PASCAL DE PREUX
DANIEL TRAJILOVIC

BLOCKCHAIN ET LUTTE CONTRE LE BLANCHIMENT D'ARGENT

Le nouveau paradoxe?

Le ou la «blockchain» – le genre de cette nouvelle technologie étant encore controversé – est sur toutes les lèvres. Elle serait l'innovation la plus importante de ces dernières années juste derrière l'invention d'Internet, il y a maintenant 28 ans. Initialement, son application était intimement liée au «Bitcoin» monnaie virtuelle qui a pu défrayer la chronique par le passé et dont nous expliquerons également les contours dans la présente contribution.

1. INTRODUCTION

Nous constatons que, depuis quelque temps, l'utilisation de la blockchain pourrait s'écarter de son but originel et devenir le futur outil des gouvernements (cryptomonnaies), des administrations (collecte d'impôts, registre foncier), de certains secteurs de l'économie (comptabilité, approvisionnements, systèmes d'information), mais surtout des marchés financiers. En particulier, les banques prédisent que la *blockchain* serait l'avenir de la compliance. Si l'enthousiasme des milieux bancaires et financiers pour cette nouvelle technologie est légitime, elle ne doit pas les détourner d'une de leurs obligations légales principales, la lutte contre le blanchiment d'argent.

La *blockchain* présente dès lors deux faces. D'un côté, elle sert d'interface à l'utilisation de la monnaie virtuelle «*Bitcoin*» et de ses dérivés tels que l'«Ether». Dans cette configuration, la *blockchain* peut présenter un risque en matière de criminalité économique. D'un autre côté, la *blockchain* pourrait s'avérer être un outil efficace de lutte contre le blanchiment d'argent.

C'est en cela que la technologie *blockchain* peut paraître paradoxale. Elle permettrait aux organisations criminelles d'entraver l'origine criminelle de leurs avoirs, mais elle viserait également à éviter que ces mêmes fonds ne puissent être introduits dans le circuit économique ordinaire.

La présente contribution s'attachera ainsi à expliquer les deux faces de cette technologie innovante, avec leurs risques respectifs.

2. NOTION

2.1 L'utilisation originelle de la Blockchain et l'exemple du Bitcoin. Le concept de *blockchain* est inventé par *Satoshi Nakamoto,* en 2008 [1]. Il s'agit d'un pseudonyme, l'identité réelle de l'inventeur demeure toujours un mystère. Le but initial de la *blockchain* était de donner une infrastructure logicielle à la création et au transfert du *Bitcoin*.

La *blockchain* est une base de données décentralisée (registre distribué ou *distributed ledger*) qui compile toutes les transactions déjà réalisées et les valeurs ou données s'y trouvant au sein d'une «chaîne de blocs» [2]. La *blockchain* permet de stocker des données qui ne sont par la suite plus modifiables. Il est alors possible de transférer, d'enregistrer et de prouver la propriété de valeurs numériques sans avoir à faire appel à une tierce personne [3]. Le fonctionnement d'une *blockchain* est plus aisément compréhensible avec l'exemple du *Bitcoin*.

Jusqu'à présent, une transaction bancaire impliquait deux personnes et une entité centralisée, une banque. Schématiquement, le donneur d'ordre intimait à sa banque de transférer un montant donné de son compte bancaire sur celui du bénéficiaire qui peut se trouver auprès de la même banque ou d'une banque tierce. La banque exécutait cet ordre, selon le contrat de *giro bancaire* [4]. Un ordre de débit est opéré sur le compte du donneur d'ordre et un ordre de crédit est opéré sur le compte bancaire du bénéficiaire. Il s'agit d'un simple jeu d'écritures entre le compte du donneur d'ordre et le compte du bénéficiaire, sans que l'argent «physique» ne transite réellement. Ainsi, dans cette configuration, la banque

PASCAL DE PREUX,
LL.M BOSTON UNIVERSITY,
AVOCAT, ASSOCIÉ,
RESOLUTION LEGAL
PARTNERS, LAUSANNE/VD

DANIEL TRAJILOVIC,
AVOCAT,
RESOLUTION LEGAL
PARTNERS, LAUSANNE/VD

agit comme un intermédiaire à travers lequel les deux parties ont confiance dans la réalisation de cette transaction.

Dans le cadre du *Bitcoin,* l'objectif est de permettre des paiements en ligne, envoyés directement d'une partie vers une autre sans passer par l'intermédiaire d'une institution financière [5]. Le *Bitcoin* est une monnaie dite cryptographique,

> *«La blockchain est une base de données décentralisée (registre distribué ou distributed ledger) qui compile toutes les transactions déjà réalisées et les valeurs ou données s'y trouvant au sein d'une ‹chaîne de blocs›.»*

dont le système repose sur le système *peer to peer,* soit un réseau où les parties communiquent directement entre elles, sans devoir passer par un gestionnaire de réseau centralisé [6]. C'est ici que la *blockchain* entre en jeu.

La *blockchain* contient une sorte de grand livre comptable complet et non-modifiable de l'ensemble des transactions *Bitcoin* qui ont déjà eu lieu. Le registre n'est pas maintenu au sein d'une autorité centrale unique, mais au sein des nœuds du réseau *(nodes),* soit des milliers d'ordinateurs qui résolvent des problèmes cryptographiques nécessaires à valider la transaction. Ce travail de résolution est effectué par des personnes ou des institutions appelées les «mineurs» *(miners).* Tous les nœuds du réseau *(nodes)* disposent d'une copie complète de la *blockchain.* La fonction des *miners* est de mettre à jour toutes les nouvelles transactions en *Bitcoin* qui sont effectuées sur le réseau *Blockchain* [7].

Dans le cadre du *Bitcoin,* il existe ainsi deux types d'acteurs: les utilisateurs du système *Bitcoin* et les *miners.* Chaque utilisateur dispose d'une paire de clés cryptographiques publique/privée [8]. On parle à cet égard de cryptographie asymétrique.

Pour effectuer une transaction, chaque utilisateur dispose d'un ou plusieurs porte-monnaie (wallet). Un porte-monnaie peut disposer d'une ou plusieurs adresses qui correspondent en quelque sorte au numéro de compte dans les opérations de paiement [9]. Il s'agit de la clé publique *(public key),* soit une clé de vérification de signature selon la Loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certifcats numériques du 18 mars 2016 (Loi sur la signature électronique, SCSE) [10]. La clé publique est liée à une clé privée *(private key)* permettant de signer une transaction et partant d'effectuer un paiement. Chaque utilisateur peut générer autant de comptes qu'il le souhaite sans recourir à des tiers. La signature numérique identifie l'utilisateur de manière certaine en tant que détenteur du compte correspondant, mais ni son nom ni ses autres caractéristiques personnelles n'apparaissent [11].

