'autres investisseurs, puis convertis en monnaie légale. Il apparaît donc nécessaire d'identifier l'origine des fonds des l'investissement.

---

317 « *Blanchiment, financement du terrorisme, escroqueries : mais que font les cryptos* ? », C. Perreau, le Journal du Net, 10 décembre 2018.

318 « *Two criminal groups dismantled for laundering EUR 2.5 million through smurfing and cryptocurrencies* », Communiqué de presse, Europol, 11 juillet 2018.

319 « *Cryptocurrency Laundering As a Service: Members of a Criminal Organisation Arrested in Spain* », Communiqué de presse, Europol, 8 mai 2019.

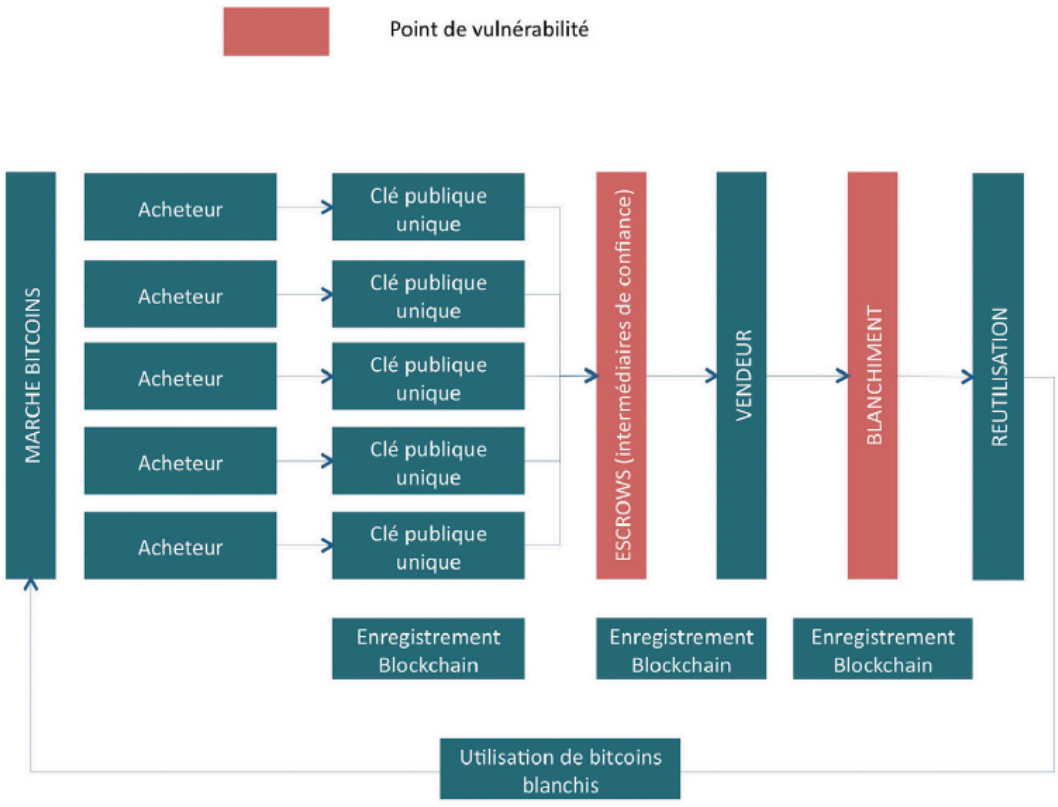
En France, cependant, de nombreux acteurs du marché ont compris l'intérêt qu'ils avaient à vérifier l'identité de leurs investisseurs, ne serait-ce que pour se prémunir en cas d'évolution de la réglementation en ce sens. Les porteurs de projets ne maîtrisent pas pour autant le dispositif LCB/FT et n'ont pas toujours les moyens de procéder à des mesures de connaissance client satisfaisantes. Le plus souvent, ils font appel à des prestataires de services spécialisés, dénommés KYC providers, établis généralement hors de France, qui proposent des prestations de prise d'identité et de vérification d'identité.

Ces prestations externalisées peuvent représenter un coût élevé pour un porteur de projet, alors qu'elles restent insuffisantes. Les KYC providers ne stockent aucune donnée et n'engagent pas leur responsabilité sur la décision d'un porteur de projet d'accepter ou non un investisseur. *Know Your Customer* (KYC) désigne le processus permettant de vérifier l'identité des clients d'une entreprise, dans le but de prévenir, notamment le blanchiment d'argent, mais également la fraude fiscale ou encore l'usurpation d'identité.

La directive (UE) 2015/849, dite « 4e directive anti-blanchiment », n'abordait pas le sujet des crypto-actifs. La France a néanmoins choisi d'assujettir les plateformes de change dès décembre 2016[320]. La directive (UE) 2018/843 du 30 mai 2018 modifiant la 4e directive prévoit l'obligation pour l'ensemble des États membres de l'UE d'assujettir au dispositif LCB/FT les plateformes de change et les fournisseurs de services de portefeuille de conservation (*custodian wallet providers*), et ce avant le 10 janvier 2020.

La loi Pacte fait du processus KYC une condition dont le respect conditionnera l'octroi par l'AMF du visa optionnel (« *le repect des règles en vigueur en matière de lutte contre le blanchiment et le financement du terrorisme (LCB/FT)*[321]. De même que l'agrément des prestataires de services sur actifs numériques (PSAN) qui comprennent notamment « *le service de conservation pour le compte de tiers d'actifs numériques ou d'accès à des actifs numériques* » (1°) *« le service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal* » (2°). Étrangement, les ICOs non labellisées par l'AMF et les PSAN ne demandant pas d'agrément ne seront pas soumis aux obligations LCB-FT…

[320] 7° bis de l'article L.561-2 du CMF
[321] L.552-5 nouveau du Code monétaire et financier



Blanchiment de Bitcoins

Schéma provenant de « *Monnaies virtuelles et cybercriminalité, état des lieux et perspetives* » M. Even, A. Gery, B. Louis-Sidney, Les notes stratégiques, Ceis

113.- Interractions entre crypto-actifs et économie réelle. Tracfin constate que le couplage entre les services de paiement ou de transfert de fonds en monnaie fiat et l'utilisation des crypto-actifs permet le blanchiment en ce qu'il rompt la traçabilité. Il s'agit des cartes de paiements adossées à des portefeuilles en crypto-actifs

Un risque important issu de l'hybridation entre les services de paiement en monnaie légale et les crypto-actifs (cartes dites « BTC2plastic »), elles permettent d'effectuer des achats auprès d'un commerçant physique ou en ligne, ou de retirer des espèces dans les distributeurs automatiques, commercialisées par des sociétés spécialisées qui assurent les fonctions de marketing et s'appuient sur des établissements de paiement ou de monnaie électronique pour gérer les flux de paiement et les contraintes réglementaires y afférentes.

Au début de l'année 2018, ces cartes ont connu un revers du fait de la faiblesse des dispositions LCB/FT de leurs émetteurs. La majorité des cartes utilisées au sein de l'Union européenne, commercialisées sous différentes marques, étaient émises par un seul et même établissement de monnaie électronique, Wavecrest Holdings Ltd, enregistré à Gibraltar. Au début de l'année 2018, les organismes VISA et Mastercard ont décidé d'exclure cet EME de leur réseau pour non-respect de ses obligations contractuelles de conformité. Toutes les cartes de paiement émises par cet EME ont alors été désactivées. Les sociétés commerciales concernées ont dû suspendre les fonctionnalités de leurs cartes prépayées dans l'EEE, ne laissant à leurs utilisateurs qu'un accès à leur portefeuille de crypto-actifs[322].
On remarque, comme mentionné dans la première partie que Visa a conçu une telle carte, en partenariat avec Coindesk.

LocalBitcoins, fondé en 2012 en Finlande se présente comme « *un service entièrement décentralisé, répondant parfaitement à la philosophie Bitcoin* ». Il permet aux utilisateurs d'acheter et vendre des bitcoins dans leur monnaie fiat. Les membres publient leurs offres de vente/achat et fixent eux-mêmes leurs prix. Les échanges se font donc de personne à personne, sans intermédiaire et donc sans vérification d'identité et où la réputation constitue l'une des seules protections aux arnaques. En mai 2019, un américain a été condamné à 21 mois d'emprisonnement et s'est vu saisir 80 000 dollars de profits, pour avoir procédé à plus de 1000 transactions avec des centaines d'utilisateurs, pour avoir opéré sans être enregistré[323].
Un précédent s'était déjà produit en avril 2019. En juillet 2018, une américaine, 'Bitcoin Maven' a été condamné pour avoir réalisé plus de 900 000 dollars de bénéfice en trois ans et réalisé des transactions pour 7 millions de dollars, pour blanchiment d'argent et d'exercice sans agrément.
En juin 2019, LocalBitoins a retiré la possibilité de payer en numéraire et ajouté un processus *Know Your Customer* (KYC) en raison d'une évolution de la législation finlandaise. Un concurrent a été annoncé, sous la dénomination Local. Bitcoin, ce qui n'est au demeurant pas sans poser des questions de parasitisme et qui annonce ne pas envisager de processus d'identification des clients.

