☐ Copie Juré
☐ Copie Conseiller
☐ Copie Infothèque

h e g

Haute école de gestion
Genève

Evaluation du risque de blanchiment d'argent lié aux cryptomonnaies

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Théo MALACARI

Conseiller au travail de Bachelor :

Jonathan MASSONNET

Genève, le 12 Juillet 2019

Haute École de Gestion de Genève (HEG-GE)

Filière Economie d'entreprise, Orientation Banque et Finance

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre de Bachelor of Science en économie d'entreprise orientation Banque et Finance.

L'étudiant a envoyé ce document par email à l'adresse d'analyse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND. http://www.urkund.com/fr/student/392-urkund-faq

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 12 Juillet 2019

Théo Malacari

Remerciements

Ce mémoire est l'aboutissement de ces 4 années passées à la Haute Ecole de Gestion de Genève au sein de la filière Economie d'entreprise en emploi. Ce fut une expérience très enrichissante d'un point de vue humain et intellectuel qui m'a permis de trouver l'orientation à donner à ma carrière professionnelle.

Je tiens à remercier Monsieur Jonathan Massonnet pour son aide et ses précieux conseils tout au long de la réalisation de ce travail. J'aimerai également remercier tout le corps enseignant de la Haute Ecole de Gestion de Genève pour avoir pris le temps de partager leurs connaissances et leurs expériences tout au long de ces 4 années.

Finalement, je tiens à remercier ma famille ainsi que mes amis proches pour leur soutien et leurs encouragements.

Résumé

Depuis l'envolée du prix du Bitcoin en décembre 2017, les cryptomonnaies n'ont cessé d'intriguer et d'intéresser les investisseurs, les entreprises, les gouvernements et même les personnes lambda sans expérience particulière dans le milieu de l'investissement. Le nombre de cryptomonnaies différentes ne cesse de se multiplier et se monte, à la moitié de l'année 2019, à plus de 2'200. Leur technologie sous-jacente est également très particulière et offre de nombreuses opportunités. Elle se base principalement sur la désintermédiation financière et l'anonymat des transactions. Du point de vue purement économique, elles ne peuvent pas être considérées comme des monnaies à proprement dites mais plutôt comme des actifs financiers numériques qui se différencient par leur volatilité très élevée. Légalement, elles ne sont encore que très peu réglementées, ce qui offre des opportunités pour les criminels.

L'objectif de ce travail est de comprendre les risques de blanchiment d'argent liés aux cryptomonnaies et à leur technologie sous-jacente qu'est la blockchain. La Suisse est très présente dans le monde des monnaies virtuelles. Une analyse sera effectuée sur la législation suisse en vigueur et le positionnement du gouvernement. Il sera également important de comprendre si ce sont simplement des actifs financiers utilisés principalement par les escrocs à des fins de blanchiment d'argent ou réellement un moyen qui révolutionnera entièrement le monde financier.

Ce travail rappellera dans un premier temps ce qu'est le blanchiment d'argent et comment il est combattu en Suisse. Puis, une analyse sera effectuée sur les cryptomonnaies et la blockchain. Enfin, les risques de blanchiment d'argent liés aux cryptomonnaies ainsi que les règlementations en vigueur à leur encontre seront exposés.

Les résultats qui ressortent de ce travail montrent que de nombreux risques de blanchiment d'argent sont spécifiques aux cryptomonnaies et que leurs caractéristiques possèdent beaucoup plus d'atouts positifs que négatifs pour les criminels souhaitant blanchir de l'argent illégalement obtenu. Plusieurs études réalisées démontrent que le Bitcoin est très apprécié par les escrocs. Au niveau Suisse, le Conseil fédéral est ouvert au développement de la blockchain et souhaite que le pays s'établisse en tant que place économique innovante et durable de premier plan pour les sociétés Fintech et Blockchain. Il considère également que la Suisse a mis en place actuellement la meilleure législation possible autour des cryptomonnaies.

Table des matières

Liste des tableaux

Liste des figures

1. Introduction

La Suisse est depuis tout temps une plaque tournante de la gestion de fortune internationale pour la clientèle privée et institutionnelle. Grâce à son expertise, son expérience, son envergure et sa stabilité économique et politique, la place financière suisse est devenue un leader mondial dans la gestion de fortune. Selon une récente étude nommée « Deloitte International Wealth Management Centre Ranking 2018 », le marché financier suisse se trouve en première position des pays en termes de compétitivité, de taille et de performance (Deloitte 2018). Comme le montre le tableau ci-dessous, la Suisse est toujours le plus grand centre financier du monde avec 1'840 USD milliards de volume de marché international.

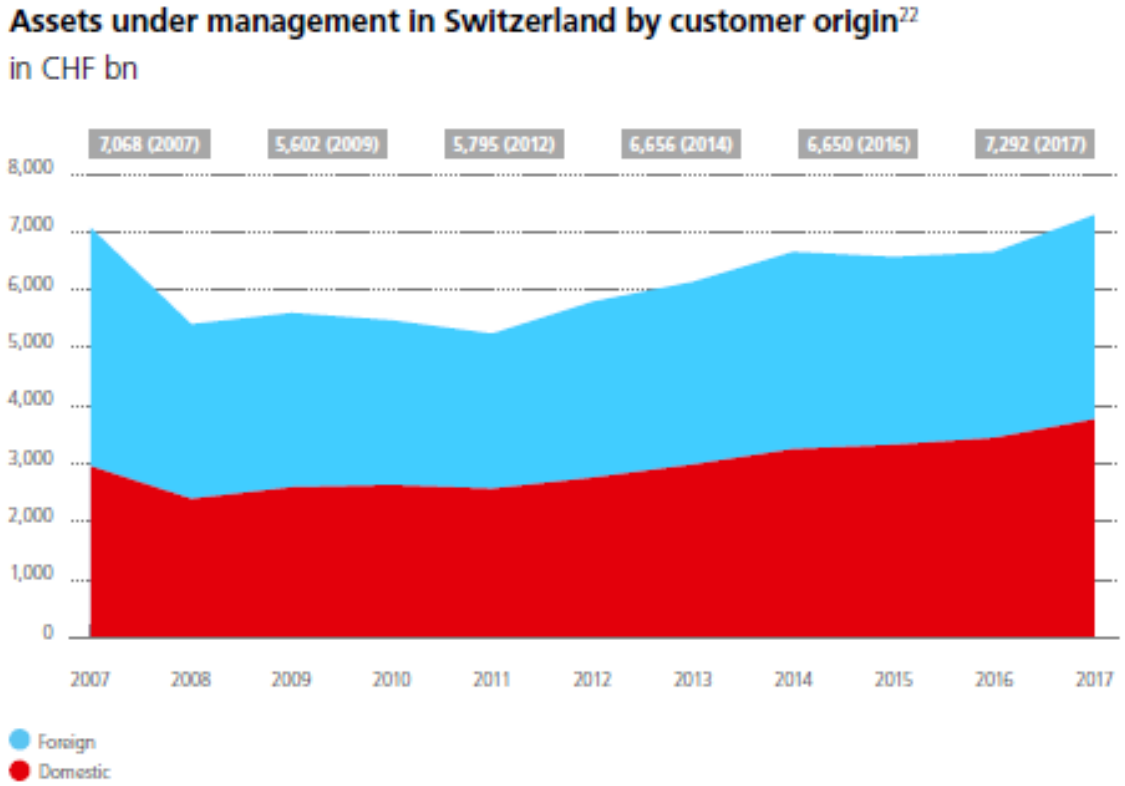
Tableau 1 : WM AuM par pays 2010-2017 (en USD billions)

WM centre	2010	2011	2012	2013	2014	2015	2016	2017E	Δ 2010–2017E
	1.98 21 %	1.80 22 %	2.11 24 %	2.14 23 %	2.14 23 %	1.94 23 %	2.01 25 %	1.84 21 %	−0.13 −7 %
	1.65 18 %	1.52 18 %	1.68 19 %	1.77 19 %	1.86 20 %	1.71 21 %	1.68 21 %	1.79 21 %	0.15 +9 %
	1.00 11 %	1.09 13 %	1.21 14 %	1.31 14 %	1.39 15 %	1.27 15 %	1.41 17 %	1.48 17 %	0.48 +48 %
	0.35 4 %	0.37 4 %	0.48 5 %	0.59 6 %	0.64 7 %	0.71 9 %	0.73 9 %	0.79 9 %	0.43 +122 %
	1.82 20 %	1.25 15 %	1.05 12 %	1.11 12 %	0.99 11 %	0.72 9 %	0.56 7 %	0.60 7 %	−1.22 −67 %
	0.42 5 %	0.41 5 %	0.36 4 %	0.43 5 %	0.46 5 %	0.47 6 %	0.44 5 %	0.47 5 %	0.05 +12 %
	0.21 2 %	0.20 2 %	0.23 3 %	0.24 3 %	0.25 3 %	0.24 3 %	0.23 3 %	0.26 3 %	0.05 +25 %
	0.07 1 %	0.06 1 %	0.06 1 %	0.07 1 %	0.07 1 %	0.06 1 %	0.06 1 %	0.06 1 %	−0.02 −24 %
	0.02 0 %	0.02 0 %	0.02 0 %	0.01 0 %	0.02 0 %	0.02 0 %	0.02 0 %	0.01 0 %	−0.00 −21 %
Other[1]	1.76 19 %	1.64 20 %	1.67 19 %	1.69 18 %	1.34 15 %	1.18 14 %	1.05 13 %	1.32 15 %	−0.44 −25 %
Total	**9.28** 100 %	**8.37** 100 %	**8.86** 100 %	**9.36** 100 %	**9.15** 100 %	**8.31** 100 %	**8.18** 100 %	**8.62** 100 %	−0.66 −7 %

Source : (Deloitte 2018)

La gestion de fonds privés transfrontaliers représente une partie importante de l'activité des banques suisses. A la fin de l'année 2017, les actifs sous gestion transfrontaliers représentaient près de la moitié des AuM totaux, soit 48.3% (Banque nationale suisse 2019).

Figure 1 : AuM en Suisse par origine du client



Source : (Banque nationale suisse 2019)

L'importance de l'activité de Wealth Management aussi bien pour les clients nationaux qu'internationaux implique inévitablement des risques d'utilisation de la place financière à des fins criminelles, notamment à travers le blanchiment d'argent. Selon l'Office des Nations Unies contre la drogue et le crime, le montant estimé du blanchiment d'argent chaque année est de 2 à 5% du PIB mondial, soit entre 800 et 2'000 USD milliards (Office des nations unies contre la drogue et le crime 2019). La Suisse dispose d'un système solide et complet en termes de lutte contre le blanchiment d'argent qui est reconnu mondialement.

Depuis une dizaine d'années, de nombreuses avancées technologiques importantes modifiant le paysage social et économique ont vu le jour. Parmi elles, la blockchain, qui a été créée la première fois en 2009 lors de l'invention du Bitcoin, est inévitablement une des plus intéressantes. Outre le Bitcoin qui constitue la monnaie virtuelle la plus populaire, le nombre global de cryptomonnaies ne cesse de croître et se monte à ce jour à plus de 2'200 (CoinMarketCap 2019).

La Suisse est devenue en très peu de temps une place convoitée et appréciée des entreprises actives dans la technologie blockchain. Le canton de Zoug, dans lequel sont implantées plus de 200 start-ups actives dans la monnaie virtuelle, est surnommé la « Crypto Valley » en référence à la « Silicon Valley » à San Francisco. C'est notamment

dans ce canton que la fondation Ethereum, qui a pour mission la promotion et le soutien de la plateforme Ethereum, s'est installée. En termes de capitalisation de marché, la cryptomonnaie Ethereum est à la deuxième position juste derrière le Bitcoin avec plus de 29 USD milliards (CoinMarketCap 2019). D'autres sociétés actives dans les cryptomonnaies et la blockchain se sont installées à Zoug comme les fondations Icon, Tezos, Lisk ou encore Cardano (GCBF 2018).

Inévitablement, les monnaies virtuelles sont devenues de plus en plus populaires auprès des investisseurs. La demande est grandissante et explique notamment la multiplication de leur nombre. Leur technologie sous-jacente, qui se base principalement sur la décentralisation et l'anonymat des transactions, augmente-elle le risque de blanchiment d'argent ? Ce travail permettra de comprendre et d'évaluer le risque de blanchiment d'argent provenant des cryptomonnaies et plus particulièrement de leur technologie sous-jacente qu'est la blockchain.

2. Contexte

2.1 L'histoire du terme de blanchiment d'argent

L'histoire de la lutte contre le blanchiment d'argent telle que nous la connaissons aujourd'hui s'étend sur près d'un demi-siècle, voire plus si on inclut les cas des gangsters américains d'avant la Seconde Guerre mondiale. Le terme de « blanchiment » vient historiquement des années 20 aux Etats-Unis à l'époque de la prohibition. La mafia avait pris le contrôle de laveries automatiques et les revenus touchés alors illicitement provenant notamment de la vente d'alcool, qui était prohibé à ce moment-là, étaient investis dans ces chaînes de laveries automatiques. Le but était de mêler l'argent « sale » qui provenait des activités illégales à l'argent « propre » qui provenait des clients venant laver leur linge. L'argent « sale » était ainsi « lavé » en effaçant complètement son origine. Le plus célèbre des gangsters ayant utilisé ce procédé aux Etats-Unis est Al Capone, chef de la famille mafieuse de Chicago. Dans les années 20, il avait racheté une chaîne entière de laveries automatiques afin de blanchir ses revenus provenant d'activités illégales. Il a été condamné en 1931 pour fraude fiscale, la police n'ayant pas réussi à le faire condamner pour vente de substances interdites ou pour blanchiment d'argent, délit encore inconnu à ce moment (Van Duyne, Harvey et Gelemerova 2018).

2.2 Les sources de blanchiment d'argent

Deux sources de risques de blanchiment d'argent sont à distinguer (Gomez et Matelly 2018) :

- L'argent noir ;
- L'argent sale.

L'argent noir provient d'activités légales mais non déclarées. Par conséquent, il s'agit de pratiques telles que l'évasion fiscale et la fraude fiscale. La fraude fiscale est le fait de falsifier sa déclaration fiscale afin de payer moins d'impôts en ne déclarant par exemple pas tout son patrimoine imposable. L'évasion fiscale quant à elle consiste à éviter ou à faire diminuer ses impôts en se faisant imposer dans un autre pays, notamment dans un paradis fiscal. Plusieurs banques suisses ont récemment eu des problèmes avec la justice internationale pour des motifs d'aide à l'évasion fiscale. La plus célèbre d'entre elles est UBS qui a été condamnée à plusieurs reprises pour avoir aidé des contribuables à se soustraire à l'Administration fiscale de leur pays respectif. En 2009, UBS s'est acquittée d'une amende de 780 USD millions car elle était accusée d'avoir aidé 20'000 citoyens américains à se soustraire au fisc (AGEFI 2019). Plus récemment, en février 2019, elle a été condamnée par la justice française à une amende record de 3.7 EUR milliards (AGEFI 2019). Dans cette affaire, il est reproché à UBS d'avoir, entre 2004 et 2012, envoyé des

commerciaux en France et d'avoir démarché des riches citoyens français en leur convainquant d'ouvrir des comptes non déclarés en Suisse.

L'argent sale quant à lui provient d'activités illégales et criminelles. C'est l'argent qui provient principalement du trafic de drogue et du crime organisé. La transformation de cet argent « sale » en argent « propre » est le mécanisme de blanchiment.

2.3 Mécanisme de blanchiment d'argent

Le blanchiment d'argent s'exécute généralement en trois phases distinctes (Deblis 2016). Tout débute par le placement, aussi appelé le prélavage. Cette première phase consiste à se débarrasser de l'argent provenant d'activités illégales en l'introduisant dans le système financier. La pratique la plus courante est le « smurfing » qui consiste à effectuer, par le biais de plusieurs personnes, des dépôts sous le seuil de déclaration réglementaire de l'origine des avoirs.

La deuxième phase se nomme l'empilage, aussi appelée le lavage. Cette deuxième étape consiste à dissimuler la réelle origine des fonds en effectuant de nombreuses transactions entre différents comptes, et la majorité du temps entre plusieurs pays, dans le but de rendre le traçage complexe.

La troisième est l'intégration, aussi appelée l'essorage. Cette troisième et dernière étape consiste à rendre licite les fonds provenant des activités illicites par l'achat de sociétés cotées ou non cotées ou l'achat de biens immobiliers par exemple.

2.4 La Lutte contre le blanchiment d'argent

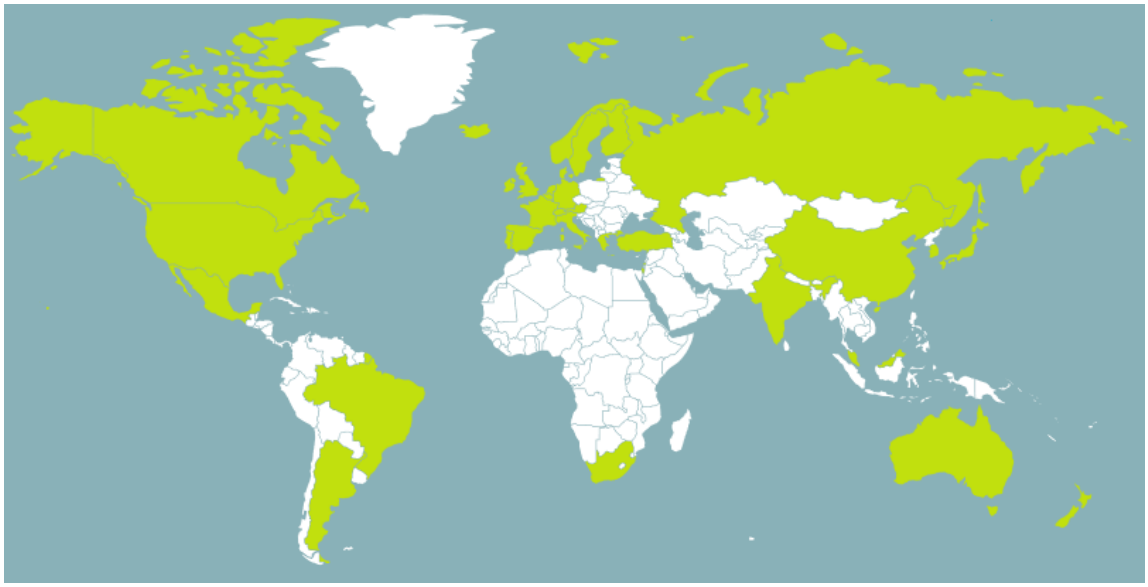
2.4.1 Cadre réglementaire international

2.4.1.1 Le GAFI

Au niveau mondial, la lutte contre le blanchiment d'argent et le financement du terrorisme est dirigée par le Groupe d'action financière (GAFI). Le GAFI, dont le siège est à Paris, est un organisme intergouvernemental qui a été créé en 1989 par le G7 et qui représente l'organisation internationale de référence contre la lutte de ces infractions. Le GAFI a pour but l'élaboration des normes en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. En 1990, l'organisme a élaboré 40 recommandations visant à définir un cadre global que chaque pays devrait mettre en place afin de se prémunir contre le blanchiment d'argent et également le financement du terrorisme. Ces recommandations sont par conséquent les normes internationales que tous les pays devraient appliquer. Suite notamment à l'évolution des techniques de blanchiment, elles ont été mises à jour plusieurs fois au fil du temps, la dernière fois étant en 2012. Tous les pays membres doivent impérativement respecter les normes du GAFI. Le GAFI dispose

également de membres associés spécialisés dans diverses parties du monde comme le Groupe d'Action Financière du Moyen-Orient et de l'Afrique du nord (GAFIMOAN) ou encore le Groupe d'Action Financière d'Amérique latine (GAFILAT).

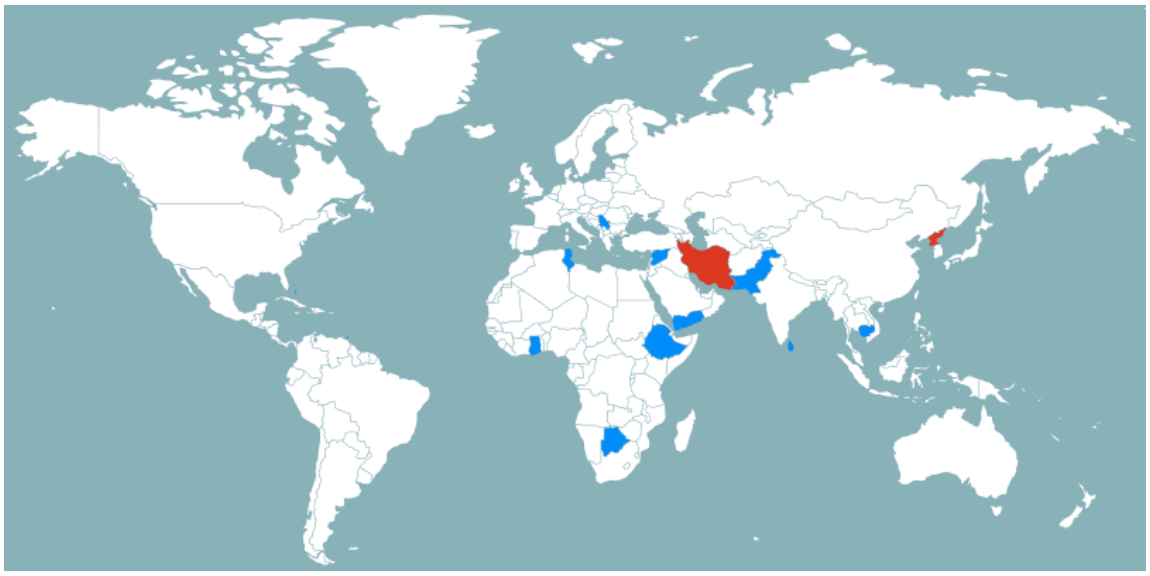
Figure 2 : Pays membres du GAFI



Source : (GAFI 2019)

Le GAFI évalue également le respect des normes par les pays qui ne sont pas membres de l'organisation. Le 23 février 2018, dans le cadre de son examen permanent de la conformité aux normes de lutte contre le blanchiment d'argent visant à protéger le système financier international, le GAFI a identifié les juridictions qui présentent des défaillances stratégiques et travaille avec elles pour combler les lacunes qui posent un risque pour le système financier international. Les pays identifiés sont notamment l'Ethiopie, l'Iraq, la Serbie, le Sri Lanka, la Syrie et la Tunisie. Chaque administration a fourni un engagement politique écrit de haut niveau pour combler les lacunes relevées par le GAFI à leur encontre (GAFI 2019). Le GAFI permet par conséquent aux autorités mondiales d'avoir connaissance des juridictions dans lesquelles les normes de blanchiment d'argent ne sont pas respectées ou suffisantes et permet la normalisation de cette lutte au niveau mondial.

Figure 3 : Juridictions à hauts risques selon GAFI



Source : (GAFI 2019)

2.4.2 Cadre réglementaire suisse

2.4.2.1 La FINMA

Au niveau Suisse, c'est l'Autorité fédérale de surveillance des marchés financiers (FINMA) qui représente le fer de lance de la lutte contre le blanchiment d'argent et le financement du terrorisme. La mission principale de la FINMA est la surveillance prudentielle du marché financier en mettant au premier plan la protection des créanciers et des investisseurs. Elle est indépendante sur le plan institutionnel, fonctionnel et financier (FINMA 2019).

La FINMA délègue et mandate la surveillance des intermédiaires financiers à des sociétés d'audit externes qui ont comme responsabilité de vérifier que les banques et autres intermédiaires financiers respectent toutes les dispositions de la loi. Les sociétés d'audit les plus connues sont les membres du célèbre « big four » comprenant EY, PwC, Deloitte et KPMG. Chaque année, ces sociétés contrôlent les intermédiaires financiers sous surveillance de la FINMA.

La protection des investisseurs et la garantie de l'intégrité du système se base sur une surveillance prudentielle de certains intermédiaires financiers (banques, négociants, assurances, etc.). Cependant, les aspects relatifs à la lutte contre le blanchiment d'argent sont surveillés chaque année pour tous les intermédiaires financiers (y compris les gérants de fortune, avocats, bureaux de change, fiduciaires, etc.) (Winiker 2019).

2.4.2.2 Code pénal

En Suisse, la notion de blanchiment d'argent est de source pénale. Selon l'article 305bis al.1 du code pénal suisse : « Celui qui aura commis un acte propre à entraver

l'identification de l'origine, la découverte ou la confiscation de valeurs patrimoniales dont il savait ou devait présumer qu'elles provenaient d'un crime ou d'un délit fiscal qualifié, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire ». Les valeurs patrimoniales doivent provenir d'un crime ou d'un délit fiscal qualifié.