Lors d'une transaction, un utilisateur donne un ordre sur le réseau, qui doit être validé par plus de 50% des *miners.* Le processus de validation appelé minage *(mining)* vise à confirmer les transactions en attente en les incluant dans un bloc. La validation d'un bloc nécessite la résolution par un mineur d'une preuve de travail *(proof of work).* Cela consiste à coder l'ensemble des transactions d'un bloc et les transactions chiffrées de la chaîne de blocs précédente en utilisant d'importantes puissances de calcul (le minage). Ainsi, les *miners* vérifient que l'utilisateur possède effectivement le nombre de *Bitcoins* qu'il entend transférer et qu'il ne les a pas dépensés précédemment. Afin d'inciter les *miners* à mettre à disposition une puissance de calcul aussi importante que possible et à rendre le système plus sûr, ceux-ci sont récompensés par des *bitcoins* nouvellement créés et perçoivent des taxes sur les transactions [12]. Au début du *Bitcoin,* le travail de minage était effectué par des particuliers par le biais de leur propre ordinateur. Néanmoins, la taille des chaînes devenant de plus en plus grande et engendrant une puissance de calcul nécessaire de plus en plus importante, ce sont aujourd'hui des institutions qui effectuent ce travail de minage [13]. Fin décembre 2017, il existait 11 891 nœuds de traitement de la *blockchain Bitcoin* à travers le monde dont la majorité se trouve aux États-Unis, en Allemagne, en France et en Chine [14]. Des entreprises offrent désormais des services de *mining* à partir de leurs datacenters *(cloud mining)* [15].

Dès qu'un *miner* a validé la transaction, celle-ci est transmise à l'ensemble du réseau. Dès que la majorité des *miners* a validé la transaction (environ 10 minutes), le mécanisme donne naissance à une nouvelle chaîne de blocs reposant les uns sur les autres dans l'ordre chronologique de leur création (d'où le nom «chaîne de blocs»). Pour manipuler la *blockchain,* il faudrait disposer de plus de la moitié de la puissance de calcul participant à celle-ci. L'interposition des blocs permet ainsi de retracer et de vérifier toutes les transactions passées en remontant jusqu'au premier bloc [16].

Les données contenues dans une *blockchain* ne peuvent être modifiées sans qu'il soit nécessaire de déployer à nouveau toute la puissance de calcul fournie jusque-là par tous les ordinateurs participant au système. Il faudrait ainsi contrôler 51% des *miners* [17]. Ainsi validée, la chaîne de blocs devient la chaîne de blocs officielle pour l'ensemble du réseau de la *blockchain.*

2.2 L'utilisation innovante de la blockchain. La technologie de la *blockchain,* telle que décrite précédemment, se caractérise par sa publicité. La *blockchain* est totalement publique *(unpermissioned).* Tout individu a accès au registre en temps réel et peut entrer une nouvelle opération et augmenter la chaîne de blocs [18]. Néanmoins, il est tout à fait possible de rendre la *blockchain* «privée» *(permissioned),* restreignant la possibilité de consulter et de mettre à jour la *blockchain* à un nombre limité de participants connus à l'avance [19].

En d'autres termes, il est possible de restreindre le réseau à quelques membres identifiés par un contrôle de permission d'accès, comme les banques par exemple.

Pour simplifier, la technologie *blockchain* permet de stocker des données qui ne sont par la suite plus modifiables ni supprimables, du moins selon le rapport du Département fédéral des finances (DFF) [20].

Dans cette optique, la technologie *blockchain* peut être utilisée dans des domaines nombreux et variés, comme la création d'un registre foncier virtuel dans certains États africains [21], l'e-voting, le paiement des impôts [22] ou le traçage de produits alimentaires [23].

Récemment, de nombreuses institutions financières et des sociétés actives dans le domaine technologique ont créé une alliance, afin d'explorer les nombreuses possibilités de la *blockchain* afin de les intégrer dans le cadre des échanges financiers [24].

«La technologie Blockchain a développé également les smart contracts, qui ne sont pas à proprement parler des contrats, mais plutôt des protocoles d'instructions automatiques.»

À cet égard, nous verrons que la *blockchain* pourrait être utilisée dans le cadre de la lutte contre le blanchiment, en particulier dans la connaissance de l'arrière-plan économique, de l'ayant-droit économique ou du bénéficiaire final d'une opération financière.

Enfin, la technologie *Blockchain* a développé également les *smart contracts,* qui ne sont pas à proprement parler des contrats, mais plutôt des protocoles d'instructions automatiques qui exécutent les termes d'un contrat. Des algorithmes informatiques fixent quelles conditions conduisent à quelle décision. L'exécution des contrats et leur surveillance sont entièrement automatisées. Cela permettrait de réduire les risques de contrepartie ainsi que les risques opérationnels inhérents à chaque partie [25]. La technologie des *smart contracts* peut notamment être utilisée dans le cadre des assurances. Dans ce cadre, les assurés seraient automatiquement indemnisés dès la survenance du risque assuré (indemnisation de passagers en cas de vol en retard en fonction de la base de données de l'aéroport) [26].

3. BLANCHIMENT D'ARGENT, INFRACTIONS CONTRE LE PATRIMOINE ET BLOCKCHAIN ET L'EXEMPLE DU BITCOIN

3.1 Définitions

3.1.1 Introduction. L'infraction de blanchiment d'argent est entrée en vigueur le 1er août 1990.

Selon l'art. 305bis du *Code pénal (CP),*

«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.»

L'art. 305bis CP nécessite dès lors la réalisation des éléments constitutifs objectifs suivants: la provenance criminelle (1) des valeurs patrimoniales (2) et un acte d'entrave à l'identification de l'origine, la découverte ou la confiscation de ces valeurs patrimoniales (3). Par ailleurs, le blanchiment d'argent est une infraction intentionnelle, le dol éventuel suffit.

3.1.2 Valeurs patrimoniales. La notion de valeurs patrimoniales s'interprète de façon très large. Elle correspond à la notion définie à l'art. 70 CP. Elle englobe tous les avantages pécuniaires imaginables, tels que notamment les choses mobilières ou immobilières, l'argent quel que soit sa forme, les créances et tout autre droit [27].