---

322 « *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017 – 2018* », Tracfin, p.55 et suiv.
323 « *Man Sentenced for Illegal Money Transmission Services on LocalBitcoins* », L. Manning, BitcoinMagazine, 31 mai 2019.

114.- ***Mixer, tumbler*****.** Pour éviter le traçage des crypto-actifs, en particulier des cryptomonnaies et des bitcoins, lorsqu'ils sont liés à des activités illégales (*tainted*), les cybercriminels peuvent recourir à des mixer ou tumbler. L'objectif étant ainsi de permettre à une adresse A d'envoyer des bitcoins vers une adresse B sans qu'il soit possible d'établir un lien entre ces deux adresses. En pratique, A envoie les bitcoins vers une adresse C, le service de mixing en question, qui les centralise (ce qui constitue une vulnérabilité) qui les envoie vers D, adresse communiquée par A. D peut alors envoyer les bitcoins à B. Les bitcoins envoyés par l'adresse D ne sont donc pas ceux envoyés par A[324]. Le procédé est donc efficace, sous réserve évidemment, comme dans tout réseau (cf. Bitcoin, Tor) d'un grand nombre d'utilisation pour ne éviter les éventuelles corrélations temporelles. Le 22 mai 2019, Europol en coopérant avec les autorités néerlandaises et la société de cybersécurité McAfee a procédé à la fermeture, pour la première fois d'un service de ce type, le site BestMixer.io, ouvert en mai 2018 et devenu premier service de mixing au niveau mondial. Il aurait permis le blanchiment de fonds criminels pour un montant d'environ 200 millions de dollars via bitcoins, bitcoin cash et litecoins[325]. Peu de temps après, c'est Bitcoin Blender qui a volontairement fermé. Ce service était connu pour pratiquer des *dusting attacks*[326] pour faire sa publicité, c'est à dire le fait d'envoyer (de manière non justifiée) des montant infimes en cryptomonnaies à une multitude d'adresses, la multitude de micro-transactions permettant de dissimuler les transactions douteuses. Des utilisateurs reçoivent donc par ce biais des fonds potentiellement liés à des activités illicite sans leur consentement[327].

115.- ***Altcoins*****.** Si Bitcoin ne garantit pas l'anonymat, d'autres cryptomonnaies apportent cet avantage. Monero, à laquelle nous avons déjà fait référence, permet un anonymat renforcé par un procédé de signature de cercle (*ring signature*) ce procédé cryptographique nécessite de disposer d'une clef cryptographique publique, il permet de signer électroniquement de façon anonyme un message au nom d'un « cercle ». Les membres de ce cercle sont choisis par l'auteur de la signature et ne sont pas nécessairement informés de leur implication dans la

---

[324] « *Le Bitcoin devient monnaie courante : les monnaies digitales entre transparence, régulation et innovation* », V. Charpiat, Revue des Juriste de Sciences Po, 2014, n°9 p.47-48.

[325] « *Multi-million euro cryptocyrrency laundering service bestmixer.io taken down* », Communiqué de presse, Europol, 22 mai 2019

[326] Dans l'environnement des crypto-actifs, *dust* fait référence à un montant si insignifiant qu'il n'est pas même remarqué par l'utilisateur, par exemple quelques centaines de satoshi. L'objet de l'attaque est donc d'envoyer des montant insignifiants à une multitude d'adresses afin de procéder ensuite à leur analyse dans le but d'identifier celles qui appartiennent à la même personne lorsque ces mêmes fonds sont dépensés et la cibler ensuite avec des attaques plus classiques comme le phishing ou le ransomware.

[327] « *Bitcoin mixeurs : Bitcoin Blender ferme sa boutique* », Journal du Coin, 3 juin 2019.

création de la signature électronique. Avec la ring signature, l'émetteur est anonymisé ; avec le *ring confidential transactions (Ring CT)*, le montant des transactions est secret ; l'utilisation d'adresses furtives (*stealth adress*) c'est à dire à usage unique, permet au destinataire d'être anonyme. Une autre technologie devrait être implémentée, *Kovri* devrait permettre de masquer l'adresse IP de l'utilisateur, en utilisant Invisible Internet Project (I2P), réseau décentralisé analogue à Tor.

L'ensemble de ces procédés permet donc une protection accrue des utilisateurs, et a les faveurs des crybercriminels. Monero est par ailleurs ainsi l'une des seules cryptomonnaies fongible[328].

Zcash (ZEC) est basé sur une variante de la preuve à divulgation nulle de connaissance (*Zero Knowledge Interactive proof ou ZKIP*), il s'agit d'un protocole sécurisé basé de cryptologie dans lequel une entité, le « fournisseur de preuve », prouve mathématiquement à une autre entité, le vérificateur, qu'une proposition est vraie sans révéler d'autres informations. Le protocole ZCash lui utilise un protocole dit de non-interactive zero-knowledge proof, zk-SNARK (*zero-knowledge succinct non-interactive argument of knowledge*) où aucune interaction n'est nécessaire entre le fournisseur de preuve et le vérificateur.

En pratique, Zcash s'appuie sur une blockchain avec deux types d'adresses, certaines transparentes (*t-adress*), d'autres protégées (*z-adress*). Les transactions effectuées entre les z-adresses sont chiffrées dans la blockchain. On ne connaît donc ni l'émetteur, ni le destinataire, ni le montant. Comment néanmoins résoudre le problème de la double-dépense, comme le fait Bitcoin ? C'est ce que zk-SNARK permet, vérifier la validité de la transaction sans en connaître les éléments[329].

Plus généralement, on constate sur ce sujet un double mouvement général, d'une part d'anonymisation des altcoins, V. Buterin, le fondateur d'Ethereum ayant récemment annoncé vouloir rendre le rendre plus anonyme par un système de mixer utilisant deux smart contracts, le mier et un registre relai, gérant les adresses IP[330] ; d'autre part, Ripple, dont l'on rappelle qu'elle vise surtout les acteurs institutionnels tels que les banques a récemment confirmé ne

---

328 « *Mastering Monero, The future of private transactions* », SerHack ainsi que la communauté Monero, première édition, p.60 et suiv.

329 « *Totalement anonyme, Zcash est-elle la cryptomonnaie ultime ?* » G. Kallenborn, 01net.com, 4 mars 2017

330 « *We need a first step toward more privacy* », V. Buterin.

pass vouloir aller dans le sens de l'anonymat[331]. Un juste milieu est certainement possible, JPMorgan ayant récemment ajouté une extension, basée sur le protocole Zether utilisant la preuve à divulgation nulle de connaissance (ZKP) accroissant l'anonymat sur sa blockchain propre blockchain privée, Quorum, basée sur Ethereum, masquant le montant ainsi que l'émetteur des transactions[332].

116.- Crypto-tracking. Il est important de doter les forces de l'ordre de nouveaux outils d'investigation, ce champ, appelé *digital forensic* (informatique légale), comprend des moyens spécifiques d'analyse des transactions en cryptomonnaie appelées crypto-tracking. En effet, les transactions sont intégralement enregistrées de façon indélébile dans la blockchain, par croisement d'information il est possible de retracer les transactions suspectes afin de remonter jusqu'à l'adresse d'une plateforme d'échange ou d'un service de portefeuilles en ligne. Ces derniers, qualifiés de prestataire de services d'échange entre monnaies virtuelles et monnaies légales (PSEMV) et prestataires de services de portefeuille de conservation (PSPC) déjà avant l'entrée en vigueur de la loi Pacte, étaient soumis, par la directive anti-blanchiment du 30 mai 2018 à une obligation de *Know Your Customer* (KYC) et d'identification des bénéficiaires effectifs. Ces services ont une obligation de déclaration à Tracfin des opérations complexes, inhabituellement élevées ou ne paraissant pas avoir de justification économique ou d'objet licite[333].

Le ministère de l'Intérieur a lancé un appel d'offres afin d'équiper ses agents (gendarmerie, police nationale, douane) d'outils spécialisés dans l'analyse des transactions. L'objet est d'acquérir un outil permettant de « surveiller, analyser et de suivre les transactions en ve de désanonymiser les utilisteurs de bitcoins ». Comme démontré plus avant, les utilisateurs de Bitcoin ne sont pas tout à fait anonymes, ils sont plutôt pseudonymisés (par leur adresse). Néanmoins, il est remarquable de constater l'évolution des moyens d'enquête, prenant pleinement en compte la technologie elle même, en l'espèce la blockchain qui enregistre toutes les transactions de manière irrévocable afin de lutter contre la cybercriminalité.

---

331 « *Vitalik Buterin propose une solution pour anonymiser les transactions Ethereum uniques* », M. Debelloir, Cryptoast, 24 mai 2019.
332 « *JPMorgan Adds*
333 « *Crypto-tracking : les nouveaux outils d'enquête pour les forces de l'ordre* », A. Jomni, Revue de la gendarmerie nationale, n°263, décembre 2018.