Selon l'article 10 al.2 du code pénal suisse, les crimes sont des infractions passibles d'une peine privative de liberté de plus de trois ans. De plus, l'acte doit être fait par intention (savait) ou par dol éventuel (devait présumer). Il n'est par conséquent pas nécessaire de connaître le crime, il suffit de présumer une infraction grave. Selon le CPS, il ne peut pas y avoir blanchiment d'argent par négligence.

L'article 305bis al.2 du code pénal suisse précise également que « Dans les cas graves, la peine sera une peine privative de liberté de cinq ans au plus ou une peine pécuniaire. En cas de peine privative de liberté, une peine pécuniaire de 500 jours-amende au plus est également prononcée ». Le cas grave implique que le délinquant agit comme membre d'une organisation criminelle, d'une bande formée pour se livrer de manière systématique au blanchiment d'argent ou réalise un chiffre d'affaires ou un gain important en faisant métier de blanchir de l'argent.

Par conséquent, la législation distingue clairement deux cas. Le premier cas dans lequel l'intermédiaire financier se retrouve face à un auteur de blanchiment d'argent et ne va pas chercher concrètement au-delà du minimum légal, notamment à bien identifier l'origine de la fortune. Dans le deuxième cas, l'intermédiaire financier serait directement complice du blanchiment d'argent et aurait très certainement un membre de ses organes de décision qui serait corrompu.

2.4.2.3 Bases légales

L'Assemblée fédérale de la Confédération suisse a créé le 1er avril 1998 la loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (LBA). Cette loi a pour but de régler la lutte contre le blanchiment d'argent au sens de l'article 305bis du code pénal suisse, la lutte contre le financement du terrorisme et la vigilance requise en matière d'opérations financières (LBA 2019).

Dans la section 3a de la LBA, la Confédération délègue la surveillance des intermédiaires financiers à la FINMA. Sur la base des articles 17 et 18, al. 1, let. e, LBA, la FINMA a mis en place l'Ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA), entrée en vigueur le 1er janvier 2016. Cette ordonnance a pour but de préciser les obligations des intermédiaires financiers en matière de prévention contre le blanchiment d'argent et le financement du terrorisme (OBA-FINMA 2019).

En accord avec la FINMA, les intermédiaires financiers peuvent adopter des règles déontologiques provenant de directives et de conventions d'organismes d'autorégulation (OAR). Les OAR sont des associations professionnelles qui ne sont pas étatiques et représentent les intérêts de leurs membres. Les organismes reconnus par la FINMA figurent sur son site internet. Le système d'autorégulation est spécifique à la Suisse et provient d'une grande tradition. La motivation principale de ces organismes est qu'ils préfèrent anticiper les éventuels manquements de la loi sur certains thèmes en mettant en place des directives et conventions avec l'objectif qu'elles soient par la suite reprises officiellement par la FINMA. Le but est d'anticiper la mise en place d'une loi directement par la FINMA et ainsi éviter une règlementation qui pourrait être, à leurs yeux, trop restrictive pour leur industrie.

La circulaire 2008/10 de la FINMA indique quelles sont les normes d'autorégulation reconnues comme standards minimaux. La FINMA a ainsi décidé d'élever au rang de standard minimum la Convention relative à l'obligation de diligence des banques (CDB 16). La CDB 16 est une autoréglementation de l'Association suisse des Banquiers, à la base mise en place pour les banques uniquement, imposée aux banques et aux négociants en valeurs mobilières de la place financière suisse soumis à la LBA. Ils doivent signer cette convention afin d'attester qu'ils la respecteront. Le but principal de cette autoréglementation est de fixer les obligations relatives à l'identification du cocontractant, du détenteur de contrôle et de l'ayant droit économique des valeurs patrimoniales d'un compte. Elle précise ainsi les articles 3 à 5 de la LBA (CDB 2016).

2.4.3 Surveillance des intermédiaires financiers

Comme expliqué précédemment, la surveillance des intermédiaires financiers suisses est exercée par la FINMA qui délègue et mandate cette responsabilité à des sociétés d'audit. Sur la base de papiers de travaux fournis et disponibles sur le site Internet de la FINMA, les auditeurs effectuent des contrôles au sein des établissements sous revue afin de s'assurer que toutes les règles en vigueur de lutte contre le blanchiment d'argent soient respectées. Dans leur mission, les auditeurs travaillent en étroite collaboration avec le département Compliance des intermédiaires financiers qui est chargé de fournir toutes les informations disponibles. Chaque année, la FINMA rédige un « formulaire de saisie » dans lequel les informations à contrôler sont listées. Sur la base de la population de tous les clients et contreparties de l'intermédiaire financier, les sociétés d'audit effectuent une sélection d'un échantillon à contrôler. Dans cette sélection, le contrôle des clients comportant des risques accrus est privilégié. Les conclusions des tests sont envoyées chaque année en janvier à la FINMA par le biais du formulaire de saisie. Les points

principaux contrôlés devant être respectés par les intermédiaires financiers sont définis ci-dessous.

2.4.3.1 Identification

La première étape pour un intermédiaire financier est de devoir identifier correctement le cocontractant, le détenteur de contrôle et l'ayant droit économique du compte selon les articles 3 à 5 de la LBA, précisés par la CDB 16. Cette identification doit être faite à l'aide de formulaires spécifiques liés à la forme juridique de la contrepartie qui se trouvent en annexe de la CDB 16. Ainsi, un formulaire A doit être utilisé pour l'identification des personnes physiques et des sociétés de domicile, un formulaire K pour les individus qui contrôlent une société opérationnelle non cotée en bourse, un formulaire T pour les trusts, un formulaire S pour les fondations et un formulaire I pour les insurance wrappers (assurances-vie avec gestion de compte/dépôt séparée).

L'intermédiaire financier doit pouvoir prouver qu'il a la certitude et la connaissance de l'identité de la personne ayant ouvert le compte et de la personne ayant le contrôle des avoirs de ce compte. Dans le cas des personnes physiques, la grande majorité du temps, le cocontractant est également l'ayant droit économique du compte. Mais si tel n'est pas le cas, les deux personnes doivent être distinctement identifiées. Dans le cas d'ouvertures pour le compte de sociétés opérationnelles, il est nécessaire d'identifier les détenteurs de contrôle de la société qui contrôlent 25% ou plus du capital ou des voix.

2.4.3.2 Obligations de diligence générales

Les articles 10-12 de l'OBA-FINMA énumèrent les obligations de diligence générales devant être respectées par l'intermédiaire financier. L'article 10 de l'OBA-FINM exige notamment que tous les ordres de paiements réalisés doivent impérativement contenir le nom, le numéro de compte et l'adresse du donneur d'ordre ainsi que le nom et le numéro de compte du bénéficiaire.

2.4.3.3 Obligations de diligence particulières

Les articles 13-21 de l'OBA-FINMA énumèrent les obligations de diligence particulières devant être respectées par l'intermédiaire financier.

2.4.3.3.1 Relations d'affaires comportant des risques accrus

Suite à l'évaluation de leur risque spécifique, les clients comportant des risques accrus sont classés dans deux catégories. La première catégorie concerne les clients de type PEP (Personnalité Exposée Politiquement) qui représente la catégorie de risque la plus élevée. Les clients définis comme PEP exercent ou ont exercé par le passé une fonction publique importante. Il y a également une séparation entre les PEP nationaux, étrangers

et tenant des fonctions de direction au sein d'organisations intergouvernementales ou de fédérations sportives internationales. Les personnes proches d'un PEP doivent également être définies comme PEP. Les PEP sont les types de clients les plus étroitement contrôlés en raison de leurs relations et leur pouvoir importants.

La deuxième catégorie concerne les clients de type RA (Risques Accrus). Les clients identifiés comme risques accrus sont des clients qui, de par leur situation, remplissent certains critères de risques mis en place par l'intermédiaire financier. Les critères à prendre en compte sont définis dans l'article 13 de l'OBA-FINMA. Il y a par exemple le siège, le domicile et la nationalité du cocontractant, du détenteur de contrôle ou de l'ayant droit économique. Peuvent être également utilisés comme critère le lieu et le type d'activité commerciale du cocontractant ou de l'ayant droit économique ainsi que la complexité de la structure mise en place, notamment en cas d'utilisation de sociétés de domicile. Les critères à prendre en compte sont mis en place par l'intermédiaire financier dans le cadre de l'article 13 de l'OBA-FINMA. Afin qu'un client soit défini comme risques accrus, il est nécessaire, pour la plupart des critères de risque, qu'il y ait une cumulation de deux critères au minimum. Néanmoins, des clients de type PEP ou proches de PEP doivent automatiquement être définis comme des clients à risques accrus.

Selon l'article 18 de l'OBA-FINMA, l'admission de l'ouverture d'une relation à risques accrus doit être validée par un supérieur hiérarchique, un organe supérieur ou la direction. De plus, selon l'article 19 de l'OBA-FINMA, les relations avec des PEP doivent être revues annuellement par la direction de l'intermédiaire financier.

2.4.3.3.2 Transaction comportant des risques accrus

Les intermédiaires financiers doivent avoir mis en place des critères internes définissant les transactions à risques accrus. Ces transactions doivent être identifiées par le système informatique de contrôle de l'établissement et vérifiées en interne par le département Compliance. Les critères doivent permettre de détecter des transactions préalables au blanchiment d'argent en se basant sur les mécanismes connus. L'article 14 de l'OBA-FINMA définis le type de critères qui peuvent être mis en place. Ainsi, cela peut être le montant important des entrées et sorties de valeurs patrimoniales, la fréquence élevée de transactions de petits montants, ou encore les apports et retraits effectués en espèce.

2.4.3.3.3 Clarifications complémentaires

Il est du ressort de l'intermédiaire financier de documenter de manière plausible et compréhensible les clarifications complémentaires concernant les différents types de relations d'affaires nécessitant des obligations de diligence particulières. Cela est fait au travers d'un KYC (Know Your Customer), nom donné au processus d'identification du

client comportant notamment les informations sur ses activités passées et actuelles, sur l'origine de sa fortune, sur ses motivations de l'ouverture du compte et sur toute autre information complémentaire personnelle et professionnelle. Un point d'attention particulier est porté sur l'identification de l'origine de la fortune. En effet, la fortune peut provenir des bénéfices des activités professionnelles de la personne, d'un héritage, de dividendes ou encore de la vente d'actifs. Dans ce cas, il s'agit de s'assurer que les fonds ne proviennent pas d'activités illicites ou d'un délit fiscal.

Selon l'article 16 de l'OBA-FINMA, les intermédiaires financiers ont divers moyens permettant de s'assurer de la provenance des fonds ainsi que des informations données par le client. Il est par exemple vivement conseillé de rencontrer le client physiquement lors du processus d'ouverture du compte ou encore d'effectuer une visite du lieu dans lequel le client exerce son activité (entreprise, usine, bureau, etc.). Les sources d'informations externes telles que les bases de données « World-check » et « Lexis Nexis » sont également systématiquement utilisées. Elles permettent d'identifier des éventuels événements négatifs ayant eu lieu dans la vie du client telle que des soupçons de blanchiment d'argent ou de corruption. Les intermédiaires financiers peuvent également mandater des entreprises externes spécialisées dans l'identification des personnes, de leur vie privée et de leur activité professionnelle. Cela est généralement utilisé dans les cas délicats pour lesquels des doutes subsistent quant aux réelles activités du client et la provenance de ses fonds. L'établissement d'un rapport en profondeur sur le client permettra ainsi au département Compliance d'avoir plus d'informations crédibles permettant d'effectuer son choix quant à l'autorisation ou au refus de l'ouverture du compte. La documentation de ces clarifications complémentaires est essentielle et doit être compréhensible pour des tiers.

2.4.3.4 Mesures organisationnelles

Les articles 23-27 de l'OBA-FINMA énumèrent les mesures organisationnelles devant être mises en place par l'intermédiaire financier. Il doit mettre en place un service spécialisé de lutte contre le blanchiment d'argent, organisé de manière adéquate et suffisamment qualifié. Selon l'article 25 de l'OBA-FINMA, les tâches effectuées par ce service doivent être conformes aux dispositions légales. Selon l'article 26 de l'OBA-FINMA, l'intermédiaire financier doit avoir mis en place une directive interne de lutte contre le blanchiment d'argent couvrant tous les aspects légaux. La directive est passée sous revue par les auditeurs afin de détecter d'éventuels manquements à certaines dispositions légales LBA et certaines ambiguïtés dans la rédaction. Selon l'article 27 de l'OBA-FINMA, l'intermédiaire financier doit engager dans son département de lutte contre le blanchiment d'argent des employés intègres et les former de manière adéquate.

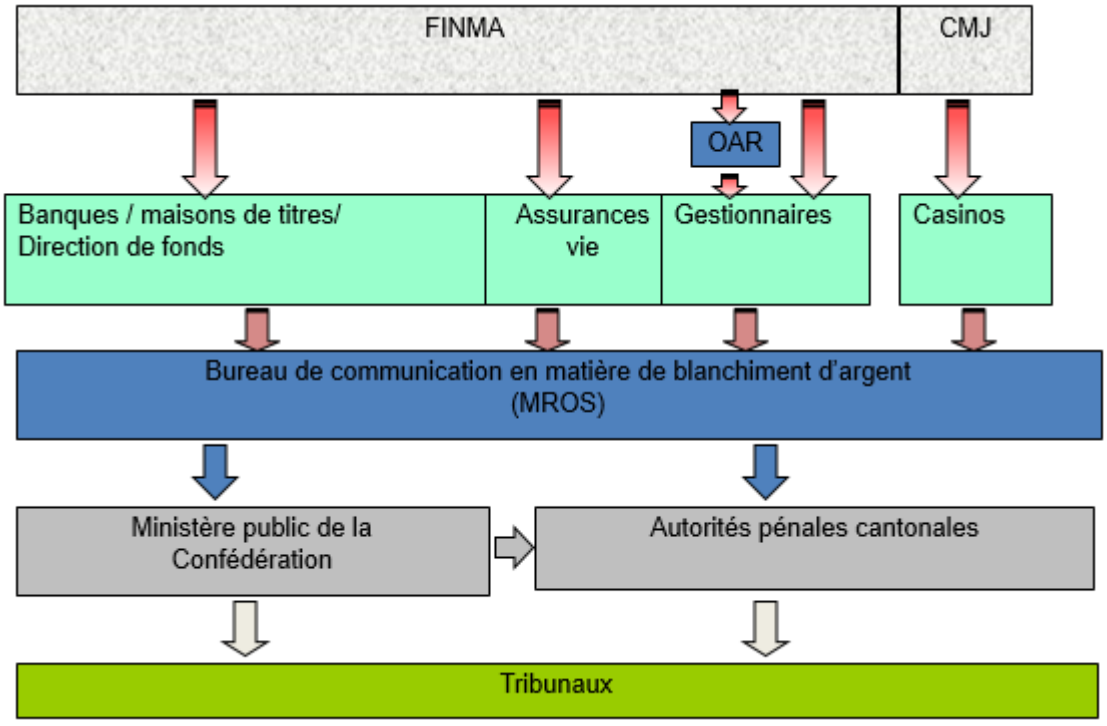
2.4.4 MROS

Le bureau de communication en matière de blanchiment d'argent (MROS) est le service national de l'Office fédéral de la police (fedpol) qui reçoit et analyse les soupçons de blanchiment d'argent provenant des intermédiaires financiers.

Selon l'article 9 al.1 de la LBA, il est obligatoire pour l'intermédiaire financier d'informer sans délai le MROS lorsqu'il sait ou qu'il présume sur la base de soupçons fondés que les valeurs patrimoniales impliquées dans une relation d'affaire ont un rapport avec une infraction au sens de l'article 305bis ou 260ter, ch. 1 du code pénal suisse, qu'elles proviennent d'un crime ou d'un délit fiscal qualifié, qu'une organisation criminelle exerce un pouvoir de disposition sur ces valeurs ou qu'elles servent au financement du terrorisme.

Lorsqu'un intermédiaire financier a un soupçon avéré, il en informe le bureau de communication en matière de blanchiment d'argent, il bloque les avoirs déposés sur le compte en vertu de l'article 10 LBA et n'informe en aucun cas le client de la procédure en cours conformément à l'article 11 LBA. Si le MROS considère qu'il y a un réel risque, il transmet alors l'information aux autorités de poursuite pénale. Inversement, si le MROS considère qu'il n'y a aucun risque, le compte du client sera débloqué.

Figure 4 : Schéma administratif MROS



Source : (FINMA 2019)

Des statistiques anonymes sont publiées tous les ans par le MROS sur l'évolution de la lutte contre le blanchiment d'argent, le crime organisé et le financement du terrorisme en Suisse.

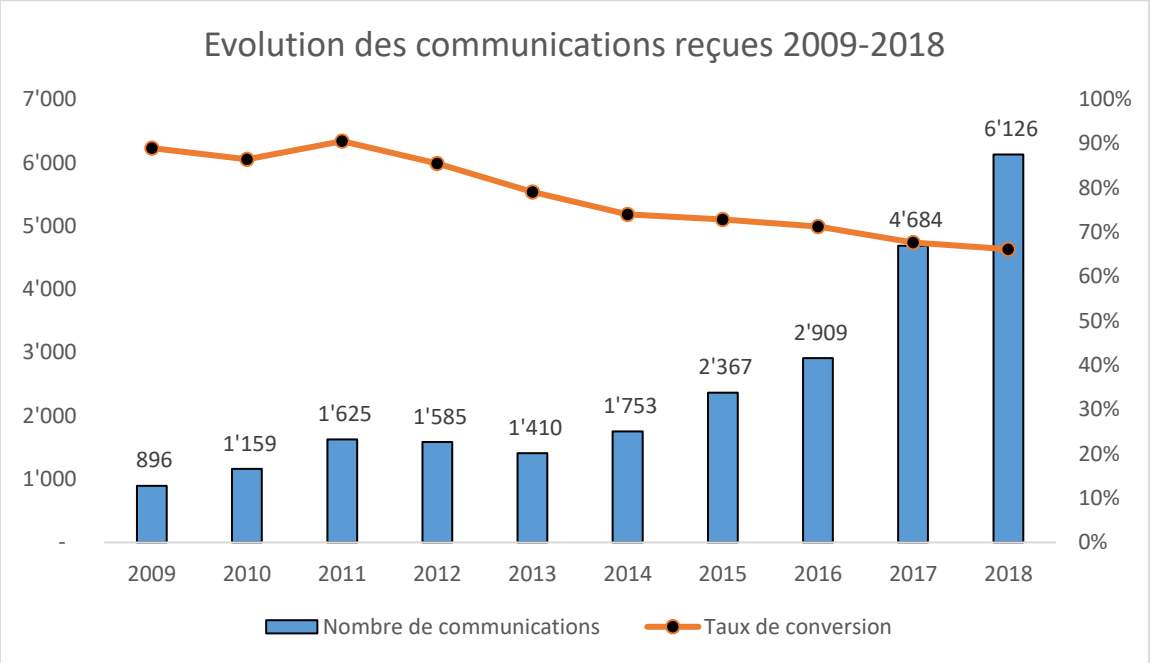
2.4.4.1 Evolution des communications

L'évolution des communications au MROS entre 2009 et 2018 se trouve dans l'Annexe 1 de ce travail. Mis à part pour la période 2011-2013, nous constatons une augmentation continuelle du nombre de communications transmises par les intermédiaires financiers au MROS.

Depuis 2016, le nombre de communications transmises est devenu très important et le service n'arrive pas à traiter toutes les demandes. C'est pourquoi, à fin 2018, 42% des transmissions relatives à 2018 n'avaient pas encore pu être traitées. De plus, certaines communications relatives à 2016 et 2017 n'ont également, au 31.12.2018, pas été traitées.

Etant donné que certaines communications n'ont pas encore été traitées à l'heure actuelle, le taux de conversion annuel a été théorisé. Afin de déterminer le taux de conversion théorique pour les années 2016 à 2018, les données connues en termes de nombre de communications transmises aux autorités de poursuite pénale et de communications non transmises sur les communications en cours de traitement ont été extrapolées. Nous retrouvons un taux de conversion théorique de 71% pour 2016, 68% pour 2017 et 66% pour 2018.

Figure 5 : Evolution des communications effectuées 2009-2018



Source : adapté de MROS (2009-2018)

Les années 2017 et 2018 se démarquent par une augmentation annuelle de respectivement 61% et 31% du nombre de communications transmises et de 210% et 7% du montant total de ces communications. Les taux de conversion ont légèrement diminué depuis 2011. L'augmentation du nombre de communications transmises combinée à la baisse du taux de conversion démontre que les intermédiaires financiers sont de plus en plus sensibilisés au blanchiment d'argent et qu'ils hésitent moins à communiquer leurs soupçons au bureau de communication en matière de blanchiment d'argent. Le durcissement toujours plus important des lois en la matière est également un facteur expliquant l'augmentation importante du nombre de communications. De plus, les moyens informatiques à disposition des départements Compliance permettant l'identification d'éventuels soupçons de blanchiment d'argent sont chaque année plus nombreux et développés.

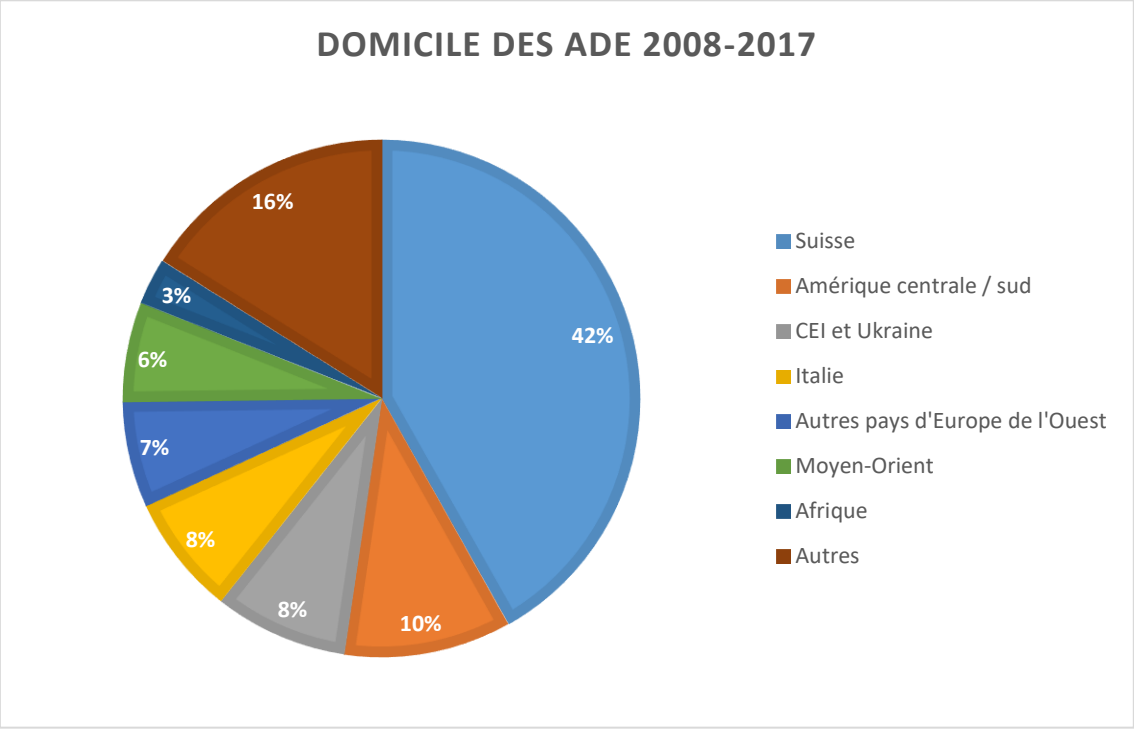
2.4.4.2 Intermédiaires financiers

Les intermédiaires financiers les plus exposés au risque de blanchiment d'argent sont inévitablement les banques. En effet, selon le MROS (MROS 2018), sur la période 2009-2018, 84% des communications proviennent de banques. Pour l'année 2018 uniquement, ce chiffre est de 89%. Les prestataires de services de paiement sont à la seconde position avec 272 communications effectuées en 2018, soit 4% du total. La particularité de l'année 2018 est que la catégorie des « autres intermédiaires financiers » occupe la troisième position en passant de 21 pour l'année 2017 à 143 pour l'année 2018. Cette catégorie comprend notamment les intermédiaires financiers actifs dans le domaine des monnaies virtuelles. Cette augmentation annuelle importante de 581% des signalements sont en partie imputables au nombre élevé de communications de soupçons dans le domaine des monnaies virtuelles. Les communications effectuées depuis le canton de Zoug, surnommé la « Crypto Valley » pour son nombre élevé de start-ups actives dans le domaine des cryptomonnaies, ont subi une augmentation de 96% par rapport à 2017.