Pour être qualifié de «valeur patrimoniale», l'objet sur lequel porte le blanchiment d'argent doit avoir une valeur. Le Tribunal fédéral a considéré qu'il n'y a pas de blanchiment d'argent lorsque les valeurs patrimoniales se trouvent être des faux billets de banque [28].

3.1.3 Infraction préalable. Les valeurs patrimoniales doivent provenir d'un crime au sens de l'art. 10 al. 2 CP. Il peut s'agir notamment d'un vol (art. 139 CP), d'une escroquerie (art. 146 CP), d'un abus de confiance (art. 138 CP) ou d'une gestion déloyale aggravée (art. 158 al. 2 CP) [29].

L'exigence d'un lien avec un crime en amont suppose que l'on établisse de quelle infraction principale les valeurs proviennent. Cette preuve est difficile à apporter, raison pour laquelle le Tribunal fédéral a assoupli les exigences quant à l'établissement de l'infraction en amont et renoncé à une preuve stricte de l'acte préalable [30].

Il ne peut y avoir blanchiment sans crime préalable [31].

Le Tribunal fédéral exige l'existence

«entre l'infraction et l'obtention de valeurs patrimoniales un lien de causalité tel que la seconde apparaisse comme la conséquence directe et immédiate de la première. Tel est le cas lorsque le produit original de l'infraction peut être identifié de façon certaine et documentée, à savoir aussi longtemps que «sa trace documentaire» («Papierspur», «paper trail») peut être reconstituée de manière à établir son lien avec l'infraction. Ainsi, lorsque le produit original formé de valeurs destinées à circuler (billets de banque, effets de change, chèques, etc.) a été transformé à une ou plusieurs reprises en de telles valeurs, il reste confiscable aussi longtemps que son mouvement peut être reconstitué de manière à établir son lien avec l'infraction [32].»

3.1.4 Acte d'entrave. Est punissable selon l'art. 305bis CP celui qui commet «un acte propre à entraver l'identification de l'origine, la découverte ou la confiscation de valeurs patrimoniales». Le blanchiment peut donc être réalisé par n'importe quel acte propre à entraver l'établissement du lien entre le crime préalable et la valeur patrimoniale qui en provient, ou à faire échapper la mainmise sur ces valeurs par les autorités. En d'autres termes, l'acte doit être propre à introduire la valeur patrimoniale dans l'économie légale [33].

Peuvent ainsi être considérés comme des actes d'entrave, le change d'argent (dans d'autres coupures de la même espèce ou dans une autre devise) [34], la dissimulation d'argent provenant d'un trafic de drogue chez soi [35] ou chez un tiers [36], l'enfouissement du butin [37], le transfert de la propriété, par exemple en exécutant une vente, une donation ou un échange [38], le paiement d'argent sur un compte ouvert au

nom d'un titulaire qui n'en est pas l'ayant droit économique [39], le virement des fonds à l'étranger [40], le retrait en espèces des avoirs déposés sur un compte bancaire (les avoirs ne peuvent plus être surveillés à l'aide de documents bancaires *(paper trail)* [41].

3.2 Le Bitcoin et le risque de blanchiment d'argent

3.2.1 Généralités. Selon le rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme rendu par le *Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF)* en juin 2015 [42] à propos des monnaies virtuelles, la menace potentielle principale des monnaies virtuelles réside dans le nombre croissant d'intermédiaires financiers en Suisse qui accepteront de changer, à plus grande échelle, des monnaies virtuelles contre des valeurs non virtuelles, que ce soit en argent scriptural ou liquide, pour le compte du client. En effet, grâce aux modalités des monnaies virtuelles, le dépositaire réel des monnaies virtuelles peut ne pas être identique au récipiendaire.

La seconde menace réside dans la transmission de fonds à l'étranger sans passer par l'utilisation d'un intermédiaire financier traditionnel. L'attrait principal des monnaies virtuelles est la possibilité de cacher l'identité du pourvoyeur de fonds et du destinataire des fonds. Les principales infractions préalables pointées par le rapport du GCBF sont le trafic de stupéfiants, les escroqueries commises sur Internet, y compris le financement des actes préparatoires liés au *phishing* et le financement du terrorisme. Les monnaies virtuelles permettent ainsi de faciliter les activités de blanchiment d'argent des organisations criminelles [43].

L'ensemble du dispositif mis en place par la Loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme du 10 octobre 1997 *(Loi sur le blanchiment d'argent, LBA)* (RS.955.0) est rendu obsolète dès lors qu'il n'existe plus d'intermédiaire financier permettant de vérifier l'identité du cocontractant, l'ayant droit économique, l'origine des fonds ainsi que le destinataire des fonds. De plus, si l'intermédiaire n'est pas soumis à la LBA, de par sa domiciliation à l'étranger ou d'une activité qui n'entre pas dans la définition de l'intermédiaire financier selon la LBA, il demeure très difficile de tracer les flux des monnaies virtuelles et notamment du *Bitcoin*.

Le rapport annuel de l'Office fédéral de la police fedpol 2015 confirme la difficulté à tracer le *Bitcoin,* dans la mesure où il garantit l'anonymat, rendant impossible l'identité du destinataire des *bitcoins*. L'utilisation des monnaies virtuelles augmente le risque de blanchiment d'argent car les cybercriminels peuvent facilement reconvertir leurs profits illicites en *Bitcoin,* dans des devises officielles, les intégrant dans l'économie réelle [44].

Cette facilitation de la conversion des *bitcoins* en devises officielles place cette monnaie virtuelle comme un des nombreux moyens utilisés par des organisations criminelles dans la commission de certaines infractions. Il s'agit du moyen préféré des plates-formes de vente de produits illégaux tels que des drogues, des armes, des biens falsifiés ou des données de cartes de crédit volées [45].

La conversion des fonds provenant de ces crimes en *Bitcoin* est une infraction assimilable au blanchiment d'argent [46]. En effet, à l'instar d'un retrait des avoirs bancaires d'un compte en banque, la conversion des *bitcoins* constitue une espèce de rupture du *paper trail* (le *Bitcoin* étant enregistré sur la *blockchain,* le retrait des *bitcoins* et leur conversion en monnaie officielle ne permet ainsi plus de tracer le flux de fonds).

> *«Les monnaies virtuelles permettent ainsi des activités de blanchiment d'argent des organisations criminelles.»*

Par ailleurs, les transactions subséquentes d'achat et de vente compliquent encore la traçabilité, ce qui renforce l'attrait pour les blanchisseurs. Selon le rapport annuel fedpol [47], les grandes affaires de blanchiment d'argent liées au *Bitcoin* sont encore rares en Europe, même si des enquêtes seraient actuellement en cours dans plusieurs pays européens.

