Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Janvier 2024

Évaluation nationale des risques – *National Risk Assessment* (NRA)

Risque de blanchiment d'argent et de financement du terrorisme lié aux crypto-actifs

Table des matières

1. Glossaire

AV	Actif virtuel
BA	Blanchiment d'argent
CEX (*centralized exchange*)	Échange centralisé
CRF	Cellule de renseignement financier
DAO (*decentralized autonomous organization*)	Organisation autonome décentralisée
DEX (*decentralized exchange*)	Échange décentralisé
FiCe	Finance centralisée
FiDé	Finance décentralisée
FT	Financement du terrorisme
GAFI	Groupe d'action financière
GCBF	Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme
KYC (*Know Your Customer*, litt. "connais ton client")	Procédure appliquée par les intermédiaires financiers afin de vérifier l'identité des clients, d'évaluer et de surveiller le risque client, et de prévenir les activités illégales comme le BA.
Métavers	Monde virtuel combinant des éléments physiques et numériques qui permet aux utilisateurs d'interagir dans un environnement immersif.
Monnaie fiat	Moyen de paiement légal émis par les banques centrales qui, contrairement à la monnaie-marchandise, n'est plus adossé à des marchandises physiques ou à des matières premières.
NFT (*non-fungible token*)	Jeton non fongible
Portefeuille hébergé	Portefeuille d'un client auprès d'un intermédiaire financier exerçant une activité de PSAV, qui peut y accéder.

Portefeuille multisignature	Portefeuille numérique qui requiert plusieurs clés privées (autrement dit plusieurs personnes doivent donner leur accord) pour effectuer une transaction, ce qui accroît la sécurité.
Portefeuille non hébergé	Portefeuille privé non accessible par des tiers
PPE	Personne politiquement exposée
Privacy coin	Cryptomonnaie qui vise à mieux protéger la vie privée et l'anonymat des utilisateurs lors des transactions (par ex. Monero ou Zcash).
PSAV	Prestataire de services d'actifs virtuels
P2P (*peer-to-peer* ou pair-à-pair)	Terme qui désigne un modèle d'échange en réseau où les appareils participants sont directement connectés entre eux sans transiter par un serveur central, ce qui donne lieu à une interaction décentralisée et égalitaire entre les appareils.
Rug pull (litt. "retirer le tapis de sous les pieds")	Expression utilisée lorsqu'une équipe de développeurs abandonne soudainement un projet (par ex. une plate-forme de FiDé) et vend ou retire toutes ses liquidités.
Smart contract (litt. "contrat intelligent")	Contrat numérique automatisé régissant les conditions et l'exécution des transactions entre les parties sans intermédiaire ni intervention humaine.
Smurfing	Pratique visant à fractionner une transaction unique d'une valeur élevée en plusieurs montants partiels, afin de dissimuler la contre-valeur réelle de la transaction et de contourner ainsi les mesures de lutte contre le BA et le FT qui s'appliquent en fonction des montants maximaux autorisés.
Stablecoin	AV offrant une valeur de conversion stable du fait qu'il est adossé à une matière première (par ex. 1 g d'or = 1 unité de *stablecoin*) ou à une monnaie (par ex. 1 CHF = 1 unité de *stablecoin*).
Technologie de la blockchain	Variante parmi les différentes technologies des registres distribués (TRD) possibles

Travel rule	Règle de transparence reposant sur la recommandation n°16 du GAFI, qui impose aux intermédiaires financiers, exerçant ou non une activité de PSAV, d'échanger les données personnelles de leurs clients lors des transactions transfrontalières.
TRD	Technologie des registres distribués qui permet d'enregistrer et de gérer des données de manière décentralisée sur un réseau d'ordinateurs, rendant les transactions transparentes, sûres et infalsifiables.
Web3	Développement de l'Internet, dans lequel des applications et des systèmes décentralisés reposent sur la technologie de la blockchain.

2. Résumé

Alors qu'elles étaient une activité de niche, les cryptomonnaies (actifs virtuels [AV]) sont devenues au cours de la dernière décennie un phénomène de masse avec des répercussions sur le système financier traditionnel. L'utilisation d'AV s'est répandue tant auprès des particuliers que des entreprises. En Suisse, de plus en plus d'intermédiaires financiers proposent des services dans ce domaine – il s'agit des prestataires de services d'actifs virtuels (PSAV). Cependant, les criminels aussi ont reconnu le potentiel de ce système de paiement et recourent désormais aux AV aux fins illégales les plus diverses, allant des "simples" vols ou escroqueries aux formes les plus graves de criminalité transnationale, y compris le blanchiment d'argent (BA) et le financement du terrorisme (FT). Ces évolutions posent des défis majeurs à toutes les parties prenantes engagées dans le dispositif de lutte contre le BA.

En 2018, le Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF) a publié une première analyse des risques liés à l'usage abusif de cryptomonnaies aux fins de BA ou de FT et a qualifié de "considérables" la menace qu'elles constituent et les vulnérabilités de la Suisse à cet égard. Or, le Bureau de communication en matière de blanchiment d'argent (MROS) n'avait reçu à ce stade qu'une poignée de communications de soupçons concernant des AV.

Depuis 2018, l'influence et l'importance des AV ont fondamentalement changé. La sensibilisation et la prise de conscience se sont nettement accrues sur le marché. À l'heure actuelle, le MROS reçoit tous les jours des communications de soupçons liées aux AV – ces derniers faisant désormais partie du quotidien des autorités de poursuite pénale. Il a pu constater quatre évolutions principales :

1. En Suisse, le nombre d'intermédiaires financiers exerçant une activité de PSAV a nettement augmenté, passant de moins de 10 en 2018 à 204 à la fin 2022. Au moins 180 d'entre eux n'ont pas transmis de communication de soupçons au MROS.

2. Entre 2018 et 2023, l'utilisation d'AV s'est multipliée en Suisse ; toujours plus de particuliers et d'entreprises recourent aux AV et les acceptent pour des paiements dans le commerce, pour des services et pour des investissements. La frontière entre le secteur financier traditionnel et le secteur des AV se brouille de plus en plus. Les AV étant de plus en plus intégrés sur les plates-formes de paiement traditionnelles, les "deux mondes" sont en train de fusionner.

3. L'usage criminel d'AV a augmenté tant en Suisse que dans le monde et s'est en outre nettement diversifié. Les autorités de poursuite pénale sont davantage confrontées à des procédures portant sur divers secteurs économiques, où il existe des liens avec des AV. Ainsi sont déposées un nombre croissant de dénonciations pour vol ou d'autres détournements d'AV (par ex. escroquerie, gestion déloyale). Le montant des préjudices en lien avec des AV s'est fortement accru et s'élève en Suisse, pour l'année 2022, à des dizaines de millions de francs au moins (à titre de comparaison, il atteignait à peine 7 millions de francs en 2007). L'utilisation d'AV est devenue la norme dans certaines infractions (notamment la fraude à l'investissement et les rançongiciels). Les AV sont désormais un outil courant de la criminalité financière.

4. En Suisse, les intermédiaires financiers ont constaté ces dernières années sur les comptes qu'ils gèrent un nombre exponentiel d'opérations d'AV pouvant être liées au BA et au FT. Cette hausse s'est traduite par une forte augmentation des communications de soupçons adressées au MROS en 2022 : déjà près de 14 % de ces dernières concernaient des AV. Y ont notamment été constatés des liens avec

des personnes politiquement exposées (PPE), des affaires de corruption internationales, des groupes transnationaux de la criminalité organisée ou des acteurs étatiques.

L'analyse des risques conclut que les risques de BA et de FT dans le domaine des AV sont plus marqués qu'en 2018. Les menaces et les vulnérabilités déjà identifiées en 2018 se sont largement aggravées et étendues. En raison de leur importance accrue et des risques qui en découlent, les AV requièrent une attention suffisante de la part de toutes les parties prenantes.

Outre l'identification des menaces et des vulnérabilités de la Suisse pour ce qui est du BA et du FT dans le domaine des AV, divers facteurs contribuent à atténuer ces risques :

- La coopération internationale dans le cadre d'enquêtes sur des AV montre qu'une meilleure traçabilité, le blocage et la confiscation des AV permettent de lutter efficacement contre le BA et le FT.

- De nombreux petits fournisseurs d'AV ont aujourd'hui disparu ou ont fusionné. Cette évolution a contribué à ce que de grandes bourses de cryptoactifs renforcent leurs mesures de compliance, ce qui consolide le dispositif de défense dans le monde entier.

- Les blockchains ("chaînes de blocs" en français) sont par nature plus transparentes que les systèmes de paiement traditionnels. Les outils d'analyse des blockchains permettant de détecter et de suivre plus facilement les activités suspectes, il en résulte une meilleure traçabilité des AV.

- Enfin, étendre la définition de l'intermédiation financière au secteur des AV en Suisse contribue à faire entrer un plus large éventail d'acteurs dans le champ d'application de la loi du 10 octobre 1997 sur le blanchiment d'argent (LBA). Des lacunes dans les mesures de lutte contre le BA et le FT s'en trouvent ainsi comblées.

Le GCBF propose quatre mesures visant à renforcer le dispositif de lutte contre le BA et le FT dans le secteur des AV :

1. **Amélioration des données et des connaissances relatives au secteur des AV en Suisse**
   Les informations sur le secteur des AV et sur l'utilisation criminelle de ces derniers en Suisse sont indispensables pour identifier, comprendre et évaluer de façon adéquate les risques de BA et de FT.

2. **Incitation à la proactivité en matière de communication de soupçons auprès des intermédiaires financiers exerçant une activité de PSAV**
   Les intermédiaires financiers exerçant une activité de PSAV devraient à l'avenir approfondir les clarifications visant à détecter le BA et le FT, afin de repérer plus efficacement les opérations suspectes et les communiquer au MROS.

3. **Mise à disposition de capacités et de ressources suffisantes aux fins de lutte contre le BA et le FT dans le secteur des AV**
   Il convient de renforcer la coopération entre toutes les parties prenantes concernées, afin de relever les défis posés par la lutte contre le BA et le FT dans le secteur des AV.

4. **Renforcement de la coopération internationale**
   La Suisse doit continuer à s'engager au niveau international afin de lutter efficacement contre les risques de criminalité dans le secteur financier et faire progresser la mise en œuvre des recommandations du Groupe d'action financière (GAFI).

En résumé, il importe que la Suisse prenne au sérieux les risques liés aux AV et adopte des mesures appropriées pour combattre de manière efficace le BA et le FT. L'importance des AV dans le secteur financier ne cessant de croître, la Suisse doit relever les défis qui se posent afin de suivre le rythme des évolutions fulgurantes.

3. Introduction

L'utilisation de monnaies virtuelles (ou actifs virtuels, AV ; cf. chap. 4.1) a nettement augmenté au cours des cinq dernières années, notamment, à des fins légales, dans les investissements, le paiement de biens et de services ou les virements internationaux. Toutefois, les AV possèdent également des caractéristiques qui les rendent propices au BA et au FT. Leur utilisation croissante à des fins criminelles en général et aux fins de BA et de FT en particulier pose des difficultés majeures aux intermédiaires financiers ainsi qu'aux autorités de surveillance et de poursuite pénale.

La première évaluation générale des risques de BA et de FT induits par des AV ayant un lien concret avec la Suisse a été publiée en 2014[1]. À l'époque, il est noté qu'aucun cas majeur de BA ou de FT concernant des AV ne serait connu en Europe et que le MROS avait reçu "peu de communications en lien avec le bitcoin". En 2018, le GCBF a publié sa première analyse sectorielle des risques sur cette thématique[2]. Y étaient analysés en détail les risques de BA et de FT liés à l'utilisation de monnaies virtuelles courus par la place financière suisse, les menaces et les vulnérabilités qui en découlaient ayant été qualifiées de "considérables". Après une première en 2016, le GCBF a publié en 2021 la deuxième évaluation intersectorielle globale des risques de BA et de FT en Suisse[3]. Il y était recommandé de suivre de près la situation, compte tenu de la menace croissante que faisaient peser les AV sur la Suisse, du développement rapide de ce secteur et de la difficulté à mesurer les risques, et de mettre à jour si nécessaire l'analyse sectorielle sur les AV de 2018. Le présent rapport vise à mettre en œuvre cette dernière recommandation.

Le MROS a repris ce mandat du GCBF, le groupe interdépartemental de coordination permanent mis en place par le Conseil fédéral à la fin de 2013, qui est chargé de coordonner la politique en matière de lutte contre le BA et le FT et d'évaluer les risques dans ces domaines[4]. Le présent rapport est le résultat de l'analyse sectorielle des risques effectuée par ce groupe en étroite coopération avec des autorités de surveillance et de poursuite pénale, ainsi que d'autres autorités et offices de la Confédération.

L'exécution du mandat s'est avérée difficile, car la plupart des données nécessaires à une évaluation précise des risques de BA et de FT pour la Suisse en lien avec des AV n'étaient pas entièrement disponibles. Il s'agissait, d'une part, de données relatives au nombre de personnes morales et physiques[5] opérant dans le secteur des AV et, d'autre part, de données sur l'utilisation criminelle d'AV en Suisse, comme des chiffres consolidés relatifs au nombre de procédures dans notre pays, les éléments constitutifs d'infraction analysés, les montants concernés et les décisions qui en ont résulté. Malgré cette difficulté, il est possible de tirer, bien que dans une mesure limitée, certaines conclusions sur l'importance et la croissance du secteur des AV et les risques de BA et de FT qui en découlent. Pour ce faire, divers relevés ont été effectués et certaines sources ont été analysées dans le cadre du présent rapport. Certes, cela ne remplace pas le besoin de chiffres fiables permettant de classer les risques, mais permet d'obtenir une estimation fondée, qui peut être résumée comme suit :

---

[1] Conseil fédéral, *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070)*, p. 21 s.

[2] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 4

[3] GCBF, *Deuxième rapport national sur les risques de blanchiment d'argent et de financement du terrorisme*, octobre 2021, p. 53

[4] Mandat et composition du GCBF, qui est rattaché au Secrétariat d'État aux questions financières internationales (SFI): *Mandat du groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme*, approuvé sur décision du Conseil fédéral du 17 novembre 2021

[5] Par exemple la fortune ou les revenus gérés, imposés ou liquidés en AV par ces derniers, ou les flux financiers d'AV entrant dans la place financière suisse ou en sortant.

Premièrement, le secteur des AV a connu une forte croissance aux niveaux mondial et national depuis 2018. Cette année-là, la capitalisation totale du marché des AV représentait encore moins de 1 % du produit intérieur brut (PIB) mondial – à son dernier plus haut niveau en 2021, elle atteignait déjà 2,7 %[6]. Même si ces données sont en partie dues aux fluctuations très volatiles des prix, il semble que l'utilisation d'AV ait fortement augmenté ces dernières années. Les estimations indiquent qu'en 2023, près de 420 millions de personnes, soit plus de 4 % de la population mondiale, possédaient des AV[7]. Cette hausse marquée a également eu lieu en Suisse. Diverses enquêtes menées dans notre pays ont révélé qu'en 2020, entre 7 et 10 % des personnes interrogées avaient acheté des AV, et qu'en 2022, cette part atteignait 18 à 20 %[8]. Les flux financiers d'AV restent toutefois relativement modestes par rapport à d'autres flux financiers. Alors que le volume mondial des transactions d'AV a atteint son plus haut niveau annuel en 2021 avec 15,8 milliards de dollars, par exemple le volume mondial des transactions de change de gré à gré est lui d'un tout autre ordre de grandeur, à savoir 7,5 milliards de dollars *par jour* (avril 2022)[9].

Deuxièmement, l'utilisation criminelle d'AV a augmenté et s'est diversifiée dans le monde entier depuis 2018. Les rapports de plusieurs pays, d'organisations supranationales et de sociétés spécialisées dans l'analyse de blockchain montrent clairement que l'utilisation criminelle d'AV s'est depuis lors accrue et diversifiée à l'échelle mondiale. Depuis longtemps, les risques de BA ne proviennent plus uniquement des infractions préalables dans le domaine de la cybercriminalité ou des infractions "spécifiques aux cryptos"[10]. Ils émanent également des infractions les plus diverses commises dans le monde "hors ligne", à savoir notamment des formes les plus graves de criminalité économique et, enfin, également de l'utilisation d'AV par des réseaux professionnels de blanchiment de capitaux[11]. En outre, l'usage d'AV dans certaines infractions, notamment les attaques de rançongiciel et les fraudes à l'investissement en ligne, est devenu courant et constitue plutôt la règle que l'exception.

Troisièmement, le nombre d'intermédiaires financiers avec activité de PSAV domiciliés en Suisse a fortement augmenté depuis 2018 : alors qu'ils étaient moins de 10 cette année-là, leur nombre était de 204 au moins à la fin de 2022. On observe également que les intermédiaires financiers suisses *sans* activité de PSAV ont de plus en plus de liens avec le secteur des AV – par exemple en raison des activités menées par leurs clients et des transactions ordonnées par ces derniers. Compte tenu de l'accroissement général de ces liens et de l'utilisation plus fréquente d'AV à des fins criminelles, la place financière suisse est globalement devenue plus vulnérable aux risques de BA et de FT résultant de l'utilisation abusive d'AV.

---

[6] Conseil de stabilité financière (CSF), *FSB Chair's letter to G20 Finance Ministers and Central Bank Governors*, mars 2018, p. 2. Selon le CSF, la capitalisation du marché des AV a été multipliée par 3,5 en 2021, pour atteindre 2,6 milliards de dollars (cf. CSF, *Assessment of Risks to Financial Stability from Crypto-assets*, février 2022, p. 1). Selon les estimations de la Banque mondiale, le PIB mondial a atteint 96,1 milliards de dollars en 2021 (cf. Banque mondiale, *GDP (current US$) – World*, consulté en mai 2023).

[7] Triple-A, *Global Cryptocurrency Ownership Data*, consulté en mai 2023

[8] Moneyland, *Comment les Suisses placent leur argent*, 22 avril 2020. Moneyland, *Comment les Suisses investissent-ils leur argent*, 19 juillet 2022. Bien qu'affichant quelques points de pourcentage de plus ou de moins, d'autres sondages de conception similaire dessinent la même tendance (par ex. Banque Migros, *Les jeunes préfèrent les cryto-monnaies à l'or*, 27 février 2020; Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, 22 juin 2021).

[9] Concernant le volume mondial des transactions pour tous les AV: Chainalysis, *The Crypto Crime Report 2022*, février 2022, p. 3. Concernant le volume mondial des transactions de change de gré à gré: Banque des règlements internationaux (BRI), *OTC foreign exchange turnover in April 2022*, octobre 2022)

[10] Par exemple, les escroqueries liées à des ICO (*Initial Coin Offerings*, en français "levées de fonds en cryptomonnaie") et autres fraudes aux investisseurs, ou l'utilisation d'AV dans divers systèmes de mules financières (*money mules*)

[11] Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, décembre 2021, p. 2

Quatrièmement, la nette augmentation des communications de soupçons transmises au MROS et présentant un lien avec des AV semble confirmer ce qui précède. L'analyse des risques publiée en 2018 indiquait que les autorités suisses n'avaient jusqu'alors identifié aucun cas de FT au moyen d'AV et que seuls de rares cas de BA au moyen des nouvelles technologies avaient été recensés[12]. Mais ce constat n'est plus d'actualité. Le MROS reçoit désormais tous les jours des communications de soupçons liées à l'utilisation d'AV à des fins de BA ou de FT. Près de 10 % des communications de soupçons qui lui ont été adressées entre 2020 et 2022 présentaient des liens avec des AV, cette proportion atteignant pas moins de 13,8 % en 2022.

Afin de tenir compte des évolutions résumées ici et de renforcer la lutte contre le BA et le FT dans le secteur des AV, diverses modifications ont été apportées au droit matériel suisse depuis 2018 (cf. chap. 4.4). Certaines d'entre elles vont au-delà des recommandations formulées par le GAFI. La mise en œuvre du droit matériel fait toutefois naître des difficultés spécifiques, qui influent sur l'efficacité du dispositif de la Suisse visant à combattre le BA et le FT dans ce domaine :

Premièrement, la détection du BA et du FT au moyen d'AV dépend fortement en Suisse du comportement en matière de communications adopté par les intermédiaires financiers avec activité de PSAV. Les chiffres disponibles indiquent que ces derniers émettent nettement moins de communications de soupçons que les intermédiaires financiers *sans* activité de PSAV. Depuis 2020, seuls 24 sur 204 intermédiaires financiers avec activité de PSAV ont transmis une communication, alors que, durant la même période, 118 intermédiaires financiers *sans* activité de PSAV ont envoyé chacun au MROS au moins une communication de soupçons présentant un lien avec des AV.

Deuxièmement, l'une des spécificités du secteur des AV est le caractère fortement international des prestataires de services, des activités, des personnes et des transactions concernés. Le fait que la plupart des pays n'ont pas (encore) mis en œuvre les recommandations du GAFI en matière d'AV, notamment en ce qui concerne la règle de transparence des virements ou *travel rule* (cf. chap. 4.3.2), constitue l'une des plus grosses difficultés. En comparaison internationale, la Suisse a rapidement déclaré sa législation en vigueur compatible avec la *travel rule*. Néanmoins, les PSAV établis à l'étranger sont susceptibles d'être utilisés comme porte d'entrée de valeurs patrimoniales criminelles (en AV ou en monnaie fiat) dans le circuit financier légal. En outre, il importe de souligner qu'il suffit d'une seule transaction pour que ces AV se retrouvent en un clin d'œil en Suisse. La non-application des recommandations du GAFI en matière d'AV par des pays tiers fait donc également augmenter le risque que la place financière suisse soit utilisée de façon abusive à des fins de BA ou de FT. Cette situation exige une attention accrue de la part des intermédiaires financiers, qui sont tous susceptibles, qu'ils soient ou non des PSAV, d'être utilisés, par le biais de virements indirects, comme bénéficiaires de valeurs patrimoniales incriminées provenant de ces pays.

Troisièmement, les autorités de poursuite pénale suisses en particulier – mais aussi d'autres autorités et offices chargés de la lutte contre le BA et le FT – font face à des problèmes spécifiques dans le secteur des AV. Près de la moitié ont déjà commencé à mettre en place des ressources humaines, des connaissances et des moyens techniques pour apporter des solutions.

[12] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 4

Quatrièmement, la coexistence de divers systèmes de paiement comporte un risque depuis toujours du point de vue de la lutte contre le BA et le FT. Ce risque a pris une nouvelle dimension avec l'existence simultanée de systèmes de paiement en monnaies fiat et en AV, qui sont fondamentalement différents et dont les données et les informations sont aussi diversement structurées, conservées et mises à disposition. En outre, il existe également différents flux de paiement possibles et simultanés pour certains AV, qui offrent parfois un grand anonymat[13]. La concomitance de divers systèmes de paiement rend la vue d'ensemble bien plus difficile pour certains acteurs, comme les intermédiaires financiers ou les autorités de poursuite pénale. Les criminels en profitent pour blanchir des valeurs patrimoniales obtenues illégalement et effacer leurs traces. Cette problématique s'est nettement accentuée avec les moyens permettant de convertir en quelques secondes, par voie électronique et dans le monde entier, des monnaies fiat et des AV, ainsi qu'avec la possibilité offerte aux utilisateurs d'AV de les retirer de l'intermédiation financière et de les transférer, également en un rien de temps, sur des portefeuilles gérés par des particuliers. La rapidité et l'absence de frontières en ligne rendent difficile une approche globale.

Les risques existants dans le secteur des AV ont évolué ces dernières années et le recours aux cryptomonnaies à des fins de BA ou de FT s'est accrue. Il est hautement improbable que les AV disparaissent dans un avenir proche. En même temps, mesurer les risques de BA et de FT dans ce domaine reste une tâche ardue. Quinze ans après l'apparition du plus ancien AV, à savoir le bitcoin, il n'existe pas de données consolidées fiables sur la taille et la structure du secteur, tant au niveau mondial qu'en Suisse, pas plus que sur les flux financiers en monnaies fiat et en AV. Par conséquent, on ne dispose pas non plus d'informations sur la part de ces flux financiers qui pourraient être d'origine criminelle. Comme indiqué dans le présent rapport, il n'existe pas de dispositions en Suisse définissant la compétence en matière de collecte de chiffres en vue d'un monitoring national.

Alors que l'argument selon lequel l'engouement pour les AV serait amené à disparaître rapidement justifiait pendant un temps de renoncer à cette collecte, l'évolution rapide du secteur a fait que l'absence de monitoring national est devenue entre-temps un risque en soi. De meilleures données sur la taille réelle du secteur des AV et sur l'utilisation criminelle de ces derniers en Suisse permettraient d'évaluer plus aisément dans quelle mesure les cas (suspects) déjà détectés sont représentatifs des opérations qui y ont cours et de déterminer quelles recommandations de modification du dispositif semblent appropriées.

Les succès récents en matière de blocage et de confiscation d'AV incriminés montrent en même temps que le secteur offre des opportunités considérables et des possibilités jusqu'ici insoupçonnées en matière de lutte contre le BA et le FT. Les intermédiaires financiers et les autorités de poursuite pénale peuvent tirer parti de la transparence fondamentale de la plupart des AV afin de détecter directement les activités suspectes et de suivre les flux financiers concernés. Dans le contexte de la lutte contre le BA et le FT, le secteur des AV offre ainsi un avantage décisif par rapport au trafic de paiements traditionnel – pour autant que les moyens et l'expertise nécessaires soient disponibles.

[13] On peut prendre pour exemple la plus ancienne cryptomonnaie, à savoir le bitcoin: les transactions peuvent être effectuées directement sur la blockchain (*on-chain*), mais également hors de la blockchain (*off-chain*), notamment par des réseaux de paiement reposant sur les blockchains du bitcoin (*second layers* ou secondes couches) ou reliés à ces dernières, par exemple via Lightning Network ou via CoinSwap au moyen de *statechains*.

4. Contexte

Ce chapitre a pour but la classification juridique et économique des AV dans les cadres national, respectivement international. Les termes *actifs virtuels (AV)* et *prestataire de services d'actifs virtuels (PSAV)* y sont interprétés à la lumière des définitions du GAFI et comparés à leurs équivalents dans les actes législatifs et les publications officielles suisses. Afin de donner un aperçu des personnes et des services couverts par ces définitions, il s'agira de schématiser les aspects fondamentaux et les spécificités de l'écosystème des AV ainsi que ses interactions avec le secteur financier traditionnel. Seront examinés également les développements réglementaires pertinents survenus depuis 2018 tant en Suisse qu'à l'étranger, notamment l'état actuel de la mise en œuvre des recommandations du GAFI relatives aux AV et aux PSAV[14]. Enfin, la structure actuelle du secteur des AV et l'utilisation de ces derniers en Suisse seront décrites le plus précisément possible malgré des données limitées.

4.1 Monnaies virtuelles, AV et PSAV

Le rapport de juin 2014 du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab et Weibel définissait le terme *monnaie virtuelle* comme suit : "Par monnaie virtuelle, on entend une représentation numérique d'une valeur, négociable sur Internet et remplissant les fonctions de la monnaie. Elle peut certes être utilisée comme moyen de paiement pour des biens et des services réels, mais n'est acceptée nulle part comme moyen de paiement ayant cours légal. Les monnaies virtuelles ont chacune leur dénomination et se distinguent de la monnaie électronique en ceci qu'elles ne s'adossent pas à une monnaie ayant cours légal. Les monnaies virtuelles n'existent que sous la forme d'un code numérique et n'ont donc pas de pendant matériel, par exemple sous la forme de pièces ou de billets. En raison de leur négociabilité, elles sont à classer parmi les valeurs patrimoniales"[15].

En octobre 2018, le GAFI[16] a donné pour la première fois sa définition des termes *actifs virtuels* et *prestataire de services d'actifs virtuels* – en les distinguant du celui de *monnaie virtuelle* qu'il utilisait auparavant[17]. Les nouvelles définitions ont été ajoutées à la recommandation n° 15 du GAFI (*"Nouvelles technologies"*) afin de clarifier les exigences applicables à ces valeurs patrimoniales d'un nouveau genre et à leurs fournisseurs :

"Un *actif virtuel* est la représentation numérique d'une valeur qui peut être échangée de manière digitale, ou transférée, et qui peut être utilisée à des fins de paiement ou d'investissement. Les actifs virtuels n'incluent pas les représentations numériques des monnaies fiduciaires, titres et autres actifs financiers qui font déjà l'objet d'autres dispositions des Recommandations du GAFI"[18].

[14] Pour des informations sur les développements réglementaires relatifs aux AV et aux PSAV en Suisse jusqu'en 2018 compris: cf. GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018

[15] Conseil fédéral, *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070)*, p. 8

[16] Le GAFI est considéré comme l'organisme international de normalisation en matière de lutte contre le BA et le FT.

[17] GAFI, *Outcomes FATF Plenary, 17-19 October 2018*, octobre 2018. Autres publications importantes du GAFI sur le sujet, qui reflètent ces évolutions: GAFI, *Guidance for a Risk-Based Approach to Virtual Currencies*, juin 2015; GAFI, *Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels*, juin 2019, p. 4; GAFI, *Les recommandations du GAFI*, février 2023, pp. 157 s.

[18] GAFI, *Les recommandations du GAFI*, février 2023, p. 136

Le GAFI a également donné une définition des PSAV :

> "Le terme *prestataire de services liés à des actifs virtuels* désigne toute personne physique ou morale qui ne fait pas l'objet d'autres dispositions des Recommandations du GAFI, et qui exerce à titre commercial une ou plusieurs des activités ou opérations suivantes au nom d'un client ou pour son compte :
> i. échange entre actifs virtuels et monnaie fiduciaire;
> ii. échange entre une ou plusieurs formes d'actifs virtuels;
> iii. transfert d'actifs virtuels;
> iv. conservation et/ou administration d'actifs virtuels ou d'instruments permettant le contrôle d'actifs virtuels; et
> v. participation à et prestation de services financiers liés à l'offre d'un émetteur et/ou à la vente d'actifs virtuels"[19].

Le terme *monnaie virtuelle* a été inscrit pour la première fois le 1er janvier 2016 dans un acte législatif suisse, à savoir l'ordonnance sur le blanchiment d'argent (OBA)[20]. Pendant ce temps, le GCBF utilisait dans son analyse des risques de 2018 le terme *monnaie virtuelle* comme synonyme de *crypto-monnaie* et définissait un terme générique supplémentaire, à savoir *crypto-asset* (anglicisme de *cryptoactif*):

> "[L]es crypto-assets sont une représentation digitale d'une valeur qui peut être échangée de manière numérique sur une blockchain et employée à des fins de paiement (fonction de paiement), d'utilisation (fonction d'utilisation) ou d'investissement (fonction d'investissement)"[21].

L'utilisation de ce terme générique dénotait un certain esprit d'anticipation dans la mesure où il ne couvrait pas seulement les cryptomonnaies au sens classique du terme, mais aussi, par exemple, de nouveaux phénomènes comme les jetons non fongibles (*non-fungible tokens*, NFT, cf. chap. 6.2) – s'il n'y avait pas dans la définition l'indication qu'ils peuvent être échangés sur une blockchain[22]. Plusieurs pays utilisent par ailleurs des termes différents, comme *digital currencies* ou *digital assets*, dont la définition et l'utilisation divergent selon le pays (le terme français *actif virtuel (AV)* utilisé dans le présent rapport étant la traduction du terme anglais *virtual asset*).

D'après l'Autorité fédérale de surveillance des marchés financiers (FINMA), la terminologie usitée en Suisse (*monnaies virtuelles*) est identique à celle du GAFI (*actifs virtuels*). Ainsi, l'évaluation des NFT par la FINMA repose sur la fonction économique et non, par exemple, sur la représentation technique, la question centrale étant de savoir quel type de droit représente le NFT. Dans le présent rapport, *monnaie virtuelle* est donc synonyme d'*actif virtuel (VA)*.

---

[19] Ibid., pp. 150 s.
[20] Art. 4, al. 2, let. a, *OBA* (RS **955.01**, version du 1er janvier 2016)
[21] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 7
[22] La technologie de la blockchain est une variante des différentes technologies des registres distribués (TRD) possibles (*distributed ledger technology* [DLT]; elle représente la catégorie supérieure des structures de données, qui se trouvent réparties sur plusieurs ordinateurs en divers lieux). Sont ainsi théoriquement envisageables (voire parfois déjà existants) des cryptomonnaies ou des NFT basés sur d'autres TRD que la technologie de la blockchain.

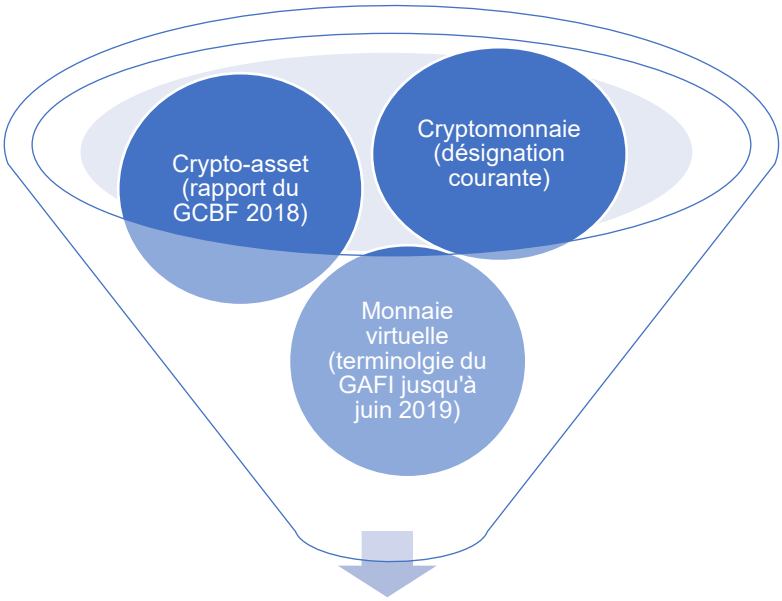

Fig. 1 : Les synonymes *monnaie virtuelle* (CH) et *actif virtuel* (GAFI) sont des termes juridiques génériques, qui englobent également par exemple les NFT.