2.4.4.3 Cocontractants – ADE

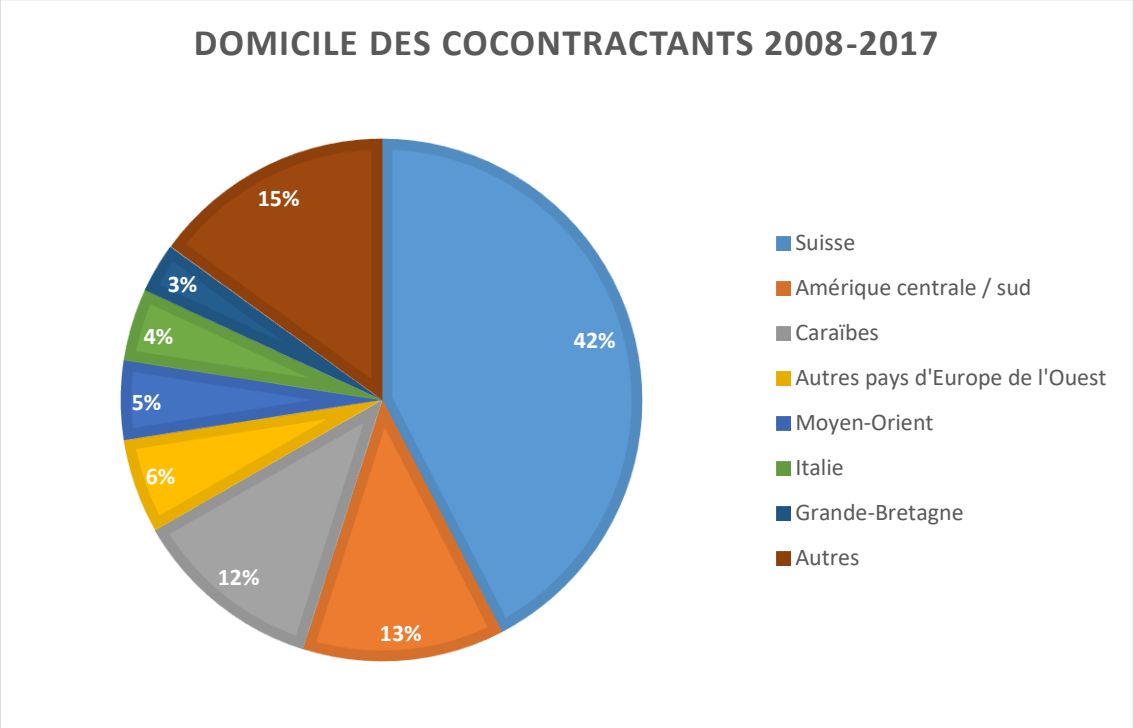
Les données concernant la nationalité des cocontractants et des ayants droit économiques aux valeurs patrimoniales ayant fait l'objet d'une communication ne sont pas disponibles dans le rapport annuel MROS 2018. C'est pourquoi, les données relatives aux années 2008-2017 ont été analysées. Entre 2008 et 2017, 42% des communications concernaient des ayants droits économiques (Figure 6) et des cocontractants (Figure 7) résidants en Suisse. Par conséquent, 58% concernaient des personnes résidantes à l'international

Figure 6 : Domicile des ADE 2008-2017



Source : adapté de MROS (2008-2017)

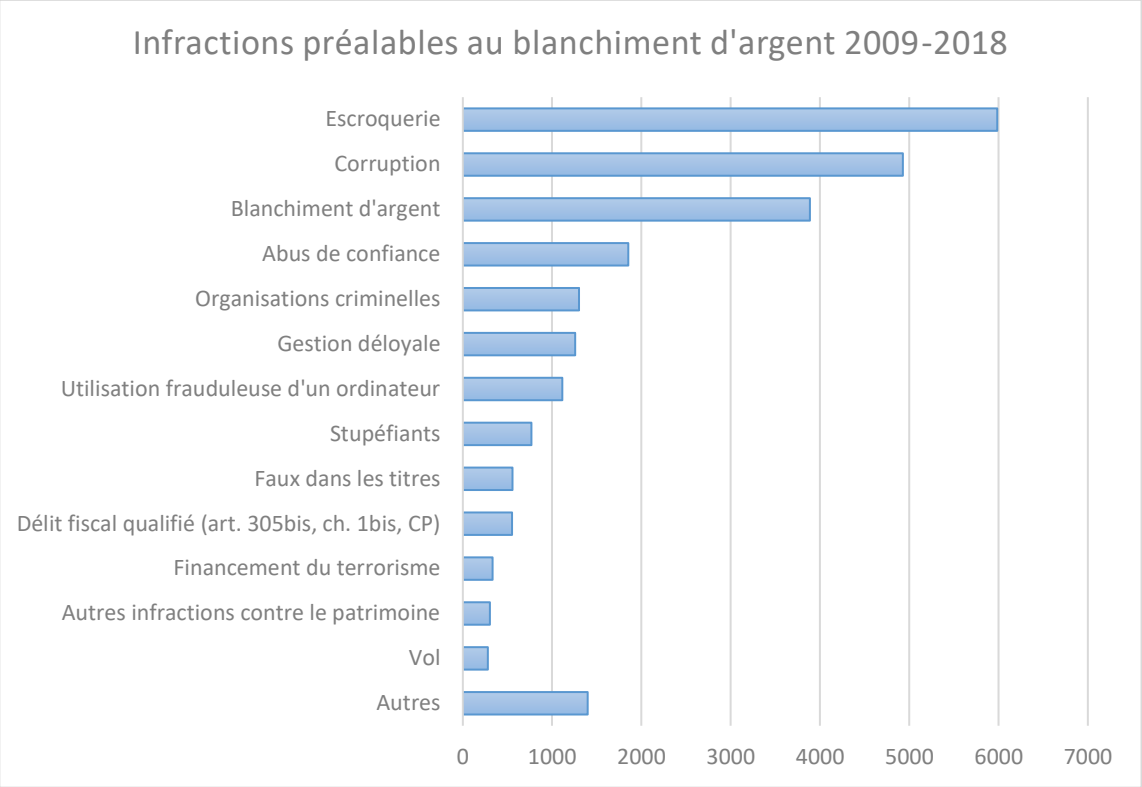
Figure 7 : Domicile des cocontractants 2008-2017



Source : adapté de MROS (2008-2017)

2.4.4.4 Infractions préalables

Figure 8 : Infractions préalables au blanchiment d'argent 2009-2018



Source : adapté de MROS (2009-2018)

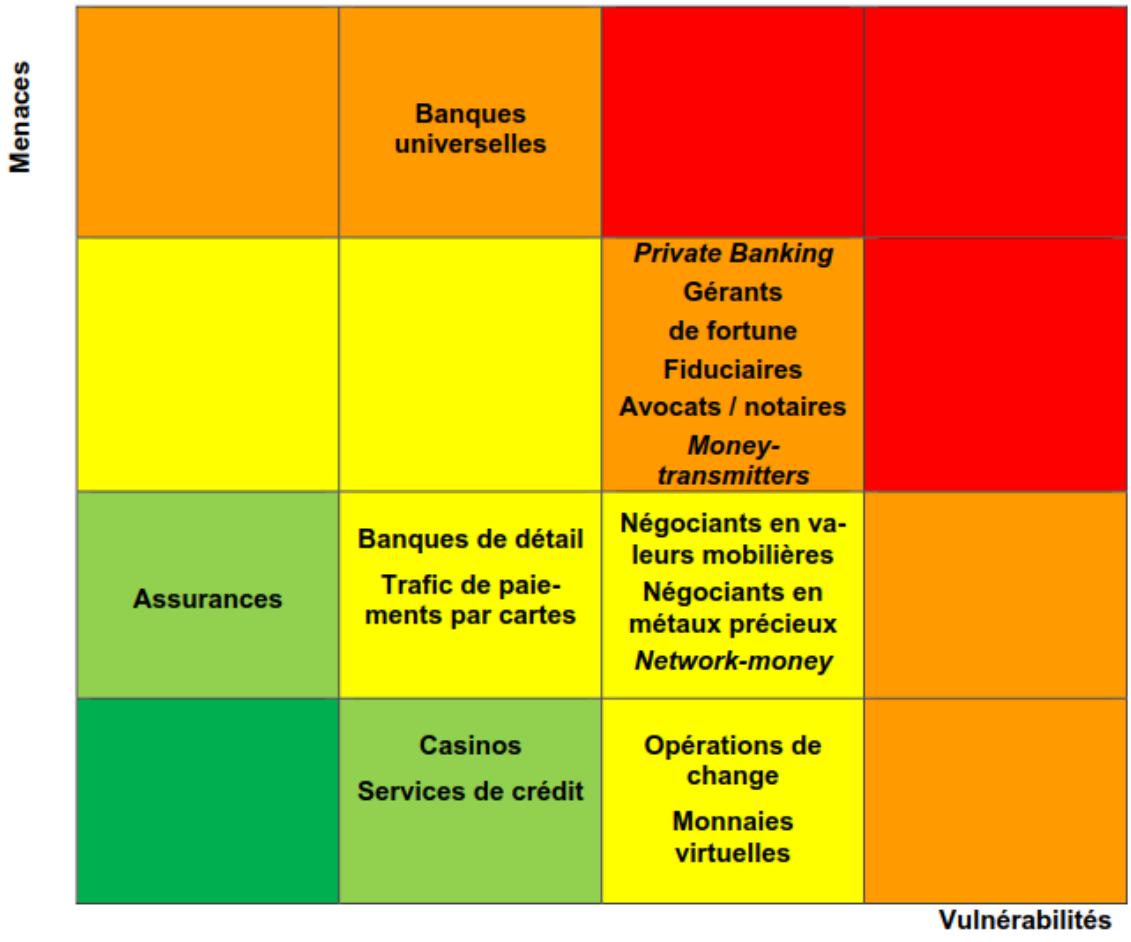
Le graphique ci-dessus montre les types prédominants d'infractions préalables au blanchiment d'argent présumées au moment de la transmission de la communication aux autorités de poursuite pénale. Depuis 2014, ce sont les communications pour présomption d'escroquerie et de corruption qui prédominent, avec une domination de la catégorie de corruption depuis les deux dernières années. La catégorie de « blanchiment d'argent » comprend les cas dans lesquels ni l'intermédiaire financier ni le MROS n'ont été en mesure de lier la communication à une infraction préalable déterminée. La catégorie « utilisation frauduleuse d'un ordinateur » quant à elle concerne principalement les cas d'hameçonnage.

2.5 Evaluation du risque de blanchiment d'argent

D'après les informations récoltées auprès du MROS, ce sont clairement les banques qui sont les intermédiaires financiers les plus exposés au risque de blanchiment d'argent. Néanmoins, ce risque est atténué par la réglementation solide et complète mise en place par la Confédération et la FINMA. Le GAFI a notamment pris exemple sur la réglementation suisse lors de la mise en place de ses recommandations (Winiker 2019). Les intermédiaires financiers sont dans l'obligation d'appliquer rigoureusement la loi car

ils subissent un audit externe annuel sur le blanchiment d'argent. L'augmentation importante des communications effectuées ces dernières années montre également que les intermédiaires financiers essayent de réduire le plus possible leur risque en collaborant au maximum avec les Autorités fédérales. Le Groupe de coordination interdépartemental sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF), structure mise en place par le Conseil fédéral en 2013, évalue globalement le risque de blanchiment d'argent en Suisse comme « moyen » (GCBF 2015). Au niveau des banques, ce sont les banques universelles et les banques privées qui sont le plus menacées par le risque de blanchiment d'argent, tout comme les gérants de fortune. Cela vient du fait que ces intermédiaires financiers ont régulièrement à faire avec des relations comportant des risques accrus, des PEP et des structures complexes comportant des sociétés de domicile.

Figure 9 : Evaluation du risque de blanchiment d'argent



Source : (GCBF 2015)

La principale difficulté, qui représente également le principal risque, repose sur l'identification de l'origine de la fortune du client. Les clients n'aiment pas se justifier sur la provenance de leurs avoirs et les gestionnaires s'intéressent à acquérir des avoirs sans

réellement se soucier de leur provenance. Il est par conséquent primordial pour un intermédiaire financier d'avoir un département Compliance indépendant, rigoureux et compétent en la matière qui contrôle cela. Néanmoins, avec les moyens actuels, il est souvent difficile de remonter avec certitude à la réelle origine de la fortune. De nouvelles technologies pourraient être utiles dans le processus d'identification. Les banques et tous les intermédiaires financiers suivent de très près l'évolution de la technologie blockchain et sa possible utilisation au sein du système économique. En effet, cette révolution technologique permet, entre autres, d'assurer une transparence ainsi qu'une traçabilité complète de l'historique des transactions.

3. Les cryptomonnaies

3.1 Historique

L'histoire des cryptomonnaies a commencé en 1990 lorsque le cryptographe américain David Chaum a créé DigiCash aux Pays-Bas, ce qui est considéré comme le premier type d'argent en ligne. A ce moment-là, les cryptographes étaient considérés comme paranoïaques et pensaient notamment que les paiements par carte de crédit n'étaient pas sûrs. En 1993, il a inventé le système de paiement numérique Ecash. Il s'agissait d'un produit techniquement parfait qui permettait de payer en toute sécurité et anonymement sur Internet. Ce système mettait ainsi fin à la surveillance et aux contrôles des intermédiaires financiers sur les transactions puisqu'il se basait sur une désintermédiation des transactions (De Filippi 2018). La technologie qu'il a créée, ainsi que son produit Ecash, a attiré l'attention des médias et d'importantes entreprises. Goldman Sachs, ING et même Microsoft se sont alors intéressés à DigiCash. Microsoft a notamment essayé d'acheter DigiCash pour 180 millions de dollars mais a essuyé un refus de la part de David Chaum. Les mauvaises décisions effectuées par le fondateur et directeur ont finalement conduit à la faillite de la société en 1998 (Pitta 1999).

La deuxième génération d'argent sur Internet est née des expériences d'apprentissage de DigiCash. L'entreprise qui a réussi à se démarquer et à vaincre la concurrence a été PayPal qui a été créée en 1998. PayPal a permis à ses utilisateurs de pourvoir disposer d'argent sur les plates-formes de navigation Web et de pouvoir transférer cet argent de façon transparente. PayPal est devenu très populaire (Pitta 1999).

Un autre évènement important dans l'histoire des cryptomonnaies est la crise financière de 2008 connue sous le nom de crise des subprimes. En effet, cette crise avait presque paralysé le système financier des États-Unis en atteignant de nombreuses institutions financières importantes. Les consommateurs ont alors douté du système financier et cela a conduit à l'émergence de la blockchain qui est à la base de la technologie utilisée dans les cryptomonnaies. Le retour de la confiance devenait alors l'enjeu principal auquel il fallait répondre (De Filippi 2018).

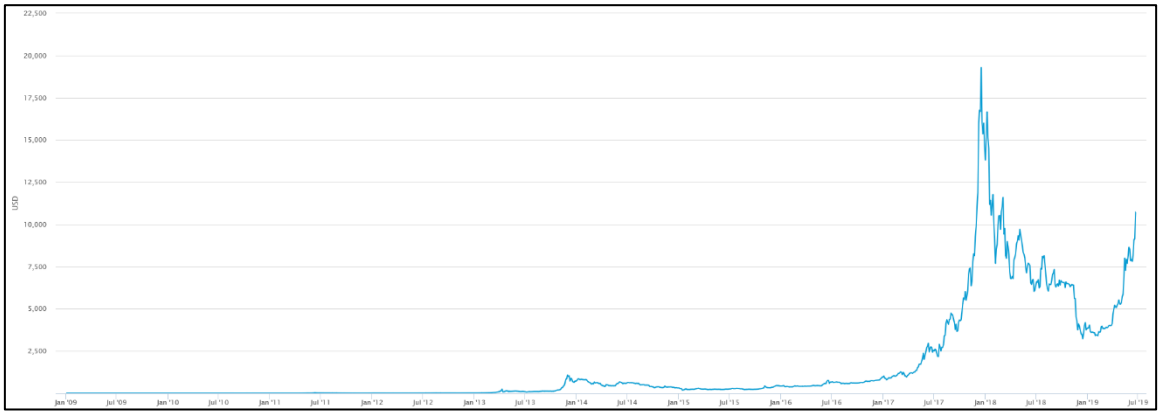
C'est le 31 octobre 2008 qu'une personne (ou un groupe de personnes) anonyme qui s'identifiait sous le pseudonyme de Satoshi Nakamoto a publié un livre blanc intitulé « Bitcoin : A Peer-to-Peer Electronic Cash System ». Ce livre décrivait un système de paiement décentralisé qui pouvait fonctionner sans l'intervention d'une autorité de confiance. Une monnaie virtuelle pouvant être échangée directement entre les utilisateurs

était également décrite dans ce livre. C'est le 3 janvier 2009 que le logiciel informatique du réseau Bitcoin a été officiellement lancé (De Filippi 2018).

Depuis 2009, la popularité de la blockchain et du Bitcoin est montée en flèche. Cela a donné naissance à de nombreuses autres cryptomonnaies alternatives au Bitcoin. Elles sont appelées les « altcoins ». Le premier altcoin est « Namecoin » qui a été créé en avril 2011 (De Filippi 2018). Aujourd'hui, plus de 2'200 cryptomonnaies différentes sont répertoriées sur le marché (CoinMarketCap 2019). Les altcoins les plus connus sont l'Ethereum, le Litcoin, Monero ou encore le Bitcoin Cash.

Les cryptomonnaies sont principalement devenues populaires en 2017 lorsque la valeur du Bitcoin est passée de 998 USD le 1er janvier 2017 à son pic historique de 19'891 USD le 17 décembre 2017 (Blockchain Luxembourg 2019). Le Bitcoin a suscité un engouement inouï de la part des professionnels et des particuliers qui se sont littéralement rués sur cette cryptomonnaie pour laquelle ils voyaient une façon de se faire de l'argent facilement et rapidement tant sa progression était fulgurante. Des fortunes se sont créées en quelques mois grâce au Bitcoin. Il n'y avait pas de limite à la progression du Bitcoin car sa valeur ne dépend d'aucun actif sous-jacent mais uniquement de l'offre et de la demande. Sa valeur, c'est le marché qui la détermine. La bulle a finalement éclaté à la fin du mois de décembre 2017 et le cours du Bitcoin s'est très rapidement effondré à 6'839 USD le 5 février 2018 (Blockchain Luxembourg 2019). Depuis le mois d'avril 2019, le cours du Bitcoin est reparti à la hausse et se monte à fin juin 2019 à environ 10'000 USD (Blockchain Luxembourg 2019).

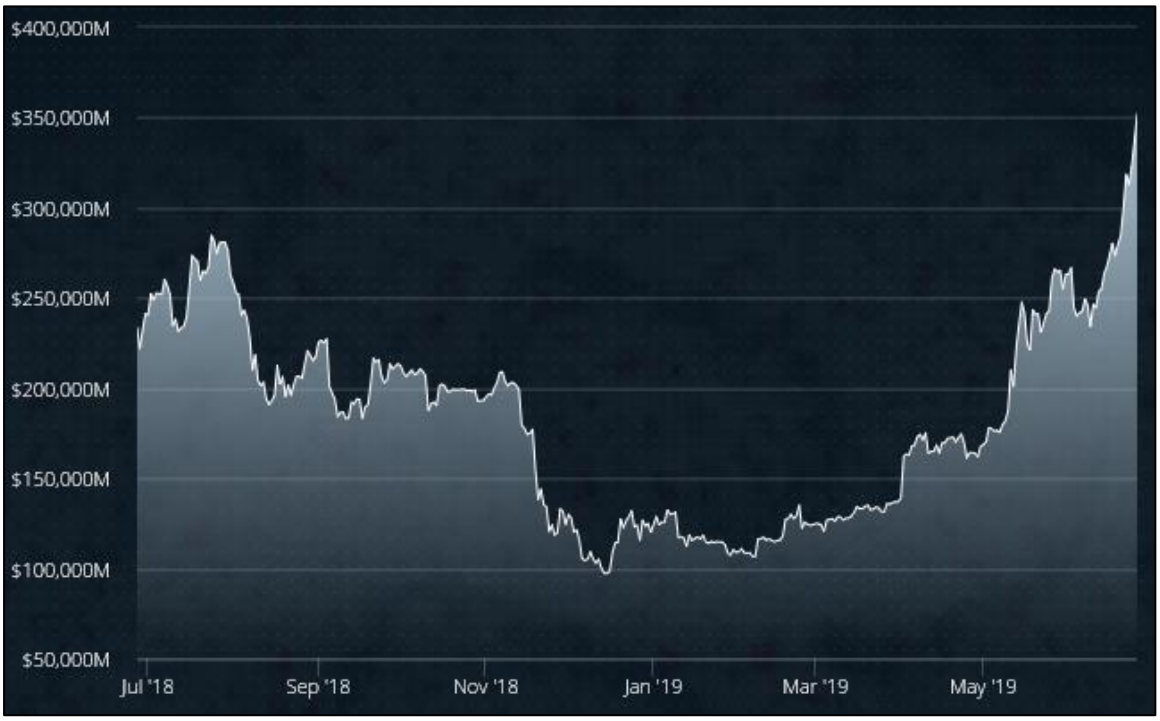
Figure 10 : Prix du Bitcoin (USD)



Source : (Blockchain Luxembourg 2019)

A la fin du mois de juin 2019, le Bitcoin représente 63% de la capitalisation boursière de toutes les cryptomonnaies avec près de 223 USD milliards pour un total de 352 USD milliards (Cryptolization 2019).

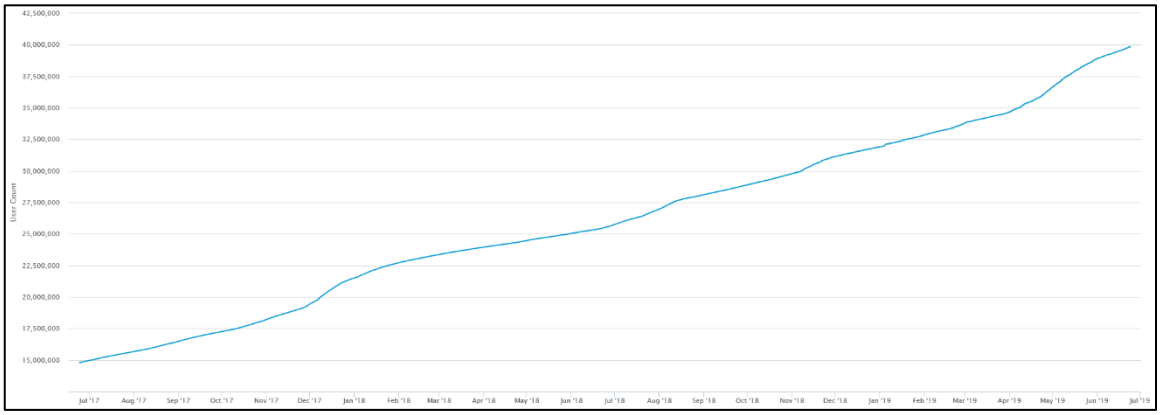
Figure 11 : Capitalisation boursière des cryptomonnaies (en USD millions)



Source : (Cryptolization 2019)

Malgré un effondrement du prix du Bitcoin à la fin du mois de décembre 2017, l'engouement envers les cryptomonnaies reste important et ne cesse de grandir. En effet, le nombre d'utilisateurs de portefeuille blockchain est en constante augmentation avec plus de 39 millions de wallets recensés à fin juin 2019 (Blockchain Luxembourg 2019).

Figure 12 : Nombre d'utilisateurs de portefeuille blockchain (Blockchain Wallet)



Source : (Blockchain Luxembourg 2019)

3.2 Fonctionnement

Afin d'analyser et de comprendre plus en profondeur les risques possibles de blanchiment d'argent liés à l'utilisation de ces monnaies virtuelles, il est nécessaire de s'intéresser à leur technologie sous-jacente, soit la blockchain ou chaîne de blocs en français.