Néanmoins, il est indispensable que l'infraction préalable du blanchiment d'argent soit un crime ou un délit fiscal qualifié. Il est dès lors nécessaire de définir le *Bitcoin* sous l'angle du droit pénal.

3.2.2 L'utilisation du Bitcoin en tant qu'infraction préalable au blanchiment d'argent. Comme indiqué précédemment, la valeur patrimoniale se caractérise comme tout avantage économique susceptible d'être estimé ou tout élément doté d'une valeur pécuniaire [48]. Il s'agit plus particulièrement de choses fongibles introduites dans la propriété de l'auteur par mélange, les créances ou autres droits ayant une valeur patrimoniale et également les créances comptables et les comptes en banque [49].

Par conséquent, les monnaies virtuelles doivent être considérées comme des valeurs patrimoniales. Dans cette optique, toutes les infractions contre le patrimoine sont susceptibles de s'appliquer, lorsque la notion de valeur patrimoniale est une des composantes de ces infractions [50].

En revanche, le «vol» de *Bitcoin* ne peut être réprimé par l'infraction de vol au sens de l'art. 139 CP, car il implique la notion de chose mobilière et non de valeurs patrimoniales [51], au même titre que le recel [52]. Ainsi, lorsque des auteurs échangent des *bitcoins* auprès d'un tiers qui savait ou devait présumer qu'ils proviennent d'une infraction patrimoniale, à l'instar de l'abus de confiance (art. 138 CP) ou de l'escroquerie (art. 146 CP), le tiers ne pourra être puni de l'infraction de recel, selon la définition du droit suisse.

Dans l'hypothèse où une victime aurait validé des *Bitcoins* pour une opération de change sur une plateforme commerciale, mais qui ne reçoit pas sa contrepartie en francs, l'infraction d'escroquerie pourrait entrer en ligne de compte, pour autant que la victime ait été induite en erreur de manière astucieuse par les auteurs [53]. Les auteurs qui se sont procuré les *bitcoins* par la commission d'une infraction d'escroquerie pourraient échanger les bitcoins dans une autre monnaie virtuelle, tel que l'Ether. Si le tiers détenteur d'Ether devait savoir ou présumer que les *bitcoins* proviennent

d'une escroquerie, il ne pourrait être reconnu coupable de recel. En revanche, la conversion des *bitcoins* en *Ether* pourrait constituer un acte d'entrave rendant difficile l'identification de l'origine des valeurs patrimoniales et partant, le tiers pourrait être condamné pour blanchiment d'argent, au sens de l'art. 305bis CP.

Outre que les monnaies virtuelles peuvent être considérées comme des valeurs patrimoniales, elles peuvent être qualifiées de données, soit des informations traitées, mémorisées et transmises au moyen d'un ordinateur, de sorte que les données ne bénéficient d'une protection qu'à partir de leur saisie par l'ordinateur, jusqu'au moment de leur impression [54]. Ainsi, les infractions telles que la soustraction de données (art. 143 CP) (par le piratage de *bitcoins* directement dans le portemonnaie d'un utilisateur ou par une attaque sur une plateforme d'échange de *bitcoins*) ou l'utilisation frauduleuse d'un ordinateur (art. 147 CP) peuvent être envisagées [55]. En Suisse, un tel procédé a déjà été constaté dans un cas où un particulier s'est vu subtiliser ses *bitcoins* pour une valeur de plus de CHF 100 000 [56]. Si, par la suite, les auteurs de cette infraction convertissent les *bitcoins* soustraits en monnaie officielle, l'infraction de blanchiment d'argent pourra également être retenue, dans la mesure où tant la soustraction de données (art. 143 CP) que l'utilisation frauduleuse d'un ordinateur (art. 147 CP) sont des crimes, et donc, constituent une infraction préalable au blanchiment d'argent.

«L'utilisation de la technologie des smarts contracts dans la technologie de la blockchain peut rendre compliquée leur appréhension sous l'angle du droit pénal suisse.»

À titre d'exemple, en août 2016, des pirates informatiques ont réussi à pénétrer dans le système de la société Bitfinex, une plateforme d'échange et de stockage de *bitcoins,* de prendre le contrôle de la moitié de la clé cryptographique des utilisateurs ce qui leur a permis de détenir la signature nécessaire à l'exécution d'une transaction. Une fois l'ordre donné, la majorité des *miners* de la *blockchain* a validé la transaction, à raison (en détenant la moitié de la clé cryptographique et ayant une emprise sur le *wallet* des utilisateurs, l'opération paraît légitime). Les pirates informatiques ont réussi à s'emparer de *bitcoins* pour une valeur d'USD 65 millions, soit l'un des plus grands «vols» de *bitcoins* dans l'histoire [57]. Les pirates informatiques n'ont toujours pas été retrouvés.

Une autre possibilité de manipulation est intervenue dans le courant de l'été 2014. Un consortium de minage «Ghash.io» est parvenu à détenir 51% de la puissance de calcul de la *blockchain Bitcoin* ce qui leur donnait la faculté d'effectuer une transaction fictive sur la *blockchain,* de la faire valider à l'aide de ses propres «*miners*» détenant la majorité de la puissance de calcul, et de l'inscrire sur la chaîne de blocs [58]. Sous l'angle du droit suisse, une telle prise de contrôle de la majorité de la puissance de calcul d'une *blockchain* dans le but de procéder à des ordres de transfert de monnaies virtuelles, ce alors qu'il n'existe aucun arrière-plan économique justifiant un tel transfert, pourrait être appréhendée sous l'angle de la soustraction de données (art. 143 CP) ou de l'utilisation frauduleuse d'un ordinateur (art. 147 CP).