4.2 Écosystème des AV

Il existe différents modèles pour schématiser l'écosystème des AV et catégoriser les activités liées à ces derniers, qui varient en fonction des axes prioritaires retenus et de la perspective adoptée. Le modèle présenté ici aborde l'écosystème des AV sous l'angle de la création de valeur, depuis la création de l'AV jusqu'à son utilisation pour un service précis. Des exemples d'intermédiation financière au sens de la LBA dans le cadre de la chaîne de création de valeur sont également cités et leurs interactions avec les acteurs de l'écosystème des AV sont mises en évidence à l'aide d'un schéma type montrant les flux financiers possibles (en monnaie fiat ou en AV). En raison de l'évolution fulgurante du secteur des AV, il convient de noter que ni les catégorisations ni les exemples présentés ne prétendent à l'exhaustivité. Par ailleurs, certaines catégories ou services peuvent se recouper selon les cas.

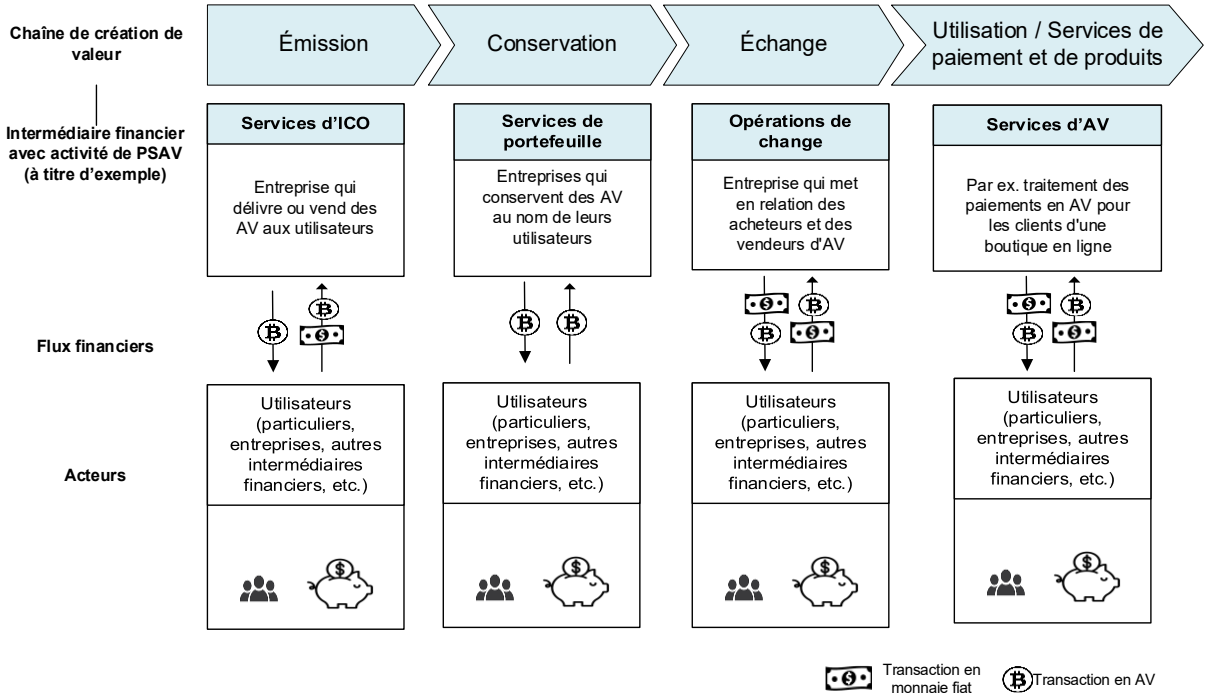

Fig. 2 : Schéma type de la chaîne de création de valeur d'AV et de l'intermédiation financière correspondante

Il existe dans le monde différents modèles de catégorisation des AV, basés sur leurs caractéristiques respectives. Il peut y avoir des recoupements entre les catégories ; le classement des AV dans les catégories dépend souvent de divers facteurs, comme les évolutions technologiques ou le cadre réglementaire spécifique à chaque pays.

Modèle 1: catégorisation selon l'usage prévu et/ou les caractéristiques techniques	Modèle 2: catégorisation selon le statut juridique	Catégorisation selon la fonction (cf. chap. 4.4.3)
• **Jeton fongible** (par ex. bitcoin ou ETH) vs **Jeton non-fongible** (par ex. jetons Bored Ape Yacht Club) • **AV non adossés** (par ex. bitcoin ou ETH) vs **AV adossés** (par ex. *stablecoins* comme le DAI ou l'USDT) • **Preuve de travail** (*proof of work*, PoW; par ex. bitcoin ou Monero) vs **Preuve d'enjeu** (*proof of stake*, PoS; par ex. Ethereum ou Tezos) • **Pseudonyme** (par ex. bitcoin ou Litecoin) vs **Anonyme** (par ex. Monero ou Zcash) • **Cryptomonnaies** (par ex. bitcoin ou Litecoin) vs **Plates-formes smart contract** (par ex. Ethereum ou BNB Smart Chain)	• AV **réglementés** vs AV **non réglementés** (selon la juridiction) • AV **interdits** vs AV **autorisés** (selon la juridiction) • AV comme **moyen de paiement officiel** (par ex. bitcoin en El Salvador) vs AV comme **moyen de paiement non officiel** (par ex. Monero sur les marchés du darknet)	• **Jetons de paiement** • **Jetons d'utilité** • **Jetons d'investissement** • **Jetons hybrides** (formes mixtes, par ex. jetons de paiement *et* d'utilité, ou jetons d'investissement, d'utilité *et* de paiement)

Fig. 3 : Exemples de catégorisations possibles des AV

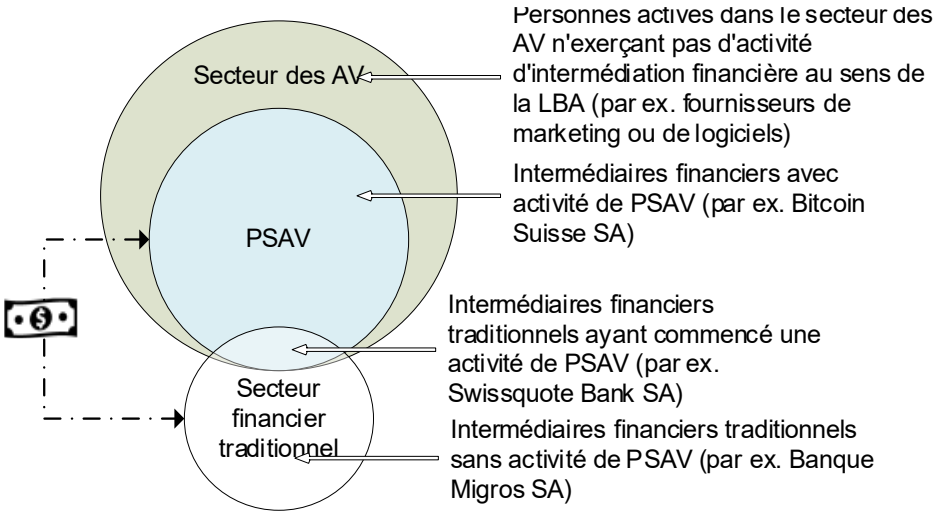

Fig. 4 : Distinction et interaction des intermédiaires financiers avec et sans activité de PSAV

Le secteur des AV englobe l'ensemble des activités portant sur des AV. Ces dernières ne relèvent pas toutes du domaine de l'intermédiation financière au sens de la LBA (cf. chap. 4.4.1 et 4.4.2). Le présent rapport se concentre sur les intermédiaires financiers dont les activités peuvent être liées à des AV. Les intermédiaires financiers avec activité de PSAV ne sont pas les seuls concernés, ceux qui n'exercent pas une activité de PSAV peuvent également avoir des activités commerciales en lien avec des AV – par exemple lorsqu'ils exécutent pour un client un ordre de virement vers une bourse d'AV ou qu'ils mettent un compte commercial à la disposition d'un intermédiaire financier avec activité de PSAV. Il est également à noter que toutes les activités des intermédiaires financiers avec activité de PSAV ne présentent pas nécessairement un lien avec des AV. Par exemple, certains d'entre eux proposent également des services financiers traditionnels sans nul rapport avec des AV[23].

Encadré n° 1

La frontière entre intermédiaires financiers exerçant ou non une activité de PSAV se brouille de plus en plus

Sous l'angle de la lutte contre le BA, les infractions préalables au BA et le FT, la distinction entre intermédiaires financiers avec activité de PSAV et ceux sans une telle activité ne semble jouer guère, tant à moyen qu'à long terme, qu'un rôle mineur. Il y a à cela plusieurs raisons. Premièrement, l'intégration croissante des AV a pour effet que les intermédiaires financiers traditionnels proposent de plus en plus eux aussi des services dans ce domaine. Cette évolution est déjà observée et va probablement se poursuivre. Deuxièmement, les communications de soupçons transmises par les intermédiaires financiers traditionnels présentent toujours plus souvent des liens avec le secteur des AV. Troisièmement, la croissance du secteur des AV a poussé certains intermédiaires financiers sans activité de PSAV à développer des modèles d'affaires axés explicitement sur ce secteur, quand bien même ils n'y exerceront pas eux-mêmes l'activité de PSAV (par ex. mise à disposition de comptes commerciaux et de comptes de paiement en monnaie fiat pour des intermédiaires financiers avec activité de PSAV, qui exécutent ensuite des paiements en AV sur les plates-formes d'intermédiaires financiers avec activité de PSAV; cf. 6e vulnérabilité au chap. 7.5.1).

[23] Par ex. la mise à disposition d'un dépôt d'actions

Dans le suivi des flux financiers suspects, opérer une distinction entre ceux en monnaie fiat et ceux en AV n'est en fin de compte qu'un détail technique. La frontière entre les deux catégories d'intermédiaires financiers correspondantes est déjà floue actuellement. La poursuite de la croissance du secteur des AV et l'intensification des activités et des liens entre intermédiaires financiers exerçant ou non une activité de PSAV peuvent aboutir à une fusion grandissante de ces catégories. Leur distinction pourrait n'avoir d'importance, notamment du point de vue de la lutte contre le BA et le FT, que pour déterminer quelles formes de flux financiers (en AV ou en monnaie fiat) doivent être considérées dans l'analyse et le suivi des transactions suspectes[24].

4.3 Normes internationales en matière de lutte contre le BA et le FT dans le secteur des AV

Depuis 2018, le secteur mondial des AV a connu une forte croissance. D'une part, cette évolution s'est traduite par une acceptation désormais largement répandue des AV, y compris dans le secteur financier traditionnel. D'autre part, le secteur des AV a fait l'objet d'une attention accrue de la part des autorités de régulation nationales et internationales, des autorités de poursuite pénale, des cellules de renseignement financier (CRF) et du secteur privé (par ex. sociétés spécialisées dans l'analyse de blockchain). Tous ont commencé à s'intéresser de plus près à la problématique du BA et du FT dans le secteur des AV et ont étendu leurs capacités. Dans le même temps, le GAFI s'est mis à appliquer systématiquement ses recommandations au secteur des AV, publiant à cet égard très fréquemment des aperçus et des lignes directrices, qu'il s'agira d'aborder plus en détail dans ce qui suit.

[24] Basel Institute On Governance, Europol, *Seizing the Opportunity: 5 recommendations for crypto-assets-related crime and money laundering*, 2022, p. 1 s

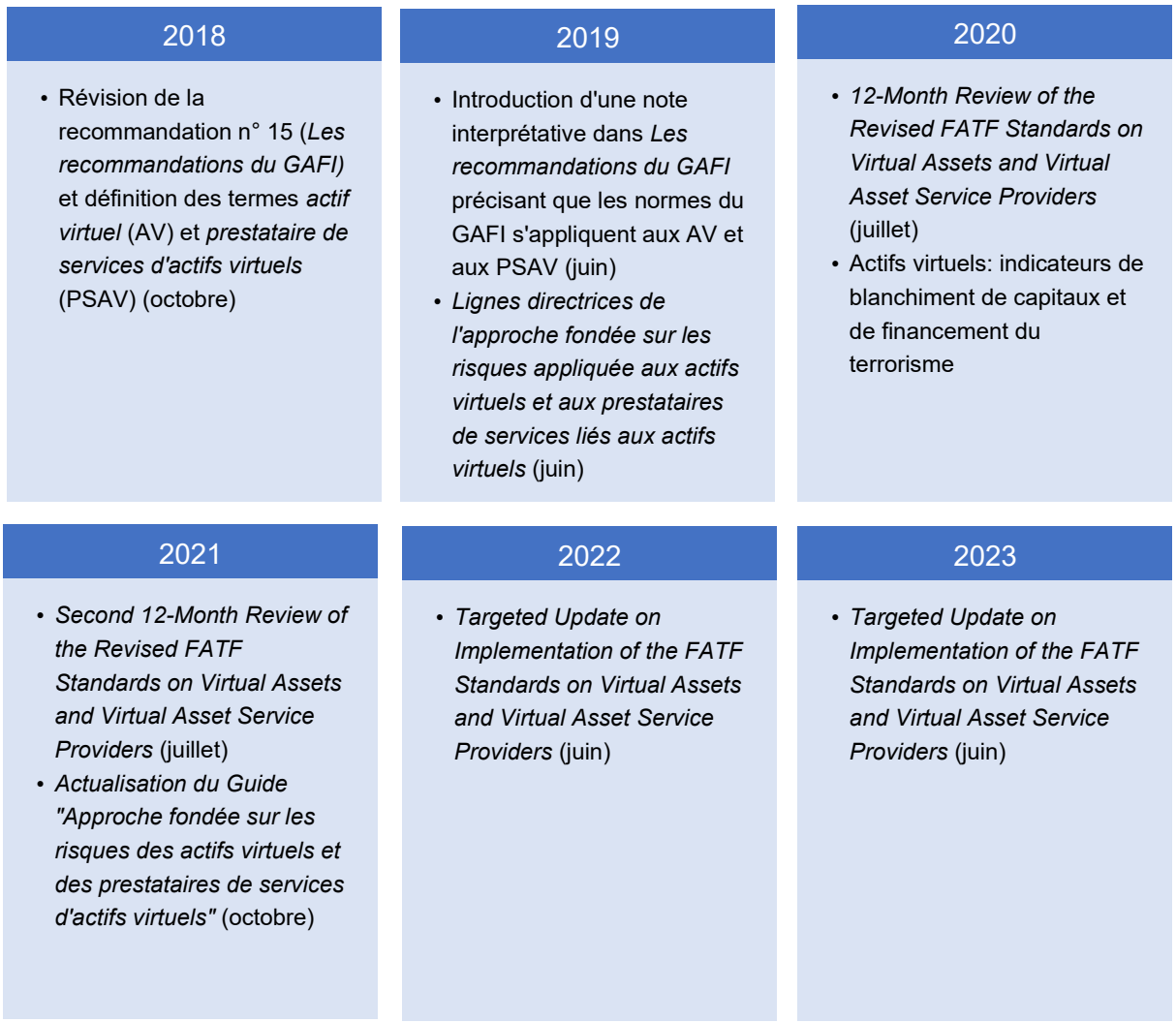

Fig. 5 : Principales publications du GAFI concernant les AV et les PSAV (de 2018 à 2022)

4.4 Règle de transparence (travel rule), cryptomonnaies stables (*stablecoins*) et finance décentralisée (FiDé)

La définition d'*actif virtuel* et de *prestataire de services d'actifs virtuels*, établie en octobre 2018 et inclue dans la recommandation n° 15 du GAFI ("Nouvelles technologies"), peut être considérée comme le point de départ de la réflexion approfondie menée par le GAFI à ce sujet[25]. La note interprétative correspondante, adoptée en juin 2019, vise à expliquer la manière dont les PSAV doivent mettre en œuvre les recommandations n° 10 à 21[26]. L'application de la *travel rule*, depuis longtemps mise en œuvre dans les opérations de paiement traditionnelles, en était la principale obligation : désormais, les virements d'AV entre PSAV doivent contenir des informations sur le donneur d'ordre et le bénéficiaire – comme lors d'un virement bancaire –, afin que le PSAV destinataire puisse vérifier le nom du donneur d'ordre et l'exactitude des informations relatives au bénéficiaire.

[25] GAFI, *Outcomes FATF Plenary, 17-19 October 2018*, octobre 2018
[26] GAFI, *Les recommandations du GAFI*, février 2023, p. 157

	Travel rule du GAFI (Recommandation n° 16)
Données du donneur d'ordre	• Nom • N° de compte • N° de référence de la transaction • Adresse / Date et lieu de naissance / Numéro de client / N° du document d'identité
Données du bénéficiaire	• Nom • N° de compte
Seuil	• EUR 1000 / USD 1000

Fig. 6 : Données qui doivent être échangées lors d'une opération de paiement – également lors du paiement d'AV entre PSAV

En juin 2019, le GAFI a publié *Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels* en réponse au bouleversement profond du secteur financier induit par les AV[27]. Ces lignes directrices visent à montrer que les AV et les PSAV entrent dans le champ d'application des recommandations du GAFI et comment les autorités nationales peuvent mettre en œuvre ces dernières.

En juin 2020, le GAFI a rédigé un rapport sur les cryptomonnaies stables (*stablecoins*)[28]. Les projets de *stablecoin* ont pour but de limiter la volatilité des prix qui a caractérisé jusqu'à présent les AV, en adossant le jeton concerné à des valeurs patrimoniales spécifiques, comme des monnaies fiat, des matières premières, des biens immobiliers ou des valeurs mobilières. Un jeton peut par exemple donner droit à un franc, à un gramme d'or, à une part d'un portefeuille immobilier ou à une certaine quantité de matière première. Le GAFI a constaté que les *stablecoins* sont généralement soumis aux mêmes nombreux risques potentiels de BA et de FT que les autres AV, en raison de la possibilité d'anonymat lors du transfert via des portefeuilles non hébergés, de leur portée internationale et du fait qu'ils se prêtent à la dissimulation dans le processus de BA[29]. Ces caractéristiques constitueraient des vulnérabilités au BA et au FT. En conséquence, le GAFI a demandé à ses pays membres de prioriser la mise en œuvre de ses normes relatives aux AV et aux PSAV. Il a également appelé les pays du G20 à montrer l'exemple à cet égard[30]. En septembre 2020, il a publié une liste d'indicateurs d'alerte destinée aux intermédiaires financiers avec activité de PSAV, afin de les aider à détecter les opérations et les transactions suspectes[31].

Après l'adoption de la norme relative aux PSAV en juin 2019, le GAFI a mis à jour ses lignes directrices à la fin de 2021 afin de traiter des questions en suspens et de réagir aux récents développements du secteur des AV, notamment l'apparition du nouveau domaine de la finance

[27] GAFI, *Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels*, juin 2019
[28] GAFI, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, juin 2020
[29] Un portefeuille non hébergé permet à son utilisateur de conserver des AV sans que des tiers ne puissent y accéder (cf. glossaire).
[30] GAFI, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, juin 2020, pp. 2 à 4
[31] GAFI, *Actifs virtuels - Indicateurs d'alerte de blanchiment de capitaux et de financement du terrorisme*, septembre 2020

décentralisée (FiDé)[32]. Selon le GAFI, il convient de définir très largement les termes *AV* et *PSAV*, de manière à inclure également les plates-formes de FiDé. Et ce notamment lorsque ces plates-formes sont dans une certaine mesure centralisées, par exemple en raison de certains moyens de contrôle ou d'intervention utilisés par leurs développeurs[33]. Par conséquent, ces derniers pourraient être soumis au même devoir de diligence et à la même obligation de communication que les autres intermédiaires financiers. Cette approche comporte des risques pour la lutte contre le BA et le FT, dans la mesure où, en réaction contre elle, les évolutions futures du secteur des AV pourraient tendre à rendre les prestations concernées encore plus anonymes et décentralisées (cf. chap.6.2.1). Néanmoins, cette approche garantit que les personnes physiques ou morales, pour autant qu'elles contrôlent effectivement ou influencent suffisamment une plate-forme ou un protocole dans le domaine de la FiDé, ne se déresponsabilisent pas sous le couvert de *FiDé* et ne négligent leur devoir de diligence et leur obligation de communication.

1re vulnérabilité

La perte tendancielle d'importance de l'intermédiation financière dans le secteur des AV pose des difficultés pour appliquer les approches réglementaires existantes concernant le BA et le FT (identifiée en 2023).

De par leur conception technique, les AV fonctionnent par principe comme un réseau universellement accessible permettant le transfert de valeurs patrimoniales indépendamment des frontières territoriales et de l'identité des donneurs d'ordre et des bénéficiaires. L'architecture pair-à-pair (*peer-to-peer*, P2P) de ces réseaux implique qu'ils soient organisés de façon décentralisée et que la participation des utilisateurs soit anonyme ou pseudonyme. La mise en place de ces réseaux P2P semble une tendance durable. Le transfert d'AV via ces réseaux ne nécessite pas d'intermédiaires financiers au sens traditionnel du terme, bien que ces derniers aient joué jusqu'à présent un rôle important dans le secteur des AV, notamment en tant que *on* ou *off ramps* (rampes d'entrée ou de sortie) assurant l'échange de monnaie fiat et d'AV. Divers scénarios sont concevables, qui pourraient réduire l'importance du rôle que les intermédiaires financiers jouent encore actuellement dans l'échange numérique de valeurs patrimoniales. Ainsi, par exemple la popularité croissante des AV, notamment des *stablecoins*, associée à leur acceptation grandissante comme moyen de paiement dans le monde entier, pourrait, à moyen ou à long terme, réduire le besoin de conserver les AV auprès d'intermédiaires financiers ou même de les convertir en monnaie fiat. Aujourd'hui, la plupart des *stablecoins* sont encore émis par des entreprises du secteur des AV, mais il en existe déjà derrière lesquels se trouvent des organisations autonomes décentralisées (DAO), dont le statut juridique n'est, pour la plupart, pas clair à ce jour. Les approches réglementaires du GAFI concernant le BA et de FT, ainsi que spécifiquement celles de la Suisse, reposent sur le rôle central joué par les intermédiaires financiers, leur devoir de diligence et leur obligation de communication. Si leur rôle disparaît, la réglementation servant à endiguer les risques de BA et de FT se heurtera à des difficultés nouvelles[34].

[32] La FiDé permet aux utilisateurs d'accéder à divers instruments financiers liés aux AV, comme des paires de devises ou des produits dérivés en AV, sans l'intervention d'intermédiaires financiers traditionnels (cf. chap. 6.2.1).
[33] GAFI, *Actualisation du Guide "Approche fondée sur les risques des actifs virtuels et des prestataires de services d'actifs virtuels"*, octobre 2021, pp. 30 à 40
[34] Cf. FINMA, *Monitorage FINMA des risques 2022*, novembre 2022, p. 19; GAFI, *Actualisation du Guide "Approche fondée sur les risques des actifs virtuels et des prestataires de services d'actifs virtuels"* , octobre 2021, p. 19 s.

4.5 Stagnation de la mise en œuvre de la travel rule au niveau international

Aux mois de juin de 2022 et de 2023, le GAFI a publié des rapports sur l'état de la mise en œuvre de la *travel rule* dans le monde montrant à chaque fois des résultats décevants[35]. Pour l'année 2023, la majorité des pays interrogés (73 sur 135[36]) ont indiqué n'avoir pris aucune mesure dans ce sens. En mars 2023, seuls 35 pays sur 135 auraient adopté une législation relative à la *travel rule* et 27 seraient en train d'adopter des lois en la matière. Cependant, seul environ un cinquième de ce groupe a déclaré avoir commencé à appliquer effectivement la réglementation et à prendre les mesures de surveillance correspondantes. Le GAFI en a conclu que cette lacune rendait les AV et les PSAV perméables aux abus et qu'il était urgent d'accélérer la mise en œuvre et l'application de la *travel rule*[37]. Tant le Conseil de stabilité financière de la Banque des règlements internationaux que le GAFI ont mis en garde à cet égard contre le risque d'arbitrage réglementaire : plus les différences nationales en matière de réglementation du secteur des AV sont marquées, plus elles sont susceptibles d'être exploitées par les criminels, qui délocalisent leurs activités dans des pays où la surveillance est moindre, voire insuffisante. En outre, les intermédiaires financiers avec activité de PSAV implantés dans les pays n'appliquant pas la *travel rule* aux transactions d'AV sont avantagés, car ils ne sont pas tenus de consacrer des ressources à la lutte contre le BA et le FT. Les efforts fournis par les pays et par les intermédiaires financiers avec activité de PSAV qui respectent la *travel rule* pourraient ainsi être sapés et certaines parties du secteur pourraient se tourner vers des pays où celle-ci n'est pas appliquée. Il en résulterait un accroissement supplémentaire des risques de BA et de FT dans le secteur des AV à l'échelle mondiale – y compris en Suisse[38].

Depuis l'enquête menée par le GAFI en mars 2023, plusieurs pays, dont l'UE et Singapour[39], se sont néanmoins inspirés de la mise en œuvre de la *travel rule* en Suisse, qui interdit le transfert d'AV vers des portefeuilles non hébergés et non vérifiés. Le règlement révisé de l'UE sur les transferts de fonds (RTF) comprend des dispositions spécifiques relatives au transfert d'AV entre PSAV et portefeuilles non hébergés. Par conséquent, les exigences en matière de transferts d'AV concernent également les transferts effectués vers ou depuis des portefeuilles non hébergés, dès lors qu'intervient un PSAV ou un autre intermédiaire financier (c'est-à-dire une entité assujettie) (cf. consid. 38 RTF). Dans le cas d'un transfert de crypto-actifs effectué vers ou depuis un portefeuille non hébergé, les intermédiaires financiers du donneur d'ordre et du bénéficiaire doivent collecter les données requises les concernant. Lorsque le montant de l'ordre de paiement est supérieur à 1000 EUR, ils doivent en outre vérifier, à l'aide de mesures appropriées, si le portefeuille non hébergé appartient effectivement au client ou est contrôlé par celui-ci (cf. consid. 39 en relation avec l'art. 14, par. 5, et 16, par. 2, RTF)[40]. À Singapour, les transactions réalisées avec des portefeuilles non hébergés ne sont pas soumises aux exigences de la *travel rule*, mais devraient être considérées et traitées comme

[35] GAFI, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, juin 2022; GAFI, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, juin 2023

[36] Il n'est pas tenu compte des pays interdisant les PSAV.

[37] GAFI, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, juin 2023, pp. 16 et 17

[38] Financial Stability Institute, *Supervising cryptoassets for anti-money laundering*, avril 2021, p. 19 s.; GAFI, *Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels*, juin 2019, p. 9

[39] S'agissant de l'application de la *travel rule* à Singapour, cf. Monetary Authority of Singapore, *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, mars 2020

[40] Journal officiel de l'Union européenne, *Règlement (UE) 2023/1113 du Parlement européen et du Conseil du du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849*, JO L 150 du 9 juin 2023

présentant des risques de BA et de FT plus élevés. Le prestataire de services de paiement devrait donc appliquer des facteurs d'atténuation des risques plus importants[41].

En outre, l'UE a adopté une loi qui fournit un cadre juridique aux PSAV et met en œuvre la *travel rule*. Le règlement de l'UE sur les marchés de crypto-actifs (règlement MiCA), qui harmonise la réglementation des AV au sein de l'UE, devrait entrer en vigueur à partir de 2024[42]. Cela portera à 58 le nombre de pays ayant adopté des lois ou des règlements visant à mettre en œuvre la *travel rule*.

2e vulnérabilité

Mise en œuvre et application internationales insuffisantes et inégales de la *travel rule* dans le secteur des AV (identifiée en 2023)

Alors que les développements technologiques et économiques dans le secteur des AV se succèdent à toute allure, les projets réglementaires semblent avoir du mal à suivre la cadence. L'application de la *travel rule* aux transactions d'AV a été explicitement recommandée par le GAFI à partir de 2018, soit près de dix ans après la première transaction mondiale de bitcoins. Pour l'heure, il n'est pas possible de prévoir le moment où tous les pays du GAFI appliqueront effectivement la *travel rule* aux transactions d'AV. La non-application de cette règle accroît le risque que des valeurs patrimoniales sous forme d'AV d'origine criminelle soient introduites, faute de contrôles, dans le circuit financier légal par le biais des nombreux canaux possibles – que ce soit en monnaie fiat ou en AV. En conséquence, tous les intermédiaires financiers (avec ou sans activité de PSAV) risquent davantage de servir de point de passage ou d'arrivée à des flux financiers d'origine criminelle (cf. 6e vulnérabilité au chap. 7.5.1). En outre, les intermédiaires financiers avec activité de PSAV implantés dans les pays n'appliquant pas la *travel rule* aux transactions d'AV sont injustement avantagés, car ils ne sont pas tenus de consacrer des ressources à la lutte contre le BA et le FT. Les efforts fournis par les pays et par les intermédiaires financiers avec activité de PSAV qui respectent la *travel rule* pourraient ainsi être sapés et certaines parties du secteur pourraient se tourner vers des pays où elle n'est pas appliquée. Il en résulterait un accroissement supplémentaire des risques de BA et de FT dans le secteur des AV à l'échelle mondiale – y compris en Suisse.

4.6 Cadre juridique national

Depuis 2018, de nouvelles réglementations ont vu le jour en Suisse, qui mettent en œuvre les recommandations du GAFI relatives au secteur des AV – parfois de manière plus restrictive en comparaison internationale. Le cadre juridique suisse relatif au BA et au FT a été étendu aux monnaies virtuelles (ou AV) et aux intermédiaires financiers avec activité de PSAV (ou aux PSAV). L'ensemble des activités d'intermédiation financière liées aux AV entrent ainsi dans le champ d'application de la LBA. La FINMA a précisé sa pratique et ses interprétations à cet égard dans plusieurs publications. Le droit suisse des marchés financiers repose sur des principes, dont celui de la neutralité technologique. Seule la préservation de l'objectif de la réglementation concernée est déterminante – par exemple la limitation du risque de BA –, indépendamment du fait que les acteurs du marché proposent leurs prestations sous forme analogique ou numérique[43]. En 2020, au cours du processus de suivi renforcé de la Suisse, le

[41] Cf. *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, mars 2020, p. 41 s.
[42] Parlement européen, *Crypto-actifs: feu vert à de nouvelles règles de traçabilité des transferts*, avril 2023
[43] Cf. FINMA, *Rapport annuel 2016*, mars 2017, p. 26.

GAFI a jugé que la mise en œuvre de la recommandation n° 15 et les dispositions de la législation suisse en matière de BA lié aux AV et aux PSAV étaient largement conformes[44]. Les sous-chapitres ci-après offrent une vue d'ensemble du cadre juridique suisse relatif aux AV et aux PSAV, en évaluent la conformité avec les normes internationales et résument les modifications principales du point de vue de la lutte contre le BA et le FT.

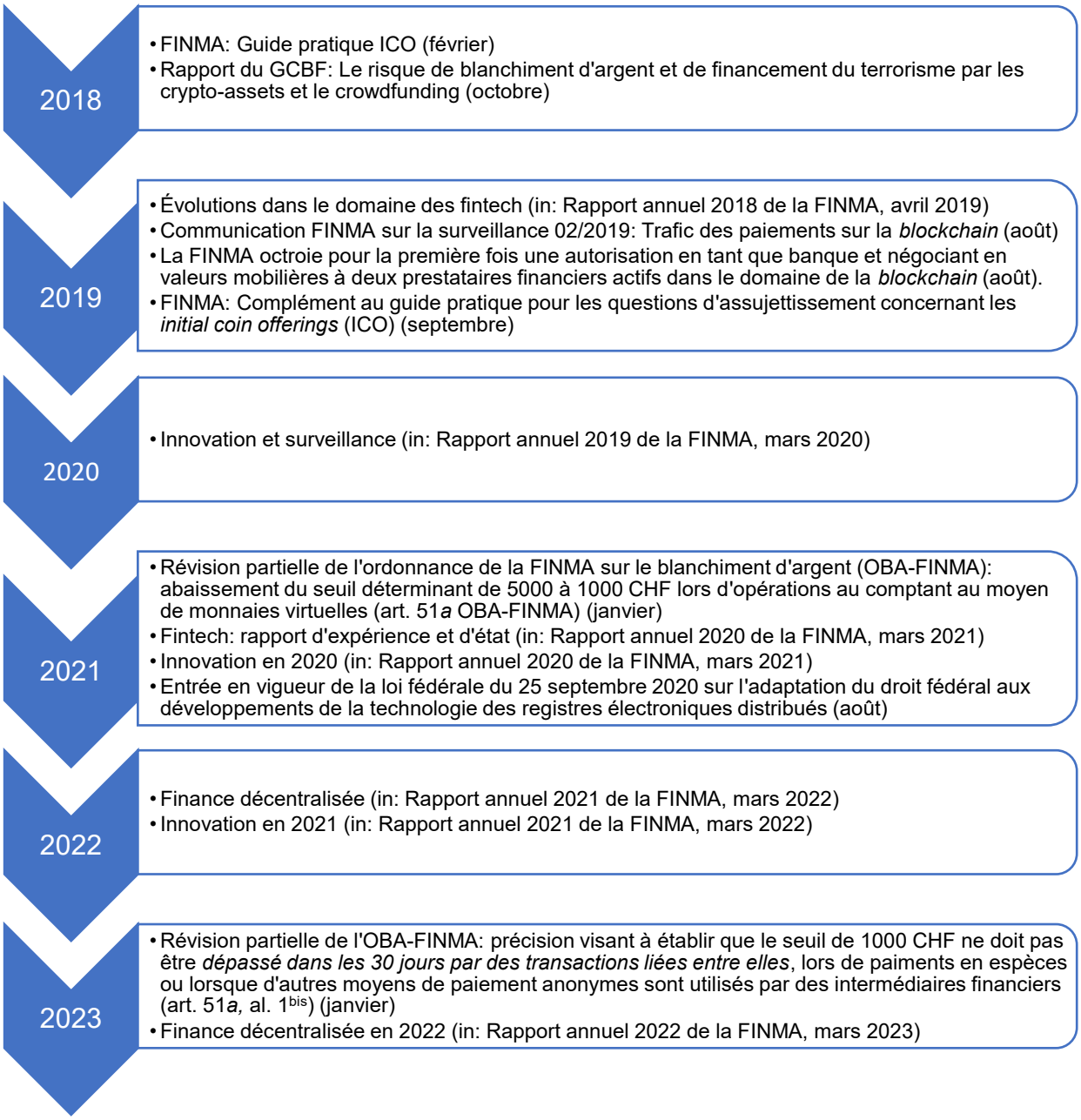

Fig. 7 : Évolutions réglementaires et publications officielles en Suisse concernant les AV et les PSAV (de 2018 à 2022)

[44] GAFI, *Mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme – Suisse – 3ème Rapport de suivi renforcé & réévaluation de notations de conformité technique*, janvier 2020, pp. 7 et 8

4.6.1 Surveillance des intermédiaires financiers en Suisse dans le cadre de la lutte contre le BA et le FT

La réglementation dans le domaine du BA repose sur deux piliers : d'une part, le BA est une infraction au sens de l'art. 305bis du code pénal (CP) sanctionnée par les autorités pénales et, d'autre part, la LBA contraint les intermédiaires financiers et les négociants à respecter le devoir de diligence et l'obligation de communication dans les transactions des clients. L'art. 2, al. 2 et 3, LBA fournit une définition des "intermédiaires financiers" en Suisse[45].