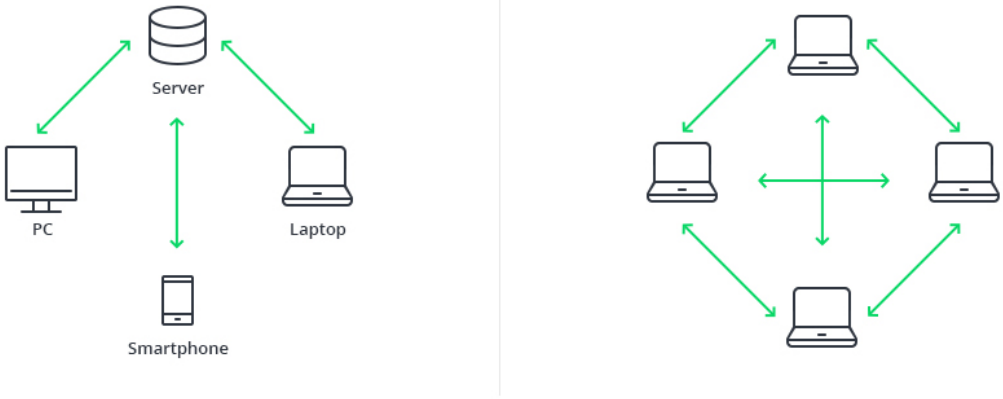
La blockchain fait partie de ce que l'on appelle les DLT (Distributed Ledger Technology). La notion de technologie des registres distribués fait référence à la diversité des systèmes créés dont la blockchain fait partie. L'utilité d'un registre est de pouvoir enregistrer des transactions financières ou administratives de façon durable et indélébile. Les DLT peuvent être considérés comme une version digitale des registres papiers. La différence notable entre les deux est que la confiance apportée dans un registre classique est garantie pas une institution centralisée comme une banque ou un Etat alors que dans le cas des DLT, c'est la technologie qui garantit la confiance en la base de données et de façon complètement décentralisée (De Filippi 2018).

La technologie blockchain a été évoquée la première fois en 2008 dans le livre blanc « Bitcoin : A Peer-to-Peer Electronic Cash System » de Satoshi Nakamoto. Le terme « blockchain » fait référence au regroupement sous forme de blocs des transactions liées entre elles par leur historique commun. C'est un registre décentralisé dans lequel les transactions sont effectuées de pair à pair sans intermédiaire financier (De Filippi 2018).

3.2.1 Base de données décentralisée

La principale innovation de la blockchain réside dans la désintermédiation des transactions par le biais de la mise en place d'une base de données complètement décentralisée. La motivation principale est l'indépendance par rapport aux intermédiaires financiers. Le fonctionnement est simple, le réseau n'est plus géré par un unique opérateur centralisé mais il est administré collectivement par l'ensemble des membres. Des règles sont mises en place à l'intérieur du protocole informatique spécifique à la blockchain. Ces règles constituent les principes devant être respectés par l'entièreté des participants du réseau. Si tel est le cas, les transactions pourront être effectuées et enregistrées de façon sécurisée et décentralisée. C'est par conséquent la totalité des participants qui s'entendent sur la véracité des transactions (De Filippi 2018).

Figure 13 : Schéma de décentralisation



Source : (Lastovetska 2019)

3.2.2 La fonction de « hachage »

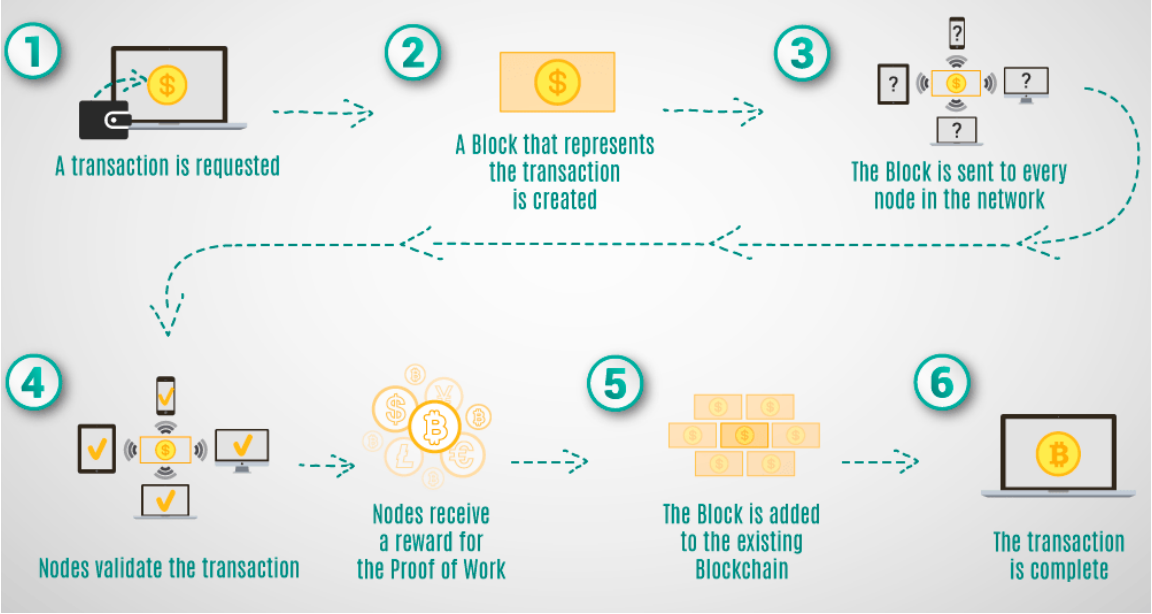
Comme expliqué précédemment, chaque transaction validée est enregistrée de façon chronologique au sein d'un bloc de transactions. Chaque bloc de la blockchain contient différentes données parmi lesquelles le hachage du bloc et le hachage du bloc précédent. Un hachage est comme une empreinte digitale composée de chiffres et de lettres. Chaque hachage de bloc est généré à l'aide d'un algorithme de hachage cryptographique (SHA 256). Tous les blocs confirmés et validés sont par conséquent dérivés du tout premier bloc. Toute tentative de corruption provoquerait alors un changement au sein d'un bloc et rendrait l'ensemble de la chaîne de blocs invalide car les blocs suivants auraient des informations erronées suite à la modification du bloc précédent. Afin de rendre impossible la possibilité que de puissants processeurs informatiques puissent ajuster tous les blocs instantanément, le système se base sur le mécanisme de la preuve de travail (proof of work) qui permet de ralentir le processus de création de nouveaux blocs. Dans la blockchain de Bitcoin, il faut environ 10 minutes pour déterminer la preuve de travail nécessaire et ajouter un nouveau bloc à la chaîne. La fonction de « hachage » aide à détecter et éviter tout changement dans l'historique des transactions et ainsi garantit leur authenticité (De Filippi 2018).

3.2.3 Le processus de minage

Le processus de minage est le processus de validation des transactions. Les ordinateurs participant à ce processus sont appelés les « mineurs ». Lorsqu'un utilisateur passe un ordre dans la blockchain, cet ordre devra être exécuté et validé par les mineurs. Pour la majorité des cryptomonnaies, dont le Bitcoin, la validation des transactions passe par le mécanisme de la preuve de travail (proof of work) pour lequel, comme dit précédemment, il faut environ 10 minutes pour trouver la solution. Les mineurs mettent ainsi à disposition leur puissance de calcul dans le but de résoudre un problème informatique mis en place

par le système. L'objectif est de trouver la bonne chaîne de caractères en réalisant des tentatives aléatoires. Lorsque la solution est trouvée par un mineur, elle est communiquée à tous les membres du réseau qui pourront vérifier son exactitude. En effet, chaque utilisateur qui rejoint le réseau pair à pair de la blockchain reçoit une copie complète du système. Si le bloc est approuvé par la totalité des membres, il sera enregistré à la fin de la chaîne de blocs (De Filippi 2018).

Figure 14 : Schéma du processus de minage

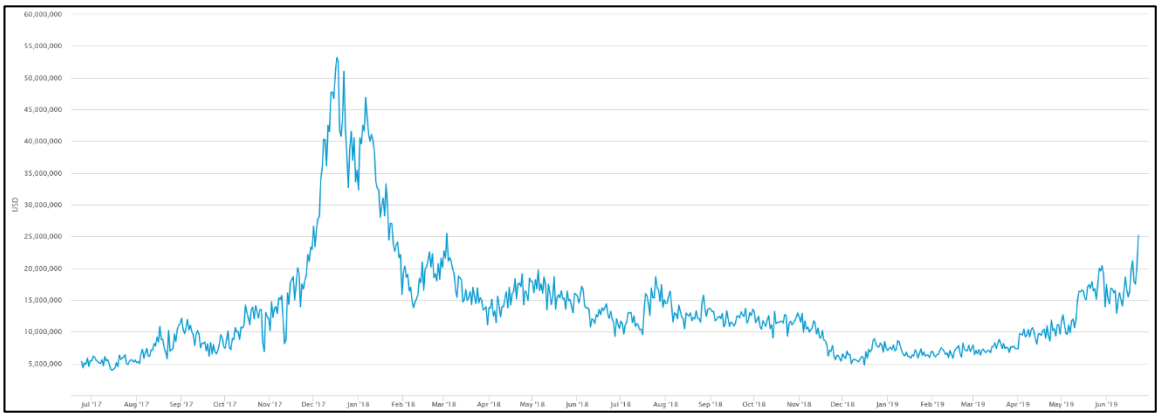


Source : (Lastovetska 2019)

En contrepartie à la tâche complexe de validation des transactions, les mineurs qui réussissent à trouver la solution au problème sont rémunérés. En effet, dans la blockchain de Bitcoin, les mineurs sont rétribués par des Bitcoins supplémentaires émis par le système. Par conséquent, les Bitcoins sont créés régulièrement et de manière progressive par le protocole informatique contrairement aux monnaies traditionnelles qui sont émises par des banques centrales. La quantité totale maximale du nombre de Bitcoins en circulation au sein du réseau est définit à 21 millions. Actuellement, chaque validation de bloc génère une création de 12.5 Bitcoins. Chaque jour, environ 144 blocs sont créés, ce qui correspond à une quantité moyenne de 1'800 nouveaux Bitcoins dans le système (De Filippi 2018).

Le graphique ci-dessous montre l'évolution des revenus des mineurs. Suite à l'augmentation du prix du Bitcoin à travers le temps, les revenus se sont vus augmentés fortement. Cette augmentation significative du prix du Bitcoin a attiré l'appétit de nombreuses personnes et les mineurs se sont ainsi multipliés. Le point positif est que cette augmentation du nombre de mineurs a permis un renforcement du système de contrôle des transactions.

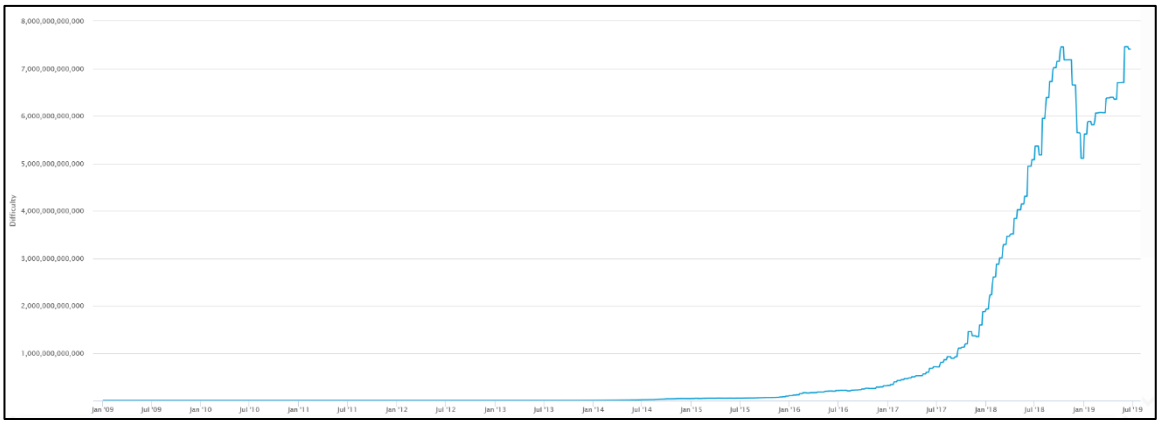
Figure 15 : Revenus des mineurs (USD)



Source : (Blockchain Luxembourg 2019)

Afin de maintenir la cadence de création de nouveaux Bitcoins chaque 10 minutes, le système modifie la difficulté du problème à résoudre par les mineurs. Cette activité est très couteuse en temps, en matériel et en énergie. Le nombre maximum de 21 millions de Bitcoins sera atteint aux alentours de 2140. Les mineurs ne pourront ainsi plus recevoir les nouveaux Bitcoins en échange de leurs services. Néanmoins, il est évoqué dans le livre blanc « Bitcoin : A Peer-to-Peer Electronic Cash System » la possibilité de la mise en place de commissions lors de chaque transaction (De Filippi 2018). Cela permettrait ainsi le maintien des mineurs au sein du réseau, ce qui est primordial et essentiel au bon fonctionnement du système.

Figure 16 : Difficulté de validation des transactions

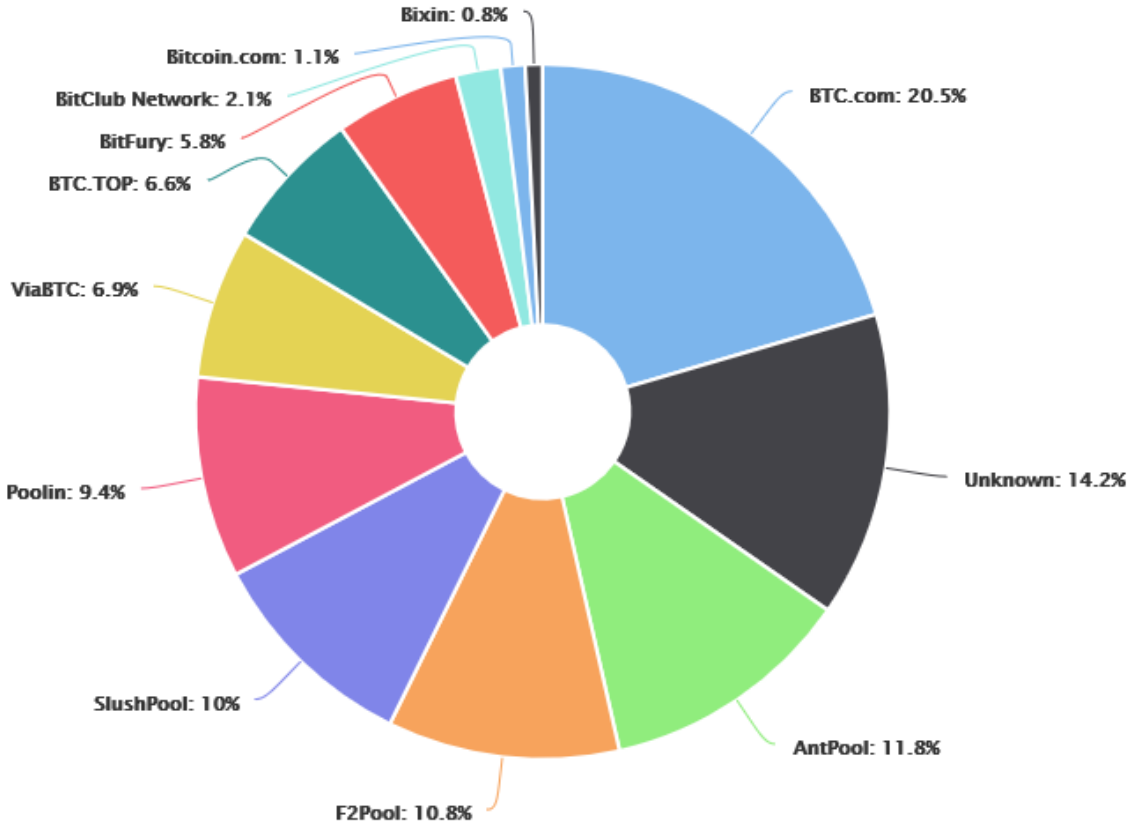


Source : (Blockchain Luxembourg 2019)

Afin d'altérer le système de la chaîne de blocs, il serait nécessaire d'altérer tous ses blocs et de recalculer la preuve de travail pour chaque bloc. Pour se faire, il serait nécessaire que le mineur soit capable de créer des blocs plus rapidement que le reste du réseau en contrôlant plus de 50% de tous les nœuds du réseau pair à pair (De Filippi 2018). Le graphique ci-dessous montre une estimation de la part de marché des différents mineurs présents sur le réseau Bitcoin. Nous constatons qu'actuellement le risque que certains

mineurs détiennent plus de 50% du réseau est encore faible. Néanmoins, certains mineurs disposent d'une part de marché significative et de possibles fusions entre mineurs pourraient être à craindre. A noter que l'origine de 14.2% de validation de blocs n'a pas pu être déterminée (Blockchain Luxembourg 2019).

Figure 17 : Répartition de la part de marché par mineur



Source : (Blockchain Luxembourg 2019)

3.2.4 L'anonymat

Dans le type de blockchain publique utilisée par les cryptomonnaies actuelles, les utilisateurs sont enregistrés sous forme de pseudonyme. En effet, n'importe qui peut participer au réseau sans même procéder à une identification. Dans la blockchain de Bitcoin, les utilisateurs sont identifiés par un pseudonyme qui correspond à leur adresse Bitcoin. Malgré cet anonymat, les transactions sont à la vue de tous car tous les acteurs du réseau possèdent l'historique complet de la blockchain et il est ainsi possible de remonter à toutes les adresses pour toutes les transactions. Ce type de registre complètement public en a dérangé certains. En effet, à titre de comparaison, les transactions effectuées au sein d'une banque ne sont visibles, disponibles et contrôlées que par la banque alors qu'ici, tout est divulgué (De Filippi 2018).

Cette absence de « vie privée » dans la technologie blockchain de Bitcoin a poussé des acteurs à créer d'autres cryptomonnaies basées sur un anonymat beaucoup plus solide. C'est ainsi que les cryptomonnaies « Monero » ou encore « Zcash » ont été créées respectivement en avril 2014 et en octobre 2016. Dans la blockchain de Monero, il est impossible de retracer les transactions. En effet, alors qu'au sein de la blockchain de Bitcoin les données des transactions telles que le montant échangé et l'adresse d'envoi et de réception des utilisateurs est accessible à tous, un anonymat complet de toutes ces informations est garanti dans la blockchain de Monero. L'anonymat est garanti par un système de signature de groupe dans lequel il est impossible de savoir de quel individu provient la transaction. Dans le cas de la cryptomonnaie « Zcash », le système cryptographique zk-SNARKs (Zero-Knowledge Succint Non-Interactive Argument of Knowledge) est utilisé. Ce système permet de prouver la véracité des transactions et des données sans en connaître le contenu. Le terme « Zero-Knowlegde » prend alors tout son sens (Dumas, Lafourcade, Tichit et Varrette 2018).

3.3 Fondements techniques

3.3.1 Nouvelle forme de monnaie ?

Le terme « cryptomonnaie » fait référence à une monnaie dite virtuelle mais est-ce que ces cryptomonnaies peuvent être considérées comme de la monnaie ?

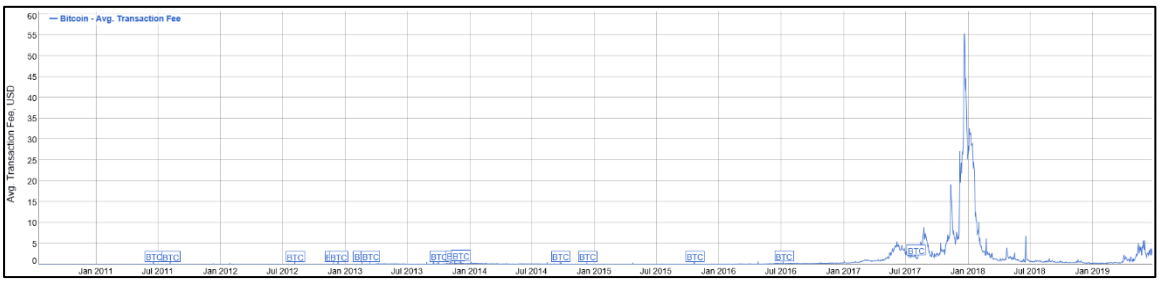
Les monnaies virtuelles se présentent comme une nouvelle monnaie dont le cours est basé sur un actif sous-jacent. Pour l'or, l'argent, le palladium ou les matières premières agricoles, l'actif est physique et existe alors que dans le cadre des monnaies virtuelles, cet actif est complétement immatériel et existe uniquement sous forme d'écriture au sein de la blockchain (De Filippi 2018).

Une monnaie doit impérativement remplir trois fonctions fondamentales. L'unité de compte est la première de ces fonctions. Elle doit permettre de fournir une mesure commune de la valeur des biens et services échangés. L'attribution d'un chiffre à la valeur d'un bien permet aux individus de pouvoir les comparer plus facilement. Cette première fonction ne peut pas être assumée par les monnaies virtuelles tant leur volatilité est grande. En effet, l'augmentation fulgurante de la valeur du Bitcoin qui s'est multiplié par 20 entre avril 2017 et décembre 2017 rend très difficile sont utilisation comme unité de compte (De Filippi 2018).

La deuxième fonction est le moyen de paiement. La monnaie fournit un moyen d'échanger des biens et des services dans une économie qui ne dépend pas du troc, ce qui facilite l'achat et la vente. Cette deuxième fonction ne peut également pas être assumée par les monnaies virtuelles tant les coûts de transactions sont élevés. En effet, le coût de

transaction pour le transfert de Bitcoins lors de son pic à fin décembre 2017 était à plus de 55 USD ce qui rendrait les échanges beaucoup trop coûteux (De Filippi 2018). Depuis la baisse du cours, les frais se situent entre 1 et 5 USD par transaction (BitInfoCharts 2019).

Figure 18 : Montant moyen des frais de transaction (USD)



Source : (BitInfoCharts 2019)

La réserve de valeur est la troisième fonction fondamentale de la monnaie. Lorsqu'un individu reçoit de l'argent, il peut décider de l'épargner et ainsi l'utiliser ultérieurement. Pour être efficace, la monnaie doit conserver sa valeur au fil du temps. De nombreuses personnes considèrent les cryptomonnaies et notamment le Bitcoin comme une réserve de valeur plutôt que comme une monnaie à proprement dite. La ressemblance et la comparaison avec l'or avait notamment été évoquée dans le livre blanc du Bitcoin de Satoshi Nakamoto. Les deux peuvent être considérés comme une ressource rare ayant une quantité limitée. Le nombre de Bitcoins est limité à 21 millions alors que le nombre d'or est limité aux ressources naturelles dont notre planète bénéficie (De Filippi 2018).

Selon David Lee Kuo Chuen, professeur de FinTech et de Blockchain à l'Université des sciences sociales de Singapour, la valeur quotidienne du Bitcoin devra devenir plus stable afin de pouvoir servir de façon fiable de réserve de valeur et d'unité de compte sur les marchés commerciaux. Sa volatilité excessive est plus conforme au comportement d'un investissement spéculatif qu'à celui d'une devise. De plus, d'autres facteurs rendent actuellement son utilisation universelle difficile comme le peu de marchands qui l'acceptent comme moyen de paiement, les délais de vérification des transactions, la lourdeur du processus d'approvisionnement en Bitcoins auprès d'un fournisseur ou encore le niveau relativement élevé de connaissances informatiques pour son utilisation. Mais aussi, le Bitcoin fait face à un problème économique structurel à long terme lié à sa limite absolue de 21 millions d'unités qui sera atteinte en 2140. Si le Bitcoin connaît un succès fulgurant et remplace les devises souveraines, il exercerait une force déflationniste sur l'économie puisque la masse monétaire n'augmenterait pas de la même façon que la croissance économique (Kuo Chuen 2015).

3.3.2 Caractéristiques

Par conséquent, les cryptomonnaies ne remplissent pas les fonctions qu'une monnaie souveraine doit impérativement avoir. Economiquement, elles sont assimilées à des actifs financiers de type numérique qui présentent des risques spécifiques tels que la faible liquidité, l'utilisation de l'effet de levier, les risques de marchés liés à la volatilité et également les risques opérationnels. Dans son rapport d'octobre 2018 nommé « Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding », la Confédération suisse définit techniquement les monnaies virtuelles de la façon suivante : « Une monnaie virtuelle est une représentation numérique d'une valeur, négociable sur Internet et qui peut être utilisée comme moyen de paiement pour des biens et des services réels. Elle a sa propre dénomination, mais elle n'est généralement pas acceptée comme moyen de paiement ayant cours légal. Une monnaie virtuelle n'existe que sous la forme d'un code numérique et n'a donc pas de pendant physique, par exemple sous la forme de pièces ou de billets. » (GCBF 2018).

3.3.2.1 Illiquidité

Plusieurs facteurs contribuent à l'illiquidité des marchés des monnaies virtuelles et limitent ainsi la capacité pour les investisseurs d'acheter ou vendre leurs actifs numériques. Le principal facteur est que la majorité des cryptomonnaies semble être concentrée entre les mains d'un nombre restreint d'investisseurs. En effet, selon le graphique ci-dessous indiquant la distribution de Bitcoins entre les différentes adresses Bitcoin, 1'993 adresses détiennent 41.9% du total des Bitcoins en circulation. De plus, 0.6% des adresses détiennent 86.9% des Bitcoins (BitInfoCharts 2019).