En revanche, l'utilisation de la technologie des *smarts contracts* dans la technologie de la *blockchain* complique leur appréhension sous l'angle du droit pénal suisse. Comme nous l'avons vu précédemment, les *smarts contracts* exécutent automatiquement un contrat en fonction d'un code informatique. Le code ainsi développé devient la loi. Sur la base des smart contracts un fonds d'investissement appelé *Decentralized Autonomous Organization (The DAO)* s'appuyant sur la plateforme Etherneum, basée en Suisse [59] a été créé. Le fonds d'investissement est financé au moyen d'Ether et chaque décision est prise à la majorité par ceux qui financent le *DAO.* Il est possible de se retirer du système et d'empocher des gains. Le *DAO* est articulé autour des *smart contracts*. Néanmoins, un utilisateur est parvenu à exploiter une faille dans le code et à se faire créditer plusieurs fois sa mise, par le biais des *smart contracts,* soit des Ether pour un montant équivalent à USD 50 millions. Une erreur de programmation serait à l'origine de la fuite de capitaux. Il n'y aurait dès lors pas eu de «vol» de données. Dans ce cadre, l'auteur de cette «attaque» prétend que celle-ci n'est pas illégale, dans la mesure où le code du *DAO* fixe les règles auxquelles il permet l'exécution du contrat. Le code du *smart contracts* aurait uniquement été utilisé et on ne pourrait parler d'un hacking [60].

Sous l'angle du droit suisse, il est évident qu'il existe une difficulté sous l'angle de la soustraction de données (art. 143 CP). En effet, l'art. 143 CP vise à protéger les données que le propriétaire ne veut pas laisser accessibles à l'auteur [61]. L'auteur ne doit en particulier pas être légitimé à disposer des données [62]. L'accès doit être interdit aux personnes non autorisées au moyen de mesures techniques [63]. Les obstacles doivent être matériels et non moraux, légaux ou contractuels. Les instructions, les interdictions orales ou écrites, ou encore les mesures d'organisation visant à séparer les fonctions au sein du personnel ne constituent pas des mesures de sécurité suffisantes au sens de l'art. 143 CP [64].

Si l'auteur est habilité à disposer des données, mais qu'il outrepasse les limites de son droit d'utilisation (posées par la loi, le contrat ou la morale), l'art. 143 CP ne s'applique pas [65].

Dans le cas d'espèce, il apparaît que l'auteur était habilité à disposer des données des *smart contracts,* en tant que membre de la communauté *DAO.* Il aurait simplement utilisé le code du *smart contracts* à son propre profit. Seul pourrait lui être reproché d'avoir outrepassé les limites du code du *smart contracts* et de l'avoir utilisé contrairement à son but.

Par conséquent, l'infraction de soustraction de données (art. 143 CP) n'apparaît pas applicable. Se pose néanmoins la question de la réalisation de l'infraction d'utilisation frauduleuse d'un ordinateur (art. 147 CP), sous l'angle de l'utilisation de données de manière incorrecte, incomplète ou indue ou en utilisant un procédé analogue [66].

En tout état de cause, si aucune infraction ne peut être reprochée à cet auteur, l'infraction de blanchiment d'argent ne pourra s'appliquer, faute d'infraction préalable.

Par conséquent, l'utilisation de la *blockchain* pourrait poser certains problèmes, en termes de punissabilité, malgré le fait que le code pénal suisse dispose déjà de dispositions pénales permettant d'appréhender l'utilisation du *Bitcoin* et de la *blockchain,* de même que le blanchiment d'argent subséquent.

En revanche, la difficulté réside dans la preuve de l'infraction préalable et de l'arrière-plan économique des transactions effectuées sur la *blockchain Bitcoin.* En effet, les utilisateurs sont, par nature, anonymes et il est dès lors difficile de connaître leur identité. En outre, les possibilités offertes aux auteurs d'infractions d'empêcher le traçage des monnaies virtuelles rendent la preuve de la réalisation d'une infraction préalable difficile.

Toutefois, dès le moment où des auteurs d'infractions patrimoniales tentent de déposer des avoirs, préalablement convertis en utilisant des *bitcoins,* auprès d'un établissement financier, la LBA s'applique pleinement. Dans ces circonstances, si une banque soupçonne que l'origine des fonds est délictueuse, elle doit procéder à des clarifications conformément à l'art. 6 LBA et éventuellement à une communication au *Bureau de communication en matière de blanchiment d'argent (MROS),* au sens de l'art. 9 LBA. Un précédent a d'ailleurs déjà été signalé par le MROS dans lequel un intermédiaire financier a été alerté via SWIFT par une banque étrangère qu'une bonification de EUR 5000 sur un compte-client serait d'origine délictueuse, soit que le paiement aurait été déclenché par piratage informatique ou par hameçonnage. Dans ce cas, les auteurs avaient préalablement procédé à une vente privée de *bitcoins* par l'intermédiaire d'une bourse en *bitcoins* [67].

S'agissant des plateformes de conversion de *bitcoins* en monnaie officielle, ces dernières sont pleinement soumises à la LBA.

3.3 La soumission des plateformes d'échanges de Bitcoin à la LBA

3.3.1 Introduction. La LBA impose un certain nombre d'obligations aux intermédiaires financiers, soit la vérification de l'identité du cocontractant (art. 3 LBA), l'identification de l'ayant droit économique (art. 4 LBA), l'obligation de clarification (art. 6 LBA) et de documentation (art. 7 LBA). Par ailleurs, la LBA impose une obligation de communication si des soupçons fondés laissent à penser que les avoirs proviennent d'un crime, notamment (art. 9 LBA).

3.3.2 Les plateformes d'échanges de Bitcoin. Le simple paiement de biens ou de services avec des *bitcoins* de même que la fourniture de ces prestations contre paiement en *bitcoins* ne constituent pas une intermédiation financière au sens de la LBA et ne sont donc pas soumis à cette loi [68].

En revanche, une activité de change exercée à titre professionnel est considérée comme une activité de négoce soumise à la LBA (art. 5 al. 1 OIF). L'achat et la vente de *bitcoins* contre des monnaies officielles à titre professionnel constituent une telle activité de change [69].

Les plateformes d'achat et de vente de *bitcoin* en échange d'une monnaie officielle sont soumises à la LBA. De telles plateformes doivent dès lors respecter les obligations en matière de lutte contre le blanchiment d'argent.

Sans approfondir l'assujettissement des plateformes de négoces de *bitcoins* à la loi sur les Banques (LB), la LBA s'applique également dans certaines circonstances à certaines de ces plateformes. C'est notamment le cas lorsque l'exploitant ne se contente pas de réunir des parties prenantes à l'achat et à la vente de *bitcoins* ou à faire correspondre des offres d'achat et de vente, auxquels cas la LBA n'est pas applicable, mais est aussi impliqué dans le processus de paiement. En effet, la LBA s'applique aux intermédiaires financiers qui fournissent un service dans le domaine du trafic des paiements [70].