La FINMA veille directement, dans le cadre de la surveillance régulière, au respect de ce devoir et de cette obligation par les banques, les maisons de titres, les entreprises d'assurance et les établissements au sens de la loi du 23 juin 2006 sur les placements collectifs (LPCC). Le respect de ces prescriptions fait l'objet d'un contrôle annuel sur place par les sociétés d'audit et, de plus en plus, directement par la FINMA.

Les gérants de fortune et les *trustees* indépendants sont placés sous la surveillance d'organismes ad hoc, qui font eux-mêmes l'objet d'une autorisation et d'une surveillance par la FINMA. Les personnes et les sociétés du secteur parabancaire (par ex. sociétés de crédit et de leasing, sociétés de cartes de crédit, prestataires de services de paiement ou changeurs) sont également soumises à la législation relative au BA. Ce second groupe doit adhérer à un organisme d'autorégulation (OAR) chargé de veiller au respect du devoir de diligence et de l'obligation de communication, qui soit autorisé et surveillé par la FINMA. Les OAR doivent contrôler si leurs membres respectent les obligations visant à prévenir le BA. Ils peuvent se charger eux-mêmes du contrôle effectif ou le confier à des sociétés d'audit mandatées.

D'autres autorités surveillent en vertu de la LBA les intermédiaires financiers actifs dans des secteurs spécifiques: les maisons de jeu au sens de la loi fédérale du 29 septembre 2017 sur les jeux d'argent (LJAr)[46] sont surveillées par la Commission fédérale des maisons de jeu (CFMJ), les essayeurs du commerce et les sociétés de groupe au sens de l'art. 42bis de la loi du 20 juin 1933 sur le contrôle des métaux précieux (LCMP)[47] par le Bureau central du contrôle des métaux précieux, et les exploitants de jeux de grande envergure au sens de la LJAr par l'Autorité intercantonale de surveillance des jeux d'argent (GESPA).

4.6.2 Aperçu des prestations d'AV et leur assujettissement à la LBA

Dans la mesure où une prestation d'AV est assujettie à la LBA, les personnes concernées doivent respecter les obligations de diligence et sont soumises, comme indiqué ci-dessus, à la surveillance de l'autorité compétente.

Catégories de prestations	Assujettissement à la LBA
Émission de jetons (ICO, jetonisation, etc.)	Assujettie lorsque, dans le cadre d'une *initial coin offering* (ICO), sont émis des jetons pouvant être assimilés à des moyens de paiement (jetons de paiement).
Fournisseur de portefeuilles hébergés	Toujours assujetti

[45] *Loi sur le blanchiment d'argent (LBA)*, RS **955.0**, version du 23 janvier 2023
[46] *Loi fédérale sur les jeux d'argent (LJar)*, RS **935.51**, version du 1er janvier 2021
[47] *Loi sur le contrôle des métaux précieux (LCMP)*, RS **941.31**, version du 1er janvier 2023

Fournisseur de portefeuilles non hébergés	Assujetti pour autant que le fournisseur dispose de certains moyens de contrôle ou d'intervention (par ex. portefeuille multisignature[48] ou applications destinées à la conservation sécurisée de clés privées, même si celles-ci ne peuvent être déchiffrées que par le client, cf. chap. 4.4.6).
Bureaux de change en ligne	Assujettis comme les bureaux de change traditionnels
Bureaux de change physiques (y c. distributeur automatique d'AV)	Assujettis comme les bureaux de change traditionnels
Plates-formes de négociation centralisées	Toujours assujetties
Plates-formes de négociation décentralisées et applications de FiDé	Si, d'un point de vue économique, l'activité exercée relève du droit des marchés financiers et serait donc soumise à autorisation, la FINMA part du principe qu'elle est soumise à autorisation même en cas de mise en œuvre technique ou juridique nouvelle (approche économique).
Mineurs	Non assujettis

Fig. 8 : Catégories de prestations d'AV et assujettissement éventuel à la LBA (modifications réglementaires intervenues après l'analyse des risques de 2018 sur fond saumon)[49]

4.6.3 Guide relatif aux ICO

La FINMA a publié en 2018 un guide pratique relatif aux ICO[50], qui établit ce qui suit : "[l]ors d'une ICO, les investisseurs virent des moyens financiers à l'organisateur de l'ICO. En échange, ils reçoivent ou s'attendent à recevoir des "*coins*", aussi appelés "*tokens*" [*jetons* en français] basés sur une blockchain, qui sont créés sur la base d'une blockchain nouvellement développée dans ce cadre ou au moyen d'un *smart contract* sur une blockchain existante et qui font l'objet d'un enregistrement décentralisé"[51]. Elle fait ainsi la distinction entre les jetons de paiement, d'utilité et d'investissement[52], ce qui a permis de déterminer quelles activités relatives aux ICO relèvent du domaine de l'intermédiation financière et sont donc assujetties à la LBA, notamment lorsque les jetons émis lors de ces opérations de levée de fonds ont une fonction de paiement (jetons de paiement)[53]. Toute personne physique ou morale agissant

[48] Cf. glossaire.
[49] Cf. tableau de 2018 in: GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 40 s.
[50] FINMA, *Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO)*, février 2018
[51] Ibid., p. 1
[52] Des formes mixtes peuvent également exister (jetons hybrides).
[53] FINMA, *Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO)*, février 2018, pp. 6 et 7

comme intermédiaire financier et étant de ce fait assujettie à la LBA doit, pour exercer son activité en Suisse, disposer d'une autorisation de la FINMA relevant du droit de la surveillance (par ex. autorisation bancaire, autorisation de négociant en valeurs mobilières) ou s'affilier à un OAR.

Encadré n° 2

Catégories de jetons selon la FINMA[54]

Jetons de paiement (synonyme de "cryptomonnaies" pures): cette catégorie inclut les jetons qui sont acceptés comme moyen de paiement pour l'achat de marchandises ou de services dans les faits ou selon l'intention de l'organisateur ou qui doivent servir à la transmission de fonds et de valeurs. Les cryptomonnaies ne confèrent aucun droit à l'égard d'un émetteur.

Jetons d'utilité : la FINMA qualifie ainsi les jetons censés donner accès à un usage ou à un service numérique et qui s'appuient sur l'utilisation d'une infrastructure de type blockchain.

Jetons d'investissement : cette catégorie regroupe les jetons qui représentent des valeurs patrimoniales. De tels jetons peuvent notamment représenter une créance au sens du droit des obligations envers l'émetteur ou un droit de sociétariat dans le sens du droit des sociétés. Des parts des revenus futurs d'une entreprise ou des flux de capitaux futurs sont par exemple promis aux détenteurs de jetons d'investissement. Sous l'angle de la fonction économique, le jeton représente ainsi notamment une action, une obligation ou un instrument financier dérivé. La catégorie des jetons d'investissement peut également inclure les jetons censés rendre négociables sur la blockchain des objets de valeur physiques.

Les différentes catégories de jetons ne s'excluent pas nécessairement les unes les autres. Les jetons d'investissement et d'utilité peuvent en outre relever de la catégorie des jetons de paiement (**jetons** dits "**hybrides**"). Dans de tels cas, le jeton peut être cumulativement considéré comme valeur mobilière et comme moyen de paiement. À partir du moment où un jeton, par exemple un NFT, est utilisé comme moyen de paiement effectif, il s'agit d'un jeton de paiement (*substance over form* ou prééminence de la substance sur la forme). Dès lors, les obligations de diligence des intermédiaires financiers s'appliquent pour ce qui est de la réception, la conservation, l'investissement ou la transmission de ces jetons. De même, les jetons de paiement sont soumis à la *travel rule* et à l'art. 10 OBA-FINMA.

4.6.4 Interprétation de la *travel rule* en Suisse

L'un des défis de la lutte contre le BA et le FT réside dans la surveillance efficace des prescriptions lorsque des transactions sont effectuées sur la blockchain. Les principes de surveillance réguliers de la lutte anti-blanchiment s'appliquent aussi dans ce domaine. À cet égard, en publiant sa communication sur la surveillance 02/2019 "Trafic des paiements sur la blockchain", la FINMA a établi que, selon le principe de neutralité technologique, elle appliquait les prescriptions suisses en vigueur sur la transmission de données dans le trafic de paiements aussi dans le domaine de la blockchain[55]. En matière d'applicabilité des prescriptions contre le BA, aucun assouplissement n'est prévu par rapport au trafic de paiements traditionnel.

L'art. 10 OBA-FINMA donne l'obligation à l'intermédiaire financier de transmettre les données relatives au donneur d'ordre et au bénéficiaire lors d'un ordre de virement, peu importe qu'il

[54] Ibid., p. 3
[55] FINMA, *Communication FINMA sur la surveillance 02/2019*, 26 août 2019

soit en monnaie fiat ou en AV. L'intermédiaire financier recevant le virement a ensuite la possibilité de vérifier si le nom de l'expéditeur est par exemple inscrit sur une liste de sanctions. Il peut également contrôler si les données du bénéficiaire sont correctes ou, dans le cas où elles ne correspondraient pas, s'il doit retourner le paiement à l'expéditeur. L'OBA-FINMA remplit ainsi les normes du GAFI revues en 2019, qui exigent que les mesures de prévention listées aux recommandations n° 10 à 21 du GAFI, y compris la *travel rule*, soient respectées par les PSAV.

Les intermédiaires financiers exerçant une activité de PSAV n'ont le droit d'envoyer des AV qu'aux portefeuilles externes de leurs propres clients déjà identifiés et de recevoir des AV que de tels portefeuilles. Tant que les données du donneur d'ordre ou du bénéficiaire ne peuvent pas être transmises de façon fiable dans le système de paiement, les intermédiaires financiers n'ont pas le droit de recevoir des AV de clients d'autres établissements ou de leur en envoyer.

	Art. 10 OBA-FINMA et communication FINMA 02/2019	*Travel rule* du GAFI NIR 15 let. 7b
Données du donneur d'ordre	• Nom • N° de compte • N° de référence de la transaction • Adresse (ou date et lieu de naissance / N° de client ou n° du document d'identité)	• Nom • N° de compte • N° de référence de la transaction • Adresse / Date et lieu de naissance / N° de client / N° du document d'identité
Données du bénéficiaire	• Nom • N° de compte (si pas de n° de compte, n° de référence de la transaction)	• Nom • N° de compte
Seuil	CHF 0.-	EUR 1000 / USD 1000
Validité pour les transactions avec des portefeuilles non hébergés	Oui, cf. Communication FINMA 02/2019	Non

Fig. 9 : Mise en œuvre de la *travel rule* en Suisse

4.6.5 *Stablecoins* et finance décentralisée

La FINMA a constaté en 2019 une augmentation des projets visant à créer des *stablecoins*. Par conséquent, elle a publié en septembre 2019 un complément à son guide pratique pour les questions d'assujettissement concernant les ICO, dans le but de fournir des indications pour pouvoir catégoriser les *stablecoins* selon le droit suisse de la surveillance[56].

La FINMA applique le principe de neutralité de la technologie aussi lorsqu'elle considère les *stablecoins* du point de vue du droit de la surveillance. Elle met l'accent sur la fonction économique et sur la finalité d'un jeton (*substance over form*), et suit aussi bien les décisions d'évaluation éprouvées (*same risks, same rules*) que les particularités du cas considéré. Les *stablecoins* sont classés dans des catégories selon le type de la valeur rattachée. Les catégories (rattachement à des monnaies, à des matières premières, à des immeubles et à des valeurs mobilières) ont ceci de commun qu'elles sont presque toujours soumises à la LBA, l'objectif étant habituellement de mettre à disposition des moyens de paiement sous la forme de *stablecoins*. Lorsqu'une banque souhaite émettre des *stablecoins* dans un système de transaction ayant un accès ouvert tel qu'Ethereum, les risques accrus en matière de réputation et de BA doivent notamment être pris en compte. Après l'émission du *stablecoin* et compte tenu de la nature ouverte du système, l'établissement émetteur ne peut plus exercer de contrôle qu'en cas d'échange contre la valeur sous-jacente. Les obligations de diligence au sens de la loi contre le blanchiment d'argent ne peuvent donc être assumées qu'à l'égard de la première et de la dernière personne qui disposent du *stablecoin*. Les personnes qui achètent ou vendent entretemps le *stablecoin* sur la plate-forme ouverte échappent au contrôle de l'établissement émetteur. Comme la FINMA l'a constaté, il s'agirait dans ce cas d'un instrument au porteur problématique du point de vue de la lutte contre le BA, sans compter que cela pourrait engendrer des atteintes à la réputation de l'établissement concerné et de l'ensemble du marché financier suisse.

Afin de prévenir ces risques, des restrictions de transmission contractuelles et, le cas échéant, technologiques s'imposent lors de l'émission de *stablecoins* par des établissements assujettis. En conséquence, l'identité de toutes les personnes disposant de *stablecoins* doit être suffisamment vérifiée par l'établissement émetteur ou par les partenaires de distribution dûment surveillés, afin d'assurer le respect des obligations de diligence visées par la LBA lors de toutes les transactions portant sur des *stablecoins*. Cela correspond à une application neutre du point de vue de la technologie de l'interdiction de livrets d'épargne au porteur (art. 5 CDB 20)[57].

La FINMA applique également les règles du marché financier existantes aux applications de FiDé et fait donc abstraction de l'utilisation de certains procédés ou technologies. Lorsqu'une application de FiDé propose le même service et comporte les mêmes risques que les intermédiaires sur le marché financier traditionnel, la FINMA applique aussi les mêmes règles. Lorsqu'une application de FiDé propose au plan économique une activité régie par le droit des marchés financiers qui serait soumise à autorisation, la FINMA considère que l'obligation d'obtenir une autorisation s'applique également pour ces nouvelles formes de mise en œuvre technique ou juridique. En conséquence, les exigences en matière de lutte contre le BA doivent aussi être respectées[58]. La FINMA suit de près la tendance croissante à développer et à utiliser des applications de FiDé, en particulier lorsque des personnes assujetties à la FINMA utilisent ou souhaitent utiliser de telles applications. Sur cette question, elle reste fidèle aux principes éprouvés de la prééminence de la substance sur la forme et des *same risks, same rules*

[56] FINMA, *Complément au guide pratique pour les questions d'assujettissement concernant les ICO*, septembre 2019.
[57] Association suisse des banquiers (ASB), *Convention relative à l'obligation de diligence des banques* (CDB 20), 2020
[58] FINMA, *Rapport annuel 2021*, mars 2022, p. 20

(mêmes risques, mêmes règles), et décide toujours en fonction des circonstances économiques réelles[59].

4.6.6 Loi sur l'infrastructure des marchés financiers

Le 25 septembre 2020, le Parlement a adopté la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués[60]. Dix lois fédérales existantes ont été modifiées, dont la LBA. Une modification importante concerne l'élargissement du champ d'application de la LBA. Tombent désormais sous le coup de cette loi les systèmes de négociation fondées sur la TRD (systèmes de négociation pour les valeurs mobilières fondées sur la TRD au sens de l'art. 73*a* de la loi du 19 juin 2015 sur l'infrastructure des marchés financiers, LIMF[61]) visés à l'art. 2, al. 2, let. d^{quater}, LBA. Dans l'ordonnance sur l'infrastructure des marchés financiers (OIMF[62]), il est en outre établi qu'un système de négociation fondé sur la TRD ne doit pas accepter de valeurs mobilières fondées sur la TRD et les autres valeurs patrimoniales qui pourraient compliquer notablement la mise en œuvre des exigences de la LBA (par ex. *privacy coins*, cf. glossaire) ou porter atteinte à la stabilité et à l'intégrité du système financier.

De même, l'OBA définit qu'il y a service dans le domaine du trafic des paiements lorsque l'intermédiaire financier "aide à transférer des monnaies virtuelles à un tiers pour autant qu'il entretienne une relation d'affaires durable avec le cocontractant ou qu'il exerce un pouvoir de disposition sur les monnaies virtuelles pour le cocontractant et qu'il ne fournisse pas le service exclusivement à des intermédiaires financiers soumis à une surveillance adéquate"[63]. Désormais, les fournisseurs de portefeuilles numériques et les plates-formes de négociation décentralisées sont donc aussi soumis à la LBA en tant qu'intermédiaires financiers, du moment qu'ils ont certaines possibilités de contrôle ou d'intervention sur les plates-formes ou les portefeuilles en question, aussi suivant l'interprétation du GAFI.

C'est par exemple le cas des plates-formes de négociation qui ne sont pas en possession de la clé privée des clients, mais qui permettent toutefois le transfert de monnaies virtuelles au moyen de *smart contracts* et peuvent ainsi confirmer, valider ou bloquer les ordres, ou exercer un contrôle d'un autre type grâce au *smart contract*. C'est aussi le cas des fournisseurs de portefeuilles numériques qui détiennent une clé, y ont accès et avec laquelle une signature est requise avant que la transaction puisse être effectuée avec succès (portefeuilles multisignatures). Les services de conservation sécurisée de clés privées peuvent aussi relever de la LBA, même si ces clés sont cryptées et ne peuvent en principe être décryptées que par les clients. Les risques encourus par les fournisseurs de portefeuilles numériques qui ne sont ni des fournisseurs de portefeuilles hébergés ni des prestataires de portefeuilles non hébergés purs résident dans le fait qu'il est possible de dissimuler l'origine des monnaies virtuelles en opérant des déplacements entre plusieurs de ces portefeuilles et au sein de structures d'adresses. Ces modifications ont été justifiées par le fait que l'intermédiaire financier n'a plus dans tous les cas le pouvoir de disposer seul des actifs, les modèles de transfert d'actifs étant

[59] FINMA, *Rapport annuel 2022*, mars 2023, p. 21
[60] FF **2020** 7559, *Loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués*, octobre 2020
[61] RS **958.1** – *Loi fédérale sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés* (Loi sur l'infrastructure des marchés financiers, LIMF)
[62] RS **958.11** – *Ordonnance sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés* (Ordonnance sur l'infrastructure des marchés financiers, OIMF)
[63] OBA, art. 4, al. 1 et 1bis, version du 1er août 2021; citation: Département fédéral des finances (DFF): *Ordonnance du Conseil fédéral sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués*, octobre 2020, p. 15

de plus en plus décentralisés[64]. Les fournisseurs de portefeuilles non hébergés purs, qui se contentent de mettre uniquement un logiciel à disposition, ne sont pas soumis à la LBA. Il peut s'agir par exemple de développeurs qui proposent seulement le téléchargement d'un logiciel, sans établir de relation d'affaires durable avec l'utilisateur. De même, les plates-formes de négociation qui mettent uniquement en contact des acheteurs et des vendeurs et organisent des transactions sans *smart contract* impliquant une possibilité d'accès de la plate-forme ne sont pas non plus régies par la LBA, puisqu'il s'agit là d'une activité d'intermédiation pure, sans transfert de monnaies virtuelles.

On a également complété l'OBA en ajoutant que l'émission de moyens de paiement à titre professionnel est considérée comme une activité d'intermédiation financière, et que les monnaies virtuelles utilisées comme moyens de paiement numériques ou prévues à cet effet par l'organisateur ou l'émetteur sont aussi soumises à la LBA[65]. Cette formulation apporte davantage de clarté sur le fait que l'émission d'AV dans le cadre d'ICO entre dans le champ d'application de la LBA. En élargissant la notion d'intermédiaire financier, la Suisse a mis en œuvre ce que le GAFI recommande aux pays de faire dans son "Actualisation du Guide Approche fondée sur les risques des actifs virtuels et des prestataires de services d'actifs virtuels", à savoir avoir une conception aussi large que possible de la définition de PSAV[66].

4.6.7 Surveillance de la FINMA en matière de blanchiment d'argent et modification de l'ordonnance de la FINMA sur le blanchiment d'argent

Fin août 2019, la FINMA a accordé pour la première fois à deux prestataires financiers de blockchain l'autorisation d'exercer respectivement à titre de banque et de négociant de valeurs mobilières. Comme il est d'usage pour les autres intermédiaires financiers, l'exercice de l'activité commerciale a été assortie de diverses conditions et exigences censées garantir une structure commerciale régulière. Déjà au cours de la procédure d'autorisation, la FINMA a accordé une attention toute particulière aux risques "crypto-spécifiques" notamment. Eu égard aux risques opérationnels, il a fallu définir des critères stricts et des processus de contrôle serrés. En vue de la conservation sûre des jetons, l'infrastructure technologique des deux requérants a été testée minutieusement, avec le soutien des examinateurs compétents, afin de prévenir les risques accrus que comportent les technologies de l'information (TI) ainsi que les cyberrisques. Dans le cadre des principes réglementaires de surveillance en vigueur en matière de lutte contre le BA, les prescriptions *Know Your Customer* (KYC) usuelles doivent également être respectées et les clarifications sur les transactions doivent être effectuées selon les règles.

Ces dernières années, les établissements assujettis à la surveillance de la FINMA ont proposé toujours davantage de services dans le domaine de la crypto-finance ou prévoient des offres de ce type. Forte de ce constat, la FINMA a analysé en 2021 diverses activités commerciales prévues dans ce domaine auprès des banques et vérifié les dispositions légales en matière de BA[67]. La FINMA a également précisé ses attentes relatives à l'audit des établissements qui œuvrent dans le domaine de la crypto-finance. En été 2021, elle a complété les cinq modules existants[68], qui sont utilisés de manière axée sur les risques pour les audits en vertu de la LBA, par un sixième module sur les AV et les PSAV[69].

---

[64] Ibid., p. 7
[65] OBA, art. 2, al. 3, let. b, LBA en relation avec l'art. 4, al. 1bis, let. c, OBA, version du 1er août 2021
[66] GAFI, *Actualisation du Guide "Approche fondée sur les risques des actifs virtuels et des prestataires de services d'actifs virtuels"*, juin 2022, pp. 24 à 40, notamment par. 91, p. 40
[67] FINMA, *Rapport annuel 2021*, mars 2022, p. 32
[68] *Booking centers*, règles d'identification, structures complexes, traitement approfondi des personnes politiquement exposées ainsi que *trade finance*
[69] FINMA, *Rapport annuel 2021*, mars 2022, p. 32

Le 1er janvier 2021, le seuil à partir duquel l'identification du cocontractant doit être vérifiée a été abaissé de 5000 à 1000 francs pour toute transaction ne constituant pas de transmission de fonds ou de valeurs et non liée à une relation d'affaires durable (art. 51*a* OBA-FINMA)[70], ce qui satisfait aux exigences formulées à la recommandation n° 15 du GAFI. L'adaptation du seuil reprend les recommandations du GAFI et tient compte des risques élevés dans ce domaine[71]. Ce seuil n'est pas seulement valable pour les transactions uniques, mais aussi lorsque plusieurs transactions paraissent liées entre elles. Le principal cas d'application de ce seuil de 1000 francs est le change dans des distributeurs automatiques d'AV. Cette règle a été reprise par les OAR auxquels sont affiliés les intermédiaires financiers exerçant une activité de PSAV. La révision partielle de l'ordonnance de la FINMA sur le blanchiment d'argent, entrée en vigueur le 1er janvier 2023, a en outre permis de préciser que le seuil de 1000 francs s'applique en cas de paiements en espèces ou d'acceptation d'autres instruments de paiement anonymes (comme les cryptomonnaies ou certaines cartes prépayées) pour la vente ou l'achat de monnaies virtuelles (art. 51*a*, al. 1bis, OBA-FINMA)[72]. Les intermédiaires financiers doivent en outre prendre des mesures techniques pour éviter que le seuil de 1000 francs ne soit dépassé dans les 30 jours par des transactions liées entre elles.

4.7 AV et PSAV en Suisse

Un aspect méthodologique important de la présente analyse de risques consiste à fournir une vue d'ensemble de la manière dont les AV sont utilisés en Suisse et dans quelle mesure. À cet égard, il est essentiel d'en savoir plus sur les prestations spécifiques au domaine des AV qui sont proposées en Suisse et qui sont utilisées dans notre pays et dans le monde. Il est également indispensable d'avoir des informations sur la fréquence de l'interaction du secteur des AV suisse avec le secteur économique et financier traditionnel[73].

Depuis la dernière analyse de risques sectorielle sur la présente thématique effectuée en 2018, l'utilisation générale d'AV a considérablement augmenté en Suisse, et le secteur des AV y est en forte croissance. Mais on manque largement d'indications précises sur la forme réelle que prend le secteur des AV en Suisse. Il existe néanmoins des indices concrets laissant penser que la Suisse fait partie des pays qui sont à la pointe dans ce domaine.

Traditionnellement, la place financière suisse joue un rôle capital de plaque tournante pour la finance internationale, notamment dans les secteurs de la gestion de fortune transfrontalière, de la réassurance mondiale, du négoce des matières premières et du financement de ce négoce (*trade finance*), sans compter que s'y trouve aussi la troisième bourse d'Europe[74]. La Suisse est aussi l'une des places financières les plus avancées dans le domaine des AV[75]. L'écosystème fintech et de la blockchain s'y est fortement développé, en particulier dans le domaine de la finance, et compte déjà plus de 1000 entreprises selon les chiffres du Secrétariat d'État aux questions financières internationales[76].

---

[70] RS **955.033.0** – *Ordonnance de la FINMA sur le blanchiment d'argent, OBA-FINMA*, art. 51*a*, version du 1er janvier 2021

[71] Il y a eu des cas concrets en Suisse de distributeurs automatiques de cryptomonnaies utilisés abusivement par certains réseaux criminels de narcotrafiquants pour effectuer des opérations; cf. par ex. *Tages Anzeiger*, *Schweizer Online-Drogenversand – «Hippe Kleider, Typ Studentin, und das Täschli voller Drogen»*, 18 mars 2021.

[72] OBA-FINMA, art. 51*a,* al. 1bis, version du 1er janvier 2023

[73] Banque mondiale, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, juin 2022, p. 14 s.

[74] Conseil fédéral, *Leadership mondial, ancrage en Suisse: Politique pour une place financière suisse tournée vers l'avenir*, décembre 2020, p. 5

[75] Secrétariat d'État aux questions financières internationales (SFI), *Feuille d'information crypto*, janvier 2022

[76] SFI, *Blockchain/DLT*, consulté en mai 2023; SFI, *Place financière suisse - Chiffres-clés 2023,* avril 2023, p. 13

La grande majorité de ces sociétés actives dans le secteur des AV ne sont toutefois pas des intermédiaires financiers au sens de la LBA. Elles offrent plutôt des logiciels, des conseils juridiques ou technologiques, ou d'autres services similaires qui sont à leur tour sollicités par d'autres sociétés (dont des intermédiaires financiers) de l'écosystème des AV (cf. fig. 4 au chap. 4.2). Il existe aussi plusieurs associations professionnelles qui ambitionnent d'élargir et de développer le secteur suisse des AV. En outre, bon nombre des principaux créateurs de cryptomonnaies du monde ont créé une fondation en Suisse (en fonction de leur capitalisation sur le marché)[77]. La plupart de ces fondations se trouvent dans le canton de Zoug. En 2022, ce dernier a enregistré une croissance nette de 25 fondations, dont 20 cryptofondations nouvellement créées[78]. L'essor des cryptofondations propulse Zoug au deuxième rang en termes de concentration du nombre de fondations par habitant (après le canton de Bâle-Ville)[79]. Les cryptofondations, souvent fortement capitalisées par les gains de change des AV qu'elles détiennent, financent des personnes physiques et morales ainsi que des projets qui visent à développer la blockchain sur laquelle elles se basent. Dans le cadre du présent rapport, l'Autorité fédérale de surveillance des fondations (ASF) n'a pas pu fournir d'indications concrètes sur le nombre réel de cryptofondations et sur leur bilan.

4.7.1 Informations sur les intermédiaires financiers exerçant une activité de PSAV en Suisse

La présente analyse de risques se concentre sur les intermédiaires financiers au sens de la LBA. En fonction de leur activité, ces établissements sont assujettis directement à la FINMA (par ex. les banques) ou ils doivent s'affilier à l'un des OAR reconnus et surveillés par la FINMA (cf. ch. 4.4.1).

	2018	2020	2022
Nombre d'intermédiaires financiers exerçant une activité de PSAV (établissements assujettis à la FINMA et membres d'OAR)[80]	Au moins 5[81]	Au moins 89	Au moins 204

Fig. 10 : Augmentation des intermédiaires financiers exerçant une activité de PSAV en Suisse de 2018 à 2022

Selon les renseignements fournis par la FINMA, il existait à fin 2022 au moins 204 intermédiaires financiers exerçant une activité de PSAV, dont 174 étaient affiliés à un OAR et 30 étaient assujettis à la FINMA[82].

[77] Par ex. Ethereum Foundation, Cardano Foundation, Tezos Foundation, Solana Foundation, Polkadot Foundation, etc.
[78] Centre d'études de la philanthropie en Suisse (CEPS) de l'Université de Bâle, SwissFoundations association des fondations donatrices suisses, Centre pour le droit des fondations de l'Université de Zurich, *Rapport sur les fondations en Suisse 2023*, juin 2023
[79] 30,7 fondations par 10 000 habitants, cf. Centre d'études de la philanthropie en Suisse (CEPS) de l'Université de Bâle, SwissFoundations association des fondations donatrices suisses, Centre pour le droit des fondations de l'Université de Zurich, *Rapport sur les fondations en Suisse 2022*, mai 2022, p. 8.
[80] Ces données reposent sur les informations de la FINMA et ont été complétées par des informations du MROS.
[81] Les informations recueillies dans le cadre de la présente analyse des risques montrent qu'en 2018, il existait en Suisse déjà au moins cinq intermédiaires financiers exerçant une activité de PSAV, alors que le deuxième rapport national sur les risques de blanchiment d'argent et de financement du terrorisme de 2021 faisait état de seulement deux intermédiaires financiers de ce type pour l'année 2018; cf. GCBF, *Deuxième rapport national sur les risques de blanchiment d'argent et de financement du terrorisme*, octobre 2021, p. 51.
[82] Selon les indications de la FINMA, à fin septembre 2023, 38 établissements assujettis à la FINMA exerçaient une activité de PSAV.

La FINMA a constaté que la plupart des banques se préoccupent de plus en plus de la question de la numérisation. Dans le cadre de l'adaptation ou de l'élargissement des modèles d'affaires, on peut observer une certaine dynamique à l'œuvre dans le négoce des AV, lors de l'ouverture d'interfaces (*open banking*) et sous la forme d'une collaboration accrue avec les compagnies d'assurance. Toutefois, on constate dans l'ensemble encore une certaine retenue dans l'adaptation stratégique des modèles d'affaires. Les établissements assujettis à la FINMA offrent toujours davantage de prestations liées à des valeurs patrimoniales virtuelles ou planifient d'inclure de telles offres dans leur catalogue de prestations. Les banques et les maisons de titres qui exercent actuellement des activités en lien avec les AV en Suisse s'occupent essentiellement de la conservation de jetons et du négoce pour le compte de la clientèle ainsi que du négoce pour compte propre, suivis de l'émission de produits et de prêts garantis.

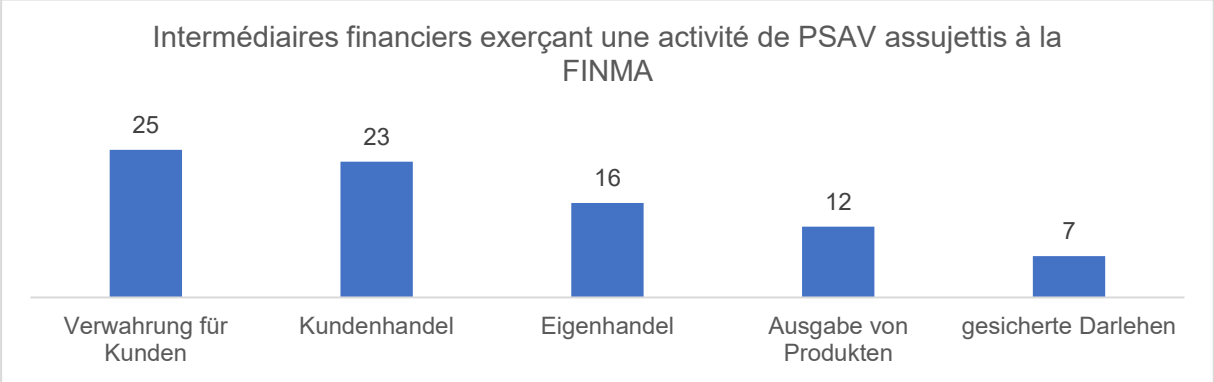

Fig. 11 : Services PSAV proposés par les banques et les maisons de titres exerçant des crypto-activités et assujetties à la FINMA (état à fin 2022)[83]

L'écrasante majorité des intermédiaires financiers suisses exerçant une activité de PSAV sont affiliés à un OAR. Selon les renseignements de la FINMA, les opérations de change (de fiat en AV et d'AV en AV) et les transactions d'AV sont les prestations principales de ces intermédiaires financiers et aussi les plus utilisées.