Tableau 2 : Distribution de Bitcoins par adresses

Bitcoin distribution					
Balance	**Addresses**	**% Addresses (Total)**	**Coins**	**$USD**	**% Coins (Total)**
(0 - 0.001)	12571607	48.75% (100%)	2,517 BTC	22,897,631 USD	0.01% (100%)
[0.001 - 0.01)	5916151	22.94% (51.25%)	24,047 BTC	218,776,271 USD	0.14% (99.99%)
[0.01 - 0.1)	4598738	17.83% (28.3%)	150,047 BTC	1,365,082,783 USD	0.84% (99.85%)
[0.1 - 1)	1962014	7.61% (10.47%)	615,724 BTC	5,601,666,009 USD	3.47% (99.01%)
[1 - 10)	585974	2.27% (2.86%)	1,533,630 BTC	13,952,502,577 USD	8.63% (95.54%)
[10 - 100)	135040	0.52% (0.59%)	4,406,209 BTC	40,086,353,871 USD	24.8% (86.91%)
[100 - 1,000)	14199	0.06% (0.06%)	3,581,387 BTC	32,582,367,336 USD	20.16% (62.1%)
[1,000 - 10,000)	1881	0.01% (0.01%)	4,553,186 BTC	41,423,501,719 USD	25.63% (41.94%)
[10,000 - 100,000)	109	0% (0%)	2,523,480 BTC	22,957,857,670 USD	14.2% (16.31%)
[100,000 - 1,000,000)	3	0% (0%)	374,653 BTC	3,408,482,128 USD	2.11% (2.11%)

Source : (BitInfoCharts 2019)

Cette contraction des cryptomonnaies entre quelques investisseurs réduit la capacité des marchés à absorber d'importants volumes de transactions. Cela contribue également à accroître la volatilité des actifs (Financial Stability Board 2018).

De plus, les plateformes d'échanges de cryptomonnaies qui ont pour but de mettre en relation un acheteur avec un vendeur ont subi différents problèmes opérationnels qui fragilisent et fragmentent la structure du marché. Les activités de ces plateformes ne sont pour la majorité pas supervisées contrairement aux intermédiaires financiers traditionnels. Plusieurs de ces plateformes ont subi des interruptions de service ou des piratages qui ont contribué à limiter la capacité des acheteurs et vendeurs à effectuer des opérations mais également ont entraîné des vols massifs de cryptomonnaies détenues par les clients (Financial Stability Board 2018). Ces cas seront détaillés dans le chapitre 3.5 consacré aux risques de blanchiment d'argent liés aux cryptomonnaies.

3.3.2.2 Utilisation de levier

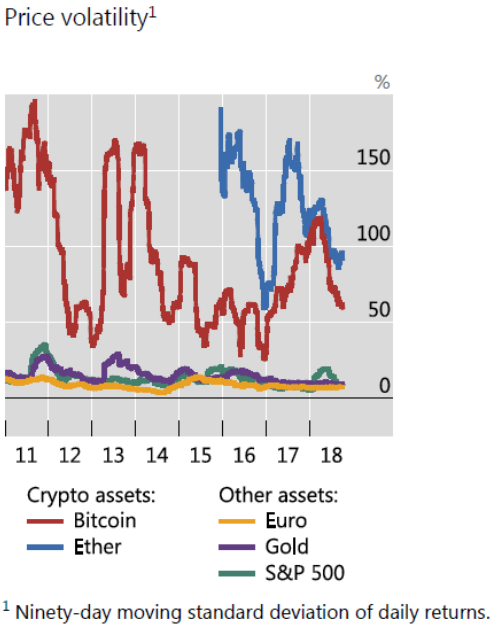
L'effet de levier peut amplifier la volatilité et la transmission des risques car son utilisation signifie que les investisseurs disposent de moins de capitaux propres pour absorber les pertes potentielles dues aux fluctuations du marché (Financial Stability Board 2018).

Selon une enquête récente parue sur Bloomberg (Kharif 2018), près de 20 % des propriétaires de cryptomonnaies ont eu recours à la dette pour financer leurs achats. De plus, certaines plateformes d'échanges proposent des services de trading sur marges. Elles permettent par conséquent aux investisseurs d'investir plus que leur montant d'investissement disponible (Financial Stability Board 2018). Les pertes subies avec l'utilisation de l'effet de levier peuvent ensuite s'étendre aux autres entités qui représentent la contrepartie.

3.3.2.3 Volatilité

Une des principales caractéristiques des monnaies virtuelles est leur très grande volatilité. Leur valeur n'étant pas dépendante d'un actif réel ou d'un sous-jacent, leur prix fait l'objet de spéculations. Les investisseurs doivent par conséquent être conscients et préparés à des cycles très rapides d'accroissement et d'effondrement de valeur. En effet, certaines cryptomonnaies comme le Bitcoin ont été soumises à des augmentations brutales mais également des chutes soudaines du prix de l'actif. Le graphique ci-dessous démontre l'extrême volatilité des monnaies virtuelles par rapport aux autres actifs financiers. La volatilité des cours des deux principales cryptomonnaies par capitalisation boursière (Bitcoin et Ethereum) était entre 6 et 13 fois supérieure à celle de l'euro, de l'or et de l'indice S&P 500 actions américaines au 4 octobre 2018 (Financial Stability Board 2018).

Figure 19 : Volatilité des cryptomonnaies



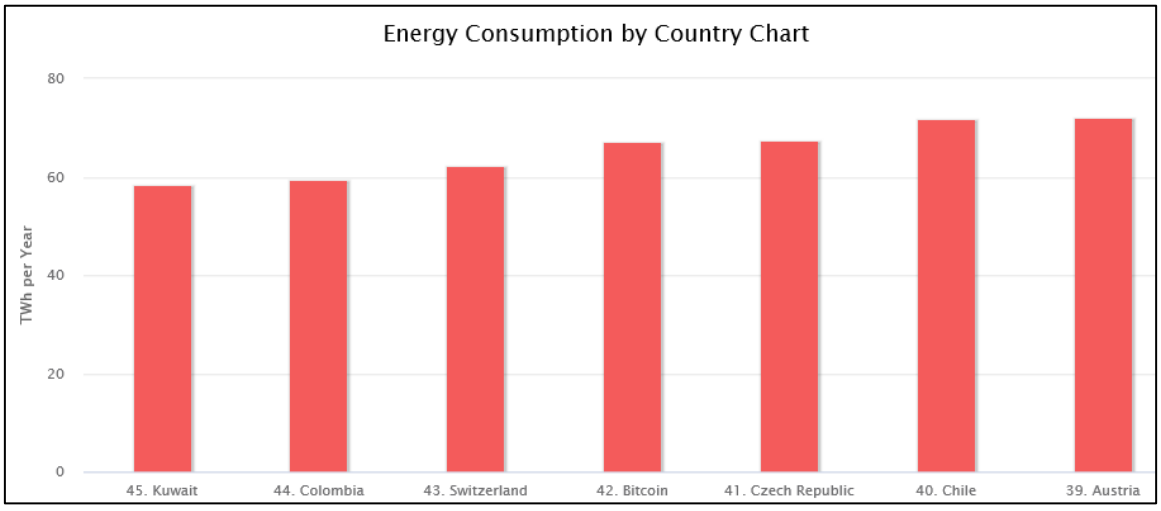
[1] Ninety-day moving standard deviation of daily returns.

Source : (Financial Stability Board 2018)

3.3.2.4 Risques opérationnels

Dû à l'utilisation de la DLT, les cryptomonnaies présentent des risques technologiques et opérationnels particuliers par rapport aux autres actifs financiers. Outre les risques liés aux interruptions de service ou des piratages des plateformes d'échanges évoqués précédemment, d'autres risques opérationnels sont spécifiquement liés aux monnaies virtuelles. L'un des plus important concerne l'énorme consommation énergétique liée aux services des mineurs qui pourrait ne pas être durable si la taille du marché venait à augmenter. Selon le graphique ci-dessous qui se base sur un rapport de l'Agence internationale de l'énergie (IEA), l'ensemble du réseau Bitcoin consomme déjà plus d'énergie qu'un certain nombre de pays (Digiconomist 2019).

Figure 20 : Consommation énergétique du Bitcoin



Source : (Digiconomist 2019)

3.3.3 Masse monétaire

Une bonne manière de se rendre compte de l'impact que pourrait avoir les cryptomonnaies sur l'économie globale est de comparer leur capitalisation boursière avec d'autres actifs, entreprises et personnes. Leur capitalisation boursière se relève être relativement faible par rapport à l'ensemble de toutes les monnaies ou tout simplement par rapport à certaines entreprises. En effet, selon le tableau ci-dessous, l'ensemble des cryptomonnaies représente 0.2% de l'ensemble des monnaies et 5.7% d'une entreprise comme Apple. La valeur des cryptomonnaies étant extrêmement volatile, leur capitalisation boursière peut changer chaque jour de plusieurs USD milliards ce qui rend cette comparaison plutôt éphémère. Néanmoins, cela donne une bonne image de l'impact économique des monnaies virtuelles.

Tableau 3 : Masse monétaire des cryptomonnaies

Source	**Capitalisation* (USD)**
Bill Gates (PDG Microsoft)	90 milliards
Bitcoin	**109 milliards (juin 2019 : 223 milliards)**
Jeff Bezos (PDG Amazon)	112 milliards
Ensemble des cryptomonnaies	**183 milliards (juin 2019 : 352 milliards)**
Novartis	198 milliards
Nestlé	253 milliards
Facebook	464 milliards
Apple	1'052 milliards
Amazon	931 milliards
Microsoft	860 milliards
USD en circulation	1'500 milliards
Réserves d'or	7'800 milliards
Totalité des monnaies physiques	34'400 milliards
Ensemble de toutes les monnaies	86'500 milliards

*dernières données disponibles au 17 septembre 2018

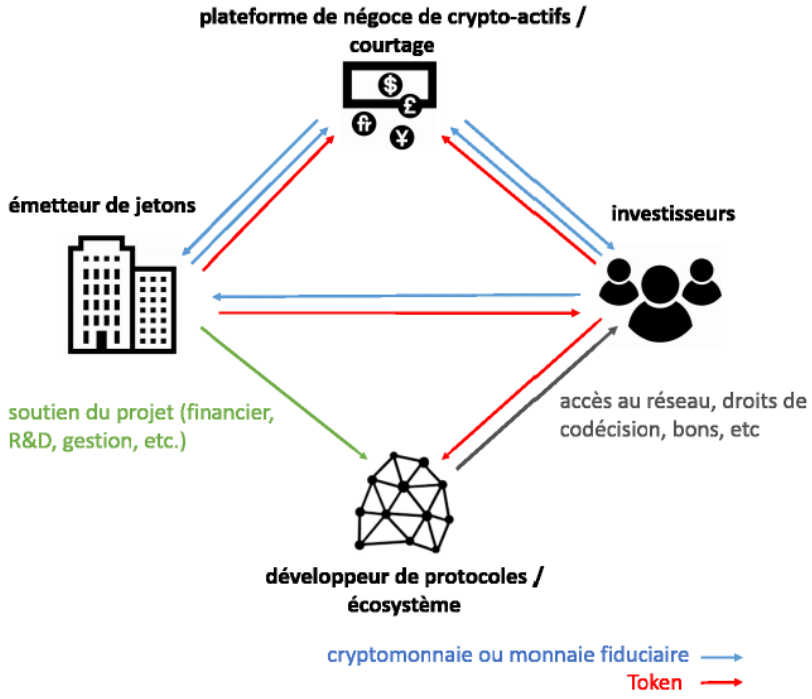
Source : adapté de Board of Governors of the Federal Reserve System (2019), Cryptolization (2019) Amoros (2018), Yahoo ! Finance (2019)

3.4 ICO

La naissance de la blockchain et des cryptomonnaies a permis l'apparition des Initial Coin Offering (ICO). Une ICO est l'équivalent approximatif d'une introduction en bourse dans le monde de l'investissement classique à travers une IPO (Initial Public Offering). Cette « offre publique de tokens » est réalisée dans le but de financer le développement d'une nouvelle cryptomonnaie, application ou service au sein de la blockchain. Les ICOs sont utilisées par les start-ups pour contourner le processus rigoureux et réglementé de capital minimum requis par les banques. Les caractéristiques principales des ICOs sont qu'elles sont décentralisées, en grande partie pas réglementées et par conséquent pas surveillées (GCBF 2018).

Le mécanisme est simple, les investisseurs intéressés souscrivent à l'ICO en achetant des « tokens » par le biais de monnaie fiduciaire ou de cryptomonnaies. Ces « tokens » peuvent être assimilés à des actifs qui permettront d'utiliser la plateforme qui sera créée. Contrairement à un crownfunding lors duquel les fonds obtenus proviennent principalement de dons, les investisseurs qui souscrivent à une ICO le font car ils espèrent que le token acheté leur procurera un rendement rapide et important dans l'avenir. Les ICOs les plus réussies de ces dernières années donnent aux investisseurs des raisons de maintenir cet espoir, car elles ont produit d'énormes rendements. En effet, de nombreux ICOs ont rapporté un rendement sur investissement invraisemblable à certains investisseurs (Conseil fédéral 2018).

Figure 21 : Schéma ICO



Source : (Conseil fédéral 2018)

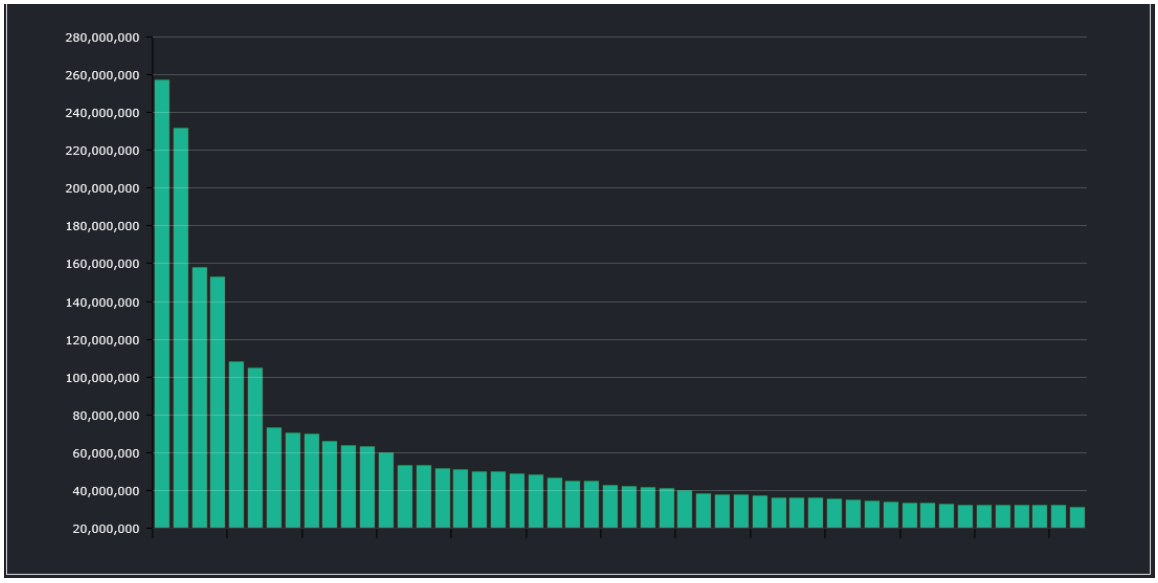
A ce jour, le rendement sur investissement le plus élevé réalisé suite à une ICO concerne le token NXT dont sa valeur a augmenté de 200'485% entre la date de l'ICO le 28 septembre 2013 (0.0000168 USD) et le 19.04.2019 (0.0337666 USD). Mais ce n'est pas un cas unique car la valeur du token IOTA a augmenté de 71'358%, celle d'Ethereum de 55'439%, celle de NEO de 34'710% ou encore celle de Spectrecoin de 25'109%. A ce jour, plus de 15 ICOs ont généré un ROI de plus de 1'000% et 27 de plus de 100% (CoinMarketCap 2019). Les succès et rendements phénoménaux de ces ICOs ont intéressé de plus en plus d'investisseurs à souscrire à ce type d'investissement. Le tableau ci-dessous montre effectivement l'intérêt important et croissant pour les ICOs depuis la fin de l'année 2017.

Figure 22 : Nombre d'ICOs effectuées 2014-2019

Source : (CoinDesk 2019)

Plus récemment, les ICOs ont généré des montants beaucoup plus importants en termes de fonds totaux collectés. Le graphique ci-dessous répertorie les 50 plus gros ICOs. L'ICO la plus importante est Filecoin, un projet de stockage de type cloud qui a levé au total 257 USD millions dont 200 USD millions en environ1 heure. D'autres projets ont pu voir le jour grâce aux ICOs. Tezos, qui est un système de « smart contract » disposant de sa propre blockchain, a levé 232 USD millions par le biais d'une ICO. Le projet « Sirin Labs » qui a développé le premier smartphone blockchain a quant à lui réalisé une ICO qui lui a permis de lever plus de 157 USD millions (Coinist 2019).

Figure 23 : Top 50 ICOs par fonds récoltés

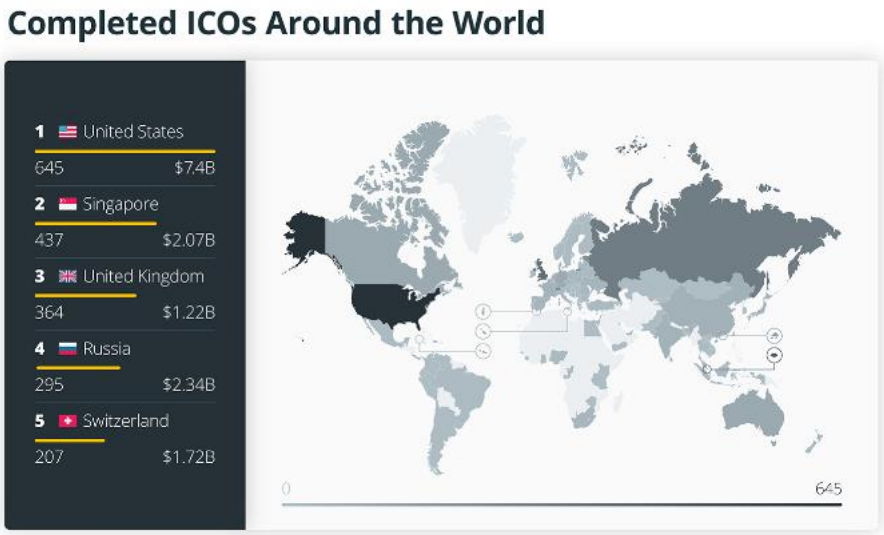


Source : (Coinist 2019)

Hormis d'être uniquement un moyen d'effectuer un retour sur investissement, les tokens ont diverses utilités au sein-même de la blockchain. Les tokens de paiement peuvent être assimilés à des cryptomonnaies à proprement dit et servent de moyen de paiement. Les tokens d'utilité donnent l'accès à un usage ou à un service numérique. Par exemple, les tokens applicatifs donnent le droit d'utiliser une application, les tokens de participation donnent le droit de voter et de participer à la gouvernance d'une application. Enfin, les tokens d'investissement représentent des valeurs patrimoniales. Les émetteurs peuvent promettre aux investisseurs des parts de revenus futurs d'une entreprise ou des flux de capitaux futurs. Ces tokens peuvent représenter notamment une action, une obligation ou un instrument financier dérivé (Conseil fédéral 2018).

Par rapport à sa taille, la Suisse représente une plaque tournante mondiale de l'ICO et figure à la 5ème position des pays dans lesquels des ICOs ont été effectuées. Mis à part Singapour, qui constitue tout de même un centre financier mondial, seuls des pays importants comme les Etats-Unis, la Royaume-Uni et la Russie ont effectué plus d'ICOs qu'en Suisse (Pozzi 2019).

Figure 24 : ICOs achevées à travers le monde



Source : (Pozzi 2019)

Cet enthousiasme grandissant des investisseurs attire également des escrocs. En effet, en raison qu'elles sont en grande partie non réglementées, les ICOs sont devenues une plaque tournante de fraudes et d'escroqueries, cherchant à s'en prendre à des investisseurs trop enthousiastes et mal informés. Il est très facile pour une entreprise qui lance une ICO de fabriquer des jetons. Il existe des services en ligne tels que Token Factory qui permettent la génération de tokens de cryptomonnaies en quelques secondes. Contrairement à une action, un token n'as pas de valeur intrinsèque (Conseil fédéral 2018). Les cas d'ICOs frauduleux seront détaillés dans le chapitre 3.5 consacré aux risques de blanchiment d'argent liés aux cryptomonnaies.

3.5 Risques de blanchiment d'argent

Le nombre de cryptomonnaies en circulation ainsi que leur utilisation globale a énormément augmenté ces dernières années ce qui inévitablement augmente le risque de leur utilisation dans un cadre criminel. Dans un premier temps, les risques proviennent de la technologie sous-jacente à ces monnaies virtuelles, la blockchain.

3.5.1 Risques liés à l'utilisation de la blockchain

3.5.1.1 L'anonymat du système

La notion d'anonymat, qui a été expliquée précédemment, est une des caractéristiques principales de la blockchain et constitue également un des risques principaux. En effet, la création d'un portefeuille virtuel sur Internet est gratuite, anonyme et ne demande aucune compétence particulière. Alors que dans la technologie de la blockchain de Bitcoin la traçabilité des transactions est totale et pour tous, l'identité des personnes se trouvant derrière l'adresse Bitcoin est inconnue. De plus, l'association d'un individu à une adresse

Bitcoin est de plus en plus difficile étant donné qu'un utilisateur peut disposer de nombreux portefeuilles différents et que plusieurs adresses différentes peuvent être générées pour un portefeuille (De Filippi 2018).

Le phénomène de mélange (Cryptocurrency tumbler) est également un procédé qui menace la traçabilité et l'identification des adresses impliquées dans un échange. En effet, il vous permet de dissocier votre cryptomonnaie de votre identité très simplement et à moindre coût. Ce procédé consiste à transférer un montant de cryptomonnaies sur une plateforme qui se chargera de transférer à son tour à coup de petites sommes et à destination de multitudes d'adresses différentes le montant mis à disposition. Un montant équivalent provenant d'autres individus sera par la suite restitué vers la première adresse et les pistes seront ainsi brouillées (GCBF 2018). Les plateformes fournissant ces services sont connues sous le nom de « Bitcoin Laundry », « BitMix » ou encore « CryptoMixer ».

La création de nouvelles monnaies virtuelles basées sur une blockchain différente et moins transparente telles que Monero ou Zcash rendent cet anonymat encore plus solide avec la non-traçabilité complète des transactions qui est la base du protocole mis en place. Le risque provenant de l'anonymat des individus et la non-traçabilité des transactions pourrait être assimilé à celui d'une transaction en argent liquide entre deux individus. Cependant, dans le cadre des cryptomonnaies, la menace est encore plus grande car, en plus de la caractéristique de l'anonymat, il y a une rapidité et une mobilité bien plus importante que pour les monnaies fiduciaires. En effet, il est possible de transférer entre deux comptes des sommes importantes en quelques secondes (De Filippi 2018).

L'adresse Bitcoin d'une personne est liée à sa véritable identité et toute transaction à partir de cette adresse est entièrement visible sur la blockchain. La monnaie virtuelle Monero a quant à elle la particularité d'être intraçable, anonyme, opaque et parfaitement fongible. Contrairement au Bitcoin qui est une cryptomonnaie non fongible, chaque Monero ne peut pas être différencié. Ce genre de cryptomonnaie alternative est plus à même de dissimuler l'activité des utilisateurs ou tout simplement de préserver des informations considérées comme privées comme le solde du portefeuille virtuel et le montant des transactions qui sont disponibles à tous dans la blockchain de Bitcoin (Dumas, Lafourcade, Tichit et Varrette 2018).

Monero est la deuxième cryptomonnaie la plus acceptée au sein du darknet, juste derrière le Bitcoin qui est accepté comme moyen de paiement sur tous les darknets les plus populaires. En termes de capitalisation boursière, Monero est la 13ème cryptomonnaie

avec un total, à fin juin 2019, de 1'984 USD millions (CoinMarketCap 2019). Comparativement au Bitcoin, elle n'est encore que très peu utilisée. En effet, Selon les données de CoinMetrics, les transactions quotidiennes en Monero ont oscillé autour de 8'000 pour le mois de juin 2019 alors que les transactions journalières en Bitcoins ont oscillé entre 300'000 et 400'000. De plus, le nombre d'adresses de portefeuille numérique actif pour Monero s'élève à environ 5'000 alors que pour Bitcoin, le nombre se monte à environ 785'000 (CoinMetrics 2019).