Selon ces considérations, lorsqu'un négociant professionnel en *bitcoins* exerce uniquement une activité qualifiable de change, il n'est tenu de vérifier l'identité du cocontractant que si une ou plusieurs transactions liées entre elles atteignent ou excèdent la somme de CHF 5000 (art. 45 al. 1 let. a OBA-Finma) ou si l'on est en présence d'indices de blanchiment d'argent ou de financement de terrorisme (art. 45 al. 4 let. b OBA-Finma). Dans le cas contraire, il n'est pas nécessaire d'identifier l'ayant droit économique (art. 51 OBA-Finma) [71].

Malgré ces obligations, le Conseil fédéral constate que la mise en œuvre des divers devoirs de diligence se heurte à des difficultés en raison des particularités techniques et l'anonymat inhérent à Internet. Il peut dès lors s'avérer impossible pour les autorités de poursuite pénale de garantir que l'identité du destinataire sera établie *a posteriori.* Il existe des risques de blanchiment d'argent et de financement du terrorisme que les devoirs de diligence prévus par la loi ne sauraient à eux seuls permettre de contrôler [72].

Récemment, la Finma a retiré du marché et a procédé à la liquidation des fournisseurs et créateurs de la pseudo-cryptomonnaie «E-Coins», ce alors qu'ils ne disposaient pas d'autorisation bancaire [73]. Contrairement aux cryptomonnaies sauvegardées de manière décentralisée et reposant sur la technologie de la *blockchain,* les E-Coins étaient contrôlés exclusivement par les fournisseurs et sauvegardés sur leur serveur local. Les fournisseurs promettaient que ladite monnaie était couverte à hauteur de 80% par des valeurs matérielles, ce qui n'était pas le cas. En outre, des E-Coins ont été émis sans contre-valeur suffisante, conduisant à une dilution continuelle du système des E-Coins, au détriment des investisseurs.

4. LA BLOCKCHAIN AU SERVICE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT

Au-delà de l'application de la *blockchain* au *Bitcoin* ou d'autres monnaies virtuelles, telle que l'Ether, la *blockchain* pourrait être utilisée par les services compliance pour lutter contre le blanchiment d'argent et veiller au respect de leurs obligations LBA.

Cela peut paraître paradoxal que la technologie *blockchain* puisse être utilisée pour lutter contre le blanchiment d'argent, ce alors qu'en combinaison avec les monnaies virtuelles, elle présente un attrait tout particulier pour les blanchisseurs en raison de l'anonymat des utilisateurs, de la difficulté à

connaître l'arrière-plan économique et à tracer le flux des échanges.

Pour appréhender le rôle innovateur que pourrait avoir la *blockchain* dans la lutte contre le blanchiment d'argent, il est nécessaire de la séparer de la monnaie virtuelle et de revenir à sa définition. En effet, la *blockchain* est avant toute chose un registre décentralisé (registre distribué ou *distributed ledger*) compilant toutes les transactions déjà réalisées et les valeurs ou données s'y trouvant au sein d'une «chaîne de blocs» [74]. La *blockchain* permet de stocker des données qui ne sont par la suite plus modifiables.

De plus, il est nécessaire de développer une *blockchain* privée, soit de restreindre la possibilité de consulter et mettre à jour la *blockchain* à un nombre limité de participants connus à l'avance [75].

Ainsi, les banques et les intermédiaires financiers pourraient développer un réseau *blockchain* où les seuls nœuds du réseau sont contrôlés par les banques elles-mêmes.

Sur ce réseau, il serait dès lors possible de vérifier, valider et enregistrer l'ensemble des transactions effectuées par l'ensemble de leur clientèle. Il serait possible de partager avec l'ensemble des banques membres du réseau le dossier client, notamment la documentation KYC, le dossier LBA et les flux de fonds [76]. La documentation KYC serait incorporée au sein du réseau *blockchain* privée et partagée simultanément à l'ensemble des banques et intermédiaires financiers présents sur le réseau. Dans ces circonstances, une banque pourrait s'appuyer sur les recherches déjà effectuées par une autre banque sur un même client pour son propre dossier. Chaque banque serait informée en temps réel de soupçons de blanchiment d'argent ou de soupçons d'une provenance délictueuse des avoirs. Cela leur éviterait de réaliser leur propre analyse de conformité.

Il serait également possible d'inclure dans le réseau *blockchain* l'autorité de régulation, elle-même, qui aura un accès en temps réel à toutes les activités suspicieuses [77].

Ce procédé permettrait de réduire les risques de blanchiment d'argent. En effet, l'utilisation de plusieurs sociétés-écrans par les blanchisseurs sera rendue inefficace, dans la mesure où l'ensemble de leurs données seraient partagées par les banques et le procédé frauduleux serait rapidement détecté dans la *blockchain* [78].

Néanmoins, l'utilisation de la *blockchain* se heurte à d'innombrables difficultés.

Premièrement, le partage des données des clients à d'autres banques nécessite l'accord du client lui-même, ce d'autant plus si des intermédiaires financiers sans lien avec le client ont accès à ses données.

Deuxièmement, l'art. 17 al. 2 LPD dispose que des données sensibles ou des profils de la personnalité ne peuvent être traités par des organes fédéraux que si une loi au sens formel le prévoit expressément. Compte tenu du fait que la *blockchain* contiendrait une compilation de l'ensemble des données récoltées sur un client, il serait envisageable de considérer qu'une telle *blockchain* reviendrait à constituer un profil de la personnalité du client, ce qui nécessiterait une base légale au sens formel pour que la Finma ou le MROS soient incorporés dans la blockchain [80].

Troisièmement, il est nécessaire de déterminer si la *blockchain* est utilisée uniquement au niveau national ou au niveau mondial. Dans ces circonstances, il faut tenir compte des particularités législatives de chaque État et les intégrer dans la *blockchain*. En particulier, il y aurait lieu d'éviter que des États étrangers puissent obtenir des informations sur un client, sans passer par l'entraide internationale en matière pénale dans le cadre d'une instruction pénale.

«Il est nécessaire de déterminer si la blockchain est utilisée uniquement au niveau national ou au niveau mondial. Dans ces circonstances, il faut tenir compte des particularités législatives de chaque État et les intégrer dans la blockchain.»

Quatrièmement, une telle *blockchain* se heurterait également à la protection du secret bancaire par l'art. 47 LB. Elle nécessiterait dès lors une levée du secret bancaire par le client lui-même. La mise en place d'une *blockchain* au niveau suisse conduirait, à terme, à la fin du secret bancaire en Suisse.