Les données les plus complètes à ce jour sur les activités commerciales des intermédiaires financiers suisses exerçant une activité PSAV sont rassemblées dans une étude publiée par divers acteurs privés et une haute école intitulée *Swiss Digital Asset Market Report 2022*. Pour cette étude, 81 entreprises ayant leur siège en Suisse ont été contactées, dont 47 ont participé à l'enquête[84]. Le volume des transactions pour l'année 2021 des 17 entreprises participantes qui proposent des opérations d'AV s'est monté à 41,2 milliards de francs suisses[85]. Seize entreprises interrogées ont proposé à leurs clients de conserver des AV. Onze d'entre elles ont accepté de divulguer leurs chiffres, dont il ressort qu'elles ont conservé des AV pour leur clientèle pour une valeur de plus de 13,2 milliards de francs suisses à fin 2021[86]. Comme seule une faible proportion des intermédiaires financiers exerçant une activité de PSAV en Suisse ont participé à l'étude, on peut partir du principe que le volume des transactions effectif et les AV conservés par tous les intermédiaires financiers de ce type sont en réalité beaucoup plus élevés. Il reste difficile de savoir dans quelle mesure les indications de ces quelques intermédiaires financiers exerçant une activité de PSAV sont représentatives des activités commerciales de l'ensemble de ceux-ci en Suisse.

[83] FINMA, *Rapport annuel 2022*, mars 2023, cf. p. 23.
[84] Home of Blockchain, *Swiss Digital Asset Market Report 2022*, mai 2022, p. 16
[85] Ibid., p. 25
[86] Ibid., p. 20

4.7.2 Informations sur l'utilisation d'AV en Suisse

D'autres études ont déjà tenté de chiffrer les flux financiers transfrontaliers d'AV à destination ou en provenance de la Suisse au moyen de diverses méthodes de calcul. La société d'analyse de blockchain Chainalysis a placé la Suisse au quatorzième rang sur 154 du *DeFi Adoption Index* pour l'année 2021[87]. Sur la liste européenne du *Global Crypto Adoption Index,* la Suisse figurait à la sixième place en 2021 et à la septième place sur 30 en 2022[88]. Selon les auteurs de l'étude, des AV pour une valeur de plus de 60 milliards de dollars ont été transférés de Suisse vers des plates-formes de FiDé et de FiCe entre juillet 2020 et juin 2021[89].
Ces chiffres se situent dans le même ordre de grandeur que les résultats d'une étude menée chaque année par la Haute école de Lucerne, qui évalue le volume commercial mondial des opérations effectuées depuis la Suisse vers des plates-formes d'AV[90].

	2020	2021	2022
Bourses d'AV centralisées (CHF)	92,6 milliards	81,2 milliards	50,3 milliards
Bourses d'AV décentralisées (CHF)	4 milliards	5,1 milliards	1,5 milliard
Total (CHF)	**96,6 milliards**	**86,3 milliards**	**51,8 milliards**

Fig. 12 : Volume estimé des transactions effectuées depuis la Suisse vers des plates-formes mondiales d'AV (FiCe et FiDé) de 2020 à 2022

La part du volume commercial mondial d'AV détenue par la Suisse est toujours restée en dessous de 1 % ces dernières années. Comparés aux flux financiers dans d'autres secteurs, ces chiffres paraissent encore raisonnables : le volume commercial annuel de la bourse suisse SIX s'est monté à 1208 milliards de francs en 2022[91]. Il serait toutefois erroné d'en conclure que des chiffres en baisse depuis 2020 et toujours gérables équivaudraient à des risques de BA et de FT également en baisse et tout aussi gérables. Durant cette période, le nombre de communications de soupçons de BA en Suisse a beaucoup augmenté, tout comme la somme d'AV dérobés ou escroqués (cf. ch. 7.2).

En raison des méthodes de calcul utilisées dans les études précitées, les chiffres réels sont probablement nettement plus élevés[92]. En outre, les flux financiers en monnaie fiat qui sont en relation avec des transactions en AV ne sont pas pris en compte. Il n'y a pas d'estimations à ce sujet. De même, les chiffres ne révèlent pas à quels acteurs (personnes privées, entreprises ou intermédiaires financiers exerçant une activité de PSAV) ces flux financiers peuvent être attribués, et encore moins quelle est la part de chacun. Enfin, toutes les études susmentionnées donnent simplement une estimation de l'ordre de grandeur du secteur des AV suisse et montrent que l'utilisation d'AV en Suisse n'est plus cantonnée à un marché de niche.

[87] Chainalysis, *The 2021 Geography of Cryptocurrency Report*, octobre 2021, p. 55
[88] Ibid., p. 55; Chainalysis, *The 2022 Geography of Cryptocurrency Report*, septembre 2022, p. 29
[89] Chainalysis, *The 2021 Geography of Cryptocurrency Report*, octobre 2021, p. 55
[90] Cf. Institute of Financial Services Zug IFZ (Haute École de Lucerne), *Crypto Assets Study 2021*, p. 17 à 20, pour 2020 (données recueillies entre le 1er octobre 2020 et le 1er septembre 2021); cf. Institute of Financial Services Zug IFZ (Haute École de Lucerne), *Crypto Assets Study 2022*, p. 12, pour 2021 (données recueillies entre le 1er mai 2021 et le 30 avril 2022); cf. Institute of Financial Services Zug IFZ (Haute École de Lucerne), *Fintech Study 2023*, p. 63, pour 2022 (données recueillies entre le 1er janvier 2022 et le 31 décembre 2022).
[91] Cash, *Handelsvolumen an der SIX 2022 rückläufig*, 3 janvier 2023
[92] Chainalysis et la Haute École de Lucerne soulignent que les sommes calculées sont des indications minimales; cf. Institute of Financial Services Zug IFZ (Haute École de Lucerne), *Crypto Assets Study 2021*, p. 17; Chainalysis, *The 2021 Geography of Cryptocurrency Report*, octobre 2021, p. 5

L'augmentation des flux financiers découlant de l'utilisation d'AV est probablement aussi due aux nombreuses ICO lancées en Suisse. Les flux financiers induits peuvent toutefois être soit en AV soit en monnaie fiat, en fonction du projet. La FINMA a reçu plus de 400 demandes d'assujettissement depuis 2019 en lien avec le lancement d'ICO en Suisse. Le nombre réel d'ICO réalisées est probablement beaucoup plus élevé, car il ne s'agit pas de communications à caractère obligatoire, mais de demandes concernant un éventuel assujettissement au droit des marchés financiers (cf. ch. 4.4.3).

Il ressort des divers sondages effectués en Suisse que l'utilisation d'AV a nettement augmenté ces dernières années. Selon une enquête menée en 2018 sur le comportement en matière de placements en Suisse, 8 % des personnes interrogées avaient déjà acheté des AV. En 2022, cette proportion passait à 18 %[93]. Même si certaines de ces enquêtes doivent être considérées avec prudence, elles pointent néanmoins toutes vers une utilisation accrue des AV en Suisse[94]. Les résultats ne permettent toutefois pas de tirer de conclusions sur la fréquence des achats d'AV effectués par le biais d'intermédiaires financiers suisses ou étrangers. Les résultats montrent en revanche une corrélation évidente entre les achats d'AV effectués et l'âge des personnes sondées. Les personnes entre 18 et 49 ans ont très souvent indiqué avoir déjà acheté des AV ou envisager d'en acheter prochainement[95], un signe fort que la tendance observée ces dernières années à l'utilisation accrue d'AV va se poursuivre.

La plus ancienne cryptomonnaie, à savoir le bitcoin, peut être achetée dans tous les distributeurs de billets des CFF en Suisse depuis 2016[96]. À fin 2017, au moins 6000 personnes avaient déjà profité de ce service, dont la moitié régulièrement[97]. L'achat et parfois la vente de Monero, le *privacy coin* (cf. glossaire) le plus ancien et le plus important, est possible à plus de 60 ATM d'AV de notre pays, qui sont exploités par divers intermédiaires financiers suisses exerçant une activité de PSAV[98]. Désormais, il est même possible de payer ses impôts en AV dans certains cantons[99]. En mai 2022, la ville de Lugano a annoncé un partenariat avec le fournisseur de *stablecoin* Tether qui vise à accélérer l'utilisation de la technologie de blockchain et d'utiliser celle-ci comme base pour transformer l'infrastructure financière de la ville. Le projet prévoit que plus de 10 000 commerces et vendeurs de la ville acceptent le bitcoin comme moyen de paiement et que les services municipaux puissent être payés en bitcoins, en Tether et en LVGA, l'AV créé par la ville à cet effet[100].

Comme la liste non exhaustive de ces exemples le montre, les possibilités d'acquérir, de vendre ou d'utiliser des AV comme moyen de paiement pour divers services a fortement augmenté ces dernières années. D'autres exemples illustrent que cette hausse a aussi eu lieu dans des secteurs exposés à des risques spécifiques de BA. Il est ainsi possible de payer en AV dans de nombreux commerces, dont des bijouteries, des magasins de produits de luxe ou d'antiquités, des galeries d'art et des établissements d'hôtellerie et de restauration[101].

---

[93] Moneyland, *Wie legen Schweizer ihr Geld an?*, 22 avril 2020; Moneyland, *So investieren Schweizerinnen und Schweizer ihr Geld*, 19 juillet 2022

[94] D'autres enquêtes similaires diffèrent de quelques points de pourcentage vers le haut ou vers le bas, mais indiquent la même tendance de fond, par ex.: Banque Migros, *Les jeunes préfèrent les crypto-monnaies à l'or*, février 2020; Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, juin 2021.

[95] Ibid.

[96] Handelszeitung, *6000 Kunden kaufen bei der SBB Bitcoins | Handelszeitung*, 1er novembre 2017; Chemins de fer fédéraux (CFF), *Acheter un portefeuille papier bitcoin / CFF*, consulté en mai 2023

[97] Ibid.

[98] Coin ATM Radar, *Bitcoin ATM Map*, consulté en mai 2023

[99] Finews, *Tessiner dürfen ihre Steuern jetzt in Bitcoin zahlen*, 7 juillet 2022; Canton de Zoug, *Kanton Zug akzeptiert ab 2021 Kryptowährungen für Steuerzahlungen* (communiqué de presse), 3 septembre 2020

[100] City of Lugano, Tether, *Lugano's Plan B*, consulté en mai 2023

[101] Handelszeitung, *85'000 Händler in der Schweiz können nun Zahlungen mit Bitcoin und Ether annehmen*, 19 août 2021; pour un aperçu géographique, cf. Coinmap, *Crypto ATMs & merchants of the world*, consulté en mai 2023.

De même, il est possible d'acheter des sociétés ou des parts sociales avec des AV en Suisse[102]. Et il est également possible de fonder des sociétés avec des AV comme apport en nature (capital initial). Au début de 2023, près d'un demi-millier de sociétés ont été créées de cette manière en Suisse, dans les secteurs les plus divers et sans que leur activité soit forcément en lien avec des AV ou des services financiers.

On peut encore acheter des biens immobiliers avec des AV en Suisse[103]. L'Office fédéral chargé du droit du registre foncier et du droit foncier, de même que différents bureaux cantonaux du registre foncier, de notariat officiel et d'inspectorat du notariat indiquent que des biens immobiliers sont achetés avec des AV en Suisse[104]. Cependant, on ne dispose d'aucune donnée précise ni de la possibilité de relever ces données avec la base légale actuelle, car seuls les notariats ont accès aux termes du contrat concernant les modalités de paiement des achats immobiliers. En ce qui concerne l'utilisation d'AV dans les 21 casinos suisses concessionnaires et leur éventuelle offre de jeux en ligne, la CFMJ peut interdire certains moyens de paiement comme les AV, en vertu de l'art. 80, al. 3, de l'ordonnance du 7 novembre 2018 sur les jeux d'argent, si leur utilisation est incompatible avec les buts de la LJAr[105]. À ce jour, deux maisons de jeu se sont intéressées à l'utilisation d'AV. Selon la CFMJ, elles n'étaient toutefois pas en mesure de proposer une procédure leur permettant de remplir les exigences de la législation sur le BA. Au cours de l'année 2023, la CFMJ devait examiner si l'utilisation d'AV comme moyen de paiement dans les casinos suisses est compatible avec les buts de la loi et, si oui, à quelles conditions. Pour le moment, les AV ne sont pas acceptés comme moyen de paiement dans les maisons de jeu et les casinos.

La Suisse hébergeant la plus grosse place de négoce d'or du monde, on a dernièrement examiné si l'utilisation d'AV est courante dans les transactions commerciales autour du négoce et de la transformation de l'or en Suisse[106]. Interrogé dans le cadre du présent rapport, le Bureau central du contrôle des métaux précieux ne possède pas d'indices concrets sur l'utilisation d'AV par les essayeurs du commerce, les fondeurs et les acheteurs de produits de la fonte sous sa surveillance (état mai 2023). On ne sait pas si des transactions sont effectuées en AV dans la chaîne d'approvisionnement internationale de métaux précieux sous forme brute, qui sont acheminés dans les grandes raffineries (essayeurs du commerce). Il n'est pas exclu qu'un certain nombre des 800 à 1000 acheteurs de produits de la fonte actifs en Suisse utilisent des AV pour conclure leurs affaires.

[102] Cf. par ex. actionnariat, *Create a market for your shares*, consulté en mai 2023.
[103] Cf. par ex. bithome, *Buy and Sell Real Estate with Bitcoin or Cryptos*, consulté en mai 2023.
[104] Outre l'Office fédéral ont également été consultés le *Grundbuch- und Vermessungsamt* du canton de Bâle-Ville, l'Office du registre foncier du canton de Genève, le *Amt für Grundbuch und Geoinformation* du canton de Zoug, le Notariat de la ville de Zoug et l'Inspectorat du notariat du canton de Zurich.
[105] Cf. RS **935.511** – *Ordonnance sur les jeux d'argent* (OJAr), version du 1er janvier 2024.
[106] Le secteur suisse du négoce de métaux précieux occupe une place centrale au niveau mondial, et le négoce d'or une place prépondérante représentant près de deux tiers du négoce d'or mondial. La fonte de ce métal dans les fonderies suisses totalise environ 40 % des capacités de fonte mondiales. Parmi les neuf leaders mondiaux de la branche, quatre concentrent une partie très importante de leurs activités en Suisse; cf. GCBF, Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse (admin.ch), juin 2015, p. 101 s.

5. Acteurs, méthodologie et données utilisées

Ce chapitre détaille la méthodologie adoptée pour la présente analyse de risques dans le domaine des AV et tente de classifier les acteurs y ayant participé ainsi que les données et les informations utilisées.

5.1 Méthodologie

Les analyses de risques sont des processus itératifs, qui reposent sur un examen continu du paysage des risques. En répétant ces analyses et en comparant les résultats avec les estimations et les résultats précédents, on obtient de nouveaux éléments et on affine les appréciations qui pourront à leur tour être reprises dans l'analyse suivante. Cette itération permet d'augmenter la précision et la pertinence des résultats.

La méthode utilisée dans le présent rapport pour analyser les risques de BA et de FT est en adéquation avec les recommandations internationales relatives à l'exécution d'analyses de risques nationales[107]. L'appréciation du risque se fait au moyen de l'identification des menaces et des vulnérabilités ainsi que des facteurs d'atténuation des risques.

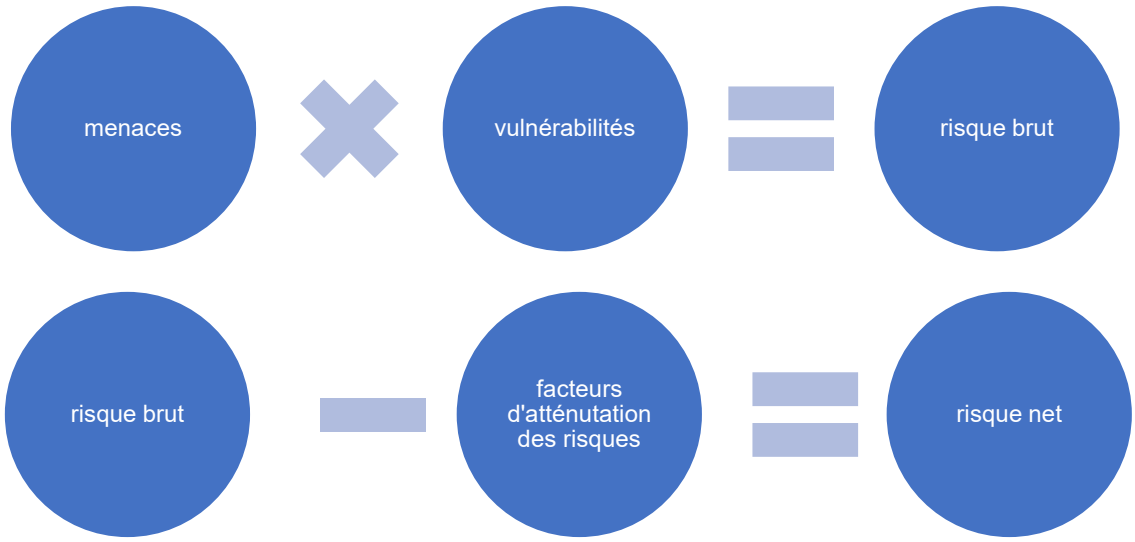

Fig. 13 : Schéma de la méthodologie utilisée pour apprécier les risques de BA et de FT

Les **menaces** désignent les risques et les dangers spécifiques au BA et aux activités de FT. Ces risques peuvent être générés aussi bien par des produits ou des services concrets que par des actes préalables au BA. Un exemple de menace posée par un produit ou un service concret est la possibilité d'effectuer des transactions anonymes. Les criminels peuvent ainsi plus facilement blanchir des fonds tirés d'activités illégales. Quant aux menaces que posent les actes préalables au BA, il y a par exemple le trafic d'armes illégal. Lorsqu'une organisation criminelle vend des armes illégalement, il en découle des risques accrus de BA et de FT, car

[107] Cf. GAFI, *Actualisation du Guide "Approche fondée sur les risques des actifs virtuels et des prestataires de services d'actifs virtuels"*, juin 2022; Banque mondiale, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, juin 2022.

en vendant ces armes, l'organisation peut blanchir des gains acquis illégalement ou utiliser ces gains pour financer des attentats terroristes.

Les vulnérabilités en revanche renvoient aux failles d'une organisation ou d'un système, qui peuvent être exploitées par des criminels pour des activités de BA ou de FT. Une vulnérabilité de ce type serait par exemple la base légale insuffisante en matière de surveillance des intermédiaires financiers, ou des processus de travail internes des intermédiaires financiers pas assez stricts (par ex. pour identifier leurs clients et leurs activités).

Dans l'ensemble, les menaces et les vulnérabilités peuvent toutes deux contribuer à accroître le risque de BA et de FT.

Les facteurs d'atténuation des risques sont tous les éléments qui contrebalancent le risque de BA et de FT, comme l'élaboration de processus de contrôle internes par les intermédiaires financiers afin de vérifier minutieusement leurs clients et leurs activités.

Risque brut et risque net : le risque brut se réfère au risque qui existe sans tenir compte de l'effet des facteurs d'atténuation des risques. Le risque net désigne en revanche le risque qui subsiste après que des mesures d'atténuation des risques ont été prises. L'objectif consiste à réduire le risque net à un niveau acceptable. Si ce risque résiduel est jugé inacceptable, l'analyse de risques doit déboucher sur des recommandations visant à concevoir et à mettre en place d'autres facteurs d'atténuation des risques afin de diminuer le risque net.

Les menaces et les vulnérabilités en lien avec les AV ont déjà été largement identifiées dans l'analyse de risques sectorielle de 2018 ainsi que dans l'analyse de risques nationale de 2021[108]. Eu égard aux changements considérables qui se sont produits dans le secteur des AV depuis 2018, le présent rapport examine si l'appréciation qui avait été faite est toujours valable et s'il est possible d'identifier de nouvelles menaces et vulnérabilités.
Selon le même procédé que dans l'analyse sectorielle de 2018, les changements intervenus dans les menaces et les vulnérabilités ainsi que les facteurs d'atténuation des risques identifiés sont mis en balance à la fin du rapport (cf. ch. 8).

[108] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowfunding*, octobre 2018; GCBF, *Deuxième rapport national sur les risques de blanchiment d'argent et de financement du terrorisme*, octobre 2021, p. 51 – 53

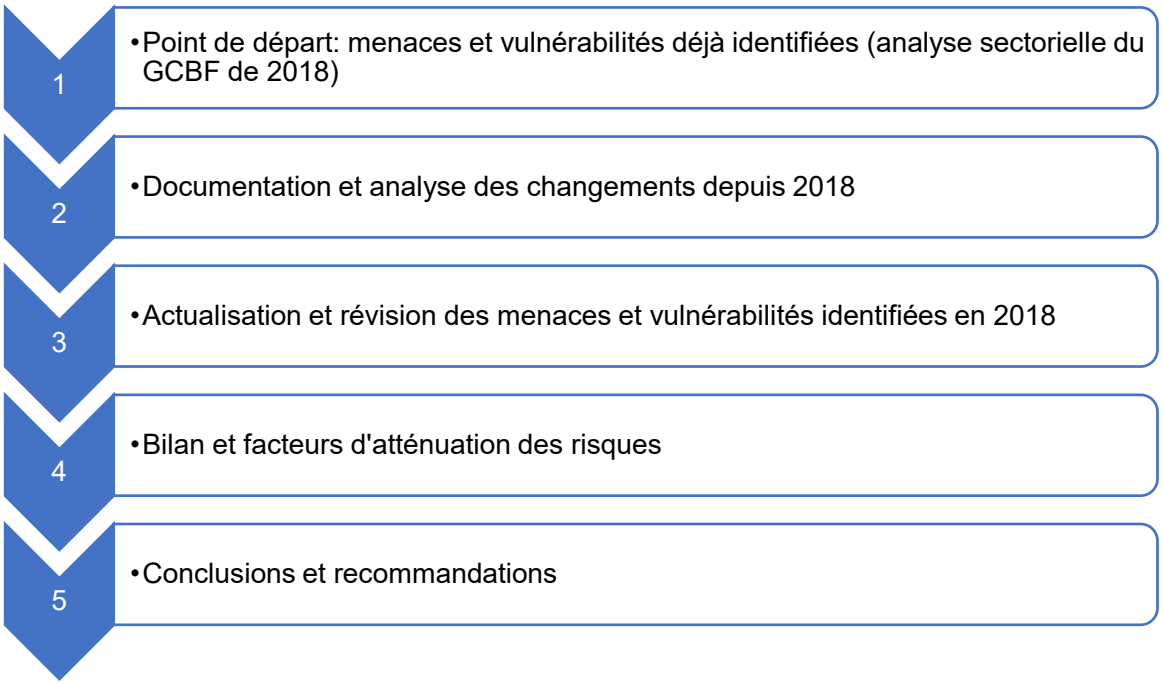

Fig. 14 : Schéma des étapes de travail suivies pour élaborer la présente analyse de risques

5.2 Acteurs et données utilisées

Le MROS a conduit l'élaboration de la présente analyse de risques. En tant que CRF, il réceptionne les communications de soupçons liés au BA et au FT qui lui sont transmises par les intermédiaires financiers et les analyse. Il décide si les informations qui en sont issues doivent être transmises à une autorité de poursuite pénale suisse. Le MROS occupe une position centrale dans le dispositif suisse de protection contre le BA et le FT. Divers offices et autorités potentiellement concernés par cette thématique ont participé à l'analyse de risques et y ont apporté des renseignements, des indications et leur expertise. Il s'agit de:

- certains bureaux cantonaux du registre foncier, notariats et inspectorats du notariat
- certaines autorités fiscales cantonales
- l'Office fédéral de la justice (OFJ)
- l'Office fédéral de la police (fedpol)
- le Ministère public de la Confédération (MPC)
- la Police judiciaire fédérale (PJF)
- l'Autorité fédérale de surveillance des marchés financiers (FINMA)
- la Commission fédérale des maisons de jeu (CFMJ)
- l'Administration fédérale des contributions (AFC)
- l'Autorité fédérale de surveillance des fondations (ASF)
- l'Office fédéral chargé du droit du registre foncier et du droit foncier (EGBA)
- le Bureau central du contrôle des métaux précieux (ZEMK)
- les ministères publics cantonaux
- les polices cantonales et municipales
- le Service de renseignement de la Confédération (SRC)
- le Centre national pour la cybersécurité (NCSC, devenu l'Office fédéral de la cybersécurité [OFCS] depuis le 1er janvier 2024)
- le Secrétariat d'État aux questions financières internationales (SFI)

Lorsqu'il s'agit d'effectuer des analyses de risques dans le domaine du BA et du FT, les principes méthodologiques et les procédures éprouvées d'organisations internationales comme le GAFI ou la Banque mondiale ont une importance primordiale. Selon leur méthodologie, il faut absolument faire preuve de minutie dans le relevé et l'analyse des données si l'on veut obtenir une appréciation des risques pertinente et nuancée[109]. Des intermédiaires financiers exerçant une activité de PSAV peuvent présenter un risque plus ou moins élevé, dépendant d'une multitude de facteurs, incluant les produits, les services, les clients, la géographie, les modèles d'affaires et la rigueur de leur programme de compliance. En conséquence, les pays devraient récolter et analyser des informations sur le nombre et le type d'intermédiaires financiers exerçant une activité de PSAV, les services qu'ils proposent et leurs activités commerciales. Disposer de données précises et complètes permet d'identifier et d'apprécier les risques avec précision dans le cadre de l'analyse et de développer des mesures adéquates pour les atténuer.

Dans le cas de la présente analyse de risques, le manque général d'informations sur les services et les activités spécifiques, en particulier dans le secteur des AV suisses, pose une difficulté d'ordre méthodologique. L'absence d'indications sur les services proposés et sur la fréquence de ces activités commerciales empêche une appréciation détaillée des risques posés par certains modèles d'affaires (par ex. conservation d'AV pour des clients, change de monnaie fiat en AV, etc.).

Afin de surmonter cette difficulté et de livrer tout de même une appréciation des risques fondée, nous avons utilisé une combinaison de sources de données disponibles, de démarches coopératives avec les autorités suisses et étrangères concernées et d'estimations pour effectuer cette analyse des risques. En appliquant les méthodologies éprouvées de la Banque mondiale et du GAFI et en les adaptant aux spécificités du secteur des AV suisse, nous avons pu évaluer les risques de BA et de FT de manière appropriée malgré les données restreintes dont nous disposions.

Nous avons pu récolter des informations sur la fréquence générale de l'utilisation d'AV et des services (financiers) proposés en Suisse dans ce domaine par le biais de divers sondages, articles de presse, études spécialisées sur le secteur des AV suisse et d'autres sources disponibles (dont des rapports internationaux qui contenaient des informations sur notre pays). Quant à l'utilisation d'AV en Suisse à des fins criminelles en général, et plus spécifiquement à des fins de BA et de FT, nous avons trouvé des informations par exemple dans les rapports annuels de fedpol, les rapports du NCSC ainsi que d'autres sources publiques comme la Statistique policière de la criminalité ou des articles de presse.

Des sources et des banques de données non officielles ont également été analysées, dont nous avons pu tirer des conclusions sur l'utilisation criminelle d'AV en Suisse en général, et à des fins de BA et de FT en particulier. Au niveau fédéral, nous avons passé en revue les procédures menées par le MPC et les enquêtes préalables de la PJF en la matière, dont le contenu a permis de conclure à l'utilisation d'AV aux fins générales et particulières précitées. Ces procédures contiennent des infractions dans le domaine de la grande criminalité et relèvent par conséquent de la compétence de la Confédération. Au niveau des cantons, nous avons analysé la banque de données intercantonale PICSEL (Plateforme d'information de la criminalité sérielle en ligne), qui contient la collection numérique des dénonciations pénales dans le domaine de la criminalité sur Internet, dans le but de favoriser la priorisation et la coordination des autorités de poursuite pénale dans la lutte contre la cybercriminalité[110]. Le nombre d'incidents et le montant du préjudice y sont notamment saisis. Ces données ne

[109] GAFI, *Actualisation du Guide "Approche fondée sur les risques des actifs virtuels et des prestataires de services d'actifs virtuels"*, juin 2022, p. 11-12; Banque mondiale, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, juin 2022, p. 14 s.

[110] Opérationnelle depuis avril 2021, la banque de données est actuellement utilisée par les neuf cantons suivants: Argovie, Fribourg, Genève, Grisons, Jura, Neuchâtel, Tessin, Vaud et Valais. Au moins un canton supplémentaire s'ajoutera bientôt à la liste (état mai 2023).

fournissent toutefois qu'une vision partielle de la situation, car moins de la moitié des cantons exploitent activement cette banque de données. En analysant les dénonciations enregistrées qui présentent un lien avec des AV, nous avons pu distinguer certaines tendances sur l'utilisation et le vol d'AV dans le domaine de la criminalité numérique en Suisse.

Le principal volume de données non public qui a été compilé pour cette analyse de risques est constitué par les communications de soupçons reçues par le MROS et les autres données dont il dispose. Les informations issues de ces communications, de l'échange d'informations international et d'autres banques de données du MROS peuvent fournir des indices concrets sur l'utilisation présumée d'AV à des fins de BA et de FT en Suisse. Dans son ensemble, l'analyse des informations dont dispose le MROS permet d'identifier les caractéristiques et les typologies en la matière, ainsi que les schémas récurrents et les modes opératoires typiques de cette forme de criminalité. À un niveau supérieur, ces informations aident aussi à résoudre la question de savoir dans quelle mesure les éléments connus du MROS sont représentatifs des opérations qui se déroulent dans le secteur des AV suisse. Enfin, évaluer le chiffre connu par rapport au chiffre noir, à savoir la proportion non découverte des opérations de BA et de FT dans le secteur des AV en Suisse permet également d'identifier des vulnérabilités spécifiques qui pourraient créer des angles morts dans ce secteur par rapport à certains phénomènes typiques de cette criminalité[111]. Par ailleurs, dans le cadre de la présente analyse, un échange d'informations a eu lieu avec des spécialistes de la poursuite pénale[112] et diverses autres autorités de surveillance[113]. À l'aide des indications d'ordre qualitatif et parfois quantitatif qui nous ont été données, il est possible de distinguer certaines tendances à l'œuvre dans l'utilisation d'AV à des fins criminelles aussi bien générales que particulières. Nous pouvons ainsi tirer des conclusions générales sur les chances et les défis actuels des autorités de poursuite pénale suisses pour élucider les infractions en relation avec l'utilisation d'AV. Ces entretiens nous ont non seulement permis d'engranger des connaissances, mais aussi de dresser un état des lieux des facilités et des difficultés qui existent aujourd'hui dans le secteur des AV pour les divers offices et autorités chargés de la lutte contre le BA et de FT. Nous nous sommes adressés en priorité aux autorités qui ont déjà une certaine expérience dans ce domaine selon les informations fournies.

Afin de pouvoir nous faire une idée globale de l'éventail des risques induits par les AV, nous nous sommes servis des analyses de risques effectuées par d'autres pays et des rapports annuels des autorités de surveillance et des bureaux de communication étrangers. Ceux-ci comportent des indices sur les tendances et les évolutions qui peuvent influencer les risques dans le secteur des AV suisse. Les rapports des organisations et des corporations internationales comme le GAFI livrent également des indices, ainsi que ceux d'entreprises privées, par exemple dans le domaine de l'analyse de blockchain. Ils contiennent de plus des informations et des chiffres importants sur les cas et les schémas découverts, ainsi que sur les champs de risques déjà identifiés en lien avec le BA et le FT dans le secteur des AV. Grâce aux sources précitées, nous obtenons un tableau aussi complet que possible de la globalité des risques, mais aussi des menaces et vulnérabilités qui existent très probablement en Suisse.

Enfin, il reste à souligner que nous avons trop peu de données pour quantifier avec précision les menaces et les vulnérabilités identifiées ainsi que les risques nets des activités spécifiques des intermédiaires financiers dans le secteur des AV (par ex. la conversion de monnaie fiat en AV, la conservation d'AV pour la clientèle). Sans chiffres fiables (par ex. le volume des transactions, la valeur totale des AV conservés, le nombre et l'origine des clients), il n'est pas

[111] Le chiffre noir désigne la différence entre le nombre d'infractions effectivement commises et le nombre de cas enregistrés dans une statistique de la criminalité officielle (chiffre connu).
[112] Des échanges ont notamment eu lieu avec des collaborateurs du réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK) ainsi qu'avec des polices et des ministères publics cantonaux.
[113] Par ex. avec la FINMA, l'Autorité fédérale de surveillance des fondations (ASF), la CFMJ et le Bureau central du contrôle des métaux précieux (ZEMK).

possible de vérifier si les menaces, les vulnérabilités et les facteurs d'atténuation des risques identifiés ont une incidence sur les risques de BA et de FT liés à ces activités commerciales et, le cas échéant, à quel point. De même, il n'est pas possible non plus d'évaluer dans quelle mesure les cas (suspects) déjà découverts dans des activités commerciales spécifiques sont représentatifs des opérations dans ce segment commercial.

6. Panorama global des risques

Bon nombre des menaces et des vulnérabilités rendant les AV susceptibles d'être utilisés à des fins de BA ou de FT sont dues à la conception technologique de ces derniers ou aux caractéristiques de ce secteur mondial. Ce constat vaut pour tous les pays – et pas seulement la Suisse[114]. Par conséquent, le présent chapitre aborde le contexte global dans lequel s'inscrit l'utilisation des AV. Il s'agira notamment de fournir un aperçu d'ensemble du secteur des AV et d'évoquer les principaux changements intervenus dans ce domaine depuis la dernière analyse sectorielle des risques de 2018.

6.1 Situation globale

Depuis 2018, l'utilisation d'AV a considérablement augmenté dans le monde entier, ce secteur ne cessant ainsi de gagner en importance. Du printemps 2020 à la fin de 2021, le secteur des AV a connu une phase de croissance. La capitalisation boursière de l'ensemble des AV est passée d'environ 830 milliards de dollars en 2018 à quelque 2400 milliards en mai 2021[115]. Des estimations indiquent que le nombre d'utilisateurs a presque triplé entre 2018 et 2020, passant de 35 millions à plus de 100 millions[116].