Il pourrait en effet être utilisé par les agents pour arrêter les vendeurs opérant sur de marchés criminels sur le dark web, lutter plus efficacement contre le blanchiment et l'évasion fiscale.

Toutefois, il ne permettra que d'analyser certaines cryptomonnaies, pas toutes, notamment pas celles qui sont le plus concernées par l'anonymat de leurs utilisateurs comme Monero et Zcash. La problématique des bitcoin mixer (ou tumbler) n'est pas adressée.
Des sociétés comme Chainalysis, Ciphertrace, Coinfirm sont à même d'analyser de telles transactions sur la chaîne de blocs, cette dernière collaborant d'ores et déjà avec Europol[334]. La coopération public-privé, indispensable est donc mise en œuvre. Un document de la N.S.A., dévoilé dans le cadre des révélations d'Edward Snowden, et analysé par The Intercept montre que l'agence a adapté l'un de ses programmes de surveillance (MONKEYROCKET) de masse pour tracer les utilisateurs de Bitcoin, vraisemblablement en infectant les utilisateurs avec un logiciel paradoxalement présenté comme protecteur de l'anonymat[335]. L'Union Européenne travaille actuellement sur un projet TITANIUM (*Tools for the Investigation of Transactions in Underground Markets*) pour surveiller les transactions opérées sur les blockchains afin de développer des outils *forensic* pour améliorer l'efficacité des enquêtes notamment pour détecter les anomalies dans l'usage des cryptomonnaies, identifier les techniques de blanchiment d'argent ainsi que les transactions criminelles. Le projet, financé à hauteur de 5 millions d'euros réunis des universitaires, des entreprises privées ainsi que des administrations[336]. Un groupe de chercheurs de l'université de Cambridge[337] ont mis au point un moyen de tracer les bitcoins et identifier ceux ayant pu servir à des transactions illégales et criminelles. Il permettra de savoir si un bitcoin détenu a été possédé par exemple par R. Ulbricht ou s'il a transité par Mt.Gox par exemple. Les chercheurs se basent sur un précédend judiciaire anglais, le Clayton's Case, traitant de l'ordre des créanciers s'agissant de la répartition des fonds d'un établissement financier en faillite. La réponse étant que celui qui a apporté ses fonds en premier doit être remboursé en premier, il s'agit de la méthode bien connue du FIFO (first-in-first-out)[338].

---

[334] « *Europol and Chainalysis reinforce their cooperation in the fight against cybercrime* », Europol, 19 février 2016.
[335] « *La NSA a traqué les utilisateurs de Bitcoin dans le monde entier* », J. Lausson, Numerama, 21 mars 2018 ; « *The NSA Worked to ''Track down'' Bitoin Users, Snowden Documents reveal* », S. Biddle, the Intercept, 20 mars 2018.
[336] « *Project to prevent criminal use of the dark web and virtual currencies launched by international consortium* », CORDIS EU research results, 1er juin 2017.
[337] « *Making Bitcoin Legal »,* R. Andeson, I. Shumailov, M. Ahmed
[338] « *A 200-year-old idea offers a new way to trace stolen bitcoins* », A. Greenberg, Wired, 4 mai 2018.

Section 3 : Crypto-actifs et délits de marché

117.- Diversité des délits de marché : **non application aux crypto-actifs**. En droit des marchés financiers, le principe d'égalité de tous les acteurs devant l'information permet la transparence et la formation du prix, selon la théorie de l'efficience des marchés. Le délit d'initié est l'infraction constituée lorsqu'une minorité, profitant d'une information dite privilégiée intervient sur le marché avant que le public en ait connaissance. L'information privilégiée est en effet précise, non publique, et dont la révélation est susceptible d'avoir une incidence sur le cours. Les initiés ont donc un devoir d'abstention et de réserve s'agissant des interventions sur les titres[339]. L'article L.465-3-4 du Code monétaire et financier vise les plateformes de négociation que sont les marchés réglementés, les systèmes multilatéraux de négociation ainsi que les systèmes organisés de négociation.

De même le délit de diffusion d'informations fausses ou trompeuses pour lequel l'article L.465-3-2 vise les émetteurs dont les titres sont admis aux négociations sur un marché réglementé, en France Euronext Paris, et a été étendu aux titres négociés sur un système multilatéral de négociation (L.421-4 Comofi). En droit français, l'infraction de manipulation de cours est prévue aux articles L. 465-3-1 et L. 465-3-3 du CMF. Est ainsi puni de cinq ans d'emprisonnement et 100 millions d'euros d'amende le fait de « *réaliser une opération, de passer un ordre ou d'adopter un comportement qui donne ou est susceptible de donner des indications trompeuses sur l'offre, la demande ou le cours d'un instrument financier ou qui fixe ou est susceptible de fixer à un niveau anormal ou artificiel le cours d'un instrument financier* ».

Cependant, les crypto-actifs ne peuvent être qualifiés d'instruments financiers. En effet, les instruments financiers sont, soit des titres financiers, soit des contrats financiers.
En ce sens, les crypto-actifs échappent donc à l'infraction de manipulation de cours.[340]

---

339 Art. L.564-1 C.mon.fin.
340 « *7*», J. Brosset, A. Barbet-Massin, Revue Lamy Droi des Affaires, Les applications de la blockchain dans le domaine de la finance, supplément, septembre 2018.

118.- Cas de manipulations de marché de crypto-actifs. Craig Wright, auquel nous avons déjà fait allusion en ce qu'il prétend être Satoshi Nakamoto, a créé une cryptomonnaie, Bitcoin SV, qui a récemment fait l'objet de manipulations de cours. Le 21 mai 2019, le cours du Bitcoin SV a ainsi augmenté de 60 dollars en moins de 10 heures du fait que certaines personnes ont publié en Chine un faux rapport prétendant que Craig Wright avait prouvé être Satoshi en transférant des bitcoins à partir de l'adresse de Satoshi, rumeur qui était un montage et qui a largement circulé[341]. Craig Wright lui même a déposé, courant mai 2019, auprès du United States Copyright Office un enregistrment des droits d'auteur sur le *white-paper* de Bitcoin, le cours de Bitcoin SV a alors progressé de plus de 100% passant de 62 à 135 dollars en moins de 12 heures. Il s'agit néanmoins seulement d'une revendication, ledit bureau ayant finalement refusé la requête[342]. En avril 2019, les plateformes d'échange de crypto-actifs Kraken et Binance ont délisté le BSV, ce qui a conduit à une baisse du cours de 20%, preuve que l'autorégulation est efficace. Les manipulations de marché sont notamment rendues hautement probables par le fait qu'une petite minorité détient souvent l'essentiel des cryptomonnaies, l'on parle de *whales* (baleines) pour désigner ces gros porteurs[343]. Des estimations affirment que 40% des bitcoins disponibles seraient détenus par seulement 1000 utilisateurs[344]. En effet, 3 adresses détiennent entre 100 000 et 1 million de bitcoins (équivalent de 3 milliards de dollars), 111 adresses détiennent entre 10 000 et 100 000 bitcoins[345]. Si ces whales se décidaient à agir de concert, elles pourraient faire varier significativement le cours. Un autre cas potentiel d'abus de marché par manipulation de cours pourrait être celui reproché à Jamie Dimon, le PDG de la banque d'affaires JPMorgan Chase, lorsqu'il était sceptique, voire critique sur la valeur des bitcoins et des cryptomonnaies en général et que ses déclarations ont fait chuté le cours de ce dernier de $ 4 340 à $ 2 981 en quelques jours.

---

341 « *Scammers Boost Price With Fake Satoshi Confirmation* », J. Biggs, Coindesk, 29 mai 2019.
342 « *Bitcoin SV pumps after fake Craig Wright Satoshi news tricks Chinese investors* », A. Martinez, Cryptoslate, 29 mai 2019.
343 Un compte twitter recense en temps réel les transactions significatives portant sur divers crypto-actifs.
344 « *The Bitcoin Whales : 1,000 People Who OWn 40 Percent of the Market* », O. Kharif, Bloomberg, 8 décembre 2017.
345 https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

119.- *Pump and dump*. Les schémas de *pump and dump* sont une technique de manipulation de marché ancienne, ils furent d'abord en vogue s'agissant d'actions de sociétés, dites « penny stocks » et popularisés par des films comme « Le Loup de Wall Street ».

Le mécanisme fonctionne de la façon suivante : tout d'abord il convient de cibler une entreprise peu capitalisée et peu liquide. L'auteur de la fraude acquerra un nombre important d'actions, il diffusera ensuite des informations trompeuses s'agissant de l'activité et des perspectives de la société en question, afin d'inciter des investisseurs (qui sont des victimes en puissance de la fraude) à en acquérir et de faire gonfler artificiellement le cours (c'est le « pump »). Enfin, l'auteur de la fraude cèdera ses actions en faisant une plus-value (c'est le « dump ») tout cela étant très discret. Les victimes se retrouvent alors titulaire de titres ayant une valeur encore moindre que celle à laquelle l'auteur de la fraude les a intialement acheté et ne trouveront difficilement une contrepartie, le titre étant par nature peu liquide et atractif.