En définitive, malgré l'enthousiasme suscité par la *blockchain* [79], son utilisation dans le cadre de la compliance pose d'importants problèmes d'application. Néanmoins, son hypothétique utilisation pourrait considérablement réduire les actes de blanchiment d'argent.

5. CONCLUSION

La technologie *Blockchain* en est encore à ses balbutiements. Elle provoque un engouement certain auprès des différents acteurs du marché, que sont les assurances, les banques ou les administrations. Toutefois, il ne faut pas perdre de vue son utilisation abusive en lien avec les monnaies virtuelles. Que ce soit le trafic de drogues, le hameçonnage, le piratage informatique, la soustraction de données ou les escroqueries opérées sur Internet, l'utilisation des monnaies virtuelles est très prisée des réseaux criminels. Elle permet de garantir l'anonymat des auteurs et des destinataires des transferts ce qui rend le traçage de cette monnaie complexe.

Si les normes légales permettant de sanctionner les comportements développés par les réseaux criminels sur Internet existent et qu'ils constituent une infraction préalable au blanchiment d'argent, la difficulté principale à laquelle se heurtent les autorités de poursuite pénale est la preuve d'une infraction préalable, la démonstration de l'arrière-plan économique et l'identité des auteurs de ces infractions.

Certes, les plateformes de négoce qui opèrent l'échange de monnaies virtuelles ou la conversion des monnaies virtuelles en monnaie officielle sont soumises à la LBA. Elles doivent dès lors vérifier l'identité du cocontractant et de l'ayant droit économique et obéir aux obligations de clarification prévues par la LBA. Néanmoins, les particularités inhérentes aux monnaies virtuelles, en particulier l'anonymat sur Internet,

rendent les mesures anti-blanchement inopérantes dans certains cas.

En revanche, l'utilisation de la *blockchain* dans le cadre de la lutte contre le blanchiment pourrait être prometteuse. Il

«L'utilisation de la blockchain dans le cadre de la lutte contre le blanchiment pourrait être prometteuse.»

est indéniable que le partage de l'information entre l'ensemble des banques et des intermédiaires financiers réduirait drastiquement le risque de blanchiment d'argent. Toutefois, la technologique *blockchain* se heurte à des difficultés insurmontables à l'heure actuelle, soit le consentement du client à une telle transmission d'information, une base légale permettant une telle récolte de données par les autorités, la législation suisse et étrangère et le secret bancaire.

En définitive, si la *blockchain* peut se targuer d'être une des inventions majeures après Internet, sa réglementation pose encore et toujours le même problème, le principe de territorialité. La *blockchain* a été créée en tenant compte d'un monde globalisé et ultra connecté. En revanche, les lois nationales ont été créées selon le principe de la territorialité et leur application s'arrête là où commence celle de la loi étrangère. Tant que ce problème n'aura pas été résolu, la technologie de la *blockchain* demeurera imparfaite. ■