Le secteur des AV a bénéficié d'une forte attention médiatique et politique, attirant ainsi de nombreux acteurs supplémentaires. Par exemple, l'annonce par certains pays de leur intention d'accepter le bitcoin comme monnaie légale, voire comme monnaie de réserve, a eu un grand écho[117]. Des entreprises connues ont également déclaré vouloir convertir une partie de leurs réserves de liquidités en bitcoins[118]. De plus, plusieurs grandes banques, gérants de fortune et prestataires de services de paiement opérant à l'échelle mondiale ont fait savoir qu'ils allaient intégrer dans leur offre de services la conservation d'AV et des produits d'investissement en AV[119].

Malgré la chute des prix des AV au cours de 2021, leur utilisation n'a pas reculé. À la fin de 2022, alors que le secteur des AV était de nouveau en perte de vitesse, la bourse d'échange de cryptomonnaies Coinbase comptait à elle seule plus de 103 millions de clients vérifiés, alors qu'ils n'étaient que 56 millions en avril 2021[120]. Des études tablent sur le fait que plus de 10 % de la population mondiale, soit jusqu'à un milliard de personnes, utilisera des AV en 2030[121].

Parallèlement à la croissance du nombre d'utilisateurs, il semble qu'une consolidation se soit produite concernant l'offre de services d'AV centralisés, permettant à certaines grandes bourses d'AV d'augmenter leurs parts de marché[122]. Compte tenu de ces évolutions, la société d'analyse de blockchain Chainalysis a prédit en février 2021 que ces entreprises devront à l'avenir vérifier plus rigoureusement leurs flux financiers, leurs clients et leurs partenaires, afin

---

[114] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 37.
[115] CoinMarketCap, *Global Cryptocurrency Market Charts*, consulté en mai 2023
[116] Cambridge Centre For Alternative Finance (CCAF), *3rd Global Cryptoasset Benchmark Study*, septembre 2020, p. 12
[117] BBC News, *Bitcoin: pourquoi la Centrafrique a adopté la monnaie numérique*, 8 juin 2022; New York Times, *In Global First, El Salvador Adopts Bitcoin as Currency*, 7 septembre 2021
[118] Bloomberg, *Tesla Trails Only MicroStrategy in Treasury Bitcoin Allocation*, 8 février 2021
[119] New York Times, *Banks Tried to Kill Crypto and Failed. Now They're Embracing It (Slowly)*, 1er novembre 2021
[120] Cf. Curry David, *Coinbase Revenue and Usage Statistics (2023)*, 28 mars 2023
[121] Finews, *1 Milliarde Krypto-Nutzer bis ins Jahr 2030*, 25 juillet 2022; Nasdaq, *Blockware Estimates 10% Global Bitcoin Adoption By 2030: Report*, 9 juin 2022
[122] Chainalysis, *Cryptocurrency Exchanges in 2021*, novembre 2021, pp. 3 à 10; Barron's, *The Cryptocurrency Crash Could Lead to a Wave of M&A*, 23 juin 2022

de ne pas compromettre leur position sur le marché et de réduire les risques de BA et de FT[123]. Depuis lors, plusieurs grands intermédiaires financiers avec activité de PSAV aux États-Unis et en Europe ont effectivement reçu des amendes s'élevant à deux voire trois millions de dollars, notamment parce qu'ils n'avaient pas pris suffisamment de dispositions contre le BA et avaient négligé la communication de soupçons[124]. Des investigations ont révélé par exemple que ces intermédiaires financiers avaient autorisé entre autres des transactions avec des bandes de cybercriminels spécialisés dans les rançongiciels, des marchés du darknet et des individus, des entités ou des adresses sanctionnés[125]. Dans ce contexte, il convient de mentionner également le règlement MiCA de l'UE, qui vise à harmoniser la réglementation des AV au sein de l'UE et devrait entrer en vigueur dès 2024[126]. Depuis environ le début de l'année 2022, on constate que les intermédiaires financiers avec activité de PSAV au niveau international se voient imposer des mesures contraignantes par les autorités de régulation et de poursuite pénale bien plus qu'il y a encore quelques années[127].

6.2 Changements sectoriels globaux de 2018 à 2023

Depuis 2018, l'ensemble du secteur des AV a fondamentalement changé tant de par sa taille que de sa structure. Les rapports des organisations internationales et des sociétés spécialisées dans l'analyse de blockchain pointent les trois changements sectoriels ci-après au cours de ces cinq années: primo, la FiDé et la popularité des NFT qui en découle ont donné naissance à un nouveau domaine d'activité dans le secteur des AV; secundo, l'émergence de ce domaine d'activité a accru fortement l'utilisation des cryptomonnaies stables; tertio, la distribution géographique de l'utilisation d'AV s'est diversifiée dans le monde entier. Ces évolutions ont entraîné de nouveaux risques de BA et de FT, qu'il s'agit d'exposer sommairement dans la partie qui suit.

6.2.1 Portée accrue et risques accrus

Le secteur de la FiDé a engendré un tout nouveau domaine de services financiers d'AV. Dans ses activités, la FiDé s'appuie généralement sur des *smart contracts* plutôt que sur l'intermédiation financière traditionnelle (FiTrad ou finance centralisée [FiCe]). Elle repose sur un ensemble d'applications et de services financiers qui se trouvent sur une plate-forme de blockchain décentralisée. Les utilisateurs peuvent recourir aux services (par ex. crédits, produits d'investissement ou traitement des paiements) de ces plates-formes sans devoir s'enregistrer ni s'identifier, contrairement à l'usage en vigueur dans l'intermédiation financière. Cela tient au fait que les transactions effectuées via ces plates-formes ne sont pas traitées par un intermédiaire financier, mais par le code sous-jacent – autrement dit le *smart contract*.

---

[123] Chainalysis, *The 2021 Crypto Crime Report*, février 2021, p. 111

[124] Financial Crimes Enforcement Network (FinCEN), *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, 10 août 2021; Monroe Brian, *FinCEN, OFAC fine crypto exchange Bittrex nearly $30 million on AML, sanctions failings, missed SARs, links to darknet markets, mixers, ransomware gangs*, 11 octobre 2022; New York Times, *Coinbase Reaches $100 Million Settlement With New York Regulators*, 4 janvier 2023; Reuters, *Dutch central bank fines cryptocurrency exchange Coinbase 3.3 mln euros*, 26 janvier 2023; Reuters, *Dutch central bank fines Binance 3.3 million euros*, 18 juillet 2022

[125] Ibid.

[126] Parlement européen, *Crypto-actifs: feu vert à de nouvelles règles de traçabilité des transferts*, avril 2023

[127] Cf. par ex.: New York Times, *Government Cracks Down on Crypto Industry With Flurry of Actions*, 18 février 2023; Europol, *Bitzlato: senior management arrested*, 23 janvier 2023; Chainalysis, *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, 5 avril 2022; Chainalysis, *The 2023 Crypto Crime Report*, février 2023, p. 12.

En 2021, le volume des transactions *on-chain* (sur la chaîne) effectuées par l'ensemble des bourses d'AV décentralisées (*decentralized exchange* [DEX]) était systématiquement plus important que celui de toutes les bourses d'AV centralisées (*centralized exchange* [CEX])[128]. La popularité croissante de la FiDé est due à l'accès simplifié et à moindre coût à ces services financiers. Pour utiliser une plate-forme de FiDé, une connexion à Internet et un portefeuille d'AV suffisent. Les utilisateurs n'ont pas besoin de s'inscrire ni de passer par une procédure KYC[129], comme c'est le cas sur les plates-formes de FiCe, et restent donc non identifiés. Étant donné que ces plates-formes sont gérées par des *smart contracts* ou des logiciels, il n'y a pas non plus d'entité centrale pouvant arrêter les transactions, geler les comptes ou procéder à une communication de soupçons de BA. Il n'y a, de fait, pas non plus d'interlocuteur pour les régulateurs ou les autorités de poursuite pénale. De même, en l'absence d'intermédiaire financier (ou de PSAV), les AV déposés sur les plates-formes de FiDé restent sous le contrôle des utilisateurs. Ce contrôle n'est toutefois "garanti" que dans la mesure où il a été prévu ou programmé dans le *smart contract* sous-jacent.

En réalité, les failles que présentent ces *smart contracts* – et qui parfois y sont même sciemment intégrées – ont conduit à de nombreux piratages spectaculaires ou à des *rug pulls* (litt. "retirer le tapis de sous les pieds"), qui se sont soldés par le détournement de tous les AV déposés sur les plates-formes visées. Des rapports issus de l'analyse de blockchain chiffrent à quelque 162 millions de dollars le montant des AV volés en 2020 lors de piratages de plates-formes de FiDé. En 2022, cette somme a atteint un total de 3,1 milliards de dollars[130]. La croissance du secteur de la FiDé a ainsi créé pour les criminels de nouvelles opportunités juteuses de détourner des sommes colossales d'AV. Les montants subtilisés doivent toutefois être par la suite blanchis. La demande de techniques de blanchiment d'AV volés a donc augmenté en conséquence, tout comme les bénéfices potentiels pour ceux qui les vendent ou les proposent. La grande majorité des plates-formes de FiDé émettent leurs propres jetons, qui permettent à leurs propriétaires par exemple de percevoir une part des frais de transaction générés sur ces plates-formes. Il est intéressant de noter que les AV détournés lors des piratages visant la FiDé ont été blanchis essentiellement via d'autres plates-formes de la FiDé, c'est-à-dire en étant échangés contre d'autres AV. On estime qu'en 2021 et en 2022, près de la moitié des cryptomonnaies volées ont été transférées vers des plates-formes de la FiDé, ce qui montre clairement leur vulnérabilité au BA[131].

1re menace

Failles de sécurité des technologies sous-jacentes aux AV (identifiée en 2018, accrue en 2023)[132]

L'analyse sectorielle des risques de 2018 avait déjà identifié comme menaces les failles de sécurité que présentent les technologies liées aux AV et le blanchiment des AV acquis illégalement. Ces deux menaces semblent s'être accentuées en raison de la croissance significative de la FiDé, d'une part, et à cause des nombreux piratages, escroqueries et *rug pulls* dans ce secteur, d'autre part. Certes, les failles de sécurité qui touchent les AV ne sont pas plus graves qu'en 2018, mais comme le nombre d'AV s'est depuis lors démultiplié, les failles de sécurité sont plus nombreuses.

[128] Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6 juin 2022
[129] *Know Your Customer* (Connais ton client) désigne la procédure appliquée par les intermédiaires financiers afin de vérifier l'identité des clients, d'évaluer et de surveiller le risque client, et de prévenir les activités illégales comme le BA (cf. glossaire).
[130] Chainalysis, *The 2023 Crypto Crime Report*, février 2023, p. 58
[131] Ibid., p. 61; Chainalysis, *The 2022 Crypto Crime Report*, février 2022, p. 74
[132] Cf. GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, pp. 22 à 24.

La disponibilité de *stablecoins* est une condition importante au fonctionnement de la plupart des services de la FiDé. Leur utilisation a donc nettement augmenté ces dernières années. De 2018 à 2022, la part de *stablecoins* dans le volume mondial des transactions d'AV est passée d'à peine 10 % à environ 45 %[133]. Outre la demande de *stablecoins* par les applications de FiDé, cette hausse est notamment due, selon Chainalysis, à leur utilisation croissante dans les pays émergents, où ils sont de plus en plus utilisés pour les virements internationaux et l'épargne personnelle[134]. Les *stablecoins* ont permis un accès indirect à des devises comme le dollar américain ou l'euro dans le monde entier, ce qui a fortement augmenté la portée des AV et le nombre d'utilisateurs. Les *stablecoins* et les AV dotés d'une fonctionnalité de *smart contract* (notamment l'ethereum) – les deux moteurs décisifs en matière de FiDé – représentaient ensemble près de 90 % du volume total des transactions d'AV en 2022[135].

Le battage médiatique autour du "métavers" et du "Web3" (le web basé sur la blockchain) a également provoqué un engouement pour les NFT, autrement dit les *non-fungible tokens* (jetons non fongibles), qui sont des AV identifiables de manière univoque, possèdent des caractéristiques uniques et sont enregistrés sur une blockchain[136]. Les NFT peuvent représenter divers médias numériques comme des œuvres d'art, de la musique, des vidéos ou des jeux et sont souvent considérés comme des pièces de collection. Le droit de disposition sur un NFT – qui détermine quelle adresse de portefeuille d'AV peut envoyer ou vendre le NFT concerné – est inscrit sur la blockchain de manière cryptographique. À l'inverse du commerce traditionnel de l'art, les œuvres d'art NFT peuvent être négociées et échangées directement entre le donneur d'ordre et le bénéficiaire, sans qu'un intermédiaire financier ou une autre entité centrale (comparable au spécialiste qui certifie l'authenticité d'un tableau de Picasso) ne soient nécessaires pour en vérifier l'authenticité ou enregistrer le changement de propriétaire.

Le métavers, le Web3 et les NFT sont des éléments qui font partie du secteur croissant de la FiDé. Derrière ces termes, il y a la vision (ou parfois déjà la réalité) de l'émergence de nouveaux domaines d'activités dans le secteur des AV, qui attirent de nouveaux utilisateurs et font entrer dans la sphère d'influence de ce secteur des branches jusqu'ici indépendantes, comme l'art, la musique, les jeux ou le sport. En 2021, des milliards ont été dépensés pour des NFT, ce qui s'explique notamment par la popularité de divers projets du métavers et par la promotion des NFT par des personnalités et des entreprises célèbres[137]. Selon la société d'analyse de blockchain Elliptic, les cas de BA au moyen de NFT détectés jusqu'à présent sont rares[138]. Depuis 2017, 8 millions de dollars au total auraient été blanchis en AV via des plates-formes basées sur des NFT, ce qui ne représente qu'une part infime des opérations liées aux NFT. Ne correspondant qu'aux actes de blanchiment déjà détectés, ce chiffre doit être considérée comme une valeur minimale[139]. À l'instar des autres projets de FiDé, les plates-formes de NFT sont sujettes aux piratages, aux escroqueries et aux *rug pulls*. Selon Elliptic, des NFT d'une valeur de plus de 100 millions de dollars ont été dérobés entre juillet 2021 et juillet 2022 au moyen de divers systèmes de fraude[140]. Les NFT pourraient en outre être détournés à des fins de BA ou de FT, notamment pour le blanchiment de capitaux basé sur le commerce ou pour la plausibilisation de la provenance de valeurs patrimoniales, étant donné que l'estimation de la valeur d'un NFT est subjective et qu'il n'existe pas de normes pour la détermination de leur prix[141]. Toutefois, l'attrait des NFT à des fins de BA ou de FT est

[133] Chainalysis, *The 2022 Crypto Crime Report*, février 2022, p. 9
[134] Cf. Chainalysis, *The State of Web3 Report*, juin 2022, p. 3.
[135] Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6 juin 2022
[136] Un NFT n'est *jamais* interchangeable avec d'autres NFT.
[137] Elliptic, *NFTs and Financial Crime*, août 2022, p. 5
[138] Ibid., p. 4.
[139] Par exemple, selon Elliptic, 328,6 millions de dollars supplémentaires d'AV transférés vers des plates-formes de NFT provenaient de services de dissimulation comme les services de mixage, ce qui pourrait indiquer qu'il s'agit du produit d'activités criminelles, cf. ibid., p. 4.
[140] Ibid., p. 4 et pp. 12 à 35
[141] Elliptic, *NFTs and Financial Crime*, août 2022, pp. 77 à 79

actuellement relativement faible, du fait qu'ils font partie des AV les plus transparents : pour presque tout NFT, il est possible de consulter l'historique complet de son prix et les adresses de ses anciens propriétaires. En revanche, il existe des techniques plus établies et plus anonymes permettant de blanchir des AV (par ex. les *privacy coins* [cryptos privées] ou les *mixers* [mixeurs de cryptomonnaie], cf. encadré n° 4 au chap. 7.4.1), de sorte que les blanchisseurs d'argent ont actuellement peu intérêt à passer aux NFT[142]. Si la popularité des NFT augmente encore et que les nouveaux domaines d'activité précités liés aux AV continuent de croître, la portée du secteur des AV s'étendra en conséquence, tout comme se multiplieront les probabilités que les criminels exploitent les NFT à des fins de BA ou de FT.

6.2.2 Diversification géographique de l'utilisation des AV

Aujourd'hui, les AV semblent être utilisés par les individus les plus variés aux fins les plus diverses. Faute de chiffres fiables à cet égard, il existe des estimations pour certaines régions du monde concernant l'utilisation générale croissante des AV ces dernières années : sur les 20 pays les mieux classés dans le *Global Crypto Adoption Index* de Chainalysis figuraient seulement 2 économies nationales à haut revenu, à savoir les États-Unis et le Royaume-Uni[143]. La moitié de ces 20 pays se situaient dans la tranche inférieure des revenus moyens (Vietnam, Philippines, Ukraine, Inde, Pakistan, Nigéria, Maroc, Népal, Kenya et Indonésie) et les 8 restants dans la tranche supérieure des revenus moyens (Brésil, Thaïlande, Russie, Chine, Turquie, Argentine, Colombie et Équateur).

Les AV étant désormais utilisés dans le monde entier par un large éventail d'individus à des fins légitimes multiples, il est plus difficile d'identifier et de prévenir les risques de BA ou de FT. Il peut y avoir utilisation abusive d'AV dans les secteurs les plus divers et via différents canaux, ce qui complique la détection de certains risques spécifiques.

3e vulnérabilité

Manque de ressources et de capacités des institutions chargées de lutter contre le BA et le FT compte tenu des développements fulgurants dans le secteur des AV (identifiée en 2023)

L'évolution rapide du secteur mondial des AV exige que les changements survenus soient suivis de près dans le monde entier par les parties prenantes nationales et internationales chargées de lutter contre le BA et le FT, ainsi que par les organisations internationales. Ce n'est qu'ainsi que l'on pourra garantir une surveillance et une réglementation pertinentes du secteur, qui tienne compte des innovations et des changement constants et permette de réduire les risques de BA et de FT. À cet effet, il est essentiel que les parties prenantes nationales et étrangères ainsi que les organisations internationales disposent des ressources et des capacités requises. Cela comprend, par exemple, un accord sur la collecte, l'analyse et la mise à disposition des données relatives au développement économique et technologique du secteur, la formation du personnel chargé des enquêtes (pénales) dans le secteur des AV et une étroite collaboration entre les parties prenantes sur les plans national et international. Il semble que de telles ressources et capacités ne soient allouées nulle part dans le monde. Des différences marquées paraissent exister entre les pays ainsi qu'en leur sein, d'une part s'agissant de la disponibilité de ressources et de capacités et, d'autre part, pour ce qui est du niveau général des connaissances et de l'attention politique accordée aux risques de BA et de FT. Bien que les milieux politiques soient plus attentifs aux changements qui se produisent

[142] Ibid., p. 79
[143] Chainalysis, *The 2022 Geography of Cryptocurrency Report*, septembre 2022, p. 7

dans le secteur des AV (cf. chap. 6.3), le temps de réaction des parties prenantes et des organisations qui combattent le BA et le FT reste trop lent par rapport à l'évolution dynamique du secteur. Tant qu'on ne parvient pas à suivre le rythme d'évolution de ce dernier, il sera impossible d'apprécier de manière appropriée l'évolution des risques de BA et de FT et de les réduire.

6.3 L'utilisation criminelle d'AV suscite l'attention des milieux politiques

Divers rapports d'organisations internationales et d'autorités nationales attestent une progression de l'utilisation criminelle des AV. De façon plus générale, cela montre également que les autorités de surveillance et de poursuite pénale accordent davantage d'attention aux risques de BA et de FT dans ce secteur. Plusieurs rapports annuels et analyses des risques effectués par des CRF de divers pays mettent en garde contre le risque que les AV soient davantage utilisés à des fins de BA et de FT. Ils soulignent que l'attrait des AV réside dans la rapidité des transactions, les techniques de chiffrement utilisées et les moyens de transfert transnationaux en ligne, qui rendent la surveillance et la traçabilité difficiles, voire impossibles[144]. Diverses CRF ont constaté une tendance à la hausse du nombre de communications de soupçons liées à des AV au cours des dernières années[145]. Plusieurs NRA publiées préviennent contre des risques accrus en matière de BA et de FT et contre une plus grande probabilité d'abus[146]. La NRA de l'Estonie – un pays d'importance au niveau mondial pour les PSAV – a par exemple montré que la majorité des prestataires qui y sont installés ne contrôlent pas suffisamment leurs risques en matière de BA et de FT. Près de 75 % des plus de 250 PSAV implantés dans ce pays n'ont fait aucune communication de soupçons en 2021, mais des enquêtes ont montré qu'ils avaient largement négligé leurs obligations de diligence à cette période[147].

Selon le GAFI, les infractions liées aux AV concernent principalement le BA ou les infractions préalables au BA, bien que les criminels utilisent également les AV pour contourner les sanctions financières ou pour se procurer des fonds visant à soutenir le terrorisme. Les infractions signalées par les différents pays du GAFI comprennent notamment le trafic de stupéfiants et d'autres marchandises (par ex. armes à feu), l'escroquerie, l'évasion fiscale, la cybercriminalité, la distribution de matériel pédopornographique, la traite d'êtres humains, le contournement de sanctions économiques et le FT. C'est dans le domaine du trafic de stupéfiants que des infractions seraient le plus souvent constatées ; il s'agit de ventes réalisées directement en AV ou de l'utilisation d'AV à des fins de BA. Le second type d'abus le plus fréquent serait lié à l'escroquerie, aux rançongiciels, ainsi qu'à l'extorsion et au chantage. En outre, les réseaux professionnels de BA utiliseraient de plus en plus les AV comme instrument de blanchiment de valeurs patrimoniales[148].

---

[144] CRF (Allemagne), *Jahresbericht 2019*, juin 2020, p. 33; Financial Crimes Enforcement Network (FinCEN), *Advisory on Illicit Activity Involving Convertible Virtual Currency*, mai 2019, pp. 1 et 2

[145] CRF (Allemagne), *Jahresbericht 2019*, juin 2020, p. 46; CRF (Allemagne), *Jahresbericht 2021*, août 2022, p. 48; CRF (Pays-Bas), *Annual Review 2019*, juin 2020, p. 13; CRF (Pays-Bas), *Annual Review 2021*, juin 2022, pp. 7 et 27; CRF (Estonie), *Yearbook 2019*, 2020, p. 29; CRF (Liechtenstein), *Jahresbericht 2020*, mars 2021, p. 5; CRF (Liechtenstein), *Jahresbericht 2021*, avril 2022, p. 6; cf. Vedrenne Gabriel, *In Europe, Suspicious Payments Triple Thanks to VASPs, Cryptocurrency*, 25 octobre 2022.

[146] HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, décembre 2020, p. 70; Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France*, septembre 2019, p. 65; State Financial Service of Ukraine, *Report on the National Risk Assessment*, 2019, pp. 78 à 80; Government Of The Grand Duchy Of Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers*, décembre 2020, pp. 3 et 4

[147] CRF (Estonie), *The Risks related to Virtual Asset Service Providers in Estonia*, janvier 2022, p. 5

[148] GAFI, *Actifs virtuels - Indicateurs d'alerte de blanchiment de capitaux et de financement du terrorisme*, septembre 2020, p. 4

Encadré n° 3

Rançongiciels : attention politique accrue accordée aux AV

Un rançongiciel est un type de logiciel malveillant (maliciel) utilisé pour bloquer l'accès à des données ou à des systèmes en les chiffrant. Les hackeurs demandent ensuite une rançon aux victimes afin qu'elles puissent récupérer les données ou l'accès. Les attaques de rançongiciel ont nettement augmenté à l'échelle mondiale ces dernières années. Les assaillants exigent presque toujours de leurs victimes que la rançon soit payée en AV[149]. L'utilisation d'AV facilite la tâche à ces pirates chevronnés, qui peuvent ainsi dissimuler leur identité et leurs flux financiers. Par rapport au trafic de paiements traditionnel, les AV ont l'avantage – lorsqu'ils se trouvent dans un portefeuille non hébergé – de ne pouvoir être ni bloqués ni confisqués par des tiers.

L'attention politique portée aux AV s'est accrue ces dernières années, notamment parce que les attaques de rançongiciel se sont étendues dans le monde entier également aux institutions d'importance systémique sur les plans économique et infrastructurel, ainsi qu'aux grandes institutions financières[150]. De nombreux pays considèrent désormais les rançongiciels non seulement comme une cybermenace importante, mais également comme une menace pour la sécurité nationale[151].

Selon Chainalysis, le montant total d'AV envoyés à des adresses de rançongiciel connues a plus que quadruplé entre 2019 et 2020[152]. Il est intéressant de noter que la moitié de tous les AV envoyés depuis des adresses de rançongiciel connues à des intermédiaires financiers avec activité de PSAV, proposant la conversion d'AV en monnaies fiat (rampes de sortie de monnaies fiat), n'ont été expédiés qu'à 21 adresses, ce qui suggère une concentration et une organisation marquées dans le blanchiment des recettes provenant d'attaques de rançongiciel[153].

En Suisse, la population et les entreprises signalent les cyberincidents à l'OFCS, qui leur fournit, après analyse, une évaluation ainsi que des recommandations pour la suite de la procédure. D'après l'OFCS, il est très difficile de déterminer où vont les AV extorqués lors de ces attaques et qui sont les véritables bénéficiaires de ces paiements. Cela s'explique notamment par le fait que la mise à disposition de rançongiciels est désormais devenue une véritable prestation (*ransomware as a service*), ce type de maliciel étant loué ou vendu essentiellement sur le darknet à des "clients", qui n'ont pas besoin de disposer de connaissances informatiques. Cette évolution rend encore plus complexe la répartition des recettes ainsi générées, tout comme le traçage de ces flux de paiement. Jusqu'à présent, l'OFCS n'a pas recueilli de données sur le nombre et le montant des rançons versées. Il estime cependant que de nombreux cas où une rançon a été payée ne lui sont pas signalés.

En décembre 2022, le Conseil fédéral a annoncé vouloir introduire une obligation de signaler les cyberattaques contre les infrastructures critiques[154]. Le projet vise à créer les bases légales de l'obligation de signalement pour les exploitants des infrastructures critiques et à définir les tâches de l'OFCS (ancien NCSC), qui est prévu comme guichet unique de signalement des cyberattaques.

[149] GAFI, *Lutte contre le financement des rançongiciels*, mars 2023, p. 7
[150] Prestige Business, *Cyber-Attacken in der Schweiz nehmen auch 2023 zu*, 3 mai 2023
[151] CNET, *Ransomware rises as a national security threat as bigger targets fall*, 18 octobre 2021
[152] Chainalysis, *The 2023 Crypto Crime Report*, février 2023, p. 27
[153] Ibid., p. 50
[154] FF **2023** 84 – *Message du 18 janvier 2013 relatif à la modification de la loi sur la sécurité de l'information* (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques) du 2 décembre 2022

2e menace

Rançongiciels et maliciels (identifiée en 2018, en hausse en 2023)[155]
Le rapport sectoriel de 2018 indiquait déjà que les AV étaient un instrument apprécié des pirates perpétrant des attaques par rançongiciel. Par rapport à 2018, ces attaques ont pris une nouvelle dimension de par leur nombre, le montant des AV extorqués et les risques qu'ils représentent pour les infrastructures privées et publiques, le niveau de la menace s'en trouvant accru.

3e menace

Les AV comme moyen de paiement de biens et services illégaux (identifiée en 2018, en hausse en 2023)[156]

En 2023, les AV restent un moyen de paiement privilégié pour les biens et services illégaux sur Internet, par exemple pour acheter ou vendre sur le darknet des stupéfiants, des informations de cartes de crédit volées, ou même des rançongiciels ou d'autres logiciels malveillants[157]. Depuis 2018, les chiffres d'affaires sur les marchés du darknet sont passés d'environ 750 millions à 1,5 milliard de dollars[158].

En Suisse aussi, il y a des cas où des AV ont été utilisés comme moyen de paiement pour la vente organisée de stupéfiants[159]. La reconnaissance des risques dans ce domaine a conduit à une adaptation du seuil maximal fixé pour les transactions en monnaies virtuelles, qui est passé de 5000 à 1000 francs (art. 51*a* OBA-FINMA).

Il n'est certes pas clair dans quelle mesure l'utilisation d'AV comme moyen de paiement de biens et services illégaux a augmenté par rapport à la croissance générale du secteur des AV. Toutefois, il est prouvé que les AV sont utilisés plus fréquemment et de manière plus diversifiée comme un moyen de paiement, ce qui montre que la menace a augmenté.

6.4 Estimations des flux financiers mondiaux d'AV en lien avec le BA et le FT

A priori, il n'existe pas de chiffres fiables sur les flux financiers liés au BA et au FT dans le secteur des AV. Les estimations des sociétés d'analyse de blockchain sont souvent l'unique fondement sur lequel peuvent être tirées des conclusions quantitatives quant à l'utilisation d'AV à des fins de BA et de FT – c'est d'ailleurs l'une des raisons pour lesquelles elles sont citées dans la plupart des rapports annuels des CRF et dans les NRA. Bien qu'ils ne donnent qu'une idée de l'ordre de grandeur de ces phénomènes, les chiffres avancés par ces sociétés sont à prendre avec des pincettes à divers titres.

Premièrement, ce que les diverses sociétés d'analyse de la blockchain entendent par *crypto crime*, le terme général qu'elles utilisent, n'est pas clair, une définition précise des infractions et des paiements couverts par cette notion n'existant pas. Ainsi, il n'est pas clair non plus quels

[155] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 26
[156] Ibid., pp. 29 et 30
[157] Chainalysis, *The 2023 Crypto Crime Report*, février 2023, pp. 71 à 84
[158] Ibid., p. 71; Chainalysis, *The 2022 Crypto Crime Report*, février 2022, p. 100
[159] Cf. par ex. Tages Anzeiger, *Schweizer Online-Drogenversand – «Hippe Kleider, Typ Studentin, und das Täschli voller Drogen»*, 18 mars 2021

actes relevant du *crypto crime* pourraient être considérés comme des infractions préalables au BA selon la législation suisse. Dans son Crypto Crime Report de février 2022, Chainalysis a au moins précisé que les chiffres fournis ne concerneraient que les *cryptocurrency-native crimes* (autrement dit, les infractions liées à des cryptomonnaies), comme les ventes sur les marchés du darknet ou les attaques de rançongiciel. Il serait plus difficile de calculer quelle quantité d'argent liquide provenant de la criminalité "hors ligne", comme le trafic de drogue traditionnel, est convertie en cryptomonnaie dans le but de le blanchir.

Deuxièmement, on ignore dans quelle mesure la part de *crypto crime* dans le volume annuel de transactions d'AV est comparable aux flux financiers illégaux dans les autres secteurs.

Troisièmement, ces chiffres ont été corrigés a posteriori à la hausse, parfois de façon significative[160].

Quatrièmement, les activités criminelles, tout comme les adresses de portefeuilles d'AV qui leur sont associées, doivent déjà avoir été détectées : l'expérience montre que les rapports contiennent principalement des analyses sur les infractions commises dans le domaine de la cybercriminalité (rançongiciel, piratage, hameçonnage, fraude à l'investissement, etc.) et du commerce illégal de biens et services sur les marchés du darknet. Il semble évident que les paiements, par exemple dans les domaines du BA basé sur le commerce, de la corruption, de la traite d'êtres humains ou du FT, sont plus difficiles à repérer par les outils d'analyse de ces sociétés, à moins que des indices externes n'indiquent déjà leur nature répréhensible au pénal (couverture médiatique ou adresses de portefeuilles d'AV connues).

Cinquièmement, ces analyses ne tiennent pas compte de toutes les transactions hors de la chaîne, dont le volume est, selon les estimations, au moins dix fois plus important que celui sur la chaîne[161]. En ce sens, leurs analyses et leurs chiffres ne reflètent qu'une fraction des transactions d'AV effectives. Enfin, il n'est pas clair non plus si le recul de la proportion de transactions criminelles détectées est lié à une diminution générale des risques de criminalité dans le secteur des AV ou si, à l'inverse, la maturité croissante de ce secteur a incité les criminels à recourir davantage à des techniques de dissimulation sophistiquées – par exemple en utilisant des *privacy coins* (cryptomonnaies anonymes) qui échappent à la surveillance ou des mixeurs de cryptomonnaie et des bourses d'échange décentralisées.

Malgré ces incertitudes, il est généralement admis que les flux financiers d'AV d'origine criminelle sont en hausse. Chainalysis a estimé le total mondial de tous les AV reçus provenant d'adresses connues liées à des activités criminelles à plus de 20 milliards de dollars en 2022, contre 8 milliards en 2020[162]. À l'inverse, des AV pour un montant de quelque 23,8 milliards de dollars ont été transférés depuis ces mêmes adresses en 2022[163]. Ce chiffre représente une augmentation de 68 % par rapport aux près de 14,2 milliards de dollars de 2021[164]. Plus de la moitié de la valeur de ces AV a été transférée vers les grandes bourses d'échange. Les détenteurs des comptes concernés auprès de ces bourses d'échange étaient cependant des courtiers *over-the-counter* (OTC ou de gré à gré). Il s'agit d'intermédiaires financiers avec activité de PSAV, qui utilisent les plates-formes des grandes bourses d'échange pour leurs prestations (*nested services* ou services imbriqués, cf. encadré n° 4 au chap. 7.4.1). Ce chiffre devrait néanmoins interpeller, car c'est dans les grandes bourses d'échange que les AV peuvent être convertis en monnaie fiat et intégrer ainsi le circuit financier traditionnel. Les grandes bourses d'échange sont également les plus susceptibles de disposer d'importants

[160] McGuire Michael, *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy*, avril 2018, p. 4; Chainalysis, *The 2020 Crypto Crime Report*, février 2022, p. 4
[161] Cf. Jimenez Alison, 3 Misconceptions about Cryptocurrency Crime Estimates, 11 janvier 2022.
[162] Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12 janvier 2023
[163] Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26 janvier 2023
[164] Ibid.

départements de compliance, qui signalent les transactions concernées et prennent des mesures contre les utilisateurs impliqués.

Ces montants sont toutefois relativisés par le fait que la part de transactions d'AV ayant une origine criminelle connue, dont le BA et le FT, diminue par rapport au chiffre global de transactions d'AV. Selon la source considérée, cette part se situe entre 0,24 % (2022) et 3,3 % (2019)[165]. À titre de comparaison, l'ONU estime que la quantité d'argent blanchi dans le monde en une année représente de 2 à 5 % du PIB global[166]. Cependant, des analyses nationales des risques ainsi que des rapports consacrés à des thèmes similaires ont souligné que, malgré l'accroissement des risques, l'utilisation d'AV à des fins de BA était encore largement inférieure à celle des monnaies fiat et des méthodes plus traditionnelles[167].