Cette fraude est praticable et pratiquée s'agissant de cryptomonnaies et particulièrement des altcoins. Il est question d'acheter d'importantes quantités d'une cryptomonnaie donnée afin d'en faire gonfler artificiellement le cours, en espérant que d'autres investisseurs, voyant le rendement important du crypto-actif et attiré par l'appât du gain et la crainte de passer à côté d'une opportunité unique d'investissement (en anglais FOMO : Fear of missing out) en acquièrent à leur tour. L'auteur de la manipulation, qui a par son opération, fait gonfler artificiellement le cours et attiré d'autres investisseurs, qui ont à leur tour fait gonfler artificiellement le cours, dans un cercle vicieux, cède alors ses crypto-actifs et empoche une plus-value.

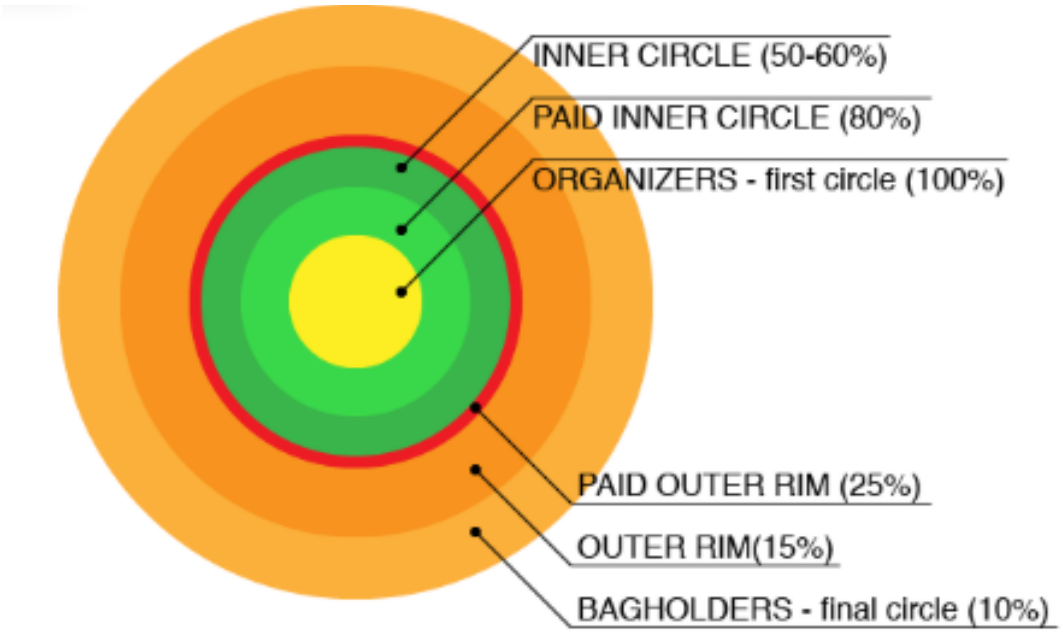
Des groupes de pump and dump exisent évidemment d'ores et déjà[346], qui consistent à se réunir et agir de manière coordonnée sur le cours d'un crypto-actifs afin d'en faire augmenter artificiellement le prix (pump) , attirant ainsi des investisseurs, avant de les revendre (dump) pour réaliser au passage une plus value. L'investisseur lui fait une moins value et trouvera plus difficilement une contrepartie.

---

346 « *University researchers identified over 4,800 pump and dump schemes involving crypto over a six month period* », Theblockcrypto, 20 décembre 2018. ; « *The Economics of Crypocurrency Pump and Dump Schemes* », JT Hamrick, F. Rouhi, A. Mukherjee, A. Feder, N. Gandal, T. Moore, M.Vasek.

Ces groupes se réunissent sur des applications de messagerie chiffrée comme Telegram, les cours les plus manipulables et les plus fréquemment manipulés étant ceux des altcoins. Ces groupes sont particulièrement organisés, en « couches » se rajoutant au fur et à mesure.

Les instigateurs originels de ces montages, au cœur du pouvoir décisionnel (notamment s'agissant de la décision de la cryptomonnaie objet de la manipulation), représentant la couche centrale disposeront de l'information d'achat/vente plus rapidement et réaliseront des profits plus importants, ce dernier se réduisant de manière proportionnelle en fonction de la couche, et de la vitesse de diffusion de l'information (quelques secondes) pour finalement représenter les victimes de la manipulation, à l'extrême couche.



Des droits d'entrée sont nécessaires pour rejoindre ces groupes. La fréquence est variable, quotidienne, hebdomadaire ou mensuelle, les participants prenant soin de se coordonner avec un compte à rebous sur un fuseau horaire commun. La cryptomonnaie objet de la manipulation, souvent listée sur une plateforme d'échange peu réputée est sélectionnée. Les participants se préparent alors en rechargeant leurs portefeuilles afin d'acquérir un maximum de ladite cryptomonnaie, la connexion internet est alors optimisée, certains recourent même à des algorithmes (bots) de manière analogue au trading haute fréquence (THF).

Il s'agit du pré-pump. L'information est ensuite communiquée aux participants d'autres couches. Le pump représente en moyenne une augmentation de 10 à 15 points du cours d'une cryptomonnaie. Vient ensuite le dump, la vente massive qui aboutira au mieux à un retour au cours initial, voire uncours inférieur.

La majorité de ces groupes procéderont à quelques pumps afin d'attiser l'appât du gains et recruter des membres pour les inciter à s'impliquer davantage dans les futurs pumps et leur prendre leurs fonds. En définitive, la minorité, les organisateurs sont toujours gagnants dans ces manipulations tandis que la majorité en sont victimes[347]. Ces méthodes suscitent le débat, certains les qualifiant d'immorales, d'autres de saines pour l'écosystème et légitimes. Il n'existe en tous les cas pas de réglementation spéciale propre à les interdire. Nous appelons de nos vœux l'émergence d'une réglementation pénale spéciale, analogue à celles s'appliquant aux marchés réglementés. En pratique, l'enquête et l'identification des auteurs de ces éventuelles infractions seraient rendues difficiles par l'extraterritorialité de ces opérations ainsi que l'usage de moyens de communications chiffrés.

120.- Dérivés sur crypto-actifs et manipulation de marché. Les crypto-actifs, et notamment les cryptomonnaies ne sont pas des instruments financiers. Les instruments financiers comprennent traditionnellement les titres financiers et les contrats financiers.

Des produits dérivés ayant pour sous-jacent des bitcoins ont vu le jour, dont certains proposés par des marchés réglementés, tels les *futures* sur bitcoins proposés par le *Chicago Board Options Exchange* ou le *Chicago Mercantile Exchange*. S'agissant de la qualification juridique de ces dérivés, l'Autorité des marchés financiers (AMF) dans une analyse sur la qualification juridique des produits dérivés sur crypto-monnaies a conclu qu'un produit dérivé ayant pour sous-jacent une crypto-monnaie et se dénouant par règlement en espèces s'analyse en un contrat financier, cette qualification étant indépendante de celle de son sous-jacent. Par conséquent la réglementation applicable à l'offre d'instruments financiers en France s'applique à ces derniers[348]. La *Commodity Futures Trading Commission* (CFTC) a ouvert une enquête s'agissant de manipulations éventuelles de *futures* sur des bitcoins portant sur quatres plateformes d'échange (Bitstamp, Kraken, iBit, Coinbase). Il s'agirait de pratiques

---

347 « *Anatomie d'un groupe de pump and dump* », Journal du Coin, 28 juillet 2018 ; « *The Anatomy of a Pump & Dump Group* », B. Skvorc, Bitfalls.com, 12 janvier 2018 ; « Walkthrough: How traders 'pump and dump' cryptocurrencies », O. Williams-grut, Business Insider, 14 novembre 2017.

348 « *Les dérivés sur crypto-monnaie sont des contrats financiers* ». P. Pailler, Revue de droit bancaire et financier, n°2, LexisNexis, mars-avril 2018

dits de spoofing, consistant à placer des ordres d'achat ou de vente et à ainsi orienter le marché pour les annuler peu avant l'exécution ainsi que de wash-trading, consistant à procéder à des transactions à soi même afin de donner l'apparence d'un marché liquide avec un volume d'échange important[349]. En effet, aux Etats-Unis, les cryptomonnaies sont considérées être des *commodities*, des marchandises (tandis que comme on l'a vu les *tokens* sont en principe considérés comme des *securities*).

En définitive, tant en France qu'aux Etats-Unis, les qualifications permettent de rattacher les dérivés sur cryptomonnaies et notamment bitcoins à des catégories existantes. Ces qualifications, notamment celle de contrat financier est susceptible de se voir appliquer les délits de marché que sont les délits d'initiés ainsi que les manipulations de cours.

En France, le règlement abus de marché (« MAR ») en son article 12, vise des comportements portant sur la manipulation d'instruments financiers, dont les contrats à terme, produits dérivés, sont une espèce. Néanmoins, la manipulation du cours du bitcoin, par exemple, par l'utilisation de contrats à termes, elle, semble n'être appréhendée par aucun texte.