Néanmoins, selon une étude réalisée en 2018 par plusieurs chercheurs de l'Université de Princeton (USA), deux faiblesses importantes limitant l'efficacité de l'anonymat complet ont été mises à jour dans le fonctionnement de Monero. En effet, il s'est révélé qu'environ 62% des informations liées aux transactions peuvent être déduites par élimination et que, dans le phénomène de mélange utilisé par Monero, l'entrée réelle est généralement la dernière entrée ce qui rendrait la déduction de l'entrée réelle avec une précision de 80% (Möser, et al. 2018).

3.5.1.2 Les mineurs malveillants

Les tâches réalisées par les mineurs sont essentielles pour sécuriser le bon fonctionnement, l'authenticité et l'irréversibilité de la blockchain. Néanmoins, en détenant plus de 50% de la puissance de minage, un mineur aurait les capacités de modifier la blockchain en effaçant des transactions ou en validant par lui-même de fausses transactions (De Filippi 2018).

Les opérations de minage sont devenues de plus en plus difficiles au fil du temps et demandent de plus en plus de puissance, de ressources et d'énergies. C'est pourquoi, des consortiums de mineurs se sont créés dans lesquels ils mettent en commun leur puissance de calcul dans le but de résoudre les problèmes avec plus d'efficacité. Par conséquent, cela augmente le risque qu'une seule personne détienne plus de 50% de la puissance de calcul (De Filippi 2018).

Cette menace n'est pas seulement théorique. En effet, cinq cryptomonnaies ont déjà été la cible de mineurs malveillants qui ont réussi à détenir plus de 50% de la puissance de minage au sein de la blockchain. Bitcoin Gold, Ethereum classic, Verge, Monacoin et ZenCash ont été la cible d'une attaque 51% de la part de mineurs (De Filippi 2018).

Dans le cadre de Bitcoin Gold, au mois de mai 2018, un mineur a réussi à prendre le contrôle de plus de la moitié de la puissance de minage du réseau et a effectué une attaque à double dépense. Il a effectué deux transactions simultanément en envoyant le même montant à destination d'une plateforme d'échange de cryptomonnaies et à

destination d'un portefeuille détenu au sein de la blockchain. Il a échangé le montant envoyé sur la plateforme avec d'autres cryptomonnaies et a retiré cette somme. Puis, il a profité d'avoir le contrôle de la blockchain pour annuler les transactions initiales. Plus de 18.8 USD millions auraient été dérobés lors de cette attaque. Une attaque à double dépense de ce type serait impossible dans un réseau blockchain dans lequel aucun mineur ne possède plus de la moitié de la puissance de minage (Cryptonaute 2019).

Dans le cas de Monacoin, un mineur a réussi à contrôler 57 % de la puissance de minage en mai 2018. ZenCash et Ethereum classic ont également subi plusieurs attaques à double dépenses au mois de juin 2018. La monnaie virtuelle Verge à quant à elle subi des attaques en avril et mai 2018 durant lesquelles un mineur a réussi à exploiter une faille du système en réussissant à faire réduire la difficulté de l'algorithme de minage. La baisse de la difficulté de minage a permis au mineur de détenir plus facilement plus de la moitié de la puissance de minage (Cryptonaute 2019).

Nous constatons que cette menace n'est pas uniquement théorique. Néanmoins, il est à l'heure actuelle peu probable que cela puisse se produire pour les principales cryptomonnaies comme le Bitcoin.

Les profits découlant de l'activité de minage sont tels que cette activité attire de plus en plus de personnes. Il est également envisageable que de l'argent provenant d'activités illégales soit utilisé pour acheter des ordinateurs puissants dans le but d'effectuer une activité de minage (GCBF 2018).

3.5.1.3 Piratage

Les cryptomonnaies ne sont également pas à l'abri des hackeurs. La grande majorité des piratages sont dirigés vers les plateformes dites « exchanges » qui permettent de trader les cryptomonnaies telles que Coinbase, Kraken ou encore Bittrex. Ces plateformes sont visées car elles centralisent un volume important de cryptomonnaies. Depuis 2011, de nombreux cas de piratage ont été répertoriés. Le montant le plus important s'est déroulé en janvier 2018 lorsqu'un équivalent de 530 USD millions a été dérobé à la plateforme Coincheck. La plateforme Mt Gox a été piratée en 2014 de 487 USD millions, Bitgrail de 170 USD millions en février 2018, Bitfinex de 72 USD millions en août 2016 ou encore The DAO de 53 USD millions en juin 2016. Plus récemment en 2019, DragonEX, Cryptopia ou encore Bithump, plus important crypto-exchange sud-coréen, ont été piratées de plusieurs millions de dollars (Cryptonaute 2019).

Selon l'enquête menée par ICORating nommée « Echange Security Report », 54% des 100 plus grandes plateformes d'échange n'ont pas mis en place des mesures de sécurités

suffisantes afin d'éviter un piratage informatique (ICORating 2018). Les pirates informatiques ciblent également les portefeuilles virtuels des particuliers qui n'ont pas recours à des plateformes d'échanges ainsi que les services de minage. Selon la société Carbon Black spécialisée dans la cybersécurité, l'équivalent d'environ 1.8 USD milliard de cryptomonnaies auraient été dérobées en 2018 et environ 1 million de cyberattaques sont effectuées chaque jour (Carbon Black 2019).

3.5.1.4 Escroqueries

L'engouement pour les cryptomonnaies a été fulgurant depuis la forte médiatisation du Bitcoin en 2017. La facilité à se créer un portefeuille virtuel a permis à de nombreuses personnes n'ayant aucune connaissance en investissement et en cryptomonnaies à investir dessus y voyant un moyen de réaliser des gains importants. Ces personnes ne sont pas forcément informées des consignes de sécurité à respecter et ils peuvent se faire subtiliser leurs avoirs. Les pirates informatiques peuvent profiter de ces proies faciles qui, parfois, ne stockent pas de manière assez sécurisé leur clé cryptographique privée donnant accès à leur portefeuille virtuel.

De plus en plus de cryptomonnaies différentes voient le jour ces dernières années. En effet, il en existe environ 2'200 actuellement (CoinMarketCap 2019). Certaines d'entre-elles se sont révélées, et d'autres se révèleront très certainement dans le futur, n'être rien d'autre qu'une simple escroquerie. L'attractivité et l'intérêt grandissant pour ce nouveau type d'investissement ont attiré des personnes qui mettent en place des cryptomonnaies dont l'unique but est d'escroquer des potentiels investisseurs. L'escroquerie est basée sur un système de pyramide de Ponzi. Dans ce système pyramidal, les escrocs promettent un retour sur investissement très important aux investisseurs qui sont rémunérés grâce aux fonds des nouveaux arrivants. Ce montage financier basé sur une promesse de gains importants permet ainsi d'attirer de nombreux investisseurs. Ceux ayant investis dans la soi-disant cryptomonnaie sont par la suite incités à recruter de nouveaux investisseurs parmi leurs connaissances afin que la valeur de la cryptomonnaie reste stable ou augmente. Le manque de connaissance des investisseurs combiné à la couverture médiatique positive ainsi qu'à de bonnes stratégies de vente sont les principales causes de ces escroqueries (GCBF 2018).

L'affaire Bernard Madoff reste le cas le plus connu d'escroquerie basée sur un système de Ponzi. Son fonds d'investissement spéculatif offrait un taux de profit de 17% annuel. Son montage financier s'est écroulé lors de la crise financière de 2008 lors de laquelle de nombreux investisseurs ont voulu sortir du fonds et récupérer leur capital mais Bernard Madoff était dans l'incapacité de les rembourser. Des banques très importantes et

connues se sont faites avoir telles que Banco Santander qui a perdu plus de 3 USD milliards ou encore UBP et HSBC 1 USD milliard (Weitmann 2009). Dans l'univers des cryptomonnaies, de nombreux cas ont déjà été répertoriés. OneCoin, Bitconnect, AriseBank, PayCoin, le fonds Gelfman Blueprint ou encore Turcoin se sont révélés être des escroqueries basées sur un système de Ponzi (Cryptonaute 2019). En septembre 2017, la FINMA a ordonné la mise en liquidation des sociétés gérantes de la cryptomonnaie « E-Coin ». Contrairement aux cryptomonnaies qui sont basées sur la blockchain et sur une base de données décentralisée, le « E-Coin » était contrôlé exclusivement par la société et était sauvegardé sur un serveur local (FINMA 2019). Dans son rapport annuel 2018, le MROS informe avoir reçu plusieurs communications liées à des cas d'escroqueries sur des cryptomonnaies.

Les escroqueries n'épargnent également pas les ICOs. En effet, plusieurs cas d'« Exit Scam » ont été répertoriés dans lesquels les startups se volatilisent avec l'argent levé par les investisseurs sans jamais n'avoir mis en place le produit sur le marché. La startup sud-coréenne Pure Bit a disparu quelques heures après avoir réalisé son ICO avec 2,8 USD millions en Ethereum. La société Pincoin a réalisé une ICO qui lui a permis de recueillir 660 USD millions auprès de plus de 32'000 investisseurs auxquels elle proposait 48% de rendement mensuel. Les fondateurs vietnamiens ont fini par quitter le pays et les 660 USD millions se sont volatilisés. Le CEO de la startup Savedroid basée en Allemagne a également disparu en avril 2018 avec 50 USD millions suite à une ICO. Il a par la suite expliqué qu'il s'agissait d'une campagne pour prouver la facilité de tromper les investisseurs avec une ICO. Les dirigeants de la startup blockchain Vanbex ont quant à eux été accusés de n'avoir jamais cherché à développer le produit promis lors de l'ICO lors duquel 22 USD millions ont été collectés et d'avoir détourné ces fonds afin de les utiliser pour leurs besoins personnels. La société de conseil en ICO Statis Group a annoncé dans une étude que 78% des ICOs effectuées en 2017 s'étaient révélées être des escroqueries avec une perte de 1.31 USD milliards (Cryptonaute 2019).

D'autres soupçons de possibles Exit Scam relatifs cette fois à des plateformes d'échanges de monnaies virtuelles ont également été répertoriés. En octobre 2018, la plateforme d'échange canadienne MapleChange a annoncé avoir été volée de la totalité des cryptomonnaies détenues par ses utilisateurs et a fermé son site et son compte Twitter dans la foulée. La même suspicion d'Exit Scam a été effectuée en février 2018 pour l'entreprise basée en Italie BitGrail qui affirmait avoir été dérobée de 17 millions de NANO (cryptomonnaie spécifique à la plateforme) soit l'équivalent de 170 USD millions. En janvier 2019, un tribunal italien a condamné le directeur et fondateur de BitGrail, Francesco Firano, à rembourser les fonds volés. En décembre 2018, une affaire

romanesque de possible Exit Scam d'une plateforme d'échange a vu le jour. La plateforme canadienne QuadrigaCX a annoncé que son PDG et fondateur, Gerald Cotten, était décédé à l'âge de 30 ans suite à des problèmes de santé lors d'un voyage en Inde. Le problème est que cet homme présumé-décédé était le seul détenteur des codes d'accès aux portefeuilles et la plateforme était donc dans l'incapacité de les récupérer. QuadrigaCX a fermé en janvier 2019 et a fait perdre plus de 125 EUR millions en Bitcoin et en Ethereum aux investisseurs (Cryptonaute 2019).

3.5.1.5 Rançongiciels

Les rançongiciels ou ransomware sont des types de logiciels malveillants conçus pour infiltrer des ordinateurs d'individus et les empêcher de pouvoir accéder à leurs fichiers. Les pirates informatiques demandent par la suite une certaine somme d'argent afin de décrypter les fichiers et de rétablir l'accès au propriétaire de l'ordinateur. Ces dernières années, les cas de rançongiciels aves des demandes de paiements en cryptomonnaies se sont multipliés. Le versement de la rançon en cryptomonnaies permet aux pirates informatiques de transférer ces cryptomonnaies dans des portefeuilles électroniques basés dans d'autres juridictions dans lesquelles ils pourront être échangés (GCBF 2018). En mai 2017, le ransomware WannaCry a réussi à subtiliser les données de plus de 200'000 ordinateurs à travers 150 pays. Des sociétés connues comme Honda, Dacia ou encore Petrobras ont été touchées. Ce rançongiciel exigeait des rançons sous forme de Bitcoin mais n'aurait permis de récolter uniquement 140'000 USD aux pirates informatiques en raison du niveau jugé comme amateur du logiciel malveillant. Les Etats-Unis ont accusé la Corée du Nord d'être responsable de cette attaque de grande ampleur. Depuis le mois d'août 2018, c'est le ransomware Ryuk qui fait parler de lui. Ce ransomware, très certainement propagé par des hackeurs russes, a permis en 5 mois de récolter 705.80 Bitcoin, soit environ 3.7 USD millions (Cryptonaute 2019).

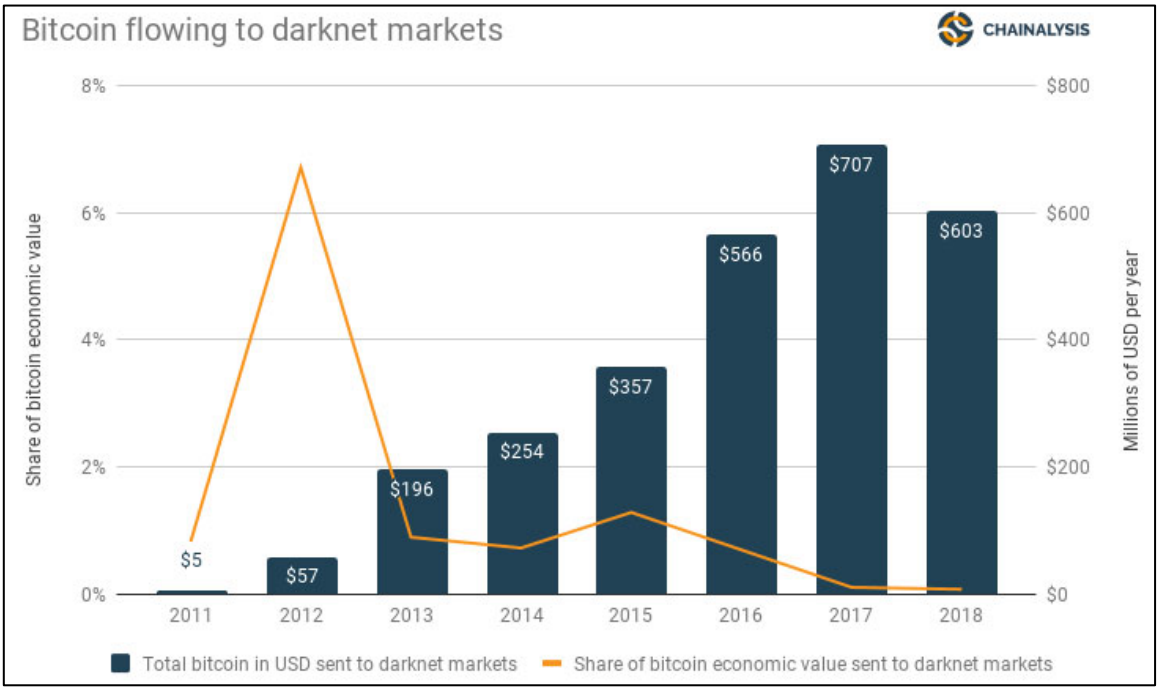
Les rançons en cryptomonnaies ne se limitent pas aux pirates informatiques, elles sont désormais également demandées lors de kidnapping ou de menaces d'attentats. Un homme d'affaire américain a été enlevé en septembre 2018 et une rançon de 950'800 USD en Bitcoin avait été payée par la famille de la victime. Le 31 octobre 2018, la femme du milliardaire norvégien Tom Hagen a été enlevée et une rançon de 9 EUR millions en Monero a été exigée par les criminels. Aux Etats-Unis, plusieurs menaces d'attentats à la bombe ont été effectuées durant lesquels les criminels réclamaient une rançon de 20'000 USD payable uniquement en Bitcoin (Cryptonaute 2019).

3.5.1.6 Blanchiment des cryptomonnaies illégalement obtenues

Le vol de cryptomonnaies et leur obtention par des fraudes aux investisseurs détaillés précédemment constituent des infractions préalables au blanchiment d'argent. Il arrive que les portefeuilles électroniques qui sont détenteurs des avoirs subtilisés soient mis sur une liste noire par les utilisateurs du réseau blockchain et qu'ainsi toutes les demandes d'utilisation ou de transfert de la cryptomonnaie soient refusées. Cela est bien évidemment uniquement possible lorsque la provenance criminelle des avoirs peut être retracée avec certitude, ce qui est rarement le cas. C'est d'autant plus difficile depuis l'apparition du phénomène de Cryptocurrency tumbler et des nouvelles monnaies virtuelles de type Monero ou Zcash qui facilitent la non-traçabilité des transactions. Ces plateformes fournissant ces services de mixing sont utilisées pour perdre la trace de l'origine des fonds et ainsi blanchir les monnaies virtuelles illégalement obtenues (De Filippi 2018).

Le recours au darknet est également souvent utilisé par les criminels pour blanchir les cryptomonnaies provenant d'actes illégaux. Il leur est alors possible de les utiliser pour acheter toutes sortes de produits ou encore de les revendre à des prix parfois sous évalués contre d'autres cryptomonnaies. 603 USD millions ont été envoyés sur le darknet en 2018. Cette baisse par rapport à 2017 serait due aux fermetures des deux marchés en ligne darknets AlphaBay et Hansa qui ont fait diminuer l'activité (Chainalysis 2019).

Figure 25 : Bitcoins au sein du darknet



Source : (Chainalysis 2019)

D'autres mécanismes sont utilisés afin de blanchir ces monnaies virtuelles. Les bornes physiques appelées GAB (Guichet Automatique Bitcoin) permettent par exemple d'acheter et de vendre des monnaies virtuelles de façon complètement anonyme contre de l'argent liquide. Des casinos et autres sites de paris en ligne qui acceptent les cryptomonnaies ont également vu le jour. Dans ce type d'établissement où les participants restent totalement anonymes, les gains peuvent être encaissés sous la forme de cryptomonnaies mais également au taux de change de n'importe quelle devise. Playamo est un site de casino en ligne où les joueurs peuvent jouer avec des cryptomonnaies comme le Bitcoin, l'Ethereum, le Litecoin et le Dogecoin. La société est située à Nicosie et le régulateur est le gouvernement de Curaçao. D'autres sites comme Crypto Sportz, LOOT.BET ou encore Bitcoincasino existent. L'utilisation de passeurs d'argent ou money mules en anglais est également une technique utilisée par les criminels. Ils ouvrent, grâce à de faux documents, des portefeuilles sur des plateformes Exchanges au nom d'individus qui sont considérés comme des passeurs d'argent et transfèrent par la suite les avoirs sur des comptes bancaires au même nom dont ils gardent le contrôle (GCBF 2018).

3.5.2 Autres risques

3.5.2.1 Acquisition et vente de produits illégaux

Un risque de blanchiment d'argent également lié aux cryptomonnaies mais pas à la technologie sous-jacente à celles-ci est le risque d'utilisation de cryptomonnaies dans le but d'acheter des produits illégaux, notamment au sein du darknet. Les vendeurs de produits illégaux comme les armes ou la drogue ont la possibilité de convertir les cryptomonnaies provenant de la vente en argent liquide auprès de bureaux de changes en ligne et ensuite blanchir cet argent en l'investissant dans des voitures ou des achats immobiliers par exemple. La traçabilité des transactions au sein même du darknet et la possibilité d'identifier l'adresse IP de l'utilisateur sont minimes. Au sein du darknet, lors d'une transaction en cryptomonnaies, il y a un recours au mixing afin d'effacer la traçabilité des transactions. De plus, sur la blockchain, il n'y a rien qui distingue une transaction passée sur le darknet d'une autre transaction. Par conséquent, il est très difficile pour un bureau de change en ligne de se rendre compte qu'un certain montant de monnaies virtuelles provient d'actes illégaux (GCBF 2018).

3.5.2.2 Investissement d'argent sale dans les cryptomonnaies

La facilité avec laquelle il est possible d'ouvrir un portefeuille virtuel et la possibilité de le faire de façon tout à fait anonyme attire les criminels qui y voient une façon simple de blanchir leur argent provenant d'actes illégaux. Les avoirs d'origine criminelle peuvent également être utilisés lors d'ICOs étant donné que ces levées de fonds ne sont que très peu contrôlées à l'heure actuelle. Par conséquent, l'argent sale est inséré au sein d'une

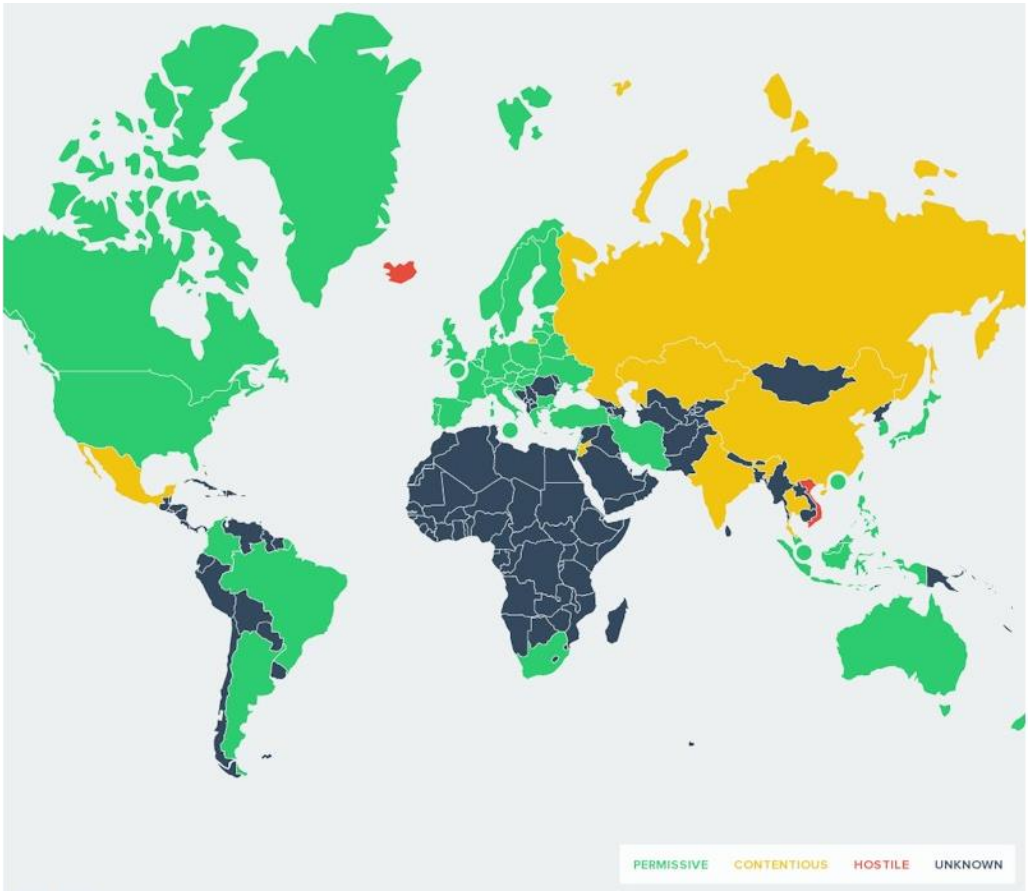
blockchain par l'achat de cryptomonnaies ou de tokens et les pistes peuvent être brouillées grâce au mixing. Les criminels pourront par la suite également chercher à cash-in leurs avoirs virtuels puis de les investir dans des actifs réels (GCBF 2018).

3.6 Règlementation

3.6.1 Perception des cryptomonnaies

L'augmentation de popularité très rapide qu'ont connu les cryptomonnaies a pris de cours la plupart des Etats du monde qui n'y étaient pour la plupart pas préparés. Actuellement, la majorité des pays, dont la Suisse, autorisent les cryptomonnaies.

Figure 26 : La perception des cryptomonnaies à travers le monde



Source : (BitLegal 2019)

Le 25 juin 2014, le Conseil fédéral a publié un rapport sur les monnaies virtuelles nommé « Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) ». C'était la première fois que le Conseil fédéral s'intéressait aux cryptomonnaies et à leur traitement juridique. Il avait alors estimé que l'importance économique des monnaies virtuelles en tant que moyen de paiement était faible et marginale pour la Suisse et que cela ne devrait pas changer dans un avenir proche. Par conséquent, il avait été décidé de ne pas légiférer sur les cryptomonnaies

estimant que les lois en vigueur encadraient suffisamment les infractions susceptibles d'être commises par leur utilisation (Conseil fédéral 2014).

Depuis, les cryptomonnaies se sont multipliées et leur capitalisation boursière a bondi passant d'un peu plus de 9 USD milliards à fin juin 2014 à plus de 830 USD milliards au début janvier 2018 (Cryptolization 2019). L'importance des monnaies virtuelles dans l'environnement économique s'est par conséquent totalement modifiée. Les enjeux et risques ne sont par conséquent plus les mêmes.