Plusieurs explications peuvent être avancées pour expliquer la hausse nominale du montant global des transactions d'AV pouvant être d'origine criminelle et la baisse simultanée du pourcentage de ces transactions par rapport au volume total de transactions d'AV. De nombreux vols d'AV ont eu lieu pendant la montée des prix, de sorte que la valeur des AV dérobés a également augmenté pour ainsi dire d'elle-même. À l'inverse, la diminution relative pourrait s'expliquer par la réglementation croissante des grands acteurs, qui ont commencé à mieux contrôler leurs clients et à utiliser des outils d'analyse de blockchain visant à suivre les transactions. Il serait de toute façon surprenant et alarmant que l'utilisation criminelle des AV ait augmenté proportionnellement à la croissance spectaculaire du secteur.

Dans le domaine du *crypto crime*, le BA semble être l'infraction ayant *le* premier rôle : les AV obtenus illégalement par piratage, attaque par rançongiciel, escroquerie, ou vente de matériel pédopornographique ou de stupéfiants sur le darknet, doivent être blanchis à un moment donné, pour autant qu'ils soient destinés à intégrer le circuit légal. Rien qu'en octobre 2022, c'est-à-dire déjà après la forte baisse des prix des AV, 718 millions de dollars d'AV ont été détournés à la suite de 11 piratages de plates-formes de FiDé[168]. En 2022, le montant total d'AV obtenus par piratage a été estimé à 3,8 milliards de dollars[169].

[165] Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12 janvier 2023; Ciphertrace, *Cryptocurrency crime and anti-money laundering*, juin 2022, p. 5; TRM Labs, *Ensuring Responsible Development of Digital Assets; Request for Comment*, novembre 2022
[166] Office des Nations unies contre la drogue et le crime (UNODC), *Money Laundering*, consulté en mai 2023
[167] Par ex. Département du trésor des États-Unis, *National Money Laundering Risk Assessment*, février 2022, p. 41; Europol Spotlight, *Cryptocurrencies: Tracing the Evolution of Criminal Finances*, décembre 2021, p. 2
[168] Finews, *Chainalysis: Crypto Hacks Reach Record $3 Billion*, 13 octobre 2022
[169] Chainalysis, *The 2023 Crypto Crime Report*, février 2023, p. 56

4e menace

Blanchiment d'AV d'origine criminelle (en monnaie fiat) (identifiée en 2018, en hausse en 2023)[170]

Depuis 2018, des criminels ont exploité diverses failles de sécurité dans les protocoles et les plates-formes d'AV et se sont emparés illégalement de milliards d'AV. Afin d'injecter ces valeurs patrimoniales incriminées dans le circuit financier légal, ces milliards doivent être blanchis. La demande de moyens de blanchiment d'AV acquis illégalement a donc aussi fortement augmenté par rapport à 2018. Certains intermédiaires financiers avec activité de PSAV risquent davantage d'être utilisés pour blanchir ces AV qu'en 2018.

Par ailleurs, les piratages de plates-formes de FiCe et de FiDé semblent être le fait non seulement de pirates informatiques "ordinaires", mais également d'acteurs étatiques à des fins de financement de la prolifération. Selon plusieurs rapports du Groupe d'experts du Comité des sanctions contre la Corée du Nord publiés par le Conseil de sécurité des Nations unies, les recettes de ces piratages seraient utilisées pour soutenir le programme nord-coréen d'armes de destruction massive et de missiles balistiques[171]. D'autres rapports indiquent que le vol d'AV serait devenu l'une des principales sources de revenus de la Corée du Nord, qui obtiendrait ainsi jusqu'à un tiers des fonds destinés à son programme de missiles[172]. Pour l'année 2022, Chainalysis a pu établir que des AV pour un montant de 1,7 milliard de dollars étaient détenus par des groupes de pirates liés à l'État nord-coréen[173]. Cette somme représente plus de 10 % du PIB de la Corée du Nord[174]. En avril 2023, le groupe chargé des AV et des PSAV auprès du GAFI a souligné, en faisant directement référence à la Corée du Nord, que les pays du monde entier devaient d'urgence mettre en œuvre les normes du GAFI, car le risque d'utilisation abusive d'AV à des fins de BA, de FT et de financement de la prolifération était en augmentation[175].

Europol a observé un changement important dans l'utilisation criminelle des AV : celle-ci ne se limite plus aux activités de la cybercriminalité, mais s'étend désormais à tous types de méfaits nécessitant le transfert de valeurs monétaires[176]. Les infractions signalées par les pays du GAFI illustrent l'hétérogénéité de l'utilisation des AV par une grande variété d'acteurs aux fins criminelles les plus diverses.

Les AV semblent être utilisés également pour blanchir les revenus que les organisations criminelles tirent de leurs activités "hors ligne". En 2021, les autorités italiennes ont saisi plus de 80 millions EUR, une somme qu'un groupe de la Cosa Nostra sicilienne aurait blanchie par

[170] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 26 s.: le titre "Le blanchiment de crypto-assets d'origine illicite" désignait cette menace dans ce rapport de 2018. Afin de distinguer plus clairement celle-ci de la menace que constitue le "Blanchiment de monnaie fiat d'origine criminelle (en AV)" (titre de l'encadré à la p. 59 du présent rapport), ce titre a été reformulé ici "Blanchiment d'AV d'origine criminelle (en monnaie fiat)".

[171] Conseil de sécurité des Nations unies, *S/2022/668 Rapport de mi-mandat du groupe d'experts du comité 1718*, septembre 2022, pp. 75 à 78; Conseil de sécurité des Nations unies, *S/2022/132 Rapport du groupe d'experts du comité 1718*, mars 2022, p. 86; Conseil de sécurité des Nations unies, *S/2021/211 Rapport final du groupe d'experts du comité 1718*, mars 2021, p. 63 s.

[172] Financial Times, *How North Korea became a mastermind of crypto cyber crime*, 14 novembre 2022; Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, 13 janvier 2022; Coindesk, *'Ship-to-Ship' Trade and Other Secrets of North Korea's Illicit $1.5B Crypto Stash*, 7 avril 2020

[173] Chainalysis, *The 2023 Crypto Crime Report*, février 2023, p. 60

[174] En 2021, le PIB de la Corée du Nord était d'environ 16,4 milliards de dollars (cf. UNdata des Nations unies, *Democratic People's Republic of Korea*, consulté en mai 2023).

[175] GAFI, *Press Release - Virtual Assets Contact Group (VACG)*, 14 avril 2023

[176] Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, décembre 2021, p. 2

le biais d'un site de paris sportifs qu'elle contrôle et qui a obtenu une licence à Malte[177]. Le même système de blanchiment aurait été appliqué par d'autres organisations criminelles, comme la N'drangheta calabraise, la Camorra napolitaine, mais aussi des groupes de la criminalité organisée roumaine et chinoise[178]. Selon le NRA maltais sur les AV, les casinos en ligne du pays présenteraient des risques élevés en matière de BA et de FT[179]. Malte abrite environ 10 % des sociétés de jeux de hasard du monde entier[180]. Les recettes fiscales qui en découlent représentaient en 2019 près de 12 % du PIB maltais[181]. Les dépôts et les retraits via des portefeuilles électroniques, qui permettent souvent aussi les transactions d'AV, constituaient près de 10 à 15 % des chiffres d'affaires réalisés de 2019 à 2021[182]. On a aussi connaissance de cas où des AV ont été utilisés pour le versement de pots-de-vin, à des fins de FT par Al-Qaïda et l'État islamique (EI), mais également, par exemple, pour le BA par des cartels de la drogue sud-américains[183].

La taille et la portée du secteur des AV se sont fortement développées à l'échelle mondiale depuis 2018. Il semble qu'un nombre nettement plus important de personnes utilisent des AV dans le monde, bien qu'on ignore dans quelle mesure leur utilisation criminelle a progressé en parallèle. Les estimations susmentionnées sont donc à considérer comme des valeurs minimales. L'augmentation des communications de soupçons de blanchiment d'argent dans divers pays indique toutefois que l'utilisation d'AV à des fins de BA et de FT est plus fréquemment présumée qu'il y a encore quelques années – cette croissance pouvant s'expliquer également par une réglementation et une sensibilisation accrues des PSAV. Cependant, les rapports de plusieurs pays, d'organisations supranationales et de sociétés d'analyse de blockchain montrent clairement que l'utilisation criminelle des AV s'est généralement accrue.

Par ailleurs, l'utilisation criminelle d'AV semble s'être diversifiée. Depuis longtemps, les AV ne se limitent plus au domaine de la cybercriminalité ; ils sont également utilisés dans le cadre des infractions les plus diverses "hors ligne". Il n'existe toutefois pas de chiffres consolidés à cet égard, ce qui rend difficile l'estimation de la fréquence à laquelle des valeurs patrimoniales acquises illégalement dans les domaines "traditionnels" de la criminalité sont blanchies au moyen d'AV, ainsi que de l'importance des montants concernés. La détection de ces opérations semble être un défi de taille pour les sociétés d'analyse de blockchain et les PSAV, de sorte qu'il devrait y avoir un nombre colossal de cas non détectés.

[177] Organized Crime and Corruption Reporting Project (OCCRP), *Italian Mafia Bets on Illegal Online Gambling*, 4 mars 2021; Süddeutsche Zeitung, *Wieso die Mafia Fan von Maltas Online-Casinos ist*, 18 décembre 2022
[178] L'avvenire di Calabria, *Boom delle scommesse online, ma per la Dia c'è l'ombra dei clan*, 23 janvier 2020
[179] National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (Malte), *Key Results of the Sectoral Risk Assessment on Virtual Financial Assets*, février 2020, p. 12
[180] Forbes, *Scandals And Mafia Allegations May Force Malta To Reconsider Its Reliance On Online Betting*, 13 mars 2021
[181] Ibid.
[182] Ibid.; Malta Gaming Authority, *Annual Report 2021*, septembre 2022, p. 79
[183] Cf. Stalinsky Steven, *The Coming Storm – Terrorists Using Cryptocurrency*, 21 août 2019; Département de la justice des États-Unis, *Two Chinese Intelligence Officers Charged with Obstruction of Justice in Scheme to Bribe U.S. Government Employee and Steal Documents Related to the Federal Prosecution of a PRC-Based Company*, 24 octobre 2022; Chainalysis, *The 2022 Crypto Crime Report*, février 2022, pp. 93 à 98; AP News, *Mexican cartels turn to bitcoin, internet, e-commerce*, 10 mars 2022; Europol, *Underground drug-money bank laundering EUR 180 million liquidated by law enforcement*, 13 avril 2023.

5e menace

Blanchiment de monnaie fiat d'origine criminelle (en AV) (identifiée en 2018, inchangée en 2023)[184]

Le rapport sectoriel de 2018 a identifié deux menaces liées à l'utilisation d'AV à des fins de BA : d'une part, le blanchiment d'AV d'origine criminelle (par ex. provenant du piratage d'une plate-forme d'échange d'AV) et, d'autre part, le blanchiment de monnaie fiat d'origine criminelle. S'agissant de la première menace, il existe des chiffres précis fournis par des sociétés d'analyse de blockchain, qui montrent que cette menace s'intensifie depuis 2018 (cf. 4e menace au chap. 6.4). Pour ce qui est de la seconde menace, on ne dispose pas de chiffres consolidés permettant de conclure à son aggravation ou à son atténuation. Toutefois, certaines informations relatives à l'utilisation d'AV à des fins de BA par des organisations criminelles montrent que cette menace ne s'est pour le moins pas atténuée, mais demeure stable.

[184] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 30 s.: le titre "L'investissement d'argent d'origine criminelle dans les crypto-assets", qui désignait cette menace dans ce rapport de 2018, a été reformulé ici "Blanchiment de monnaie fiat d'origine criminelle (en AV)".

7. Évolution des risques en Suisse

Les menaces liées aux AV et les vulnérabilités qui en découlent pour la Suisse ont déjà été identifiées dans le rapport sectoriel de 2018 sur les risques de BA et de FT dans le secteur des AV. Deux catégories principales ont été établies : les menaces inhérentes aux technologies des AV et les menaces liées à l'utilisation frauduleuse d'AV[185].

Menaces inhérentes aux technologies des AV	**Menaces** liées à l'utilisation frauduleuse d'AV	**Vulnérabilités** de la Suisse face au risque de BA et de FT induit par les AV
1. Anonymat des transactions et identification difficile des ayants droit économiques	1. FT au moyen d'AV	1. Vulnérabilités des intermédiaires financiers qui effectuent des transactions d'AV
2. Failles de sécurité des technologies qui sous-tendent les AV	2. Utilisation d'AV comme moyen de paiement de biens et de services illégaux	2. Répression difficile du BA et du FT dans le secteur des AV
3. Menaces liées à l'effet de nouveauté et à l'inexpérience des utilisateurs	3. Recours aux AV dans le cadre d'attaques d'hameçonnage	
4. Maliciels et rançongiciels	4. Blanchiment de monnaie fiat d'origine criminelle (en AV)	
5. Blanchiment d'AV d'origine criminelle (en monnaie fiat)		

Fig. 15 : Menaces et vulnérabilités liées aux AV identifiées dans le rapport du GCBF de 2018[186]

Afin d'établir une comparaison avec les résultats de 2018, le présent chapitre met en évidence les changements déterminants intervenus dans la lutte contre le BA et le FT dans le secteur des AV en Suisse. Il s'agit ainsi d'examiner dans quelle mesure les menaces et les vulnérabilités identifiées en 2018 ont évolué ou si de nouvelles sont apparues. Pour discerner avec précision ces changements, il faut idéalement disposer de données statistiques sur les phénomènes spécifiques concernés. En raison du manque massif de telles données, la tâche s'avère très difficile, ce qui constitue déjà un risque en soi (cf. chap. 7.1).

Les communications de soupçons transmises au MROS et d'autres données dont il dispose ont constitué la principale base examinée dans le cadre de la présente analyse des risques, afin de mettre en évidence les évolutions. En font partie notamment les éléments issus de l'échange d'informations avec les bureaux de communication étrangers. Les demandes

[185] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, pp. 20 à 36

[186] Ibid. Pour plus de clarté, les titres ci-après du NRA de 2018 se référant à des menaces ont été modifiés comme suit: "Le blanchiment de crypto-assets d'origine illicite" est devenu "Blanchiment d'AV d'origine criminelle (en monnaie fiat)", "L'investissement d'argent d'origine criminelle dans les crypto-assets" est devenu "Blanchiment de monnaie fiat d'origine criminelle (en AV)", et "La vulnérabilité des intermédiaires financiers actifs dans les transactions en cryptomonnaie" est devenu "Intermédiaires financiers effectuant des transactions liées à des AV (en AV ou en monnaie fiat)" afin de faire apparaître l'accroissement de cette vulnérabilité (cf. 6e vulnérabilité).

d'informations et les informations spontanées adressées par les bureaux de communication étrangers à la Suisse, qui présentent un lien avec des AV ou des PSAV, ont aussi été étudiées à cet effet. Afin d'effectuer une analyse des risques approfondie de toutes les données à sa disposition, le MROS a pu utiliser avec succès de nouvelles méthodes d'examen, qui ne sont possibles que depuis l'introduction du système de traitement des données goAML (cf. chap. 11.1). Les examens effectués montrent notamment de façon univoque que depuis 2020, les AV font de plus en plus fréquemment l'objet de communications de soupçons.

En outre, une enquête a été menée auprès des différentes polices cantonales (et municipales) et des ministères publics dans le cadre de la présente analyse des risques et de la réponse aux postulats 22.3017 "Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies" et 22.3145 "Poursuites pénales en matière de cybercriminalité. Efficacité des cantons"[187]. D'une part, elle visait à demander aux destinataires des données quantitatives sur les procédures pénales déjà menées en lien avec des AV (par ex. nombre de procédures, infractions et sommes concernées, etc.). D'autre part, elle les priait de fournir des estimations qualitatives sur les défis et les opportunités que le secteur des AV représente pour le travail des autorités de poursuite pénale. Faute d'un suivi des procédures pénales liées à des AV, seule une petite minorité des autorités de poursuite pénale interrogées a été en mesure de délivrer des données consolidées. Les résultats quantitatifs de l'enquête sont donc fragmentaires et d'une pertinence limitée. Ils ne remplacent pas le besoin d'une vue d'ensemble nationale. De façon générale, les données obtenues semblent toutefois confirmer certaines hypothèses et tendances concernant l'utilisation criminelle des AV et le travail des autorités de poursuite pénale en la matière (cf. chap. 7.2 à 7.4). Outre les réponses reçues des autorités de poursuite pénale dans le cadre de l'enquête, des entretiens approfondis ont été menés avec diverses autorités suisses de poursuite pénale et de surveillance.

Des informations quantitatives supplémentaires ont pu être obtenues grâce à l'analyse d'autres bases de données des autorités suisses de poursuite pénale, dont notamment la banque de données PICSEL (Plateforme d'Information de la Criminalité Sérielle En Ligne)) et les investigations (préliminaires) menées par la PJF, dans lesquelles l'utilisation d'AV était un élément central des faits concernés et qui ont finalement abouti à l'ouverture d'une procédure. Outre l'enquête menée auprès des autorités cantonales de poursuite pénale, ce sont les conclusions de la PJF qui se sont avérées les plus fructueuses, d'où les multiples références qui y sont faites dans le présent chapitre. Les informations dont dispose le MROS ont également permis d'établir des typologies fondées sur des critères qualitatifs, qui montrent différentes formes et caractéristiques possibles des opérations de BA et de FT réalisées avec des AV. Ces informations reposent principalement sur les communications de soupçons transmises au MROS de 2020 à 2022 et illustrent diverses techniques utilisées à des fins de BA ou de FT.

7.1 Le manque de données : un risque inhérent

Alors qu'il n'existe que très peu de données relatives à l'utilisation générale des AV en Suisse, cette lacune est encore plus béante lorsqu'il s'agit de l'utilisation criminelle de ces derniers : notre pays ne dispose que de quelques données statistiques agrégées concernant l'utilisation d'AV dans le cadre d'infractions en général. Il y a donc d'autant moins de données quantitatives sur l'utilisation spécifique d'AV à des fins de BA ou de FT, pas plus qu'il n'existe de vue d'ensemble nationale des demandes d'entraide judiciaire émanant de l'étranger et ayant pour

[187] Cf. postulat 22.3145, *Poursuites pénales en matière de cybercriminalité. Efficacité des cantons*, déposé le 16 mars 2022 par le conseiller national Andri Silberschmidt; postulat 22.3017, *Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies*, déposé le 15 février 2022 par la Commission de la politique de sécurité CN. Les deux postulats ont été adoptés par le Conseil national en juin 2022. Le Département fédéral de justice et police (DFJP) est responsable de la réponse aux deux postulats.

objet des faits concernant des AV. La fréquence de ces demandes et les difficultés qu'elles représentent pour les autorités de poursuite pénale demeurent ainsi peu claires.

Le manque de chiffres concernant les flux financiers d'AV – dont peuvent faire partie également les flux financiers en monnaies fiat – n'est pas une particularité nationale. Étant donné que, contrairement au trafic de paiements traditionnel, les paiements en AV sont en principe effectués de façon anonyme (ou pseudonyme), il est difficile de déterminer où se trouvent les parties impliquées. Il n'est donc pas aisé de tirer des conclusions précises sur l'utilisation d'AV dans une zone géographique spécifique comme la Suisse. Dire que les blockchains sont "transparentes" n'est que partiellement vrai. De même, toute indication sur le volume réel d'AV n'est possible que dans une mesure limitée, car la plupart des transactions d'AV ont lieu hors de la chaîne et ne sont donc pas enregistrées sur la blockchain (sur la chaîne)[188]. Par exemple, les transactions internes des PSAV sont souvent effectuées hors de la chaîne. Outre la première couche ou "couche principale" des blockchains, qui est accessible au public, il existe également des protocoles de seconde couche. Il s'agit là de niveaux supplémentaires, qui s'appuient sur la blockchain d'origine et servent à améliorer l'extensibilité à réduire les coûts des transactions. Un exemple courant d'un tel protocole secondaire est le Lightning Network dans l'écosystème du bitcoin. Les transactions effectuées sur ces protocoles de seconde couche n'apparaissent pas immédiatement ou avec le même niveau de détail sur la blockchain. Elles contribuent ainsi à la complexité et au manque de transparence de l'ensemble du système et rendent difficile la traçabilité des flux financiers d'AV. Selon certaines estimations, seul un dixième environ de toutes les transactions d'AV effectives seraient enregistrées sur la chaîne[189]. La majeure partie des informations sur les transactions d'AV est stockée dans les diverses banques de données privées de différentes entreprises. Par conséquent, les grandes bourses d'AV centralisées sont probablement les mieux placées pour avoir une vue d'ensemble des flux financiers mondiaux d'AV. Ces données ne sont toutefois pas publiées.

Malgré ces défis, l'existence de transactions hors de la chaîne et de protocoles de seconde couche ne signifie pas que les autorités de poursuite pénale avancent à tâtons. Certes, des efforts et des ressources supplémentaires sont nécessaires pour remonter la piste des transactions, mais ce n'est pas forcément impossible. La transparence fondamentale du système est maintenue, malgré les couches supplémentaires qui en accroissent la complexité. Ainsi, les autorités de poursuite pénale sont toujours en mesure de détecter les activités criminelles, bien qu'elles aient besoin de capacités et de ressources appropriées, car le travail de détection exige une expertise et des instruments d'enquête adéquats et peut être chronophage. La transparence des blockchains n'est donc pas perdue, mais elle est plus difficile à pénétrer et nécessite des méthodes d'investigation adaptées.

Il est par conséquent difficile de mesurer l'ampleur exacte de l'utilisation d'AV dans les diverses régions de la planète et dans les différents pays. Le Fonds monétaire international (FMI) et la Banque centrale européenne (BCE) ont déjà attiré l'attention sur ce problème. Dès 2019, le FMI a proposé un échange international de données statistiques relatives aux transactions et à la capitalisation d'AV, afin de remédier à l'indisponibilité de ces données et de permettre des estimations macroéconomiques pertinentes[190]. La BCE a également recommandé de suivre de très près les évolutions et a souligné l'absence de données statistiques fiables sur la taille réelle du secteur des AV et sur les flux financiers correspondants[191]. Toutefois, ces recommandations n'ont pas encore été mises en œuvre. En 2022, le FMI a constaté qu'il était toujours difficile d'évaluer l'étendue de l'utilisation d'AV dans le système financier en raison de lacunes très importantes en matière de données – qui en outre rendraient difficile l'analyse

[188] Jimenez Alison, *3 Misconceptions about Cryptocurrency Crime Estimates*, 11 janvier 2022
[189] Von Luckner, Reinhart & Rogoff, *Decrypting New Age International Capital Flows, NBER Working Paper No. 29337*, octobre 2021, p. 1, ndbp 2
[190] Fonds monétaire international (FMI), *Treatment of Crypto Assets in Macroeconomic Statistics*, 2019, p. 3
[191] Banque centrale européenne (BCE), *Understanding the crypto-asset phenomenon, its risks and measurement issues*, mai 2019

des risques par les autorités[192]. Actuellement, il ne semble pas y avoir de consensus quant à la manière de classer les différents types d'AV et aux techniques de mesure à utiliser afin d'analyser, pour chaque pays, les activités économiques et les flux financiers du secteur des AV, lequel est intrinsèquement mondial. De plus, le FMI estime que les recommandations sectorielles pourraient être rapidement dépassées en raison des évolutions rapides dans ce domaine.

L'absence de données fiables sur le secteur des AV était déjà soulignée dans les rapports du GCBF de 2018[193] et de 2021[194]. Le présent rapport constate également qu'il n'existe pas de chiffres fiables, notamment pour la Suisse.

Les clarifications effectuées auprès de diverses autorités et organisations suisses montrent qu'il n'y a actuellement aucun suivi permettant de connaître la croissance du secteur, les revenus et les fortunes en cryptomonnaies imposés en Suisse, ou encore la fréquence et l'ampleur des flux financiers entrants ou sortants de la place financière suisse, qui sont liés à l'achat, à la vente ou à la conservation d'AV. Un suivi de ce type n'est pas non plus prévu actuellement au niveau national[195]. Étant donné les développements fulgurants qui ont marqué le secteur des AV ces dernières années, cette absence d'informations est devenue une vulnérabilité importante, car des évolutions inattendues dans le domaine du BA et du FT pourraient ainsi rester longtemps indétectables.

4e vulnérabilité

Statistiques et chiffres insuffisants aux niveaux national et international (identifiée en 2023)

Compte tenu des évolutions fulgurantes des cinq dernières années, il peut s'avérer problématique de ne pas disposer de données globales tant à l'échelle nationale qu'internationale. Une quinzaine d'années se sont déjà écoulées depuis la création du bitcoin, la plus ancienne cryptomonnaie. La Suisse et la Crypto Valley Association ont une réputation internationale de "havre de paix" en matière de réglementation, notamment en raison des efforts relativement rapides, en comparaison internationale, qui ont été fournis pour créer une sécurité juridique dans la gestion du secteur des cryptoactifs. Il n'existe pas non plus de chiffres globaux rendant compte des flux financiers d'AV qui entrent ou sortent de la place financière suisse. Les données provenant de l'analyse de blockchain ne sont pas la seule source d'informations sur l'utilisation d'AV à des fins de BA et de FT. Par exemple, les informations fournies par le trafic des paiements traditionnel, les registres du commerce, les documents fiscaux, les divers organes de surveillance et les sources publiques peuvent également aider à évaluer et à renforcer le dispositif de lutte contre le BA et le FT dans le contexte des AV. Les autorités, les parties prenantes et les autres acteurs concernés ont besoin de ces informations afin de prendre des décisions éclairées de manière coordonnée dans le cadre de leur travail et fixer les priorités qui s'imposent. Ce manque général d'informations accroît le risque que des évolutions imprévues restent longtemps inaperçues et mettent brusquement en péril la place financière suisse ainsi que d'autres centres financiers internationaux sur les plans économique et politique.

[192] FMI, *F.18 Recording of Crypto Assets in Macroeconomic Statistics*, mars 2022, p. 40
[193] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, p. 36
[194] GCBF, *Deuxième rapport national sur les risques de blanchiment d'argent et de financement du terrorisme*, octobre 2021, p. 52
[195] Le MROS a posé la question à la FINMA, à l'Office fédéral de la statistique (OFS), à la Banque nationale suisse (BNS), au Secrétariat d'État aux questions financières internationales (SFI), à l'Administration fédérale des contributions (AFC), ainsi qu'à neuf autorités fiscales cantonales.

7.2 Croissance simultanée de l'utilisation et du risque

Comme un aperçu des données du MROS et des autorités suisses de poursuite pénale le montre, les risques de BA et de FT se sont accrus avec l'augmentation significative de l'utilisation d'AV.

Les autorités suisses de poursuite pénale et le MROS sont de plus en plus souvent confrontés, dans le cadre de leur travail, à des cas liés à l'utilisation d'AV. Ainsi, depuis le début de 2020, les informations reçues par le MROS de la part d'intermédiaires financiers suisses ou de CRF étrangères concernent de plus en plus souvent des AV[196], c'est-à-dire qu'elles portent toujours plus sur des faits ou des transactions suspectes liés à l'utilisation d'AV.

Les intermédiaires financiers exerçant ou non une activité de PSAV peuvent transmettre des communications de soupçons qui concernent des AV. Celles-ci ont été considérées comme concernant des AV lorsqu'elles correspondaient à l'un des scénarios suivants :

- la communication de soupçons portait sur des transactions d'AV, à savoir des transactions entre les comptes signalés et des comptes d'intermédiaires financiers avec activité de PSAV (communications d'intermédiaires financiers sans activité de PSAV) *ou* des transactions signalées libellées en AV (communications d'intermédiaires financiers avec activité de PSAV);
- sur la base des faits décrits par l'intermédiaire financier signalant, il existait un lien évident avec des AV, quand bien même aucune transaction telle que définie ci-dessus n'a pu être constatée sur les comptes signalés.

Les communications de soupçons concernant des AV ont nettement augmenté en nombre ainsi qu'en proportion par rapport à l'ensemble des communications de soupçons reçues depuis 2020.

Se sont également intensifiés les échanges d'informations relatives à des AV avec des CRF étrangères et la transmission d'informations sur des AV par le MROS aux autorités suisses de poursuite pénale. Ces dernières ont également enregistré depuis 2020 une nette hausse du nombre de dénonciations et de procédures pénales dont les faits présentent un lien avec des AV.

7.2.1 Hausse du nombre de communications de soupçons concernant des AV

En 2020, 5,8 % des communications de soupçons reçues ont pu être classées comme concernant des AV. En 2022, cette proportion a plus que doublé (13,8 %). Durant la période de 2020 à 2022, 10 % des communications portaient sur des AV.

[196] Cf. chap. 11.1 pour une description détaillée de la méthode d'analyse.

	2020	2021	2022	2020-2022 (total)
Communications de soupçons (chiffre annuel)	5334	5964	7639	18 937
Communications de soupçons concernant des AV (pourcentage du chiffre annuel)	312 (5,8 %)	499 (8,4 %)	1056 (13,8 %)	1867 (9,9 %)

Fig. 16 : Part de communications de soupçons concernant des AV dans le chiffre annuel de communications de soupçons

Il convient toutefois de relativiser la pertinence de ces informations. Par exemple, les informations tirées de communications de soupçons concernant l'utilisation d'AV à des fins de BA et de FT ne se réfèrent qu'à celles *reçues* de la part d'intermédiaires financiers. Il reste à déterminer dans quelle mesure ces informations sont représentatives de l'utilisation effective d'AV à des fins de BA et de FT en Suisse. Du fait notamment que les transactions d'AV peuvent être effectuées directement entre utilisateurs et ne relèvent que parfois du domaine de l'intermédiation financière – et donc ainsi de la LBA –, il est à supposer qu'un très grand nombre de cas ne sont pas détectés.

7.2.2 Intensification des échanges d'informations entre CRF

L'échange d'informations avec les CRF étrangères est un autre domaine d'activité du MROS. Il est possible de prendre contact avec le MROS depuis l'étranger dans deux buts : lui adresser des demandes ou lui transmettre spontanément des informations (sans aucune requête), qui peuvent être d'importance pour la Suisse. Dans le cadre de ces transmissions d'informations, il est également possible de déterminer si celles-ci concernent des AV. La méthode utilisée est la même que pour les communications de soupçons.

	2020	2021	2022
Informations émanant de CRF (demandes ou informations spontanées)	1397	1312	1557
Nombre de celles-ci liées à des AV	18	42	132
Pourcentage de celles-ci liées à des AV	1,3 %	3,2 %	8,5 %

Fig. 17 : Informations émanant de CRF concernant des AV de 2020 à 2022

Depuis 2020, les liens avec des AV sont plus fréquents dans les informations échangées avec des CRF étrangères, sans toutefois atteindre la même fréquence que dans les communications de soupçons reçues à la même période. Au moins une information sur douze reçue par le MROS de l'étranger en 2022 portait sur des AV.

7.2.3 Accroissement des transmissions d'informations concernant des AV aux autorités de poursuite pénale

Le MROS analyse les informations provenant de toutes les communications de soupçons reçues et décide si elles doivent être transmises à des autorités suisses de poursuite pénale. Ces dernières sont de plus en plus fréquemment confrontées à des transmissions d'informations relatives à des AV en raison de l'augmentation des communications de soupçons à ce sujet. Il s'agit notamment des ministères publics des cantons d'Argovie, de Berne, de Genève, de Vaud et de Zurich, ainsi que du Ministère public de la Confédération (MPC). Toutefois, depuis 2020, presque tous les ministères publics cantonaux ont déjà reçu des informations concernant des AV et, là aussi, ces transmissions étaient tendanciellement en augmentation.

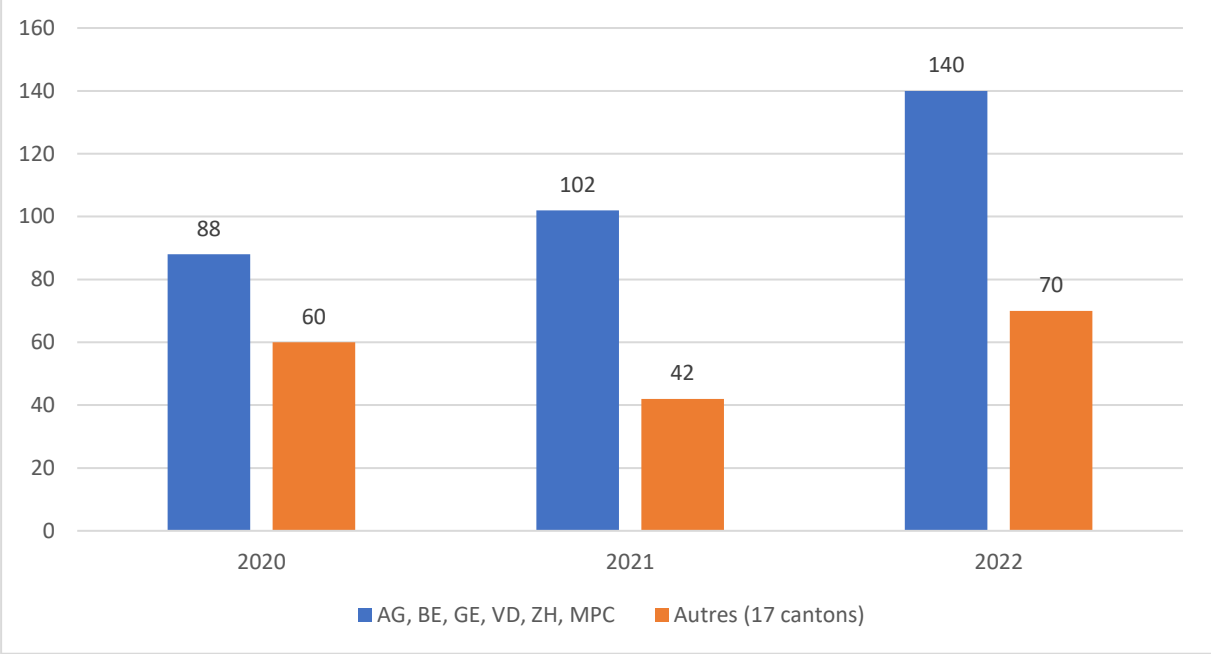

Fig. 18 : Nombre de transmissions d'informations concernant des AV aux divers ministères publics cantonaux et au MPC de 2020 à 2022

7.2.4 Hausse des procédures pénales concernant des AV

Les informations recueillies indiquent que la plupart des polices et des ministères publics suisses n'enregistrent pas systématiquement l'utilisation de cryptomonnaies dans leurs procédures pénales, de sorte qu'il n'existe pas de vue d'ensemble nationale à cet égard. De 2020 à 2022, le nombre d'infractions relevées par la police en Suisse dans le domaine de la criminalité numérique a cependant augmenté de 37 % pour atteindre 33 345 infractions (91 par jour)[197]; et 89 % (29 677) de ces dernières ont été classées dans la catégorie "Cybercriminalité économique", dont 67 % (22 207) dans la sous-catégorie "Cyber-escroquerie"[198]. Les entretiens menés avec différents experts de la poursuite pénale laissent supposer que des AV ont été utilisés très fréquemment sous une forme ou une autre dans ces

[197] Il n'existe pas de chiffres antérieurs relatifs au domaine de la "criminalité numérique", car ceux-ci ont été publiés pour la première fois dans la SPC de 2020 (cf. OFS, *SPC – Rapport annuel 2021*, mars 2022, p. 58, et *SPC – Rapport annuel 2022*, mars 2023, p. 58).
[198] OFS, *SPC – Rapport annuel 2022*, pp. 58 à 60

infractions[199]. Dans certaines infractions relevant de la cybercriminalité économique – par exemple dans les cas de rançongiciel, d'extorsion ou de chantage, et de fraude à l'investissement en ligne –, des AV sont presque toujours utilisés à un stade ou à un autre[200].