Les *futures* sur bitcoins auraient fait l'objet d'une manipulation, dont le risque avait été anticipé avant leur lancement sur le *Chicago Mercantile Exchange*, le bitcoin ayant atteint son cours le plus haut à la même période, il a été avancé que des investisseurs institutionnels aient pu ramasser des quantités importantes de bitcoins sur le marché, afin d'en augmenter le prix *spot* et donc en conséquence le cours des *futures* avant l'arrivée du terme, puis de prendre des positions de vente (*short*), sur les futures, avant de procéder à la vente des bitcoins physiques, réalisant une plus-value et un gain sur les *futures cash-settled*[350].

L'actualité la plus récente, de mai 2019 démontre les hésitations de la *Securities and Exchange Commission* (SEC) à approuver les ETF[351] sur bitcoins de VanEck, SolidX et le CBOE, ou encore Bitwise et bien d'autres auparavant, en raison, précisément, selon le Président de la SEC Jay Clayton, de manipulations de marché ainsi que des vols de bitcoins, sous-jacents de tels contrats, posant un véritable problème de contrepartie. Le New York Attorney General's office a en effet produit un rapport démontrant que les plateformes d'échange de cryptomonnaies étaient vulnérables aux manipulations de marché, pointant des

---

[349] « *U.S. Launches Criminal Probe into Bitcoin Price Manipulation* », M. Robinson, T. schloenberg, Bloomberg, 24 mai 2018.

[350] « *Bitcoin Futures Manipulation: How it Works and How to Reduce it* », N. Puckrin,CCN, 19 décembre 2018.

[351] Acronyme de Exchange Traded Fund, il s'agit en pratique de trackers, c'est à dire de fonds indiciels cotés sur un marché, qui répliquent la performance d'un indice, comme le CAC 40. Il s'agit donc de constituer un fonds qui investirait dans des bitcoins, sa valeur liquidative répliquant les performances de cette cryptomonnaie pour les investiseurs qui ne détiennent pas directement des bitcoins.

problèmes de transparence, de sécurité et de traitement équitable, les plateformes ne prenant pas les mesures nécessaires propres à les endiguer[352]. L'usage de techniques des marchés réglementés traditionnels comme la technologie SMARTS du NASQAQ afin de lutter contre de telles manipulations est déjà pratiqué, par exemple par Gemini, la plateforme d'échange de crypto-actifs des frères Winklevoss.

121.- Volumes d'échanges mensongers. La société Bitwise, dans le cadre du transfert de ses données d'échanges à la SEC pour demander le lancement de son ETF sur Bitcoin affirme que 95% des volumes d'échanges sont faux et que le marché du bitcoin est significativement inférieur. Un autre rapport de The Tie affirme que presque 90% des volumes d'échanges sont faux[353]. CoinMarketCap.com, l'un des plus grands aggrégateurs de données s'agissant du marché des cryptomonnaies a affirmé que ces inquiétudes étaient fondées et prévoit de mettre en place des nouveaux outils pour que les échanges deviennent plus transparents[354].

En avril 2019, il a été reproché par le procureur général de New York à Bitfinex[355] et sa filiale, Tether une fraude, en ce que 850 millions de dollars manqueraient, elle se serait servi de ses fonds propres pour soutenir ceux de sa filiale et ainsi maintenir la parité de son stable coin le USDT avec le dollars, utilisant ainsi l'argent de ses clients. Il n'y aurait à l'heure actuelle (mai 2019) que 2,1 milliards de dollars pour couvrir les 2,8 milliard de *stable coins* USDT en circulation, la parité de 1 : 1 n'est donc garantie qu'à hauteur de 74%[356].
Il s'agit d'un système de réserves dites fractionnaires où pour chaque coin émis, l'entité n'en détiendrait qu'une partie en réserve. L'on peut par suite raisonnablement estimer que les assertions constantes dans le passé affirmant la parité de 1 :1 garanties peuvent être assimilées à des affirmations fausses et/ou trompeuses pour le marché.

---

352 « *Virtual Market Integrity Initiative* », Report of the Office of the New York State Attorney General, B. D. Underwood, Attorney General, 18 septembre 2018.
353 « *Bitwise Tells US SEC That 95% of Volume on Unregulated Crypto Exchange is Suspect* », M. Huillet, CoinTelegraph, 22 mars 2019 ; « *New Report Warns 87 Percent of Cryptocurrency Exchange Volume Is Potentially Suspicious* », W. Suberg, 19 mars 2019.
354 « *Crypto Aggregator Says Concerns Over Inaccurate Data Are Valid* », O. Kharif, Bloomberg, 25 mars 2019.
355 « *NY Attorney General sues Bitfinex and tether to unearth "fraud being carried out" by the firms* », F. Chaparro, TheBlockCrypto, 25 avril 2019 ; « *Tether admits in court to investing some of its reserves in bitcoin* », L. Cermak, TheBlockCrypto, 21 mai 2019.
356 « *Bitfinex : un accusé de Crypto Capital sous mandat d'arrê*t », Le Journal du Coin, 7 mai 2019.

CONCLUSION

En définitive, l'on peut affirmer que les crypto-actifs ne représentent pas un sujet d'infraction. L'interdiction, tant s'agissant des cryptomonnaies que des opérations de levées de fonds par émission de jetons est une voie à écarter. Il est vrai que les crypto-actifs sont liés à des infractions, tantôt comme objets de celles-ci, tantôt comme supports facilitateurs. L'on peut constater l'émergence d'une forme particulière de cybercriminalité, la crypto-criminalité, rendue possible en raison du caractère très récent, -une dizaine d'année à peine- des crypto-actifs, le sujet évoluant en permanence et la présente contribution ayant tenté le plus fidèlement possible de rendre compte des derniers développements significatifs en ce domaine en droit français comme en droit comparé, notamment américain.

La lutte contre cette criminalité spécifique est d'ores et déjà engagée, passant notamment par une autorégulation originelle du secteur des crypto-actifs, puis une réglementation de ces derniers, en droit positif français grâce à la loi Pacte, ainsi que par la répression pénale de droit commun et de droit spécial. De plus, l'éducation et la prévention du grand public au sujet des crypto-actifs et de la cybersécurité, par les acteurs de l'écosystème ainsi que la formation des enquêteurs et magistrats spécialisés, les moyens d'enquêtes adaptés, le plus souvent issus d'une collaboration entre le public et le privé[357], au niveau européen et international permettent et permettront de lutter de manière efficiente pour, si ce n'est éradiquer, du moins diminuer significativement la cybercriminalité liée aux crypto-actifs et mettre fin à aux confusions encore trop nombreuses à leurs sujets.

---

[357] Aux Etats-Unis, la *Commodity Futures Trading Commission* (CTFC) a mis en place un système de dénonciation des arnaques liées aux crypto-actifs, notamment les escroqueries (*scams*) et les manipulations liées aux monnaies virtuelles. Tant des récompenses financières que des protections sont proposées à tout à chacun, particulier, consommateur, pour la dénonciation de comportements de pump and dump, de wash-trading ou de plateformes d'échanges non déclarées. A titre indicatif, si la dénonciation entraine une sanction supériure à un million de dollars, une récompense de 10 à 30% de la sanction ira pour le particulier.
Ce mécanisme similaire à celui du lanceur d'alerte (*whisleblower*) rappelle celui existant d'ores et déjà en France en matière fiscale. Cela montre l'innovation dans les pratiques de lutte contre les infractions et la collaboration la plus large possible des acteurs tant publics que privés.

BIBLIOGRAPHIE

Ouvrages

(J.) CARBONNIER, « Sociologie juridique », éd. A. Colin, [1972], éd. PUF, coll. Thémis, Paris, [1978], Refondue coll. Quadrige, [1994] et [2004]
(A.) LEPAGE, (P.) MAISTRE DU CHAMBON, (R.) SALOMON, Droit pénal des affaires, 5e édition, LexisNexis.