Le Conseil fédéral a publié un rapport le 14 décembre 2018 sur les DLT et la blockchain nommé « Bases juridiques pour la distributed ledger technology et la blockchain en Suisse ». Le Conseil fédéral reconnaît le potentiel important de la blockchain et sa volonté d'instaurer des conditions cadres dans le but que la Suisse puisse profiter des opportunités liées à ces nouvelles technologies pour s'établir en tant que place économique innovante et durable de premier plan pour les sociétés Fintech et Blockchain. Il estime entre autres que la Suisse est l'un des pays les plus avancés dans ce domaine. Ce rapport dresse un Etat des lieux de la réglementation en vigueur et est également utilisé afin de montrer que la Suisse est ouverte aux nouvelles technologies, qu'elle souhaite rendre ses conditions cadres favorables à l'innovation, que le cadre juridique est adapté à ces nouvelles technologies et qu'une lutte systématique sera réalisée contre les abus. En effet, il est primordial de préserver l'intégrité et la réputation de la place financière suisse (Conseil fédéral 2018).

Le Conseil fédéral a ouvert une consultation auprès du Département fédéral des finances (DFF) concernant l'adaptation du droit fédéral aux développements des DLT dans le but d'augmenter la sécurité juridique, supprimer les obstacles qui entravent les applications fondées sur la DLT et limiter les risques d'abus. La consultation se terminera à la fin du mois de juin 2019.

3.6.2 Les cryptomonnaies

Dans ce même rapport du 14 décembre 2018 sur les DLT et la blockchain, les cryptomonnaies ont été qualifiées par le Conseil fédéral de « valeurs patrimoniales incorporelles » principalement en raison de leur négociabilité. Elles sont par conséquent sujettes à un risque de blanchiment d'argent comme toute autre valeur patrimoniale et soumise à la réglementation contre le blanchiment d'argent précisée au Chapitre 2.4 de ce travail, soit l'article 305bis du Code Pénal, la LBA et l'OBA-FINMA. Néanmoins, les intermédiaires financiers actifs dans le domaine des cryptomonnaies ne sont pas les mêmes que ceux évoqués précédemment et ils ne sont pas tous soumis à la LBA. Les

intermédiaires financiers actifs dans les cryptomonnaies sont les suivants (Conseil fédéral 2018) :

- Fournisseurs de custodian wallets ;
- Fournisseur de non custodian wallets ;
- Bureaux de change online en cryptomonnaies ;
- Plateformes de négociation centralisée ;
- Plateforme de négociation décentralisée ;
- Mineurs.

3.6.2.1 Fournisseurs de custodian wallets

Les wallets sont des logiciels qui stockent les clés privées et publiques des détenteurs de cryptomonnaies. Ces deux clés cryptographiques permettent d'envoyer et de recevoir des monnaies virtuelles par l'intermédiaire de la blockchain ainsi que de surveiller le solde du compte correspondant. Les clés privées peuvent être considérées comme le code PIN nécessaire pour accéder à un compte bancaire alors que les clés publiques sont similaires au numéro de compte bancaire. Lorsqu'un détenteur de cryptomonnaies transfert une certaine valeur vers un destinataire, il utilise sa clé privée et indique la clé publique du destinataire. Lorsqu'une clé privée est perdue, les fonds seront perdus et la valeur au sein du compte ne pourra jamais être récupérée (De Filippi 2018).

Un fournisseur de custodian wallets détient les clés privées des détenteurs de cryptomonnaies qui ne bénéficient par conséquent pas d'un contrôle total sur les fonds. Il peut par conséquent envoyer et recevoir les monnaies virtuelles de sa clientèle. Cette activité est considérée comme du trafic de paiements et rentre dans le cadre juridique de la LBA au sens de l'article 2, alinéa 3, lettre b, LBA. Les fournisseurs de custodian wallets doivent s'affilier à un OAR ou se soumettre à la FINMA afin d'assurer une surveillance selon la LBA. Il leur est obligatoire de procéder à une identification sans montant minimum (Conseil fédéral 2018).

3.6.2.2 Fournisseurs de non custodian wallets

La différence avec un fournisseur de custodian wallets est qu'un fournisseur de non custodian wallets ne détient pas la clé privée des détenteurs de cryptomonnaies (De Filippi 2018). Dans ce cas-là, la FINMA estime que ce type de fournisseur n'est pas soumis à la LBA car il ne peut pas être considéré comme un intermédiaire financier étant donné qu'il ne dispose pas des valeurs patrimoniales ne détenant pas la clé privée (Conseil fédéral 2018).

3.6.2.3 Bureaux de change online en cryptomonnaies

Les bureaux de change online sont des marchés en ligne sur lesquels il est possible d'acheter ou vendre des cryptomonnaies en utilisant soit d'autres cryptomonnaies (altcoins), soit des monnaies traditionnelles (USD, EUR, GBP, etc.). Les transactions sont effectuées avec le bureau de change et pas avec une autre contrepartie. Ces opérations de change de cryptomonnaies rentrent dans le cadre juridique de la LBA au sens de l'article 2, alinéa 3, lettre c, LBA. Le risque de blanchiment d'argent lié à cette activité de change est évalué par la FINMA similaire à l'activité de change traditionnel. Il est par conséquent obligatoire pour un bureau de change online en cryptomonnaies de procéder à une identification lorsque le seuil de 5'000 CHF est dépassé (Conseil fédéral 2018).

3.6.2.4 Plateforme de négociation centralisée

Les plateformes de négociation centralisées sont des marchés en ligne sur lesquels il est possible d'échanger des cryptomonnaies contre d'autres, d'acheter et de vendre des cryptomonnaies et d'échanger de la monnaie traditionnelle contre des cryptomonnaies. Contrairement aux bureaux de change online, les plateformes de négociation centralisées exercent une activité d'intermédiaire entre un acheteur et un vendeur. Elles rentrent par conséquent dans le cadre juridique de la LBA et sont soumises au même seuil que les fournisseurs de custodian wallets (Conseil fédéral 2018).

3.6.2.5 Plateforme de négociation décentralisée

Les plateformes de négociation décentralisées fonctionnent sans serveur central et les nœuds du réseau sont répartis. Les fonds ne passent pas par une institution centralisée et sont transférés directement entre un utilisateur et sa contrepartie au sein de la blockchain. Selon la FINMA, ce type de plateforme n'est pas soumis à la LBA uniquement lorsqu'elle n'a aucune possibilité d'intervenir dans l'exécution des transactions. Dans les autres cas où elle aurait à confirmer les ordres ou elle se donnerait le droit d'intervenir dans les transactions, elle est soumise à la LBA car elle fournit un service d'intermédiaire financier dans le domaine du trafic de paiement (article 2, alinéa 3, lettre b, LBA) (Conseil fédéral 2018).

3.6.2.6 Mineurs

L'activité de minage en Suisse n'est pas soumise à autorisation selon la législation en vigueur (Conseil fédéral 2018).

3.6.3 ICO

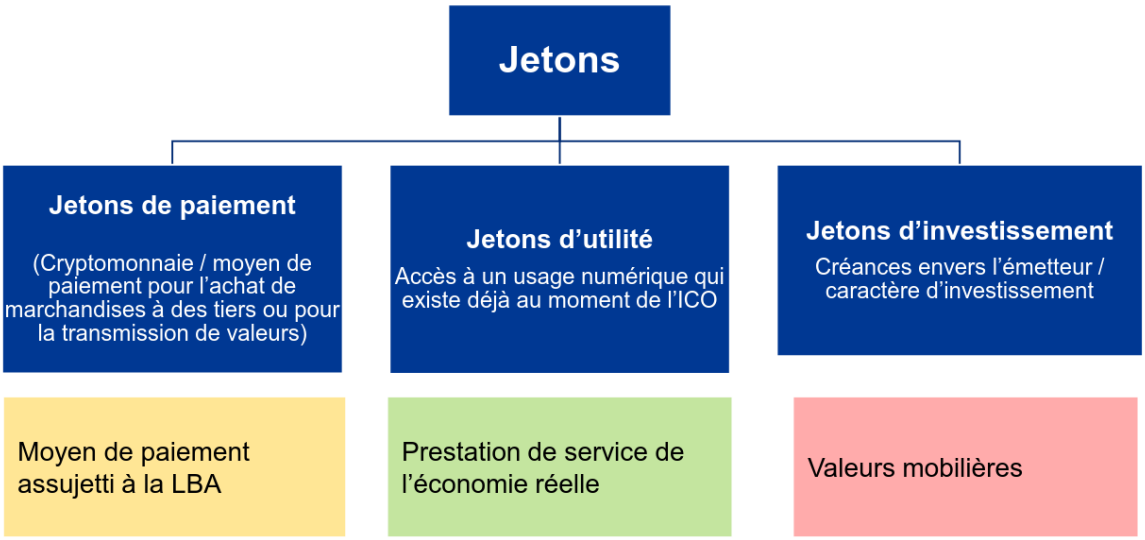
Comme la carte ci-dessous le montre, la majorité des pays qui se sont questionnés sur les ICOs se montrent méfiants à leur égard. Les seuls Etats ayant à ce jour mis en place une règlementation favorable aux ICOs sont la Suisse, la Slovaquie, la Lituanie, l'Estonie, le Japon, l'Ouzbékistan, Israël et Taiwan. Trois pays ont également interdit les ICOs. C'est le cas du Pakistan, de l'Inde et de la Chine (PwC 2019).

Figure 27 : Régulation des ICOs à travers le monde

Source : (PwC 2019)

La FINMA a publié le 16 février 2018 un guide pratique sur les ICOs dans lequel elle s'est penchée sur la qualification juridique des tokens (FINMA 2018). C'est la première instance officielle à s'être intéressée à cela. Les tokens émis lors des ICOs ont été séparés en trois types différents par une approche fondée sur leur fonction économique.

Figure 28 : Classification des jetons ICO



Source : (FINMA 2018)

3.6.3.1 Les jetons de paiement

Les jetons de paiement correspondent aux cryptomonnaies. Ils sont considérés comme les tokens devant être utilisés comme moyen de paiement au sein de la blockchain. Etant donné que ces tokens sont utilisés comme un moyen de paiement, les émetteurs sont soumis à la LBA conformément à l'article 2, alinéa 3, lettre b, LBA. Ils auront ainsi l'obligation de s'affilier à un OAR ou de se soumettre à la FINMA (FINMA 2018).

3.6.3.2 Les jetons d'utilité

Les jetons d'utilité permettent un accès futur aux produits ou services offerts par une entreprise sur un espace blockchain. Par conséquent, les jetons d'utilité ne sont pas créés pour être un investissement et ne sont pas considérés comme des valeurs mobilières (FINMA 2018).

3.6.3.3 Les jetons d'investissement

Les jetons d'investissement représentent des valeurs patrimoniales. Il peut par exemple y avoir des tokens similaires à des actions qui permettent à leurs détenteurs de recevoir un dividende ou une commission fixe. Ils pourront également participer aux décisions de l'entreprise. Il existe également des tokens similaires à des obligations qui rapportent des intérêts à ceux qui les ont acquis et à d'autres instruments financiers dérivés. Par conséquent, les jetons d'investissement sont considérés par la FINMA comme valeur mobilière au sens de la LIMF (article 2, lettre b). Les émetteurs des jetons seront ainsi soumis à la LBVM (FINMA 2018).

Le tableau ci-dessous résume les différentes catégories de services liées aux cryptomonnaies vues précédemment ainsi que l'état de leur soumission à la LBA.

Tableau 4 : Catégories de services liés aux cryptomonnaies

Catégorie de services	Soumis à la LBA	Non soumis à la LBA	Soumis à la LBA à certaines conditions
ICOs			Soumis à la LBA lorsque l'ICO émet des jetons qui peuvent être assimilés à des moyens de paiement (jetons de paiement)
Fournisseurs de custodian wallets	Soumis à la LBA dans tous les cas		
Fournisseurs de non custodian wallets		Non soumis à la LBA	
Bureaux de change online en crypto-monnaies	Soumis à la LBA au même titre que les bureaux de change traditionnel		
Plateformes de négociation centralisées	Soumises à la LBA dans tous les cas		
Plateformes de négociation décentralisées			Soumises à la LBA lorsqu'elles ont la possibilité d'intervenir dans les transactions de leurs utilisateurs, par exemple pour bloquer une transaction
Mineurs		Non soumis à la LBA	

Source : (GCBF 2018)

3.7 Evaluation du risque de blanchiment d'argent

Les risques de blanchiment liés aux cryptomonnaies présentés précédemment sont nombreux : escroqueries, piratages, rançongiciels, mineurs malveillants, utilisation des cryptomonnaies dans le but de blanchir de l'argent sale ou encore acquisitions et ventes de produits illégaux. Le mécanisme de blanchiment d'argent avec des cryptomonnaies qui consiste à donner une apparence légale à de l'argent « sale » est le même qu'avec des monnaies traditionnelles. La première phase consiste à placer l'argent provenant d'activités illicites dans le système financier en achetant des monnaies virtuelles. La deuxième phase consiste à masquer l'origine des fonds en créant plusieurs comptes de cryptomonnaies et en utilisant les services de mixing. Enfin, la troisième phase consiste à intégrer l'argent obtenu illégalement à l'argent légal en conservant les produits illicites sous la forme de cryptomonnaies pour effectuer d'autres transactions ou en effectuant un « cash out », c'est-à-dire échanger les cryptomonnaies contre des monnaies traditionnelles (Natarajan 2019).

Certaines caractéristiques spécifiques à la blockchain favorisent le développement de ces risques. La caractéristique principale est la préservation de l'anonymat qui inévitablement attire des escrocs en quête de blanchir leur argent illégalement obtenu avec un sentiment de couverture plus important. La désintermédiation financière des transactions est également une caractéristique qui favorise les possibilités de blanchiment d'argent car de ce fait, aucun contrôle n'est effectué par une entité centrale. La menace est d'autant plus grande car, dans la technologie blockchain, il est très compliqué pour un intermédiaire financier d'identifier les ayant droits économiques. L'unique moment où l'ayant droit économique doit être est identifié avec certitude, c'est lors de l'achat ou la vente de cryptomonnaies contre des monnaies traditionnelles. Cela est dû au fait que les bureaux de change online en cryptomonnaies et les plateformes de négociation centralisées sont soumis à une surveillance LBA. Même dans le cas où une autorité de justice pénale souhaiterait séquestrer certaines valeurs d'origine criminelle d'un portefeuille virtuel, elle serait dans l'impossibilité de le faire car il serait nécessaire de détenir la clé cryptographique privée du wallet (GCBF 2018).

Lors d'une étude réalisée en 2018 au Canada par Malcolm Campbell-Verduyn, il déclare que les menaces de blanchiment d'argent liées aux cryptomonnaies sont plus théoriques que réelles. En effet, selon lui, malgré une couverture médiatique parfois sensationnaliste, peu d'éléments de preuve impliquent directement les cryptomonnaies dans le blanchiment d'argent à grande échelle. Le blanchiment d'argent n'est pas né avec l'avènement des cryptomonnaies. Il estime que les monnaies nationales et beaucoup

d’autres technologies numériques présentent actuellement des défis égaux voir même plus grands en matière de blanchiment d’argent (Campbell-Verduyn 2018).

Une analyse économique approfondie sur le blanchiment d’argent par le biais de cryptomonnaies a été réalisée en 2015 par des chercheurs de l’université de Fribourg en Allemagne. Les facteurs contextuels et transactionnels propres aux cryptomonnaies ont été identifiés et analysés afin de comprendre s’ils incitent les criminels positivement ou négativement à blanchir leur argent par ce moyen. Sur les 10 principaux facteurs identifiés, seulement 2 peuvent inciter négativement les criminels à utiliser les cryptomonnaies pour blanchir de l’argent. Il s’agit de l’acceptation limitée des cryptomonnaies ainsi que leur grande volatilité. Les 8 facteurs pouvant avoir une incitation positive sont les suivants : la décentralisation du stockage des informations, l’authentification par le biais d’un pseudonyme, la flexibilité transactionnelle qui ne dépend pas d’un prestataire de service, l’irrévocabilité des transactions, le traitement des paiements qui ne requiert pas d’intermédiaire, la transférabilité internationale, la rapidité des transactions et les faibles coûts de transactions. L’analyse a été effectuée en comparant les attributs des cryptomonnaies à ceux d'instruments et de services financiers conventionnels. Il a été conclu que les propriétés présentées pourraient effectivement encourager l'exploitation des cryptomonnaies par les criminels en quête de blanchir leur argent (Brenig, Accorsi et Müller 2015). Néanmoins, avec le temps, les deux derniers facteurs évoqués se sont révélés être moins positifs que prévu. En effet, le temps de confirmation des transactions ainsi que les coûts de transactions ont explosé lors de l’envolée du prix du Bitcoin.

Plusieurs études scientifiques se sont penchées sur l’utilisation du Bitcoin pour blanchir des revenus provenant d’activités illégales. Une étude exploratoire a été réalisée en 2018 par des chercheurs néerlandais sur le blanchiment d'argent des produits de la cybercriminalité à l'aide de bitcoin. Cette étude a conclu que le blanchiment d'argent par l’utilisation du Bitcoin est un modèle facile à utiliser et efficace. Des affaires récentes et des rapports d'Europol confirment la conclusion selon laquelle les cybercriminels utilisent des bitcoins pour blanchir de l'argent. La capacité de réduire le coût du blanchiment, tout en offrant plus d'anonymat, en fait une technique de blanchiment d'argent intéressante pour les criminels (Van Wegeberg, Oerlemans, et Van Deventer 2018). Le Centre sur la sanction et la finance illicite (CSIF) a réalisé en 2018 une analyse approfondie de données de transactions en Bitcoin entre 2013 et 2016 afin de découvrir la façon dont les Bitcoins illicites sont blanchis. Il s’est révélé que la source de presque tous les Bitcoins illicites blanchis par les services de conversion provenaient du darknet. Il ressort de l'étude que certains types de services de conversion ont une plus forte propension à recevoir des

Bitcoins provenant de sources illicites comme les mélangeurs (mixing) et les sites de jeux d'argent en ligne et sont donc très préoccupants pour le blanchiment d'argent. Les mélangeurs ont constamment traité environ un quart des bitcoins illicites entrants par an alors que la proportion blanchie par les plateformes « exchanges » et les jeux de hasard s'élève entre 66% et 72% (Fanusie et Robinson 2018). Finalement, selon une étude réalisée en janvier 2018 par des chercheurs de l'Université de Sydney, près d'un quart des utilisateurs de Bitcoins et près de la moitié des transactions pourraient être liés à des activités illégales. Ces activités se montent à environ 72 USD milliard par an, soit aux marchés de la drogue européen et américain réunis (Foley, Karlsen et Putnins 2018).

Au niveau de la réglementation nationale, la LBA s'applique à de nombreux intermédiaires financiers actifs dans l'univers des cryptomonnaies. Le Conseil fédéral estime que la Suisse a développé à ce jour le meilleur dispositif réglementaire possible pour contrer les menaces des cryptomonnaies. Néanmoins, la rapidité et la mobilité importante qui caractérise les cryptomonnaies permettent en quelques secondes de transférer des fonds à l'autre bout de la Terre. Il est par conséquent très souvent nécessaire de devoir recourir à une entraide judiciaire internationale. C'est pour ces motifs que la Suisse s'est engagée, au sein du GAFI, en faveur d'une harmonisation des règlementations de chaque pays en matière de lutte contre le blanchiment d'argent par les cryptomonnaies. La diversité des juridictions pénales mondiales actuelle envers les cryptomonnaies augmente considérablement le risque. En effet, il est possible de recourir à des sociétés actives dans la blockchain et les cryptomonnaies dans une juridiction où la législation contre le blanchiment d'argent est faible ou inexistante tout en se trouvant dans une juridiction où la règlementation est solide comme la Suisse. Dans le but de continuer cette lutte, la Suisse a créé en 2018 « Cyberboard », une plateforme nationale spécialisée dans la cybercriminalité (GCBF 2018).

A ce jour, il n'y a eu que très peu de cas d'intermédiaires financiers ayant dénoncé des personnes au MROS pour soupçons de blanchiment d'argent par l'usage de cryptomonnaies (MROS 2018). Cela peut amener deux hypothèses sur le risque réel lié aux cryptomonnaies. La première serait que le risque est faible et cette nouvelle technologie, encore en développement, n'a que très peu été utilisée dans le but de blanchir de l'argent. La deuxième serait que ce faible nombre montre l'inefficience du modèle actuel d'identification de blanchiment d'argent par les cryptomonnaies. Il est très difficile de prouver la provenance criminelle de fonds au sein d'une blockchain à cause notamment de l'utilisation du mixing.

Il est par conséquent difficile d'évaluer le risque réel de blanchiment d'argent par les cryptomonnaies auquel la Suisse est exposée. Néanmoins, la forte présence de la Suisse dans le monde des cryptomonnaies et des ICO, notamment au sein du canton de Zoug, ainsi que la volonté du Conseil fédéral de s'ouvrir aux nouvelles technologies et de promouvoir l'innovation démontre une certaine et importante vulnérabilité du pays. De plus, les spécialistes s'étant déjà penchés sur le cas sont tous d'accord sur le fait que les cryptomonnaies, et en particulier le Bitcoin, sont un moyen alternatif de blanchiment d'argent qui dispose de nombreux atouts appréciés par les criminels et de peu de faiblesses. Les recherches effectuées démontrent qu'un certain nombre de criminels utilisent le Bitcoin afin de blanchir leur argent obtenu illégalement.

Selon le rapport du Conseil fédéral publié le 14 décembre 2018, le risque de blanchiment d'argent lié aux cryptomonnaies ne peut pas être formellement évalué en raison du nombre très faible de cas connus. Malgré cela, le rapport de la Confédération suisse d'octobre 2018 conclut que la Suisse est grandement vulnérable et que par conséquent la menace est réelle (GCBF 2018).

4. Conclusion

Les cryptomonnaies, en particulier le Bitcoin, ont connu une popularité immense auprès des investisseurs en très peu de temps. Certains y voient tout simplement un bon moyen de spéculer tant leur volatilité est élevée, d'autres comme une technologie innovatrice permettant de désintermédier la confiance par le biais de la décentralisation, d'autres encore comme un outil plébiscité par les criminels voulant agir dans l'anonymat le plus total. Ce qui est certain est que la blockchain est une technologie révolutionnaire qui va très certainement transformer le paysage et les habitudes de notre société. Les intermédiaires financiers traditionnels ainsi que les gouvernements ont été surpris par l'arrivée des cryptomonnaies et ont tardé à s'y intéresser. Cette technologie a créé des opportunités pour de nouveaux types d'intermédiaires financiers comme les fournisseurs de portefeuilles virtuels ou les plateformes de négociation qui ne sont pas tous soumis à la législation en vigueur.

Il est possible de comparer l'arrivée de la blockchain à l'apparition d'Internet. En effet, les développeurs d'Internet voulaient au départ créer un outil de mondialisation ne dépendant pas d'intermédiaire. Les escrocs se sont ensuite intéressés à cette nouvelle technologie leur permettant de communiquer anonymement. Puis, les Etats et les entreprises ont pris conscience des possibilités offertes par ce nouvel outil et en ont exploité les ressources (De Filippi 2018). Dans le cas de l'invention de la blockchain, les créateurs réclamaient une société plus libre et moins surveillée par les intermédiaires financiers. Par la suite, cette technologie basée sur l'anonymat et la désintermédiation a attiré les criminels qui voulaient profiter des cryptomonnaies pour blanchir de l'argent et vendre des produits illicites. Lors de l'envolée du Bitcoin, ce sont les investisseurs attirés par le gain qui sont arrivés sur le marché. Et enfin, les banques, les entreprises et les Etats s'y sont intéressés car ils y ont vu un moyen d'améliorer la productivité, l'efficacité et la transparence.

Les monnaies virtuelles ne remplissent pas les fonctions qu'une monnaie souveraine doit impérativement avoir mais sont considérées économiquement comme des actifs financiers numériques. Leur particularité réside dans leur forte volatilité qui attire les spéculateurs. Leur technologie sous-jacente qui favorise l'anonymat et la désintermédiation financière ainsi que le manque de régulation à leur encontre attirent quant à eux les escrocs désireux de blanchir leur argent obtenu illégalement. Les risques de blanchiment d'argent liés aux monnaies virtuelles sont nombreux et un certain nombre de cas ont à l'heure actuelle été répertoriés. Les études réalisées par des experts ont montré que l'utilisation des cryptomonnaies, et principalement du Bitcoin, était un moyen

apprécié par les criminels désireux de blanchir leur argent illégal. En effet, leur technologie sous-jacente dispose de nombreux atouts positifs pour les escrocs.