Diverses enquêtes et analyses de données provenant des autorités suisses de poursuite pénale semblent également confirmer que le nombre de procédures pénales liées à des AV a nettement augmenté depuis 2018 dans notre pays. Ces enquêtes indiquent en outre que les sommes concernées sont importantes et en hausse depuis 2018. Les infractions principales relèvent majoritairement du domaine de la cybercriminalité économique, ce qui laisse pense qu'elles sont donc le plus susceptibles de donner à lieu à des actes ultérieurs de blanchiment d'argent en lien avec l'utilisation criminelle d'AV.

Les réponses obtenues dans le cadre de l'enquête menée auprès des autorités suisses de poursuite pénale semblent confirmer cette tendance[201]. Par exemple, depuis 2018, 7 ministères publics cantonaux ont mené à eux seuls 119 procédures pénales dans lesquelles des AV ont joué un rôle important. Plus d'un tiers (45) de ces procédures pénales concernaient des éléments constitutifs d'une infraction dans le domaine du BA, des infractions préalables au BA, de la criminalité organisée ou du FT. Au vu du peu de réponses reçues, il y a lieu de penser que le nombre réel de procédures pénales concernant des AV est nettement plus élevé depuis 2018. Les 7 ministères publics cantonaux ayant répondu sont les seuls qui disposaient de chiffres consolidés. N'y figuraient pas notamment les données des ministères publics de plusieurs cantons très peuplés.

Seuls 6 ministères publics cantonaux ont pu fournir des informations sur les infractions faisant l'objet de ces procédures. Outre les violations de la loi du 3 octobre 1951 sur les stupéfiants (LStup), ces infractions relèvent presque exclusivement de la cybercriminalité économique, l'escroquerie (art. 146 CP) et l'utilisation frauduleuse d'un ordinateur (art. 147 CP) étant les plus fréquemment citées. Des informations précises sur les montants visés dans les procédures pénales liées à des AV n'ont pu être fournies que par trois ministères publics cantonaux ; ces montants équivalaient à plus de 130 millions de francs au total depuis 2018, dont plus de 100 millions ne sont attribuables qu'à une seule procédure. Les sommes totales annuelles concernées sont en hausse depuis 2018. Bien que seuls 3 ministères publics cantonaux aient pu fournir des indications concrètes sur les montants en cause, les analyses des données fournies par d'autres cantons dessinent la même tendance.

C'est notamment ce qui ressort d'une évaluation de PICSEL. Cette banque de données intercantonale permet d'enregistrer les dénonciations dans le domaine de la criminalité numérique, afin de centraliser les incidents et les montants des dommages et de promouvoir la priorisation et la coordination des autorités de poursuite pénale dans la lutte contre la cybercriminalité. Les dénonciations concernant la cybercriminalité déposées auprès des autorités cantonales de poursuite pénale participantes sont saisies dans PICSEL[202], puis classées notamment en fonction du phénomène concerné (par ex. rançongiciel, fraude à l'investissement en ligne, *romance scam*, etc.) et du dommage occasionné (par ex. cryptomonnaies volées d'un portefeuille, monnaies fiat détournées lors de l'accès à l'e-banking par hameçonnage ou piratage, paiement au moyen de cartes prépayées lors d'attaques de rançongiciel, etc.). Il existe en outre un projet pilote, basé sur le fonctionnement de PICSEL, qui est consacré exclusivement au thème de la fraude à l'investissement en ligne et inclut tous les cantons.

[199] Cette catégorie regroupe 12 différents types d'infractions (par ex. CEO fraud, magasins en ligne frauduleux, fraude à l'investissement en ligne, romance scam, etc., ibid., p. 60).
[200] Cf. par ex. OFCS (ancien NCSC), *Rapport semestriel 2022/II (juillet à décembre)*, mai 2023, p. 9
[201] L'enquête a été menée sous la direction de fedpol de février à avril 2023. Toutes les polices et tous les ministères publics cantonaux ont été sollicités.
[202] Opérationnelle depuis avril 2021, la banque de données est utilisée par neuf cantons: Argovie, Fribourg, Genève, Grisons, Jura, Neuchâtel, Tessin, Vaud et Valais. Il est prévu qu'un dixième canton les rejoigne prochainement (état: mai 2023).

Les cantons participants utilisent la base de données PICSEL de diverses manières. Certaines autorités cantonales de poursuite pénale ne saisissent par exemple aucune donnée sur les dénonciations qu'elles reçoivent, mais utilisent la plate-forme uniquement à des fins de recherche et de coopération avec leurs homologues. Bien que ces données ne fournissent qu'un aperçu partiel, une analyse montre de manière représentative la croissance de l'utilisation et du détournement d'AV dans le domaine de la criminalité numérique en Suisse. Comparé à d'autres formes de paiement, l'utilisation et le détournement d'AV ont fortement augmenté depuis 2020, non seulement en chiffres absolus, mais aussi proportionnellement pour ce qui est de la somme totale des dommages. De 2020 à 2021, le montant des dommages financiers subis par les dénonciateurs à la suite d'un détournement d'AV a triplé. Par rapport à 2020, la part d'AV détournés dans le montant total des dommages déclarés dans les dénonciations saisies dans PICSEL a nettement augmenté tant en 2021 qu'en 2022.

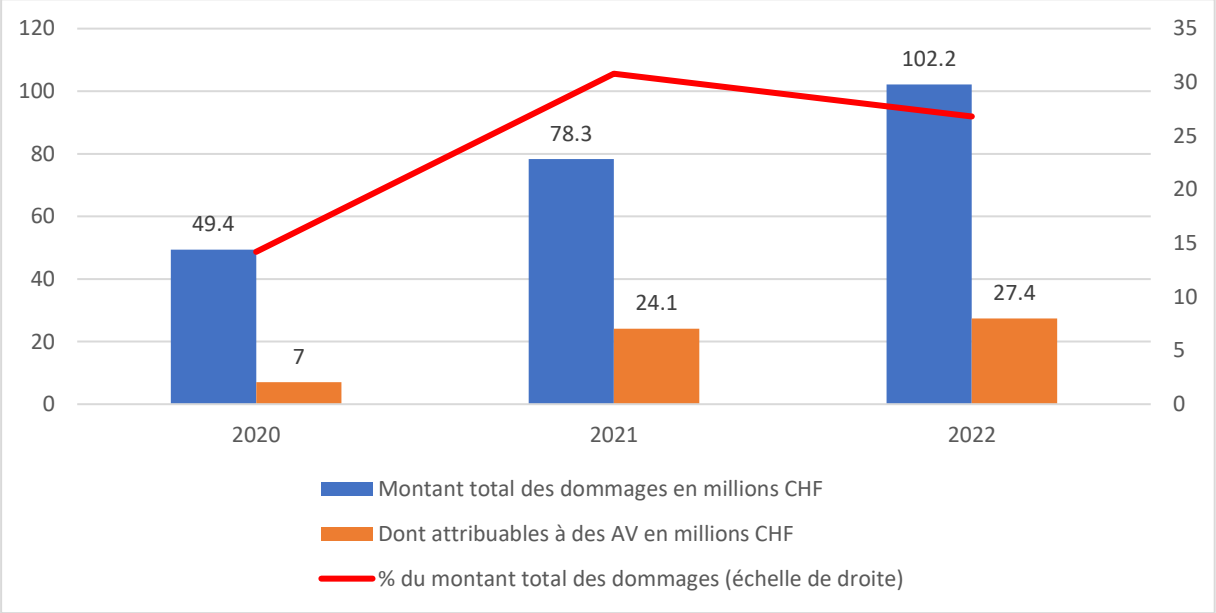

Fig. 19 : Croissance nominale et relative du montant des dommages en AV déclarés dans les dénonciations enregistrées dans PICSEL par rapport à 2020

Parmi les phénomènes recensés ces dernières années, l'utilisation et le détournement d'AV semblent être ceux qui ont le plus augmenté en lien avec la fraude à l'investissement en ligne. Leur part représentait certes déjà environ un quart du montant total des dommages en 2020, mais elle est passée à plus de la moitié à la fin de 2022.

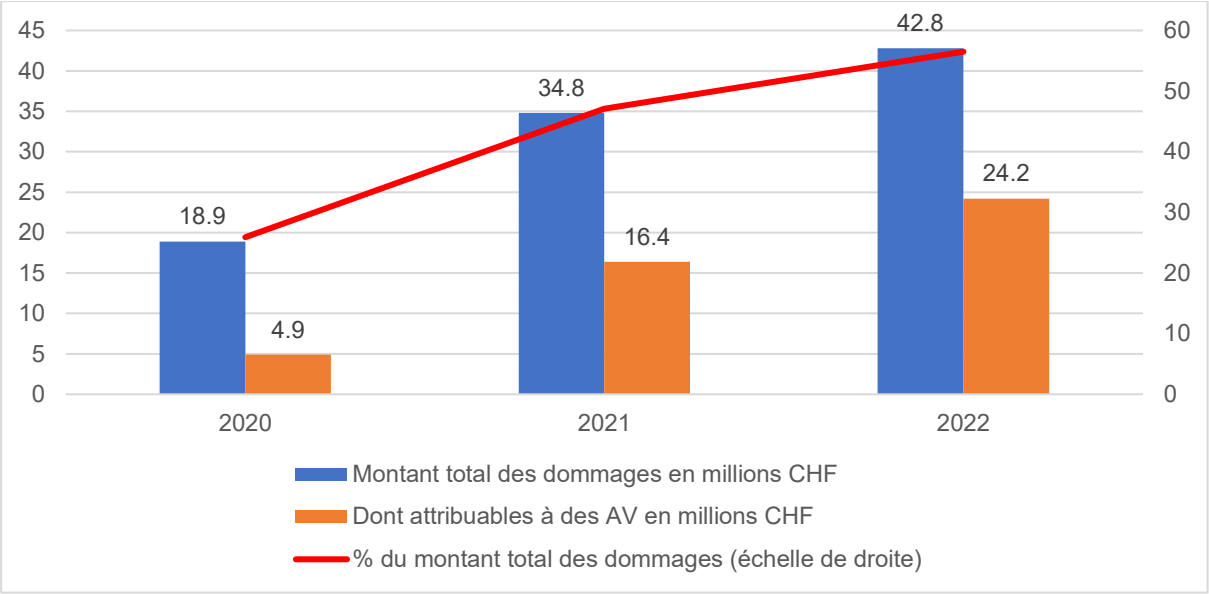

Fig. 20 : Croissance nominale et relative du montant des dommages en AV liés à la fraude à l'investissement en ligne par rapport à 2020

Bien qu'il ne soit pas possible de procéder à une évaluation définitive sur la base des chiffres présentés ici, ces derniers semblent clairement indiquer que l'utilisation criminelle d'AV a augmenté depuis 2018 en Suisse.

Selon les informations fournies par les différentes autorités de poursuite pénale interrogées, le BA en tant qu'infraction ultérieure serait certes une conséquence logique dans la plupart des cas qu'elles examinent, étant donné que les criminels doivent blanchir les AV obtenus par le biais d'infractions. Les autorités de poursuite pénale ne semblent pas disposer de données consolidées sur les actes de BA succédant aux infractions qu'elles ont examinées, que le produit financier illicite soit en monnaie fiat ou en AV. Des informations fondées relatives à ces actes de BA font défaut, notamment parce que l'enquête menée par les autorités de poursuite pénale se concentre le plus souvent sur l'élucidation des infractions dénoncés ainsi que sur une éventuelle restitution des fonds subtilisés aux victimes ; les auteurs présumés se trouvent généralement à l'étranger et leur identité ne peut pas être établie dans la plupart des cas. L'analyse de blockchain et les contacts avec des intermédiaires financiers étrangers avec activité de PSAV ont toutefois permis de recueillir quelques indices sur des réseaux de blanchiment d'AV dans des pays d'Europe de l'Est ainsi qu'au Proche-Orient et en Extrême-Orient, qui coïncident avec les conclusions fournies par d'autres recherches[203].

[203] "Les dirigeants de LockBit prétendent utiliser principalement des bourses de bitcoins à Hong Kong et en Chine pour blanchir le produit de leurs méfaits. Ils estiment que l'hostilité qui règne entre la Chine et les États-Unis rendent les opérations de blanchiment d'argent plus sûres." (traduction libre, cf. Schurter Daniel, *Das ist die gefährlichste Hackerbande, die auch in der Schweiz wütet*, 23 janvier 2023).

7.3 Principales menaces

Lors de la communication de soupçons, les intermédiaires financiers informent le MROS des infractions préalables présumées en lien avec les personnes ou les comptes signalés[204]. Même si celles-ci ne correspondent pas toujours aux résultats des analyses du MROS, une analyse quantitative des infractions préalables présumées dans les communications de soupçons portant sur des AV peut aider à identifier avec plus de précision les menaces découlant de l'utilisation d'AV à des fins criminelles en général et à des fins de BA ou de FT en particulier.

7.3.1 Menace majeure : l'utilisation frauduleuse d'AV

Dans le cadre de l'analyse des risques de 2018, le nombre de communications de soupçons liées à des AV n'était pas élevé. La plus grande menace identifiée sur la base des communications de soupçons se situait au niveau de l'émission d'AV: les faits signalés par les intermédiaires financiers et les infractions préalables présumées étaient en effet pour la plupart liés à des ICO frauduleuses. En 2018 et 2019, les ICO étaient ainsi dans le viseur des autorités de surveillance, comme le montrent les directives correspondantes de la FINMA[205]. Depuis 2020, les communications de soupçons transmises au MROS sont nettement plus diversifiées en ce qui concerne les infractions préalables présumées, et les faits signalés ne révèlent plus de risques particuliers dans le domaine des émissions. Ce sont bien plus souvent les services de conservation ou de conversion d'AV qui jouent le rôle central dans les faits signalés par les intermédiaires financiers, qui, les trouvant suspects, les portent à la connaissance du MROS dans le cadre d'une communication de soupçons.

Les quelques communications de soupçons reçues par le MROS entre 2015 et 2019 de la part d'intermédiaires financiers avec activité de PSAV se sont limitées à un petit nombre d'infractions préalables présumées, notamment l'escroquerie, le faux dans les titres et l'utilisation frauduleuse d'un ordinateur[206]. De 2020 à 2022, ces infractions préalables ont également été fréquemment suspectées – et même plus souvent que la moyenne par rapport au nombre global (cf. fig. 21).

[204] Remarque: dans une communication de soupçons, les intermédiaires financiers peuvent indiquer plusieurs infractions préalables présumées.
[205] Cf. FINMA, *Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO)*, février 2018; FINMA, *Complément au guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO)*, septembre 2019.
[206] Cela correspond également aux conclusions du premier rapport du GCBF sur les AV de 2018 (cf. GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, pp. 24 à 27).

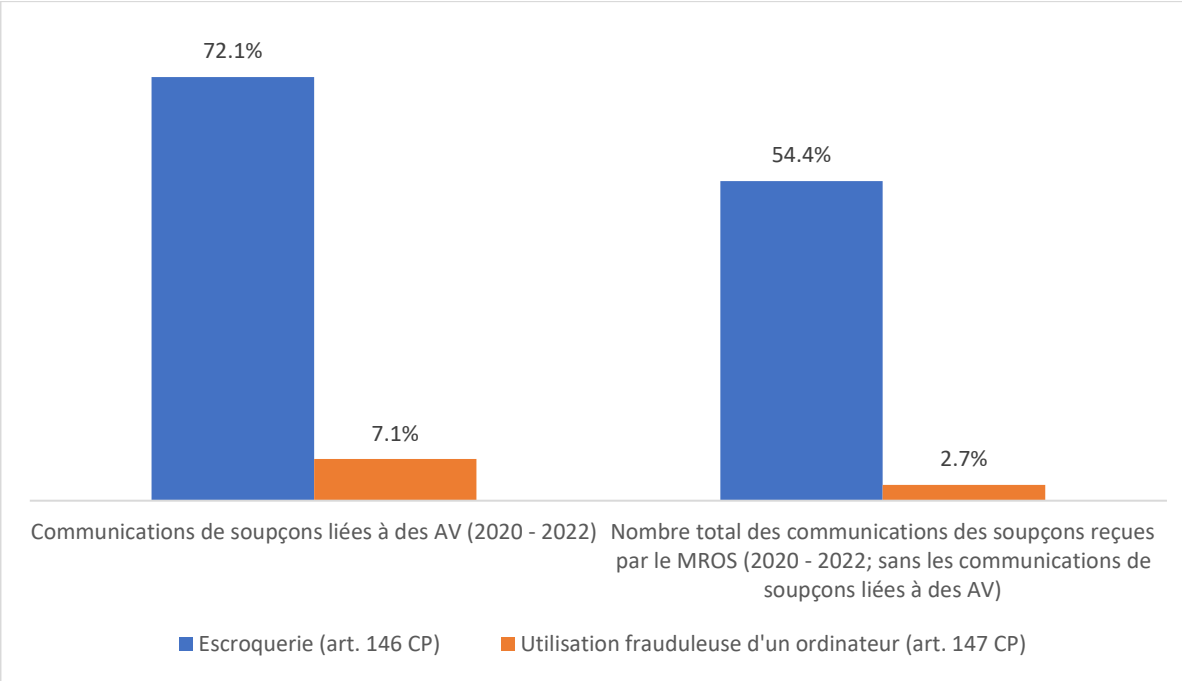

Fig. 21 : Les infractions préalables que sont l'escroquerie et l'utilisation frauduleuse d'un ordinateur sont présumées plus fréquemment que la moyenne dans les communications de soupçons concernant des AV (2020 – 2022).

Il n'est pas clair si la surreprésentation de ces deux infractions préalables est due au fait qu'elles ont été celles le plus fréquemment commises ou si les intermédiaires financiers ont pu les détecter et les signaler plus aisément que d'autres infractions préalables. Le fait que ces deux infractions préalables soient plus souvent présumées dans les communications de soupçons concernant des AV que dans celles ne les concernant pas coïncide toutefois avec les observations réalisées par des CRF étrangères[207]. D'une part, les auteurs présumés semblent profiter de la facilité et de la rapidité de la conversion d'AV en monnaie fiat (et inversement) dans des flux de paiement dans le but de compliquer ou, du moins, de retarder le traçage des flux financiers qui leur profitent. D'autre part, ils semblent également tenter d'exploiter la vulnérabilité des AV et de rendre plus difficile leur blocage ou leur confiscation par les autorités de poursuite pénale, en les transférant généralement sur des portefeuilles non hébergés. De nombreux réseaux d'escrocs semblent avoir repéré cette vulnérabilité et l'avoir instrumentalisée pour commettre diverses infractions. Les communications concernant des AV et des infractions préalables présumées dans ce domaine étaient en général liées à la fraude à l'investissement en ligne, à des systèmes "boule de neige", à des cas de mules financières, ou à une combinaison de ces phénomènes. Les comptes signalés dans ce contexte étaient pour la plupart des comptes de transit que leurs titulaires mettaient, sciemment ou non, à la disposition d'escrocs présumés[208]. Lorsque l'utilisation frauduleuse d'un ordinateur était une infraction préalable également soupçonnée, il s'agissait généralement de paiements déclenchés frauduleusement (par piratage, ingénierie sociale ou hameçonnage), qui étaient exécutés depuis des comptes ouverts auprès d'intermédiaires financiers traditionnels sans activité de PSAV (suisses ou étrangers) vers des comptes ouverts auprès d'intermédiaires financiers avec activité de PSAV (suisses ou étrangers). L'objectif des auteurs présumés était apparemment de convertir en AV sur une plate-forme de PSAV, et le

[207] Cf. par ex.: Swedish Police Authority, *The Financial Intelligence Unit Annual Report 2021*, mai 2022, p. 15 s.; CRF (Liechtenstein), *Jahresbericht 2021*, avril 2022, p. 11.

[208] Les criminels recrutent sur Internet des agents financiers, autrement dit des mules financières, principalement par le biais d'offres d'emploi attrayantes. Ces mules sont chargées de transférer des fonds d'origine illicite à des criminels (qui se trouvent généralement à l'étranger) en mettant leurs comptes personnels à disposition. Quiconque participe à ce genre d'"affaires" peut se rendre coupable de BA (cf. Prévention suisse de la criminalité (PSC), "Money Mules", consulté en mai 2023).

plus rapidement possible, les valeurs patrimoniales en monnaie fiat obtenues frauduleusement d'une victime, puis de les transférer sur un portefeuille non hébergé.

Lorsque des intermédiaires financiers suisses avec activité de PSAV ont transmis des communications de ce type, l'escroquerie ou l'utilisation frauduleuse d'un ordinateur étaient les infractions préalables soupçonnées, le plus souvent en combinaison avec des faux dans les titres, car les auteurs présumés ouvraient fréquemment un compte de PSAV avec des documents d'identité volés ou falsifiés afin d'occulter leur identité. Dans de nombreux cas, le MROS a pu constater que les intermédiaires financiers avec activité de PSAV disposaient certes des documents d'identification nécessaires à l'ouverture d'une relation d'affaires, mais que les titulaires de ces documents n'avaient eux-mêmes pas accès à ces comptes à cause des diverses astuces utilisées par les escrocs. À quelques exceptions près, ces communications portaient sur des montants relativement faibles, allant de quelques centaines à quelques milliers de francs.

6e menace

Menace liée à l'effet de nouveauté et à l'inexpérience des utilisateurs (identifiée en 2018, en hausse en 2023)[209]

Depuis 2018, le nombre d'utilisateurs d'AV s'est multiplié. Il est pratiquement tous les jours question des AV dans les médias. Les risques qui en découlent sont connus des investisseurs, ou devraient l'être. Malgré cela, la perspective de gains élevés rend encore de nombreuses personnes imprudentes, par exemple lorsqu'elles choisissent un prestataire de services pour leurs investissements ou lorsqu'elles saisissent leurs données personnelles sur Internet. Les informations du MROS et les données des autorités de poursuite pénale indiquent que, par rapport à 2018, beaucoup plus de personnes sont victimes de manœuvres frauduleuses liées à des AV, qui tirent avantage de l'inexpérience des nouveaux utilisateurs. La menace a par conséquent augmenté.

7e menace

Recours aux AV lors d'attaques d'hameçonnage (identifiée en 2018, en hausse en 2023)[210]

Parfois, les victimes se laissent persuader au téléphone ou par messagerie d'effectuer un virement aux escrocs, mais des méthodes d'hameçonnage sont aussi fréquemment utilisées. Ces cas sont nettement plus nombreux qu'en 2018 – ne serait-ce qu'en raison de l'augmentation de l'utilisation d'AV. Cette menace s'est donc également accrue.

7.3.2 Éventail des risques élargi par de nouvelles menaces

L'éventail des infractions préalables présumées par les intermédiaires financiers s'est élargi au fil du temps et en raison de l'accroissement de leurs communications de soupçons concernant des AV.

[209] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding*, octobre 2018, pp. 24 à 26
[210] Ibid., p. 30

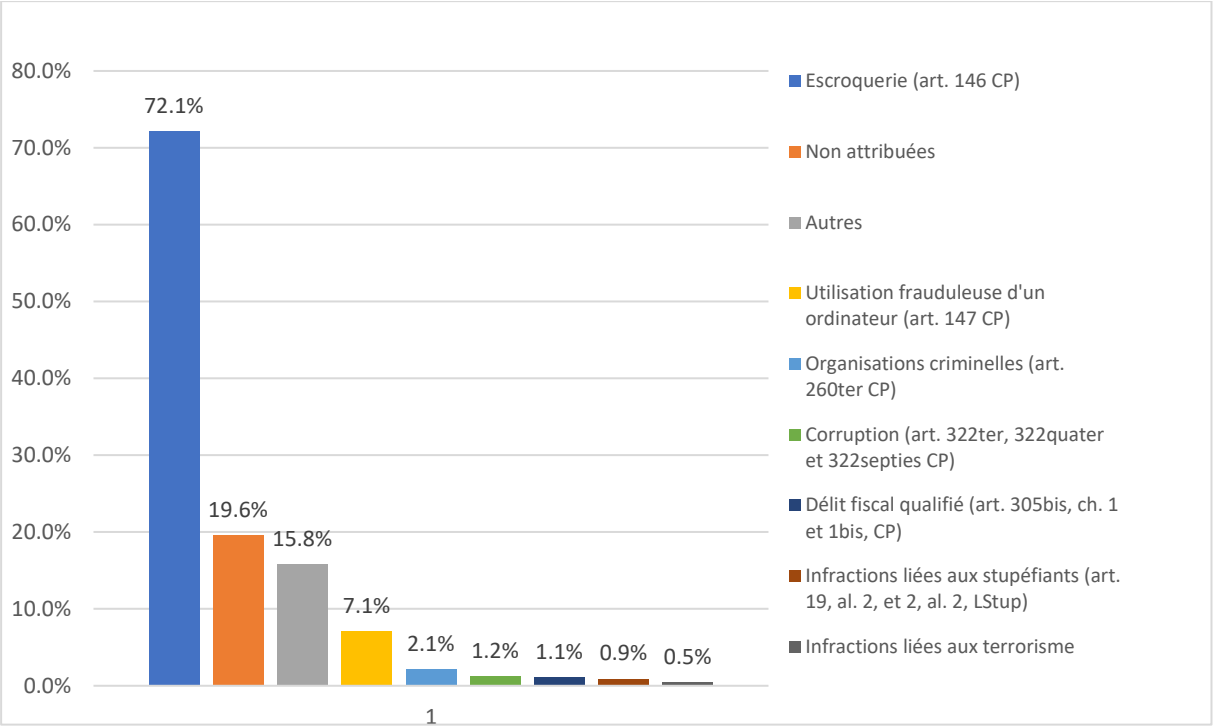

Fig. 22 : Illustration de la diversité des infractions préalables présumées dans 1867 communications de soupçons concernant des AV (2020–2022). De nombreuses infractions préalables supplémentaires, regroupées sous "Autres", sont énumérées au chap. 11.2 en annexe[211].

Comme le montre la fig. 22, les diverses infractions préalables sont relativement rarement suspectées, mais elles couvrent néanmoins un large éventail d'infractions, ce qui permet de conclure à une utilisation criminelle plus large des AV dans le trafic de paiements. La catégorie "Autres" regroupe un nombre moyen à deux chiffres d'autres infractions préalables, ce qui indique que les AV sont désormais utilisés illicitement sous les formes et dans les stratagèmes les plus divers à des fins de BA ou de FT[212]. En conséquence, parmi les communications concernant des AV figuraient également des faits incluant des indicateurs de risque que l'on trouverait normalement dans la lutte contre le BA et le FT dans le trafic de paiements traditionnel et qui suggèrent des stratagèmes "classiques" de BA et de FT. Il s'agit par exemple de l'implication inutile, du point de vue économique, de sociétés offshore dans des opérations commerciales relativement simples (par ex. importation de denrées alimentaires) ou de l'intégration du cocontractant dans un réseau complexe de sociétés dont les volumes élevés de transactions se justifient par des contrats de prêt réciproques (parfois en AV) (cf. typologie n° 1). Les analyses réalisées par le MROS viennent renforcer cette impression : d'autres infractions que celles qui étaient principalement indiquées par les intermédiaires financiers (par ex. escroquerie) sont fréquemment détectées. Il n'est pas rare que ces infractions relèvent alors de formes de criminalité plus graves.

[211] Remarque : les intermédiaires financiers peuvent suspecter diverses infractions et donc indiquer plusieurs infractions préalables présumées dans le cadre de chaque communication de soupçons. Il est donc possible de calculer le pourcentage des infractions préalables présumées et d'arriver à une somme totale qui dépasse 100 %. De même, les infractions dans le domaine du terrorisme comprennent a) le financement du terrorisme (art. 260^{quinquies} CP) et b) les actes visés à l'art. 2 de la loi fédérale interdisant les groupes "Al-Qaïda" et "État islamique" et les organisations apparentées.

[212] La liste complète des infractions préalables présumées dans les communications de soupçons concernant des AV figure au chap. 11.2 en annexe.

Typologie n° 1

Un réseau de sociétés-écrans étrangères achète des AV à des fins présumées de blanchiment de monnaie fiat

Dans le cadre de la procédure d'ouverture d'une relation d'affaires avec une société étrangère, l'intermédiaire financier émetteur de la communication de soupçons a remarqué que le modèle d'affaires de la société et les formulations utilisées par celle-ci ressemblaient beaucoup à ceux d'un client commercial déjà enregistré. Il a alors exigé du nouveau client potentiel des documents supplémentaires sur l'origine des fonds. Celui-ci a fourni des relevés bancaires et des factures pour des prestations apparemment effectuées. Ces documents lui ayant paru vraisemblables, l'intermédiaire financier a ouvert la relation d'affaires. Dans les jours qui ont suivi, le nouveau client a transféré, en plusieurs transactions, de la monnaie fiat d'un compte étranger sur la relation d'affaires, a acheté des AV avec cet argent et les a immédiatement placés dans un portefeuille non hébergé. Au cours du même mois, l'intermédiaire financier a reçu une autre demande similaire concernant l'ouverture d'une relation d'affaires par une troisième société établie dans le même pays que les deux autres. Des documents supplémentaires concernant l'origine des fonds lui ont également été demandés, mais ceux qu'elle a fournis ont été jugés insuffisants par l'intermédiaire financier, qui lui en a demandé d'autres. Le nouveau client potentiel n'a toutefois pas donné suite à cette dernière demande. L'intermédiaire financier a ensuite remarqué, lors d'un contrôle approfondi, que deux de ces sociétés utilisaient la même adresse. Il a également constaté des anomalies supplémentaires concernant les trois sociétés : les documents d'identification n'étaient parfois pas remplis correctement et les sites Internet semblaient peu sérieux et créés ad hoc. Des prises de contact supplémentaires avec ces trois entreprises n'ont pas abouti. Les doutes qui en ont résulté quant à l'origine des valeurs patrimoniales apportées ont incité l'intermédiaire financier à faire une communication au MROS.

Des communications de soupçons concernant des AV comportaient aussi parfois des indices de trafic de stupéfiants à grande échelle et de FT (cf. typologie n° 2).

Typologie n° 2

Financement présumé du terrorisme au moyen d'AV

Un intermédiaire financier a proposé le service ATM-crypto à sa clientèle. Ce service permet de verser des francs suisses dans un bancomat afin de les échanger contre des bitcoins remis par l'intermédiaire financier. Pour changer les francs suisses en bitcoins, ce dernier a collaboré avec une bourse d'AV dans un pays voisin, qui a envoyé les bitcoins achetés par les clients à l'adresse bitcoin que ceux-ci avaient indiquée. Cette bourse a signalé à l'intermédiaire financier que depuis une de ces adresses, une transaction en bitcoins d'une centaine de francs environ avait été effectuée vers une adresse bitcoin semblant appartenir au groupe Al-Qaïda, qui faisait l'objet d'une instruction par un ministère public dans un pays tiers. Les intermédiaires financiers du domaine des PSAV ont la possibilité de suivre des AV transférés, même après qu'ils ont été remis au client, ce qui a permis dans ce cas de découvrir le virement suspect. Dans le domaine du monitoring des transactions d'AV, cet avantage ouvre de nouvelles possibilités par rapport au trafic de paiements traditionnel.

La personne à l'origine du virement signalée au MROS a pu rester largement anonyme en versant l'argent à l'ATM-crypto et n'a dû indiquer qu'une information de contact. Cette indication a néanmoins suffi au MROS pour l'identifier. Les clarifications ont révélé que cette personne s'était fait remarquer sur les réseaux sociaux il y a quatre ans en diffusant de la propagande djihadiste violente. Outre la transaction précitée, l'analyse a permis d'identifier

17 autres transactions d'une valeur totale d'environ 3000 francs sur la même adresse bitcoin. Selon un outil d'analyse de blockchain, cette adresse ferait partie de l'*Al-Qaïda Bitcoin Transfer Office*.

8e menace

FT au moyen d'AV (identifiée en 2018, inchangée en 2023)[213]

Depuis 2018, le MROS a reçu plusieurs communications de soupçons en lien avec des AV de la part d'intermédiaires financiers soupçonnant des infractions dans le domaine du terrorisme[214]. Les données de la société d'analyse de blockchain Chainalysis laissent toutefois penser que le virement d'argent sur des adresses connues d'organisations terroristes est en recul depuis 2020[215]. Néanmoins, il est bien connu qu'en matière de FT, de petits montants suffisent pour causer d'importants dommages. Globalement, rien n'indique un changement significatif de la situation de la menace par rapport à 2018.