(M.) QUEMENER, Criminalité économique et financière à l'ère numérique, Economica
La Blockchain décryptée, Les clefs d'une révolution, Netexplo, Mai 2016, par Blockchain France

Articles de doctrine

« *Les mystères de la blockchain »,* M. Mekki, D. 2017
« *La mise en œuvre d'une ICO : les étapes en pratique* », P. Lorentz, L. Bensoussan, A. Barbet-Massin, Revue de droit bancaire et financier, n°1, janvier-février 2019

« *Le Bitcoin devient monnaie courante : les monnaies digitales entre transparence, régulation et innovation* », V. Charpiat, Revue des Juriste de Sciences Po, 2014, n°9
« *Le dark web ou l'internet clandestin et son encadrement juridique* », P.-X. Chomiac de Sas, Revue Lamy Droit de l'Immatériel, n°49, 1er juin 2018.
« *Les dérivés sur crypto-monnaie sont des contrats financiers* ». P. Pailler, Revue de droit bancaire et financier, n°2, LexisNexis, mars-avril 2018
« *Enquêtes dans le Darkweb* », M. Quéméner, Dalloz IP/IT 2017
« *Le Darkweb, un objet juridique parfaitement identifié* », Y. Charpenel, Dalloz IP/IT 2017

« *Le Darkweb : un nouveau défi pour le droit pénal contemporain* » L. Saenko, Dalloz IP/IT 2017
« *Darkweb : plongée en eaux troubles* », O. de Maison Rouge, Dalloz IP/IT 2017
« *Regards sur une opération juridique non identifiée : les ICOs* », D. Legeais, Dalloz IP/IT 2018
« *Le dark web ou l'internet clandestin et son encadrement juridique* », P.-X. Chomiac de Sas, Revue Lamy Droit de l'Immatériel, n°49, 1er juin 2018.
« *Fintech et droit pénal : une répression entre régulation et dématérialisation* », N. Catelan, revue de droit bancaire et financier, janvier-février 2017.
« *Les applications de la blockchain dans le domaine de la finance »*, supplément, septembre 2018 J. Brosset, A. Barbet-Massin, Revue Lamy Droit des Affaires,
« *Crypto-tracking : les nouveaux outils d'enquête pour les forces de l'ordre* », A. Jomni, Revue de la gendarmerie nationale, n°263, décembre 2018.
« *ICO, Le législateur introduit des jetons dan le Code monétaire et financier* », F. Drummond, La semaine juridique édition générale n°52, 24 décembre 2018 (Le club des juristes)
« *Vers un nouveau régime pour les crypto-actifs en France* », Dossiers thématiques, Fintech, AMF, 15 avril 2019.
« *Présentation d'une nouvelle dépêche sur les cyberfraudes par crypto-actifs* », M. Quéméner, Dalloz IP/IT 2019,
« *Une première condamnation aux USA pour la commission d'infractions sur le Dark Web* », E. Caprioli, communication- commerce électronique, LexisNexis, juillet-août 2017.

Rapports

« Le cybercrime en 2019 : impact et opportunités », rapport Accenture, 6 mars 2019.
« La monnaie », Banque de France, Publications, 17 décembre 2018
« *ICO françaises : un nouveau mode de financement* ? », C. Le Moign, AMF, novembre 2018.
« *Bitcoin, totem & tabou, que présage l'essor des cryptomonnaies* ? » Rapport de l'Institut Sapiens, Février 2018.
Rapport d'information en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles, M. Eric WOERTH, Président et M. Pierre PERSON, Rapporteur, 30 janvier 2019
« *Tendances et analyse des risques* 2016 », Tracfin
« *Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies* », Rapport du Sénat,
« *Tendances et analyses des risques de blanchiment de capitaux et de financement du terrorisme en 2017-2018* », Tracfin

« *Analyse sur la qualification juridique des produits dérivés sur crypto-monnaies* », AMF

« *Forex, options binaires, arnaques financières en ligne : l'AMF, le Parquet de Paris, la DGCCRF et l'ACPR se mobilisent* », 31mars 2016.
« *Intervention de Robert Ophèle, Président de l'AMF devant la Mission d'information sur les « Monnaies virtuelles »* de la Commission des finances de l'Assemblée nationale, 5 avril 2018

Articles de presse

« *QuadrigaCX : analyse des 5 wallets liés au ''crypto grand banditisme''* », Journal du Coin.com, 23 février 2019
« *Reports Shows QuadrigaCX ''Cold Wallets'' Actively Involved in Significant Criminal Acivity: Ties to Silk Road, Hacked Funds, Identity Theft and Drug/Human Trafficking* », blog Zerononcense.com, 16 février 2019.
« Bruno Le Maire : ''Le développement de l'écosystème blockchain est une priorité pour le Gouvernement'' », Gregory Raymond, Capital, 15 avril 2019.
« Investors Bet $4 Billion on a Cryptocurrency Startup », P. Vigna, The Wall Street Journal, 29 mai 2018
« EOS, la blockchain qui veut remplacer Ethereum », C. Perreau, Le Journal du Net, 4 mars 2019
« *Russian authorities say Bitcoin illegal* », G. Baczynska, Reuters, 9 février 2014.
« *Le Bitcoin devient monnaie courante : les monnaies digitales entre transparence, régulation et innovation* »,
« *Stolen Bitcoin ATM Owners Suspect Memphis Robbery Was Inside Job* », P.H. Madore, CCN.com, 7 mars 2019
« *Un distributeur de bitcoins à Montpellier* », Bitcoin.fr, 11 août 2016. L'article, mis à jour au 17 avril 2019 affirme désormais que le distributeur n'existe plus.
« *Visa et Coinbase lancent une carte adossée à des cryptomonnaies* », L. Mearian (adaptation J. Elyan), Le Monde Informatique, 18 avril 2019.
« J'ai acheté des Bitcoins dans un tabac et je ne sais toujours pas à quoi ça sert », D.-J. Rahmil, L'ADN, 22 janvier 2019.
« *Turkcoin : Turkish Politician Endorses Launching a National Cryptocurrency* », S. Das, CCN.com, 23 février 2018.
« *Marshall Islands to issue own sovereign cryptocurrency* », G. Chavez-Dreyfuss, Reuters.com, 28 février 2018.
« *Le Venezuela dévalue sa monnaie de 96%* », Le Monde avec AFP, 21 août 2018.
« *UK Central Bank Mulls Cryptocurrency Linked To Pounds Sterling* », S. Sundararajan, Coindesk, 2 janvier 2018
« *Les crypto-monnaie d'Etat, une arme géopolitique* ? », V. Castro, Usbek & Rica, 4 juin 2018.
« *An Inside Look At China's Government Controlled Cryptocurrency Project* », L. Coleman, CCN.com, 31 mars 2018
« *Et si la France lançais sa crypto-monnaie d'Etat* ? », J. Lausson, Numerama, 2 février 2019
« *La première crypto-monnaie étatique sera-t-elle chinoise* ? » V. Lucchese, Usbek & Rica, 27 juin 2017.
« *JP Morgan est la première banque à lancer sa cryptomonnaie* », R. Bloch, Les Echos, 14 février 2019.
« *Facebook and Telegram Are Hoping to Succeed Where Bitcoin Failed* », N. Popper et M. Isaac, The New York Times, 28 février 2019.
« *Les questions étourdissantes que soulève le FacebookCoin* », C. Jeanneau et A. Stachtchenko, Blockchain Partner, 6 mars 2019.
« *WeChat interdit les transactions en cryptomonnaies* », Journal du Coin, 8 mai 2019.