Notes: 1) New York Journal, White-Collar Crime, The promise of Blockchain Technology To Combat Money Laundering, Volume 257 – no. 62. **2)** Rapport explicatif du Département fédéral des finances (DFF) au projet mis en consultation de modification de la loi sur les banques et de l'ordonnance sur les banques (FinTech) du 1er février 2017, p. 9 (ci-après «Rapport explicatif du DFF sur les FinTech»; Luca Bianchi/Edi Bollinger, A (Legal) Perspective on Blockchain, in CapLaw – Swiss Capital Markets Law, p. 2. **3)** Rapport explicatif du DFF sur les FinTech, p. 9. **4)** Pour plus de détails, Guggenheim/Guggenhaim, les contrats de la pratique bancaire, 5ème édition, p. 565 et suivants. **5)** New York Journal, White-Collar Crime, The promise of Blockchain Technology To Combat Money Laundering, Volume 257 – no. 62. **6)** Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070) du 25 juin 2014, p. 8. **7)** New York Journal, White-Collar Crime, The promise of Blockchain Technology To Combat Money Laundering, Volume 257 – no. 62. **8)** Rapport semestriel 2013/II (juillet–décembre) de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI (ci-après «Rapport MELANI»), p. 26. **9)** Rapport sur les monnaies virtuelles, p. 8. **10)** Rapport explicatif du DFF sur les FinTech, p. 10. **11)** Rapport MELANI, p. 26; Rapport explicatif du DFF sur les FinTech, p. 10. **12)** Rapport explicatif du DFF sur les FinTech, p. 10. **13)** Yves Caseau/Serge Soudoplatoff, La Blockchain, ou la confiance distribuée, in Fondation pour l'innovation politique, juin 2016, p. 17. **14)** Il est possible de connaître en temps réel le nombre de nœuds de traitement de la blockchain Bitcoin: https://bitnodes.21.co/. **15)** Yves Caseau/Serge Soudoplatoff, op.cit., p. 17. **16)** Rapport MELANI, p. 26, Rapport explicatif du DFF sur les FinTech, p. 10; Rapport sur les monnaies virtuelles, p. 8; Luca Bianchi/Edi Bollinger, op.cit., p. 2). **17)** Rapport explicatif du DFF sur les FinTech, p. 10; Luca Bianchi/Edi Bollinger, op.cit., p. 2. **18)** Luca Bianchi/Edi Bollinger, op.cit., p. 2; Rapport explicatif du DFF sur les FinTech, p. 10. **19)** Luca Bianchi/Edi Bollinger, op.cit., p. 2; Rapport explicatif du DFF sur les FinTech, p. 10. **20)** Rapport explicatif du DFF sur les FinTech, p. 11. **21)** Article du Temps du 4 septembre 2017 de Monsieur Arturo Bris, Professeur de Finance à l'IMD, «Blockchain: tenez-vous prêts!» https://www.letemps.ch/economie/2017/09/04/blockchain-tenez vous-prets. **22)** Article du Bilan du 28 janvier 2017, «Blockchain: voter et payer ses impôts sur smartphone» http://www.bilan.ch/bilan/blockchain-voter-payer-impots-smartphone. **23)** Article du Bilan du 6 juin 2017, le «Blockchain», une arme au service de la sécurité alimentaire, http://www.bilan.ch/economie/blockchain-une-arme-service-de-securite-alimentaire. **24)** Article du Bilan du 1er mars 2017, «Credit Suisse et UBS rejoignent une alliance dans la Blockchain»,http://www.bilan.ch/argent-finances-plus-de-redaction/credit-suisse-ubs-rejoignent-une-alliance-blockchain. **25)** Rapport du DFF sur les FinTech, p. 11. **26)** https://blockchain-france.net/2016/01/28/applications-smart-contracts/. **27)** FF 1989 1961, 981; ATF 124 IV 274 consid. 3, JdT 1999 IV 81; ATF 119 IV 59 consid. 2a, JdT 1995 IV 43; PC CP, N 12 ad art. 305bis CP; BsK Strafrecht II-Pieth, N 5 ad art. 305bis CP; Cassani, Commentaire du droit pénal suisse, vol. 9: art. 303–311, Basel 1996, N 7 ad art. 305bis CP; Trechsel/Affolter-Eijsten, Das schweizerische Strafgesetzbuch: Praxiskommentar, Zurich/St-Gall 2008, N 9 ad art. 305bis CP; Corboz, Infractions en droit suisse, vol. II, 3ème éd. Berne, N 9 ad art. 305bis CP. **28)** TF 6S.426/2006 du 28 décembre 2006, consid. 2.2, in SJ 2007 I 271, 272. **29)** Cassani, op.cit., N 8ss ad art. 305bis CP. **30)** ATF 138 IV 1, p. 7; ATF 120 IV 323; TF 6B_141/2007 du 24 septembre 2007 consid. 3.3.3. **31)** Lombardini, Banques et blanchiment d'argent, 2ème édition, Schulthess 2013, Genève, Zurich, Bâle, N 266, p. 68. **32)** ATF 129 II 453, 461. **33)** PC CP, N 25 ad art. 305bis CP. **34)** ATF 122 IV 211, 215. **35)** ATF 119 IV 59. **36)** ATF 122 IV 211. **37)** ATF 119 IV 59. **38)** Cassani, op.cit., N 36 ad art. 305bis CP. **39)** ATF 119 IV 242. **40)** ATF 129 IV 271. **41)** Cassani, op.cit., N 39 ad art. 305bis CP. **42)** Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse rendu par le Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme de juin 2015 (ci-après «Rapport du GCBF»), p. 100ss. **43)** Rapport du GCBF p. 101. **44)** Rapport annuel de l'Office fédéral de la police fedpol 2015, p. 33. **45)** Rapport annuel de l'Office fédéral de la police fedpol 2014, p. 29; Rapport semestriel 2013 II MELANI, p. 28. **46)** Rapport annuel de l'Office fédéral de la police fedpol 2014, p. 29. **47)** Rapport annuel de l'Office fédéral de la police fedpol 2014, p. 29. **48)** Daniel Stoll, le Bitcoin et les aspects pénaux des monnaies virtuelles, in forumpoenale 2/2015, p. 99, p. 106 et les références citées. **49)** Daniel Stoll, op.cit., p. 106 et les références citées. **50)** Daniel Stoll, op.cit., p. 106. **51)** PC CP, N 7 ad art. 139 CP. **52)** PC CP, N 11 ad art. 160 CP. **53)** Rapport annuel 2014 de l'Office fédéral de la police fedpol, 29. **54)** Daniel Stoll, op.cit., p. 106. **55)** Daniel Stoll, op.cit., p. 106. **56)** Rapport annuel 2014 de l'Office fédéral de la police fedpol, p. 29. **57)** Article de Bloomberg du 17 mai 2017: https://www.bloomberg.com/news/articles/2017-05-17/inside-bitfinex-s-comeback-from-a-69-million-bitcoin-heist. **58)** Article du Guardian du 16 juin 2014 https://www.theguardian.com/technology/2014/jun/16/Bitcoin-currency-destroyed-51-attack-ghash-io. **59)** https://www.ethereum.org/. **60)** Article de Bloomberg du 17 juin 2016: https://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb; Article du Bilan du 14 juillet 2016 de Me Michel Jaccard, avocat, Smart contracts, dumb code ou quand le blockchain déraille: http://www.bilan.ch/michel-jaccard/droit-et-technologies/smart-contracts-dumb-code-block chain-deraille. **61)** SK.2014.46 du 27 novembre 2015, consid. 2.1. **62)** SK.2014.46 du 27 novembre 2015, consid. 2.1; TC VS RVJ 2006, 222; Philippe Weissenberger in Basler Kommentar, Strafrecht II, 3e éd., Bâle 2013, n° 18 ad art. 143 CP. **63)** SK.2014.46 du 27 novembre 2015, consid. 2.1; Jérémie Müller, La cybercriminalité économique au sens étroit – Analyse approfondie du droit suisse et aperçu de quelques droits étrangers, RJL – Recherches juridiques lausannoises Band/n° 52, 2012 **64)** Niklaus Schmid, Computer- sowie Check- und Kreditkarten-Kriminalität, Schulthess, Zurich 1994, § 4 p. 39; Sylvain Métille, Joanna Aeschlimann, Infrastructures et données informatiques: quelle protection au regard du code pénal suisse?, RPS 132/2014 238, p. 291. **65)** SK.214.46 du 27 novembre 2015, consid. 2.1. **66)** PC CP, N 8 ss ad art. 147 CP. **67)** Rapport annuel 2013 du bureau de communication en matière de blanchiment d'argent MROS, p. 47. **68)** Rapport sur les monnaies virtuelles, p. 15. **69)** Rapport sur les monnaies virtuelles, p. 15. **70)** Rapport sur les monnaies virtuelles, p. 16. **71)** Rapport sur les monnaies virtuelles, p. 17. Il existe toutefois des exceptions au seuil de CHF 5000, notamment en présence de Money Transmitting, ce qui peut être le cas dans le cadre du Bitcoin. **72)** Rapport sur les monnaies virtuelles, p. 18. **73)** https://www.finma.ch/fr/news/2017/09/20170919-mm-coin-an bieter/. **74)** Rapport explicatif du (DFF) sur les FinTech, p. 9; Luca Bianchi/Edi Bollinger, op.cit., p. 2. **75)** Luca Bianchi/Edi Bollinger, op.cit., p. 2; Rapport explicatif du DFF sur les FinTech, p. 10. **76)** New York Journal, White-Collar Crime, The promise of Blockchain Technology To Combat Money Laundering, Volume 257 – n° 62. **77)** New York Journal, White-Collar Crime, The promise of Blockchain Technology To Combat Money Laundering, Volume 257 – n° 62. **78)** Ibidem. **79)** https://www.letemps.ch/economie/2017/05/28/plusieurs-solutions-blockchain-visent-suisse. **80)** L'art. 17 al. 2 LPD prévoit certaines exceptions à ce principe dont le consentement de la personne concernée. Néanmoins, ces exigences apparaissent difficilement applicables en l'espèce.