La Suisse croit fortement en la technologie des registres distribués dont la blockchain fait partie, y est ouverte et souhaite que le pays puisse profiter des opportunités de développement de ces technologies. Cette ouverture assumée par le Conseil fédéral ainsi que l'importante présence de la Suisse dans le monde des cryptomonnaies et des ICO rend le pays forcément vulnérable contre les revers négatifs de cette technologie, notamment le risque de blanchiment d'argent. La législation suisse en vigueur couvre de la meilleure manière possible les intermédiaires actifs dans les cryptomonnaies. Néanmoins, la non-uniformisation des législations mondiales ainsi que la difficulté à identifier les ayants droits économiques contribuent à augmenter le risque. Les communications effectuées au MROS sont en forte augmentation mais très peu de cas liés à des soupçons de blanchiment d'argent par l'usage de cryptomonnaies ont été communiqués.

Il est primordial d'établir un régime réglementaire efficace dans le but de protéger les investisseurs. Néanmoins, la caractéristique principale et unique des cryptomonnaies se base sur la décentralisation. Par conséquent, préconiser la réglementation ne consiste pas à centraliser ou à confier le contrôle de la monnaie à un gouvernement ou à une institution. Si cela est fait, la monnaie perdra son caractère unique et ne deviendra qu'une autre monnaie fiduciaire. Selon une enquête réalisée au sein de l'Université d'Afrique du Sud en 2018, une solution intéressante serait que les gouvernements se penchent sur la création de plateformes permettant la conversion de cryptomonnaies en monnaie nationale sur laquelle tous les fournisseurs de services auraient l'obligation d'être titulaires d'une autorisation et d'être soumis à des contrôles de sécurité. Un KYC devrait être adopté à tous les niveaux sans être nécessairement rendu public, mais il devrait être une condition préalable à la transaction afin de donner de la crédibilité au processus de transaction (Akhigbe Iyen 2018).

La capitalisation boursière des cryptomonnaies reste faible par rapport à d'autres actifs financiers. La limite de la grande majorité des blockchains se retrouve dans la vitesse d'exécution des transactions. Dans la blockchain de Bitcoin, seules 240'000 transactions peuvent être réalisées par jour alors qu'une société comme VISA en traite environ 150'000'000 (De Filippi 2018). La consommation énergétique des mineurs qui est essentielle au bon fonctionnement de la blockchain est déjà énorme à l'heure actuelle. Tout cela montre que Bitcoin et les autres cryptomonnaies ne sont, à l'heure actuelle, pas capables d'être utilisées de manière massive au sein de l'économie.

Le potentiel de la blockchain est énorme et pourrait être utile dans la lutte contre le blanchiment d'argent. En effet, étant donné que chaque transaction est enregistrée de manière indélébile au sein de la base de données transparente, le potentiel de contrôle est plus élevé. Il serait par exemple possible pour les intermédiaires financiers comme les banques de contrôler toutes les transactions automatiquement selon certains critères préalablement saisis. L'historique de toutes les transactions permettrait ainsi d'avoir une certitude sur la provenance des avoirs. Les travaux de vérification seraient ainsi facilités pour les intermédiaires financiers et pour les sociétés d'audit. A ce sujet, la Banque populaire de Chine teste depuis décembre 2016 une application d'essai d'une monnaie virtuelle supportée par une blockchain. Elle estime notamment qu'une monnaie virtuelle gérée centralement est un excellent moyen de lutter contre le blanchiment d'argent car des informations telles que le nom et la date de toutes les transactions qui ont lieu sont disponibles en temps réel (Yap 2017). Par conséquent, les banques s'intéressent particulièrement aux blockchains privées. Contrairement à la majorité des blockchains comme celle de Bitcoin qui sont publics, ce sont des écosystèmes fermés dans lesquels les acteurs sont préalablement identifiés avant d'être autorisés à intégrer le réseau. A défaut de désintermédier le secteur financier, cela pourrait être utile dans le but d'optimiser et d'automatiser les contrôles et ainsi respecter au maximum les mesures de lutte contre le blanchiment d'argent. Néanmoins, cela impliquerait une surveillance générale et permanente car les informations telle que l'historique des transactions et le montant des portefeuilles seraient accessibles à tous les acteurs de la blockchain (De Filippi 2018).

Selon une étude réalisée par EY pour l'année 2018 (EY 2019), 28% des banques présentes en Suisse indiquent que la blockchain est la plus grande menace pour les établissements financiers. Elle représente la deuxième menace, juste derrière celle liée aux places de marchés et plateformes d'échanges. Même si la manière dont cette technologie sera utilisée au sein des nouveaux modèles d'affaires n'est à l'heure actuelle pas connue, ce sera une occasion et une nécessité de renouveler le système financier.

Bibliographie

AGEFI, 2019. « Fraude fiscale : UBS condamné à une amende record de 3,7 milliards d'euros ». *AGEFI* [en ligne]. 22 janvier 2019. [Consulté le 13 février 2019]. Disponible à l'adresse : https://www.agefi.com/home/entreprises/detail/edition/online/article/le-geant-bancaire-ubs-a-ete-condamne-ce-mercredi-a-une-amende-de-37-milliards-deuros-par-la-justice-francaise-485543.html

AKHIGBE IYEN, Joy, 2018. *The Future of Crypto-Currency in the Absence of Regulation, Social and Legal Impact* [en ligne]. Jaipur : GRDS Publishing, 21 mai 2018. [Consulté le 3 juillet 2019]. PEOPLE: International Journal of Social Sciences, 4(1), 555-570. Disponible à l'adresse : https://grdspublishing.org/index.php/people/article/viewFile/1305/1125

AMOROS, Raul, 2018. « Comparing Cryptocurrency Against the Entire World's Wealth in One Graph ». *Howmuch* [en ligne]. 17 septembre 2018. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://www.bloomberg.com/news/articles/2018-02-07/bitcoin-on-credit-for-20-percent-of-owners-that-s-a-yes

AUTORITE FEDERALE DE SURVEILLANCE DES MARCHES FINANCIERS (FINMA), 2019. *Autorité fédérale de surveillance des marchés financiers* [en ligne]. [Consulté le 20 avril 2019]. Disponible à l'adresse : https://www.finma.ch/fr/

BANQUE NATIONALE SUISSE, 2019. *Banque nationale suisse* [en ligne]. [Consulté le 23 mars 2019]. Disponible à l'adresse : https://www.snb.ch/fr/

BITINFOCHARTS, 2019. *BitInfoCharts* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://bitinfocharts.com/

BITLEGAL, 2019. *BitLegal* [en ligne]. [Consulté le 13 février 2019]. Disponible à l'adresse : https://bitlegal.net/

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, 2019. *Board of Governors of the Federal Reserve System* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://www.federalreserve.gov/

BLOCKCHAIN LUXEMBOURG, 2019. *Blockchain Luxembourg* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://www.blockchain.com/

BRENIG, Christian, ACCORSI, Rafael, MÜLLER, Günter, 2015. *Economic Analysis of Cryptocurrency Backed Money Laundering* [en ligne]. ECIS, 29.05.2015. [Consulté le 2 juillet 2019] Completed Research Papers. Paper 20. ISBN 978-3-00-050284-2. Disponible à l'adresse : https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1019&context=ecis2015_cr

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2019. Rapport annuel 2018. *Office fédéral de la police fedpol* [en ligne]. Avril 2019. [Consulté le 27 avril 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2018-f.pdf

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2018. Rapport annuel 2017. *Office fédéral de la police fedpol* [en ligne]. Avril 2018. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2017-f.pdf

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2017. Rapport annuel 2016. *Office fédéral de la police fedpol* [en ligne]. Avril 2017. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2016-f.pdf

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2016. Rapport annuel 2015. *Office fédéral de la police fedpol* [en ligne]. Avril 2016. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2015-f.pdf

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2015. Rapport annuel 2014. *Office fédéral de la police fedpol* [en ligne]. Avril 2015. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2014-f.pdf

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2014. Rapport annuel 2013. *Office fédéral de la police fedpol* [en ligne]. Mai 2014. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2013-f.pdf

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2013. Rapport annuel 2012. *Office fédéral de la police fedpol* [en ligne]. Mai 2013. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2012-f.pdf

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2012. Rapport annuel 2011. *Office fédéral de la police fedpol* [en ligne]. Mai 2012. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2011-f.pdf

BUREAU DE COMMUNICATION EN MATIERE DE BLANCHIMENT D'ARGENT (MROS), 2011. Rapport annuel 2010. *Office fédéral de la police fedpol* [en ligne]. Avril 2011. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/jabe/jb-mros-2010-f.pdf

CAMPBELL-VERDUYN, Malcolm. 2018. *Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance* [en ligne]. New York : SpringerCrime, 19 janvier 2018. [Consulté le 2 juillet 2019]. Crime Law and Social Change (2018) 69:283-305. Disponible à l'adresse : https://link.springer.com/content/pdf/10.1007/s10611-017-9756-5.pdf

CARBON BLACK, 2019. « Global Threat Report. The Year of the Next-Gen Cyberattack ». *Carbon Black* [en ligne]. 23 janvier 2019. [Consulté le 17 mars 2019]. Disponible à l'adresse : https://www.carbonblack.com/wp-content/uploads/2019/01/carbon-black-global-threat-report-year-of-the-next-gen-cyberattack-0119.pdf

CHAINALYSIS, 2019. « Crypto crime report: Decoding Hacks, Darknet Markets, and Scams ». *Chainalysis* [en ligne]. 18 janvier 2019. [Consulté le 22 avril 2019]. Disponible à l'adresse : https://blog.chainalysis.com/reports/decoding-darknet-markets

Circulaire 2008/10 « Normes d'autorégulation reconnues comme standards minimaux ». *FINMA* [en ligne]. 20 novembre 2008. Mise à jour le 20 juin 2018. [Consulté le 24 avril 2019]. Disponible à l'adresse : https://www.finma.ch/fr/documentation/circulaires/

Code pénal suisse (RS 311.0). *Les autorités fédérales de la confédération suisse* [en ligne]. 21 décembre 1937. Mise à jour le 1er mars 2019. [Consulté le 23 mars 2019]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19370083/index.html

COINDESK, 2019. *CoinDesk* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://www.coindesk.com/ico-tracker

COINIST, 2019. *Coinist* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://www.coinist.io/biggest-icos-chart/

COINMARKETCAP, 2019. *CoinMarketCap* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://coinmarketcap.com/

COINMETRICS, 2019. *CoinMetrics* [en ligne]. [Consulté le 28 juin 2019]. Disponible à l'adresse : https://coinmetrics.io/

CONSEIL FEDERAL, 2014. Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070). *Les autorités fédérales de la confédération suisse* [en ligne]. 25 juin 2014. [Consulté le 12 mars 2019]. Disponible à l'adresse : https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf

CONSEIL FEDERAL, 2018. Bases juridiques pour la distributed ledger technology et la blockchain en Suisse. *Les autorités fédérales de la confédération suisse* [en ligne]. 14 décembre 2018. [Consulté le 6 avril 2019]. Disponible à l'adresse : https://www.newsd.admin.ch/newsd/message/attachments/55151.pdf

Convention relative à l'obligation de diligence des banques (CDB). *L'association suisse des banquiers* [en ligne]. 1er juillet 1977. Mise à jour le 1er janvier 2016. [Consulté le 23 mars 2019]. Disponible à l'adresse : http://shop.sba.ch/1000020_f.pdf

CRYPTOLIZATION, 2019. *Cryptolization* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://cryptolization.com/

CRYPTONAUTE, 2019. *Cryptonaute* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://cryptonaute.fr/

DARBELLAY Aline, 2018. Le régime de responsabilité civile en matière d'émissions publiques de jetons digitaux (ICO). *Revue suisse de droit des affaires et du marché financier*. 2018, Vol. 90, no 1, p. 48-66. [Consulté le 20 avril 2019]. Disponible à l'adresse : https://archive-ouverte.unige.ch/unige:103323

DE FILIPPI, Primavera, 2018. *Blockchain et cryptomonnaies*. 1ère éd. Paris : Humensis. Que sais-je ?, n°4141. ISBN 978-2-13-081145-9

DE PREUX, Pascal, 2018. Blockchain et lutte contre le blanchiment d'argent, Le nouveau paradoxe ? *EXPERT FOCUS* [en ligne]. 5 février 2018. Pp. 64 ss. [Consulté le 13 avril 2019]. Disponible à l'adresse : https://resolution-lp.ch/wp-content/uploads/2018/02/064_L_14_De_Preux_Trajilovic.pdf

DEBLIS, Michael, 2016. « What are the three stages of money launderinf ? ». *Deblis Law* [en ligne]. 7 septembre 2016. [Consulté le 13 février 2019]. Disponible à l'adresse : http://www.deblislaw.com/wp-content/uploads/2016/09/Three-stages-of-money-laundering.pdf

DELOITTE, 2018. The Deloitte International Wealth Management Centre Ranking 2018. *Deloitte* [en ligne]. 11 mai 2018. [Consulté le 13 avril 2019]. Disponible à l'adresse : https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/financial-services/ch-fs-deloitte-wealth-managemnet-Ranking-2018.pdf

DIGICONOMIST, 2019. *Digiconomist* [en ligne]. [Consulté le 24 juin 2019]. Disponible à l'adresse : https://digiconomist.net/bitcoin-energy-consumption

DOWLAT, Sherwin, 2018. « Cryptoasset market coverage initiation: Network Creation ». *Statis Group* [en ligne]. 11 juillet 2018. [Consulté le 17 mars 2019]. Disponible à l'adresse : https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

DUMAS, Jean-Guillaume, LAFOURCADE, Pascal, TICHIT, Ariane, VARRETTE, Sébastien, 2018. *Les blockchains en 50 questions : Comprendre le fonctionnement et les enjeux de cette technologie innovante*. Malakoff: Dunod. ISBN 978-2-10-077924-6

EUROPEAN BANKING AUTHORITY (EBA), 2019. Report with advice for the European Commission on crypto-assets. *European Banking Authority* [en ligne]. 9 janvier 2019. [Consulté le 22 avril 2019]. Disponible à l'adresse : https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf

EY, 2019. Baromètre des banques 2019. *EY* [en ligne]. Janvier 2019. [Consulté le 27 juin 2019]. Disponible à l'adresse : https://www.eycom.ch/fr/Publications/20190110-EY-Barometre-des-banques-2019-Les-signes-de-lepoque/download

FANUSIE, Yaya, ROBINSON, Tom, 2018. « Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services ». *Center on San Sanctions & Illicit Finance* [en ligne]. 12 janvier 2018. [Consulté le 2 juillet 2019]. Disponible à l'adresse : https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf

FINANCIAL STABILITY BOARD, 2018. « Crypto-asset markets: Potential channels for future financial stability implications ». *Financial Stability Board* [en ligne]. 10 octobre 2018. [Consulté le 25 juin 2019]. Disponible à l'adresse : https://www.fsb.org/2018/10/crypto-asset-markets-potential-channels-for-future-financial-stability-implications/

FINMA, 2018. Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO). *FINMA* [en ligne]. 16 février 2018. [Consulté le 14 avril 2019]. Disponible à l'adresse : https://www.finma.ch/fr/news/2018/02/20180216-mm-ico-wegleitung/

FINMA, 2019. Rapport annuel 2018. *L'Autorité fédérale de surveillance des marchés financiers* [en ligne]. 4 avril 2019. [Consulté le 22 avril 2019]. Disponible à l'adresse : https://www.finma.ch/fr/documentation/publications-finma/rapport-d-activite/

FOLEY, Sean, KARLSEN, Jonathan, PUTNINS, Talis, 2018. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies". *University of Sydney Business School* [en ligne]. 17 janvier 2018. [Consulté le 27 juin 2019]. Disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645

GOMEZ, Carole, MATELLY, Sylvie, 2018. *L'argent sale : à qui profite le crime ?* Paris: Eyrolles. ISBN 978-2-212-56841-7

GROUPE D'ACTION FINANCIERE (GAFI), 2019. *Groupe d'action financière* [en ligne]. [Consulté le 30 mars 2019]. Disponible à l'adresse : https://www.fatf-gafi.org/fr/

GROUPE INTERDEPARTEMENTAL DE COORDINATION SUR LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCMEMENT DU TERRORISME (GCBF), 2015. Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse. *Les autorités fédérales de la confédération suisse* [en ligne]. Juin 2015. [Consulté le 6 avril 2019]. Disponible à l'adresse : https://www.fedpol.admin.ch/dam/data/fedpol/kriminalitaet/geldwaescherei/nra-berichte/nra-bericht-juni-2015-f.pdf

GROUPE INTERDEPARTEMENTAL DE COORDINATION SUR LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCMEMENT DU TERRORISME (GCBF), 2018. Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding. *Les autorités fédérales de la confédération suisse* [en ligne]. Octobre 2018. [Consulté le 6 avril 2019]. Disponible à l'adresse : https://www.newsd.admin.ch/newsd/message/attachments/55112.pdf

ICORATING, 2018. "Exchange Security Report". *ICORATING* [en ligne]. 02 octobre 2018. [Consulté le 17 mars 2019]. Disponible à l'adresse : https://icorating.com/report/exchange-security-report/

KHARIF, Olga, 2018. "Bitcoin on Credit? For 20 Percent of Owners, That's a Yes". *Bloomberg* [en ligne]. 7 février 2018. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://www.bloomberg.com/news/articles/2018-02-07/bitcoin-on-credit-for-20-percent-of-owners-that-s-a-yes

KUO CHENG LEE, David, 2015. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Londres : Elsevier. ISBN 978-0-12-802117-0

KUO CHENG LEE, David, LOW, Linda, 2018. *Inclusive Fintech: Blockchain, Cryptocurrency and ICO*. Singapour : World Scientific Publishing. ISBN 978-981-3272-76-7

LASTOVETSKA, Anastasiia, 2019. « Blockchain Architecture Basics: Components, Structure, Benefits & Creation ». *MLSDev* [en ligne]. 31 janvier 2019. [Consulté le 16 mars 2019]. Disponible à l'adresse : https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

Loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (LBA ; RS 955.0). *Les autorités fédérales de la confédération suisse* [en ligne]. 10 octobre 1997. Mise à jour le 1er janvier 2019. [Consulté le 23 mars 2019]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19970427/index.html

Loi fédérale sur les bourses et le commerce des valeurs mobilières (LBVM ; RS 954.1). *Les autorités fédérales de la confédération suisse* [en ligne]. 24 mars 1995. Mise à jour le 1er janvier 2016. [Consulté le 24 avril 2019]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/19950081/index.html

Loi fédérale sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés (LIMF ; RS 958.1). *Les autorités fédérales de la confédération suisse* [en ligne]. 19 juin 2015. Mise à jour le 1er janvier 2019. [Consulté le 24 avril 2019]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/20141779/index.html

LOMBARDINI, Carlo, 2016. *Banques et blanchiment d'argent*. 3ème édition. Genève/Zurich : Schulthess Editions Romandes. ISBN 978-3-7255-8569-4

MÖSER, Malte, et al., 2018. *An Empirical Analysis of Traceability in the Monero Blockchain* [en ligne]. Boston : De Gruyter, juin 2018. [Consulté le 2 juillet 2019]. Proceedings on Privacy Enhancing Technologies ; 2018 (3):143–163. Disponible à l'adresse : https://arxiv.org/pdf/1704.04299/

NATARAJAN, Mangai, 2019. *International and Transnational Crime and Justice*. 2e edition. New York : Cambridge University Press. ISBN 978-1-108-49787-9

OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME (UNODC), 2019. « Money-Laundering and Globalization ». *Office des Nations Unies contre la drogue et le crime* [en ligne]. [Consulté le 12 avril 2019]. Disponible à l'adresse : https://www.unodc.org/unodc/en/money-laundering/globalization.html

Ordonnance de l'Autorité fédérale de surveillance ces marchés financiers sur la lutte contre le blanchiment d'argent et le financement du terrorisme dans le secteur financier (OBA-FINMA ; RS 955.033.0). *Les autorités fédérales de la confédération suisse* [en ligne]. 3 juin 2015. Mise à jour le 1er janvier 2019. [Consulté le 23 mars 2019]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/20143112/index.html

Ordonnance sur la lutte contre le blanchiment d'argent et le financement du terrorisme (OBA ; 955.01). *Les autorités fédérales de la confédération suisse* [en ligne]. 11 novembre 2015. Mise à jour le 1er janvier 2016. [Consulté le 23 mars 2019]. Disponible à l'adresse : https://www.admin.ch/opc/fr/classified-compilation/20152238/index.html

PITTA, Julie, 1999. « Requiem for a Bright Idea ». *Forbes* [en ligne]. 1er novembre 1999. [Consulté le 13 février 2019]. Disponible à l'adresse : https://www.forbes.com/forbes/1999/1101/6411390a.html#6ffd1deb715f

POZZI, Daniele, 2019. « ICO Market 2018 vs 2017: Trends, Capitalization, Localization, Industries, Success Rate ». *CoinTelegraph* [en ligne]. 5 janvier 2019. [Consulté le 17 mars 2019]. Disponible à l'adresse : https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate

PRICEWATERHOUSECOOPERS (PwC), 2019. Legal Frameworks and regulation for ICOs. *PricewaterhouseCoopers* [en ligne]. Mai 2012. [Consulté le 22 avril 2019]. Disponible à l'adresse : https://www.pwc.ch/en/industry-sectors/financial-services/fs-regulations/ico.html

SPRENGER, Pascal, BALSIGER, Franziska, 2018. Anti-Money laundering in times of cryptocurrencies. *KPMG* [en ligne]. Juin 2018. [Consulté le 12 avril 2019]. Disponible à l'adresse : https://assets.kpmg/content/dam/kpmg/ch/pdf/anti-money-laundering-in-times-of-cryptocurrency.pdf

VAN DUYNE, Petrus, HARVEY, Jackie, GELEMEROVA, Liliya, 2018. *The Critical Handbook of Money Laundering*. Londres : Palgrave Macmillan. ISBN 978-1-137-52398-3

VAN WEGEBERG, Rolf, OERLEMANS, Jan-Jaap, VAN DEVENTER, Oskar, 2018. *Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin* [en ligne]. Esmerald Publishing Limited, 2018. [Consulté le 3 juillet 2019]. Journal of Financial Crime, Vol. 25 Issue: 2, pp.419-435. Disponible à l'adresse : https://www.emeraldinsight.com/doi/full/10.1108/JFC-11-2016-0067

WEITMANN, Amir, 2009. *L'affaire Madoff : Les secrets de l'arnaque du siècle*. Paris : Plon. ISBN 978-2-259-21051-5

WINIKER, Rachel, 2019. *Justification et fondements de la surveillance* [document PDF]. Support de cours : Cours « Compliance », Haute école de gestion de Genève, filière économie d'entreprise, année académique 2018-2019

YAHOO ! FINANCE, 2019. *Yahoo ! Finance* [en ligne]. [Consulté le 26 juin 2019]. Disponible à l'adresse : https://finance.yahoo.com/

YAP, Brian, 2017. PBOC uses blockchain technology to combat money laundering [en ligne]. Londres,: Euromoney Institutional Investor PLC, 14 février 2017. [Consulté le 3 juillet 2019]. International Financial Law Review. Disponible à l'adresse : https://www.iflr.com/Article/3661468/PBOC-uses-blockchain-technology-to-combat-money-laundering.html?ArticleId=3661468

Annexe 1 : Communications MROS 2009-2018

Communications	2009		2010		2011		2012		2013	
	#	MCHF	#	MCHF	#	MCHF	#	MCHF	#	MCHF
Transmises aux autorités de poursuite pénale	797	2'164	1'002	3'223	1'471	3'223	1'355	2'841	1'115	2'796
Non transmises	99	65	157	58	154	58	230	319	295	183
Total	**896**	**2'229**	**1'159**	**3'281**	**1'625**	**3'281**	**1'585**	**3'160**	**1'410**	**2'979**
dont banques	*603*		*822*		*1'080*		*1'050*		*1'123*	
Taux de conversion	**89%**		**86%**		**91%**		**85%**		**79%**	

Communications	2014		2015		2016		2017		2018	
	#	MCHF	#	MCHF	#	MCHF	#	MCHF	#	MCHF
Transmises aux autorités de poursuite pénale	1'298	2'862	1'724	3'564	1'726	2'516	2'206	10'743	2'368	11'355
Non transmises	455	478	643	1'263	696	1'837	1'055	1'538	1'212	3'453
En cours de traitement	-	-	-	-	487	969	1'423	4'190	2'546	2'781
Total	**1'753**	**3'341**	**2'367**	**4'827**	**2'909**	**5'321**	**4'684**	**16'471**	**6'126**	**17'589**
dont banques	*1'495*		*2'159*		*2'502*		*4'262*		*5'440*	
Taux de conversion	**74%**		**73%**		**59%**		**47%**		**39%**	

Source : adapté de MROS (2009-2018)