« *Zuckerberg confirme la fusion des messageries Facebook, WhatsApp et Instagram* », JournalduGeek, 1er février 2019.
« *Virtual currencies and central banks monetary policy: challenges ahead* », ECON, Monetary Dialogue, juillet 2018
« *CME Group Bitcoin Futures Hit $1.3 Billion Amid Parabolic Advance* », W. Suberg, CoinTelegraph, 14 mai 2019.
« *Bitcoin Futures: From Self-Certification To Systemic Risk* », L. Reiners
« *Bitcoin et les ETF : un mariage de raison* ? » D. Fay-Manzo, Coin house Insights, 26 octobre 2018.
« *Le bitcoin a désormais sa place dans les contrats d'assurance-vie* », R. Bloch, Les Echos, 11 avril 2019.
« *The World's Largest Hedge Fund is a Fraud* », 7 novembre 2005
« Does Satoshi have 1 million BTC ? Core Dev explains why we cannot know », R. Allen, Chepicap, 13 mars 2019.
« *17 décembre 2017 : le jour où… le bitcoin a flirté avec les 20 000 dollars* », B. Eschapasse, Le Point, 4 janvier 2018
« *Comment est fixé le prix du Bitcoin* ? », J. Moretto, Coin House Insights, 13 décembre 2018.
« *Bitcoin is a market for criminals and millennials, Dennis Gartman says* », C. Aiello, CNBC, 13 novembre 2017
« *Billionaire Warren Buffett Remains Clueless About Bitcoin, Calls It 'Delusiona*l' », B.Brown, CCN.com, 25 février 2019
« *UBS Executive Paul Donovan Blasts Bitcoin Again, States Cryptos Are 'Fatally Flawed'* », W.Suberg, CoinTelegraph, 30 novembre 2018
« *Gary Shilling : Bitcoin is a black-box* », Business Insider, 4 janvier 2019
« *Jamie Dimon, le patron de JPMorgan, qualifie le bitcoin de ''fraude''* », Les Echos, 12 septembre 2017.
« *Quelques bulles, de la tulipe au bitcoin* », S. de Rivet et L. Kortobi, Libération, 13 février 2019
« *Bitcoin : la bulle qui ridiculise toutes les autres* ! », N. Gallant, Capital, 18 décembre 2017.
« *En vingt ans, le fabuleux destin boursier d'Amazon* », P.Bertrand, Les Echos, 16 mai 2017
« *La bulle du Bitcoin explose pour la 4ème fois (et ça n'est pas la pire)* », J. Guillaume, Presse-Citron.net, 28 novembre 2018
« *Amazon posts record profits again, but stock drops as revenue of $56.8B falls short of expectations* », N. Levy, GeekWire, 25 octobre 2018.
« *Warren Buffett says he 'blew it' when he didn't invest in Amazon early, and the regret is what keeps him from investing today* », J. Bort, Business Insider, 15 mai 2018
« *Cryptomonnaies : un peu de cohérence* », N. Colin, L'Obs, 27 janvier 2018
« *La grande escroquerie de la blockchain* », N. Roubini, Les Echos, 30 octobre 2018.
« *Quelle est la vraie valeur du Bitcoin* ? », D. Fay-Manzo, Coin House Insights, 16 octobre 2018.
« *Qu'est-ce qui empêche de dépasser les 21 millions de bitcoins* ? », J. Moretto, Coin House Insights, 26 octobre 2018.
« *Lightning, la mise à jour du bitcoin qui pourrait tout changer* », G. Raymond, Capital, 23 janvier 2018
« *Introduction au Lightning Network* », D. Fay-Manzo, Coin House Insights, 19 juin 2018
« *You Say Bitcoin Has No Intrinsic Value ? Twenty-two Reasons to Think Again*. », M. Rees, Bitcoin Magazine, 5 juillet 2014.
« *Venezuela's Hyperinflation Sees Record Highs of Bitcoin Use* », R. Campbell, CCN.com, 10 août 2016.
« *What is a 51% Attack ?* », Binance, 28 novembre 2018
« *Analysis :Bitcoin Costs $1.4 Billion to 51% Attack, Consumes as Much Electricity as Morocco* », M. Moos, Cryptoslate.com, 29 novembre 2019.
« *ZenCash (ZEN) victime d'une attaque des 51%* », Cryptonaute, 4 juin 2018
« *Privacy Coin Verge Succumbs to 51% Attack (Again)* », J. Wilmoth, CCN.com, 22 mai 2018
« *Bitcoin Gold Hit By Double Spend Attack, Exchanged Lose Millions* », J. Wilmoth, CCN.com, 23 mai 2018
« *Attaque des 51% sur Ethereum Classic : 1,1 million de dollars dérobés* », Journal du Coin, 8 janvier 2019
« *Bitcoin est-il vulnérable face aux ordinateurs quantiques* ? » Bitcoin.org
« *Une monnaie quantique infaillible* », Ins2i.Cnrs.fr, 30 janvier 2018,
« *Here's The Man Who Created ICOs And This Is The New Token He's Backing* », L. Shin, Forbes.com, 21 septembre 2017.
« *Launching the Ether Sale* », V. Buterin, Blog Ethereum.org, 22 juillet 2014
« *15 insights on how Ethereum conducted its ICO in 2014* », CoinNounce.com,
« The Meaning of Decentralization », Vitalik Buterin, Medium, 6 février 2017
« *Qu'est-ce qu'une DAO* ? », Blockchain France, 12 mai 2016
« *Slock.it : la promesse des objets connectés sur la blockchain* », S. Polrot, Ethereum France, 4 avril 2016
« *Automated company raises equivalent of $120M in digital currency* », R. Waters, CNBC, 17 mai 2016 ;

« *A Venture Fund With Plenty of Virtual Capital, but No Capitalist* », N. Popper, The New York Times, 21 mai 2016
« *The DAO : post mortem* », S. Polrot, Ethereum France, 24 janvier 2017.
« *EOS ou les dessous de la plus grosse ICO de l'histoire* », Les Echos, 28 juin 2018.
« *DomRaider : une ICO sur le sol français, contre vents et marées* », L. Adam, ZDNet, 6 décembre 2017.
« *Comment le marché des ''ICO'' a pris sont essor* », N. Ait-Kacimi, Les Echos, 5 octobre 2017.
« *ICO : l'impératif de transparence* », A. Stachtchenko, Medium, 5 octobre 2017
« *The Official Guide To Tokenized Securities* », A. Pompliano, Medium, 26 février 2018.
« *Société Générale émet la première obligation sécurisée sous forme de ''security tokens'' sur une blockchain publique* », Communiqué de presse
« *Les STOs peuvent-elles sauver le marché des cryptoactifs* ? », M. Zeller, Coin House Insights, 30 janvier 2019.
« *Pourquoi les Security Tokens intéressent plus les services marketing que les services juridiques ?* », W. O'Rorke, Medium, 11 avril 2019.
« *ICO : fin du buzz et retour à la raison* », Les Echos, 22 octobre 2018.
« *La Chine interdit les levées de fonds en cryptomonnaies* », F. Schaeffer, Les Echos, 5 septembre 2017.
G. Canivet, Blockchain et régulation, JCPE n°36 – Septembre 2017
« *L'affaire Tezos : la « fièvre des ICO et ses risques* », F. G'sell, Frenchweb, 26 octobre 2017
« *Tezos : la cryptomonnaie à 400 millions de dollars victime d'un conflit juridique* », Journal du Coin, 20 octobre 2017.
Podcast « 21 millions » par Grégory Raymond, Capital, 24 avril 2019
« Tezos : la plateforme de smart-contract à la gouvernance décentralisée », D. Fay-Manzo, Coin House Insights, 27 juillet 2018.
« Bitcoin : le Français Mark Karpelès mis en examen au Japon pour détournement de fonds », Le Monde avec AFP, 11 septembre 2015.
« Former Mt.Gox CEO Mark Karpeles Gets Suspended Jail Term », Bloomberg, Y. Furukawa, 15 mars 2019.
« Bitcoin : le mystérieux Alexander Vinnik », N. Ait-Kacimi, Les Echos, 27 juillet 2018.
« Bitcoin : les secrets d'Alexander Vinnik », A. Vidalie, L'Express, 11 décembre 2018.
« Hackers Steal More Than $70 Million in Bitcoin », S. Russolillo, The Wall Street Journal, 7 décembre 2017.
« Bitcoin worth $72 mllion stolen from Bitfinex exchange in Honk Kong », C. Baldwin, Reuters, 3 août 2016.
« Details of $5 Million Bitstamp Hack Revealed », S. Higgins, Coindesk, 1er juillet 2015.
« Hackers Steal $40M Worth of Bitcoin From Binance Exchange », E. Lam, Bloomberg, 8 mai 2019.
« *Komodo Hacks Itself and Saves Crypto Worth $13M After Learning of Security Vulnerability* », T. Simms, CoinTelegraph, 6 juin 2019.
« *Binance Considered Pushing for Bitcoin 'Rollback' Following $40 Million Hack* », W. Zhao, Coindesk, 8 mai 2019.
« *RIP: Bitcoin Exchange Cryptopia Begins Liquidation After $15 Million Hacking* », M. Emem, CCN, 15 mai 2019.
« *Les malwares qui se propagent sur Facebook ont un nouveau jouet : les cryptomonnaies* », J. Cadot, Numerama, 30 décembre 2017.
« *Beapy : Cryptojacking Worm Hits Enterprises in China* », Symantec, 24 avril 2019.
« *A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth* » , S. Pastrana, G. Suarez-Tangil,
« *Australian Government Employee Charged With Mining Crypto at Work* », Y. Khatri, Coindesk, 21 mai 2019.
« U.S. investor sues AT&T for $224 million over loss of cryptocurrency », G. Chavez-Dreyfuss, Reuters, 15 août 2018.
« *'TELL YOUR DAD TO GIVE US BITCOIN:' How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers* », L. Franceschi-Bicchierai, Motherboard, 30 juillet 2018.
« *Cryptocurrency Thief Gets 10 Years in Prison* », Communiqué de presse, County of Santa Clara, Office of the District Attorney, 22 avril 2019.
« *Nine Individuals Connected to a Hacking Group Charged With Online Identity Theft and Other Related Charges* », 9 mai 2019.
« *U.S. investor awarded $75 million in cryptocurrency crime case* », G. Chavez-Dreyfuss, Reuters, 10 mai 2019.
« *Is Cryptocurrency What Makes Ransomware Possible* ? », A.Levitin, 22 mai 2019
« *Ransomware WannaCry : son impressionnant bilan en huit chiffres* », N. lellouche, 01net.com, 10 mai 2017.
« *How to Accidentally stop a Global Cyber Attack*s », MalwareTech, 13 mai 2017.
« *WannaCry, un an après : un virus trop simple à désactiver* », V. Castro, Cyberguerre (Numerama), 18 décembre 2018.
« *WannaCry, un an après : un virus trop simple à désactiver* », V. Castro, Cyberguerre (Numerama), 18 décembre 2018.

« *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware* », A. Hanel, Crowdstrike Blog, 10 janvier 2019.
« *Paralysée par un puissant ransomware depuis trois semaines, Baltimore peine à relancer ses sytèmes* », G. huvelin, Cyberguerre (Numerama)
« *Baltimore ransomware nightmare could last weeks more, with big consequences* », S. Gallagher, Ars Technica, 20 mai 2019.
« *In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc* », N. Perlroth et S.shane, The New York Times, 25 mai 2019.
« *Meet 'Tox' : Ransomware for the Rest of Us* », McAfee Labs, 23 mai 2015.
« *The Trade Secret Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers* », R. Dudley et J. Kao, 15 mai 2019.
« *Marseille : Un retraité arnaqué de 810 000 euros avec des Bitcoins* », 20 Minutes, 14 septembre 2018.
« *Cryptomonnaies : une Auvergnate perd toutes ses économies sur un site frauduleux* », E. Trujillo, BFM Business, 4 septembre 2018.
« *Cryptomonnaies : Facebook interdit leur pub pour éviter les arnaques* », A. Cherif, La Tribune, 31 janvier 2018.
« *New Ads Policy: Improving Integrity and Security of Financial Product and Services Ads* », R. Leathern, Product Management Director, Facebook.
« *Bitcoin : le gendarme des marchés tacle Nabilla* », E. Goetz, Les Echos, 10 janvier 2018.
« *Escroqueries liées aux bitcoins : réagissons* ! », S. Lebeau et W. O'Rorke, La Tribune, 17 octobre 2018.
« Founders of a cryptocurrency backed by Floyd Mayweather charged with fraud by SEC », A. Kharpal, CNBC, 3 avril 2018.
« *Two Celebrities Charged With Unlawfully Touting Coin Offerings* », Communiqué de presse, U.S. Securities and Exchange Commission, 29 novembre 2018.
« *Manhattan U.S. Attorney Announces Charges Against Leaders Of "OneCoin," A Multibillion-Dollar Pyramid Scheme Involving The Sale Of A Fraudulent Cryptocurrency* », 8 mars 2019.
« *Bitcoin : arnaque à 400 millions de dollars via une chaîne de Ponzi* », La Tribune, 10 février 2015.
« *Seeking Potential Victims in Bitconnect Investigation* », Special Agent Vicki D. Anderson, 20 février 2019
« *BitConnect 2.0 : l'arnaque ultime aux crypto-monnaies renait de ses cendres* », Presse-Citron.net, 20 mai 2019.
« *L'homme le plus connu du Dark Web* », Absol Vidéos, Youtube
« *FBI Says It's Seized $28.5 Million In Bitcoin From Ross Ulbricht, Alleged Owner of Silk Road* », A. Greenberg, Forbes, 25 octobre 2013.
« *Someone Accessed Silk Road Operator's Account While Ross Ulbricht Was in Jail* », J. Koebler, Motherboard, 2 décembre 2016.
« *U.S. Supreme Court turns away Silk Road website founder's appeal* », A. Chung, Reuters, 28 juin 2018.
« Operation Onymous », Europol, Communiqué de presse
«*Court Docs Show a University Helped FBI Bust Silk Roa 2, Child Porn Suspects* », J. Cox Motherboard, 11 novembre 2015
« *Tor security advisory : ''relay early'' traffic confirmation attack* », Tor Blog, 30 juillet 2014.
« *Massive Blow To Criminal Dark Web Activities After Globally Coordinated Operation* », Europol, Communiqué de presse, 20 juillet 2017.
« *NSA and GCHQ target Tor network that protects anonymity of web users* », J. Ball, B. Scheier et G. Greenwald, The Guardian, 4 octobre 2013.
« Technical and Legal Overview of the Tor Anonymity Network », E. Çalışkan, T.s Minárik, A.-M. Osula, CCDCOE.
« *La Main noire, première plateforme du darknet démantelée en France* », S. Ghibaudo, France Inter, 16 juin 2018.
« *Double Blow to Dark Web Marketplaces* », Europol, Communiqué de presse, 3 mai 2019.
«*How German and US authorities took down the owners of darknet drug emporium Wall Street Market* », D. Coldewey, TechCrunch
« *FBI has seized Deep Dot Web and arrested its administrators* », Z. Whittaker, TechCrunch
« *Global Law Enforcement Action Against Vendors and Buyers on the Dark Web* », Europol, Communiqué de presse, 26 mars 2019
« *Attorney General Jeff Sessions Announces Results of J-Code's First Law Enforcement Operation Targeting Opioid Trafficking on the Darknet* », 3 avril 2018
« *Changes in modus operandi of Islamic tate terrorist attacks* », The Hague, 18 janvier 2016, Europol, p.7
« Despite third party reporting suggesting the use of anonymous currencies like Bitcoin by terrorists to finance their activities, this has not been confirmed by law enforcement. »

« *Criminals hide 'billions' in crypto-cash* », S. Silva, BBC, 12 février 2018, interview de M. Wainwright, directeur d'Europol.
« *Blanchiment, financement du terrorisme, escroqueries : mais que font les cryptos* ? », C. Perreau, le Journal du Net, 10 décembre 2018.
« *Two criminal groups dismantled for laundering EUR 2.5 million through smurfing and cryptocurrencies* », Communiqué de presse, Europol, 11 juillet 2018.
« *Cryptocurrency Laundering As a Service: Members of a Criminal Organisation Arrested in Spain* », Communiqué de presse, Europol, 8 mai 2019.
« *Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2017 – 2018* », Tracfin, p.55 et suiv.
« *Man Sentenced for Illegal Money Transmission Services on LocalBitcoins* », L. Manning, BitcoinMagazine, 31 mai 2019.
« *Multi-million euro cryptocurrency laundering service bestmixer.io taken down* », Communiqué de presse, Europol, 22 mai 2019
« *Bitcoin mixeurs : Bitcoin Blender ferme sa boutique* », Journal du Coin, 3 juin 2019.
« *Mastering Monero, The future of private transactions* », SerHack ainsi que la communauté Monero, première édition, p.60 et suiv.
« *Totalement anonyme, Zcash est-elle la cryptomonnaie ultime* ? » G. Kallenborn, 01net.com, 4 mars 2017
« *We need a first step toward more privacy* », V. Buterin.
« *Vitalik Buterin propose une solution pour anonymiser les transactions Ethereum uniques* », M. Debelloir, Cryptoast, 24 mai 2019.
« *Europol and Chainalysis reinforce their cooperation in the fight against cybercrime* », Europol, 19 février 2016.
« *La NSA a traqué les utilisateurs de Bitcoin dans le monde entier* », J. Lausson, Numerama, 21 mars 2018 ; « *The NSA Worked to ''Track down'' Bitoin Users, Snowden Documents reveal* », S. Biddle, the Intercept, 20 mars 2018.
« *Project to prevent criminal use of the dark web and virtual currencies launched by international consortium* », CORDIS EU research results, 1er juin 2017.
« *Making Bitcoin Legal »,* R. Andeson, I. Shumailov, M. Ahmed
« *A 200-year-old idea offers a new way to trace stolen bitcoins* », A. Greenberg, Wired, 4 mai 2018.
« *Scammers Boost Price With Fake Satoshi Confirmation* », J. Biggs, Coindesk, 29 mai 2019.
« *Bitcoin SV pumps after fake Craig Wright Satoshi news tricks Chinese investors* », A. Martinez, Cryptoslate, 29 mai 2019.
« *The Bitcoin Whales : 1,000 People Who OWn 40 Percent of the Market* », O. Kharif, Bloomberg, 8 décembre 2017.
« *University researchers identified over 4,800 pump and dump schemes involving crypto over a six month period* », Theblockcrypto, 20 décembre 2018. ; « *The Economics of Crypocurrency Pump and Dump Schemes* », JT Hamrick, F. Rouhi, A. Mukherjee, A. Feder, N. Gandal, T. Moore, M.Vasek.
« *Anatomie d'un groupe de pump and dump* », Journal du Coin, 28 juillet 2018 ; « *The Anatomy of a Pump & Dump Group* », B. Skvorc, Bitfalls.com, 12 janvier 2018 ; « Walkthrough: How traders 'pump and dump' cryptocurrencies », O. Williams-grut, Business Insider, 14 novembre 2017.
« *U.S. Launches Criminal Probe into Bitcoin Price Manipulation* », M. Robinson, T. schloenberg, Bloomberg, 24 mai 2018.
« *Bitcoin Futures Manipulation: How it Works and How to Reduce it* », N. Puckrin,CCN, 19 décembre 2018.
« *Virtual Market Integrity Initiative* », Report of the Office of the New York State Attorney General, B. D. Underwood, Attorney General, 18 septembre 2018.
« *Bitwise Tells US SEC That 95% of Volume on Unregulated Crypto Exchange is Suspect* », M. Huillet, CoinTelegraph, 22 mars 2019
« *New Report Warns 87 Percent of Cryptocurrency Exchange Volume Is Potentially Suspicious* », W. Suberg, 19 mars 2019.
« *Crypto Aggregator Says Concerns Over Inaccurate Data Are Valid* », O. Kharif, Bloomberg, 25 mars 2019.
« *NY Attorney General sues Bitfinex and tether to unearth ''fraud being carried out'' by the firm*s », F. Chaparro, TheBlockCrypto, 25 avril 2019
« *Tether admits in court to investing some of its reserves in bitcoin* », L. Cermak, TheBlockCrypto, 21 mai 2019.
« *Bitfinex : un accusé de Crypto Capital sous mandat d'arrê*t », Le Journal du Coin, 7 mai 2019.

TABLE DES MATIERES