Une communication de soupçons a également fourni des indices de l'implication d'acteurs dans des actes présumés de BA au moyen d'AV, dont on suppose qu'ils ont servi à financer le programme d'armement d'un État étranger frappé par des sanctions de l'ONU (cf. typologie n° 3).

Typologie n° 3

Financement présumé de la prolifération au moyen d'AV

Un intermédiaire financier suisse exerçant une activité de PSAV a été utilisé à son détriment pour blanchir des cryptomonnaies volées provenant d'une cyberattaque sur une cryptobourse étrangère. Les auteurs se sont servis de la plate-forme de l'intermédiaire financier auteur de la communication pour changer les cryptomonnaies volées en une autre cryptomonnaie afin d'effacer leurs traces. Selon les estimations de divers experts dans le domaine de l'analyse de blockchain, cette attaque serait l'œuvre d'un groupe de hackers proche du régime nord-coréen.

9e menace

Financement de la prolifération au moyen d'AV (identifiée en 2023)

Selon les informations que possède le MROS, des intermédiaires financiers suisses exerçant une activité de PSAV sont aussi exposés au risque d'être utilisés comme plaque tournante de flux financiers servant au financement de la prolifération.

[213] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowfunding*, octobre 2018, pp. 27-28
[214] Les "infractions dans le domaine du terrorisme" comprennent les infractions relevant:
1.) du financement du terrorisme (art. 260quinquies CP)
2.) de l'art. 2 de la loi fédérale interdisant les groupes "Al-Qaïda" et "Etat islamique" et les organisations apparentées.
[215] Chainalysis, *The 2023 Crypto Crime Report*, février 2023, p. 6

Dans certaines communications, on a également constaté des liens avec divers scandales de corruption internationaux. Parmi les cocontractants, les ayants droit économiques ou les autres parties concernées dans des relations d'affaires qui ont également fait l'objet de communications en lien avec des AV, on a aussi identifié des personnes exposées politiquement (PPE). Dans d'autres communications, le MROS a pu identifier des personnes physiques ou morales qui étaient en contact avec des organisations criminelles, d'après des articles de presse ou des informations issues de procédures pénales.

En Suisse, les AV ne sont pas utilisés seulement pour des infractions dans le domaine de la cybercriminalité, comme l'a révélé une analyse de douze cas en lien avec des AV, qui ont donné lieu à des investigations de la PJF ces dix dernières années et ont finalement débouché sur l'ouverture de procédures. La PJF est investie des compétences d'investigation de la Confédération et mène toutes les enquêtes portant sur des infractions qui relèvent de la compétence fédérale. Même si le rôle des AV est variable dans les douze cas examinés et que ce nombre est relativement modeste, ces cas ont un point commun : ils sont tous relativement récents, puisque le plus ancien date de 2018.

Toutes les divisions d'enquête de la PJF ont déjà été confrontées à des cas dans lesquels des cryptomonnaies ont été utilisées. Le spectre couvert par les infractions instruites ou présumées montre une fois de plus les multiples possibilités d'utilisation des AV et la diversité croissante des actes criminels potentiellement associés.

Divisions d'enquête de la PJF	**Entraide judiciaire, terrorisme, droit pénal international**	**Protection de l'État, organisations internationales**	**Criminalité économique**
Infractions examinées	• Organisations criminelles et terroristes (art. 260ter CP) • Loi fédérale interdisant les groupes "Al-Qaïda" et "Etat islamique" et les organisations apparentées (art. 2) • Brigandage (art. 140 CP) • Extorsion et chantage (art. 156 CP) • Emploi, avec dessein délictueux, d'explosifs ou de gaz toxiques (art. 224 CP)	• Fabrication de fausse monnaie (art. 240 CP) • Introduction, acquisition et prise en dépôt de fausse monnaie (art. 244 CP)	• Blanchiment d'argent (art. 305bis CP) • Soustraction de données (art. 143 CP) • Détérioration de données (art. 144bis CP) • Utilisation frauduleuse d'un ordinateur (art. 147 CP)
Méthodes de BA observées	• Services de mixage et *privacy wallets* (portefeuilles privés) • *Peel chains* • *Privacy coins* • *Chain hopping* • Utilisation délibérée de PSAV ayant des exigences KYC basses voire inexistantes / Utilisation de services de broker OTC (*nested services*)		

Fig. 23 : Aperçu des enquêtes effectuées par la PJF dans le domaine des AV entre 2018 et 2022

Dans les enquêtes qu'elle mène dans le domaine de la cybercriminalité, la PJF a observé que les auteurs appliquaient toujours une méthode identique : une fois qu'ils se sont procuré l'accès à l'e-banking des personnes lésées par diverses techniques d'hameçonnage ou de cheval de Troie, ils effectuent des virements sur des comptes de PSAV étrangers, qui ont été ouverts au préalable sous le nom de la personne lésée (usurpation d'identité), ou de mules financières recrutées précédemment. Les fonds versés sont ensuite changés en cryptomonnaies sur la plate-forme du PSAV avant d'être transférés immédiatement sur un portefeuille externe. Le recours à des cryptomonnaies semble donc servir de moyen pour blanchir à l'étranger des valeurs patrimoniales volées sur des comptes bancaires en Suisse et pour brouiller les traces. À l'inverse, la PJF a déjà été confrontée à un cas de cryptomonnaies volées par le piratage d'un PSAV étranger, qui ont été virées sur une plate-forme de PSAV en Suisse afin d'être changées contre une autre cryptomonnaie, puis immédiatement retransférées ailleurs depuis la plate-forme. L'échange de cryptomonnaies semble avoir la dissimulation pour objectif, car il est nécessaire d'analyser plusieurs blockchains différentes pour retracer l'argent. Cette

technique appelée *chain hopping* est souvent répétée plusieurs fois et combinée parfois à d'autres techniques de dissimulation comme le mixage (cf. encadré n° 4 au ch. 7.4.1).

Dans les cas en relation avec le terrorisme et son financement, les cryptomonnaies semblent attrayantes aussi bien pour les donneurs d'ordre que pour les bénéficiaires, pour diverses raisons : les personnes qui contribuent à financer des organisations terroristes avec des cryptomonnaies semblent vraisemblablement penser que les transactions en AV qu'elles effectuent ne peuvent pas être retracées. Au contraire, les organisations terroristes élargissent leur visibilité en publiant leurs adresses d'AV sur Internet, ce qui leur donne accès à un réseau de financement potentiellement beaucoup plus vaste que si elles ne comptaient que sur leurs contacts personnels. L'utilisation de portefeuilles non hébergés permet en outre à ces organisations de protéger les cryptomonnaies reçues contre le blocage et la confiscation. La PJF a pu observer ce procédé aussi dans des cas de rançongiciels et d'autres cas d'extorsion.

Enfin, la PJF a aussi mené deux enquêtes dans le domaine de la fausse monnaie où elle a constaté que sur le darknet, on achetait de la fausse monnaie avec des cryptomonnaies. Une explication "simple" serait qu'on acquiert de la fausse monnaie dans le but présumé de multiplier son argent (achat d'un faux billet de 50 euros pour une fraction de sa valeur nominale), mais ce phénomène peut aussi se révéler être une technique permettant de dépenser des cryptomonnaies issues d'activités criminelles sans avoir besoin de les changer en monnaie fiat par l'intermédiaire d'un PSAV.

7.3.3 Cocontractants et sommes impliquées

Lorsqu'on compare les actes préalables présumés et les sommes impliquées, on s'aperçoit que l'éventail des actes préalables présumés était plus diversifié (délit fiscal qualifié, infractions à la loi sur les stupéfiants, participation ou soutien à une organisation criminelle, etc.) dans les communications portant sur des transactions d'une valeur totale élevée (à partir de 250 000 francs) que dans celles portant sur des montants plus modestes, où les intermédiaires financiers soupçonnent en priorité la fraude.

	2020	2021	2022
Communications en lien avec des AV d'intermédiaires financiers exerçant une activité de PSAV	104	178	143
dont communications sans transactions en AV	50	88	75
dont communications avec transactions en AV	54	90	68
Valeur totale des transactions en AV (CHF)	1,8 million	28,5 millions	50,5 millions
Valeur moyenne de toutes les transactions en AV par communication (CHF)	4976	32 477	53 618
Valeur médiane de toutes les transactions en AV (CHF)	1385	3000	3500

Fig. 24 : Les sommes impliquées dans les communications de soupçons d'intermédiaires financiers exerçant une activité de PSAV qui ont signalé des transactions suspectes ont notablement augmenté depuis 2020.

En 2020, le MROS avait reçu un total de 104 communications de soupçons en lien avec des AV de la part d'intermédiaires financiers exerçant une activité de PSAV. Dans celles portant

sur des transactions en AV suspectes, le montant total signalé s'élevait à plus de 1,8 million de francs suisses. En moyenne, cela représentait des transactions d'une valeur totale de près de 5000 francs par communication, et une valeur médiane d'environ 1385 francs par communication. En 2021, les intermédiaires financiers exerçant une activité de PSAV avaient annoncé 178 communications ayant un lien avec des AV. Pas moins de 68 d'entre elles contenaient des transactions suspectes d'une valeur totale de 28,5 millions de francs suisses, la valeur moyenne totale par communication atteignait près de 32 477 francs, et la valeur médiane autour de 3000 francs. En 2022, les intermédiaires financiers exerçant une activité de PSAV ont déposé 143 communications auprès du MROS. Parmi elles, 68 portaient sur des transactions en lien direct avec des AV, équivalant à un montant total de 50,5 millions de francs suisses, une valeur moyenne de 53 618 francs par transaction et une valeur médiane de 3500 francs. Ces valeurs médianes relativement basses reflètent le fait que dans la période considérée, le MROS a reçu de nombreuses communications portant sur des transactions signalées d'une valeur totale relativement faible. Il s'agissait en grande majorité de virements présumés frauduleux depuis des comptes d'intermédiaires financiers traditionnels sans activité de PSAV vers des comptes d'intermédiaires financiers avec activité de PSAV. Ces cas sont souvent corrélés à des soupçons de piratage ou d'hameçonnage (utilisation frauduleuse d'un ordinateur), les escrocs présumés ayant accès aux données de connexion d'e-banking des victimes et activant eux-mêmes le virement depuis le compte de la victime. Les intermédiaires financiers suisses exerçant une activité de PSAV ont remarqué ces anomalies dans certains cas, car les escrocs se connectaient à différents comptes d'utilisateurs sur la plate-forme de PSAV depuis la même adresse IP, ou le même numéro de téléphone portable apparaissait dans différents comptes d'utilisateurs et il s'agissait d'un numéro qui n'était pas enregistré dans le pays d'origine du client. On constatait toujours le même schéma, où les escrocs présumés s'efforçaient visiblement à dessein d'opérer des flux de paiements transfrontaliers, dans le but d'empêcher ou de retarder le traçage des transactions ou le blocage et la confiscation des valeurs patrimoniales. Ainsi, le compte fiat depuis lequel l'argent était viré et le compte du PSAV sur lequel l'argent était transféré pour l'achat d'AV étaient généralement localisés dans des pays différents. Si le compte d'origine du virement était détenu auprès d'un intermédiaire financier suisse sans activité de PSAV, alors le PSAV vers lequel l'argent était transféré se trouvait généralement à l'étranger et, inversement, si un intermédiaire financier suisse exerçant une activité de PSAV était impliqué, l'argent était généralement viré depuis des comptes étrangers.

Dans les communications en lien avec des AV transmises par des intermédiaires financiers sans activité de PSAV, les sommes impliquées sont beaucoup moins représentatives, car la proportion des communications en lien avec des AV provenant de ce type d'intermédiaire financier *et comportant* des transactions en AV était relativement faible. Ce sont essentiellement certains mots clés (par ex. bitcoin ou crypto) utilisés par l'intermédiaire financier pour décrire les faits qui ont permis de faire le lien avec des AV. Les intermédiaires financiers ont souvent indiqué sommairement une série de virements entre les comptes signalés et ceux d'un PSAV, mais sans saisir ces transactions dans le formulaire électronique ad hoc, si bien que l'analyse quantitative n'a pas pu avoir lieu. De même, dans de nombreux cas, les intermédiaires financiers ont certes signalé un lien avec des AV dans leur communication (par ex. activité commerciale de leur client dans le secteur des AV), mais ils n'ont pas remarqué les liens entre les transactions sur le compte signalé et le compte d'un PSAV, et n'ont donc pas reporté les transactions concernées dans le formulaire électronique prévu à cet effet.

Les chiffres suivants sont par conséquent des indications minimales absolues, les montants réels étant très probablement beaucoup plus élevés.

	2020	2021	2022

Communications en lien avec des AV d'intermédiaires financiers sans activité de PSAV	208	321	913
dont communications sans transactions en AV	166	258	835
dont communications avec transactions en AV	42	63	78
Valeur totale des transactions en lien avec des AV (CHF)	1,6 million	15 millions	7,4 millions

Fig. 25 : Sommes impliquées dans les communications de soupçons en lien avec des AV provenant d'intermédiaires financiers sans activité de PSAV entre 2020 et 2022

La place financière suisse est le numéro un mondial de la gestion de patrimoine transfrontalière pour la clientèle privée. En conséquence, les cocontractants des relations d'affaires signalées au MROS sont souvent domiciliés à l'étranger. Au moins 46 % des cocontractants signalés entre 2020 et 2022 étaient soit des personnes morales domiciliées à l'étranger, soit des personnes physiques ayant la nationalité étrangère (cf. colonne de gauche à la fig. 26).

On discerne une orientation vers la clientèle internationale encore plus forte dans les communications de soupçons d'intermédiaires financiers exerçant une activité de PSAV : dans au moins 69 % des cas, les cocontractants signalés étaient des personnes physiques de nationalité étrangère ou des personnes morales domiciliées à l'étranger. En outre, des personnes physiques étaient signalées comme cocontractants dans 72 % des cas, ce qui peut être considéré comme un bon indicateur du fait que les intermédiaires financiers exerçant une activité de PSAV sont actifs avant tout dans le segment de la clientèle privée.

Les cocontractants signalés dans les communications d'intermédiaires financiers sans activité de PSAV sont plus ou moins représentatifs de l'ensemble des signalements faits au MROS ces trois dernières années, tant en ce qui concerne le statut des entités juridiques (personnes physiques ou morales) que leur origine (nationalité des personnes physiques, domicile des personnes morales, cf. colonnes de gauche et du milieu à la fig. 26). La seule différence est la fréquence relativement grande de communications signalant des personnes physiques de nationalité suisse comme cocontractants (33 %). Plusieurs raisons plausibles pourraient l'expliquer, par exemple la forte orientation de ces intermédiaires financiers vers la clientèle privée en Suisse, en plus de la gestion de fortune internationale. Selon diverses enquêtes et études, les clients privés se sont mis à utiliser de plus en plus des AV ces dernières années, tandis que cette évolution était probablement moins marquée dans le domaine de la gestion de fortune internationale. Le fait que les cocontractants signalés sont souvent des *money mules* présumées ou des victimes d'escroquerie pourrait fournir une autre explication : on trouve en effet ces deux cas de figure plutôt dans le segment de la clientèle privée que dans la gestion de fortune internationale.

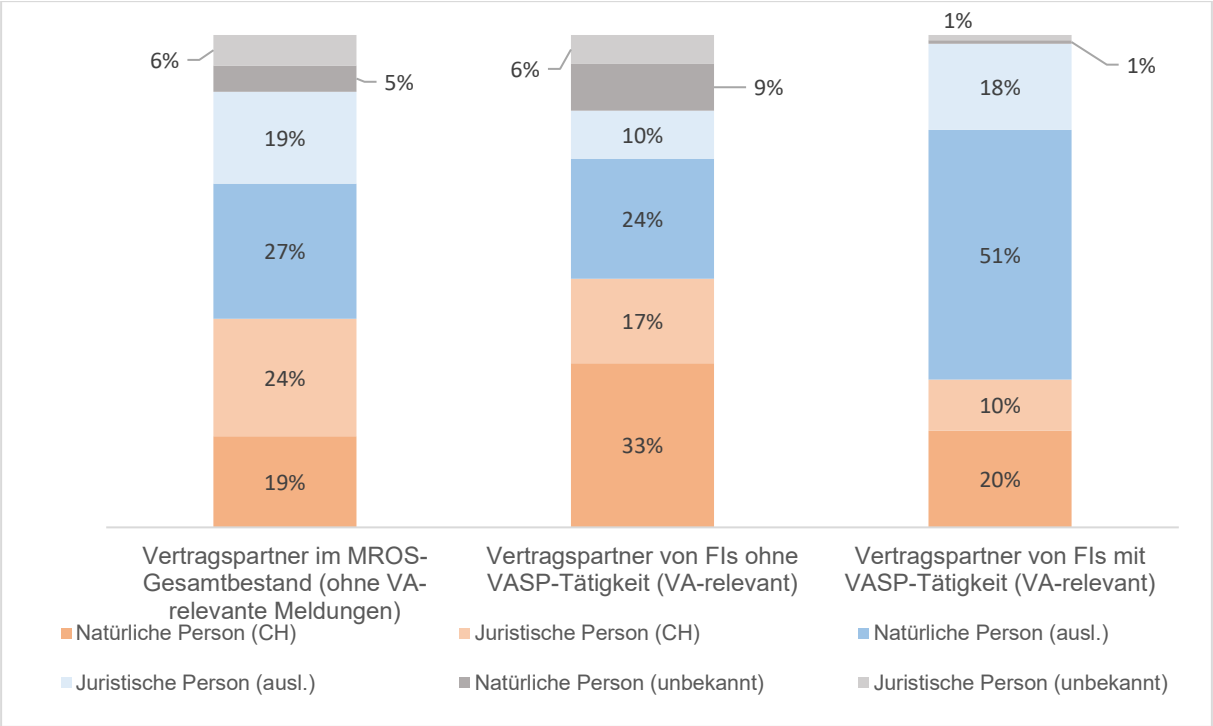

Fig. 26 : Cocontractants signalés dans les 1867 communications de soupçons en lien avec des AV (2020 – 2022) comparés aux contractants de toutes les communications de la même période (déduction faite des 1867 en lien avec des AV). Plus de la moitié des contractants de relations d'affaires signalés par des intermédiaires financiers exerçant une activité de PSAV sont des personnes physiques de nationalité étrangère[216].

7.4 Vulnérabilités de la poursuite pénale dans le domaine des AV

Dans le domaine des AV, les autorités de poursuite pénale se trouvent face à des opportunités et à des difficultés supplémentaires. On peut évoquer des problèmes d'ordre technologique et juridique, mais aussi concernant les ressources et la formation. Des difficultés concrètes se posent en particulier dans le traçage des transactions d'AV, l'identification du détenteur d'un portefeuille, la saisie d'un portefeuille et le recouvrement des AV qui y sont enregistrés et, enfin, l'obtention d'informations et de preuves transfrontalières. Quant aux opportunités, elles sont à chercher notamment dans le domaine de l'analyse de blockchain ainsi que dans une coopération nationale et internationale plus étroite et simplifiée.

[216] Remarque: pour les personnes physiques ayant la double nationalité, on a tenu compte seulement de la première ou de la plus ancienne information à leur sujet dans la banque de données du MROS. Plus il y a de personnes physiques ayant la double nationalité parmi les cocontractants signalés, moins le graphique est pertinent s'agissant de l'indication de la nationalité des personnes physiques.

7.4.1 Élucidation des infractions dans le domaine des AV

Les AV offrent l'avantage aux autorités de poursuite pénale de pouvoir suivre les activités financières d'une personne sur la blockchain en temps réel. La technologie de la blockchain permet théoriquement de retracer l'origine et la destination d'AV. C'est très important en particulier pour l'administration des preuves : lorsqu'une infraction est par exemple commise à l'étranger et que les fonds sont blanchis en Suisse, il est d'une importance cruciale de pouvoir établir le lien entre l'acte de BA et l'infraction qui l'a précédé (acte préalable). Or, des paiements sur la blockchain transparents peuvent faciliter la tâche, car dans ce cas, les transactions sont visibles et publiques.

Afin de pouvoir effectuer une analyse de blockchain de manière efficace et autonome, il faut acquérir des outils et des connaissances spécifiques. Il vaut la peine d'investir du temps et de l'argent pour développer ces capacités, comme le montrent plusieurs cas récents à l'étranger, où les autorités de poursuite pénale ont pu confisquer des AV valant plusieurs milliards, alors que les infractions associées avaient été commises il y a de nombreuses années[217].

Le sondage auprès de 27 autorités de police suisses montre que plus de la moitié d'entre elles se sont équipées avec au moins un outil d'analyse de blockchain (état à fin avril 2023)[218]. La grande majorité de l'autre moitié a toutefois indiqué disposer d'un accès indirect à de tels outils (cf. NEDIK, ch. 7.4.2). Seules deux autorités ont signalé n'avoir ni accès (indirect) à des outils de traçage, ni d'intention d'en acquérir un. Ce résultat montre que les autorités de poursuite pénale suisses ont conscience qu'il faut agir dans ce domaine et qu'elles sont prêtes à se donner les moyens nécessaires.

Cependant, la majorité des 27 autorités interrogées ont également fait part de difficultés considérables dans l'utilisation de ces outils d'analyse de blockchain, plus précisément en ce qui concerne les transactions hors de la chaîne et de seconde couche. Parallèlement aux progrès réalisés dans le traçage des transactions d'AV avec des outils d'analyse de blockchain, les techniques de dissimulation ont elles aussi évolué et sont devenues plus sophistiquées (cf. 10^{e} menace). Aussi, les analyses de blockchain n'ont fourni dans certains cas que peu voire pas de possibilités exploitables. Acquérir ces outils ne suffit donc pas pour maîtriser les défis dans ce domaine. Un haut niveau de connaissances spécialisées, un perfectionnement continu et le développement des outils d'analyse sont nécessaires pour que les autorités de poursuite pénale aient une longueur d'avance dans cette course à l'armement entre les techniques de dissimulation d'un côté et les techniques de détection de l'autre côté.

Faute d'avoir reçu des données consolidées des autorités de police cantonales et municipales, nous avons demandé, dans le cadre du présent rapport, à la PJF et au MROS à quelles techniques ils avaient déjà eu affaire dans leur travail. Ils ont cité l'utilisation de *peel chains*, mixeurs, *chain hopping*, *privacy coins*, *wash trading* ainsi que le recours à des PSAV ayant des exigences KYC faibles voire inexistantes (cf. encadré n° 4).

[217] Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26 janvier 2023

[218] Remarque: outre les polices municipales et cantonales ont également été consultés l'Institut Suisse de police (ISP) et la Prévention Suisse de la criminalité (PSC).

Encadré n° 4

Techniques de dissimulation

Services de mixage et *privacy wallets:* un service de mixage permet de mélanger des AV portant la marque d'activités criminelles avec des AV "propres". En général, la manœuvre consiste à regrouper des AV provenant de diverses sources pour une période assez longue, dans le but de les rendre impossibles à différencier. Les *privacy wallets* (par ex. Wasabi Wallet) utilisent des techniques d'anonymisation intégrées comme CoinJoin afin d'obtenir cet effet cocktail pour tous les AV déposés sur ces portefeuilles.

Peel chain : il s'agit d'une longue série de transactions consistant à répartir de gros montants en plusieurs petits montants sur des adresses qui servent à dissimuler l'origine ou le but d'un flux de transactions. Vu les faibles montants, la probabilité est d'autant plus faible que l'entrée des fonds sur des bourses d'échanges génèrent un signal d'alerte.

Privacy coins : certaines cryptomonnaies (par ex. Monero) ont été conçues dans le but de pouvoir effectuer des transactions qui ne soient pas visibles de façon transparente sur la blockchain concernée, et ne puissent donc pas être retracées.

Chain hopping : ce terme désigne le déplacement d'AV d'une blockchain à une autre, souvent plusieurs fois de suite en rafales au moyen de diverses blockchains différentes, afin d'empêcher le traçage.

Wash trading : cette technique consiste à "revendre" des AV à soi-même ou à des complices en leur faisant faire des allers-retours entre les portefeuilles. Cela permet de générer artificiellement un historique des transactions, afin de susciter l'impression que l'AV correspondant (par ex. un NFT spécifique ou une cryptomonnaie avec un faible volume commercial et une faible capitalisation boursière) est plus convoité que ce n'est réellement le cas, ce qui permet de gonfler artificiellement sa valeur. Le *wash trading* d'AV se prête au BA, d'une part parce que l'origine des fonds peut être dissimulée à l'aide d'un long historique de transactions. D'autre part, cette technique permet aussi de rendre plausible la constitution d'une fortune ou d'augmenter le montant original incriminé[219].

Recours à des PSAV ayant des exigences KYC faibles voire inexistantes (souvent des nested services) : certaines plates-formes peuvent se trouver dans des juridictions qui ne mettent pas suffisamment en œuvre les normes internationales de lutte contre le BA et le FT. De nombreux services utilisés par les criminels pour convertir des AV en monnaie fiat (*fiat off-ramps*) sont des brokers *over-the-counter* (OTC). Ils utilisent les grandes bourses de négoce d'AV pour tirer parti de la liquidité et des paires de devises de ces grands prestataires. C'est pourquoi ils sont qualifiés de *nested services*, autrement dit de services emboîtés, car dans les premiers temps de l'enquête, on constate que les adresses qu'ils utilisent mènent toujours droit aux grandes bourses de négoce. La plupart des brokers OTC sont des entreprises connues et sérieuses. Les données *on-chain* examinées provenant d'entreprises d'analyse de blockchain laissent toutefois penser qu'un petit groupe de ces brokers rend possible la majeure partie du BA en relation avec la conversion d'AV en monnaie fiat[220].

[219] Chainalysis, *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class*, 2 février 2022

[220] Wired Magazine, *Most Criminal Cryptocurrency Funnels Through Just 5 Exchanges*, 26 janvier 2023; Europol, *Bitzlato: senior management arrested*, 23 janvier 2023

Si un portefeuille lié à une activité criminelle a été identifié et si les AV incriminés se trouvent encore sur ce portefeuille, saisir ces AV n'est pas si simple non plus. Si les AV liés à l'activité criminelle se trouvent sur un portefeuille hébergé, il est possible d'accéder à ce portefeuille par le biais de l'intermédiaire financier ou du PSAV qui le gère et en possède par conséquent la clé privée. Mais à deux conditions : premièrement, il faut que les autorités de poursuite pénale aient la possibilité de prendre contact, deuxièmement, il faut que le PSAV soit disposé à collaborer. Dans plusieurs cas traités par la PJF, les AV se trouvant sur un portefeuille hébergé ont pu être saisis.

Si en revanche les AV incriminés se trouvent sur un portefeuille non hébergé, seul le détenteur en possède la clé privée (ou plusieurs personnes dans le cas d'un portefeuille multisignature). Dans ce cas, il est beaucoup plus difficile pour les autorités de poursuite pénale d'accéder au portefeuille, de confisquer les AV et de bloquer toute transaction future potentielle. Un cas traité par la PJF a toutefois révélé que, si les conditions sont favorables, il est tout à fait possible de saisir des AV aussi sur un portefeuille non hébergé.

10e menace

Anonymat des transactions et difficulté d'identification des ayants droit économiques (identifiée en 2018, inchangée)[221]

L'analyse sectorielle de 2018 notait qu'en matière d'anonymat (ou d'usage de pseudonymes), les AV étaient associés à un risque similaire que l'argent liquide. Il notait aussi que le danger que posent les AV était accru du fait de la rapidité et de la mobilité des transactions grâce à la technologie.

Depuis 2018, les outils des entreprises d'analyse de blockchain sont devenus beaucoup plus efficaces et comportent par exemple des fonctionnalités permettant la détection automatique de certaines techniques de dissimulation et certains schémas de transaction. Divers cas montrent que l'application de ces outils et la collaboration avec les entreprises d'analyse de blockchain peuvent s'avérer fructueuses (cf. ch. 8.2.2 et 8.2.4). Néanmoins, la "crypto-communauté" s'efforce de son côté de conserver et même de développer les possibilités de dissimulation et de maintien de l'anonymat. Les efforts respectifs de ces deux groupes d'intérêts antagonistes ressemblent à une course à l'armement, dont la fin n'est pas encore en vue et dont nul ne sait qui sortira vainqueur. Par conséquent, cette menace n'a pas évolué de façon significative par rapport à 2018.

7.4.2 Coopération nationale et internationale

Une autre difficulté d'ordre technologique, et soit dit en passant l'une des raisons principales du développement de la banque de données PICSEL, est la détection de cas reliés entre eux (séries d'infractions). Dans le cadre de l'enquête réalisée auprès des autorités de police suisses, certaines d'entre elles ont préconisé de renforcer l'échange de données et d'informations afin de faciliter la détection de séries.

[221] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowfunding*, octobre 2018, pp. 21-22

Typologie n° 4

La détection d'un schéma de fraude organisée

Un intermédiaire financier suisse exerçant une activité de PSAV propose à ses clients d'acheter des AV sur son application, où il est possible de payer avec une carte de crédit ou d'autres moyens de paiement électroniques comme Apple Pay ou Google Pay. L'intermédiaire financier a été contacté par une autorité de poursuite pénale étrangère qui l'a informé qu'une victime de fraude présumée avait porté plainte, car les données de sa carte de crédit avaient été utilisées à son insu afin d'acquérir des AV sur la plate-forme de l'intermédiaire financier en question. Celui-ci a réagi en déposant une communication de soupçons auprès du MROS, qui ne contenait toutefois que très peu d'informations exploitables pour retracer et tracer les flux financiers signalés et les mettre en lien avec les informations figurant déjà dans la banque de données du MROS. Le courrier annexé de l'autorité de poursuite pénale étrangère contenait le nom de la victime présumée, mais l'intermédiaire financier n'avait aucune relation d'affaires ouverte à ce nom. De plus, il ne possédait pas non plus les données de carte de crédit complètes de la victime de fraude, car les AV qu'il a délivrés lui avaient été payés indirectement, par le biais d'un terminal de paiement. Il n'a pu communiquer au MROS que les six premiers et les quatre derniers chiffres de la carte de crédit utilisée. Et il ne possédait que peu d'informations sur son "client", qui n'était manifestement pas la même personne que la victime de fraude étrangère. L'intermédiaire financier n'avait aucun renseignement sur ce client (nom, adresse, date de naissance, etc.) et n'a pu donner au MROS que l'adresse IP et le modèle de téléphone portable au moyen desquels l'escroc présumé s'était connecté sur l'application de l'intermédiaire financier. Après la réception du montant débité sur la carte de crédit de la victime, les AV achetés ont été envoyés directement sur une adresse AV, sur laquelle l'intermédiaire financier n'avait aucun pouvoir de décision et ne pouvait donc pas bloquer (portefeuille non hébergé). En analysant les informations se trouvant dans d'autres communications de soupçons du même intermédiaire financier, le MROS s'est aperçu que plusieurs transactions présumées frauduleuses, qui avaient été portées à sa connaissance dans plusieurs communications de soupçons, avaient atterri sur la même adresse finale après avoir passé par plusieurs stations intermédiaires, ce qui constitue un indice fort de schéma de fraude organisée.

Dans la période analysée, le MROS a reçu de nombreuses communications de soupçons avec un contenu similaire à celui décrit dans la typologie précitée. Les victimes de fraude présumées étaient presque toutes domiciliées à l'étranger. Ces communications ont pour dénominateur commun, d'une part, le fait que les intermédiaires financiers ne possédaient presque pas d'informations sur les relations d'affaires signalées[222] et, d'autre part, le fait que les transactions signalées dans chacune d'entre elles avaient peu de contre-valeur. Il paraît évident que des communications de soupçons aux contenus tellement semblables pointent vers des schémas de fraude organisée de grande ampleur, d'autant plus que le MROS, en traçant les AV présumés volés, a pu identifier des techniques de dissimulation. Dans le cadre de l'activité d'analyse du MROS et du traitement de ces cas par les autorités de poursuite pénale, l'établissement de liens entre ces "cas isolés", par exemple au moyen d'outils de traçage ou de l'échange d'informations avec des autorités étrangères, ne va pas sans difficultés et exige l'investissement de ressources. Les communications de soupçons ou les dénonciations pénales ne comportent souvent que peu voire pas d'informations utiles pour faire avancer l'enquête sur les auteurs présumés. Les transactions signalées n'ont en outre souvent qu'une faible contre-valeur, ce qui peut avoir pour effet que répondre aux demandes d'information déposées par les bureaux homologues étrangers prend beaucoup de temps, car ces demandes ne sont pas traitées en priorité. Cette situation fait courir le risque aux autorités

[222] Par ex. des informations personnelles sur les utilisateurs concrets de l'application et sur les comptes d'où provenaient les montants versés pour acquérir des AV.

de poursuite pénale de ne pas découvrir ces systèmes de fraude organisée visant à dérober et à blanchir des AV.

Outre la banque de données intercantonale PICSEL, qui peut servir d'instrument pour analyser les liens entre les différents cas et fournir une vision d'ensemble, il existe aussi le NEDIK (*Netzwerk digitale Ermittlungsunterstützung Internetkriminalität*) en Suisse, ce réseau de spécialistes qui permet à un corps de police cantonal de fournir des prestations en faveur de tous les corps de police suisses. Le NEDIK organise des réunions régulières sur la thématique des AV, qui visent à échanger des informations et à fixer des normes en la matière. Les petits cantons avec peu de ressources peuvent demander de l'aide à la Confédération ou aux cantons compétents via l'assistance administrative, par analogie à d'autres outils spéciaux. Selon les informations recueillies, certains grands cantons comme Zurich investissent des ressources dans le développement de leur savoir-faire et de leurs outils, afin de pouvoir effectuer des analyses dans le domaine de la cybercriminalité pour leur propre compte ou pour des autorités qui en font la demande. De même, les enquêteurs spécialisés se sont mis en réseau avec d'autres policiers spécialistes des AV. Les autorités de poursuite pénale sont en contact les unes avec les autres à travers divers réseaux internationaux et peuvent par exemple échanger des informations via Interpol ou Europol ou coordonner des enquêtes.

Une autre possibilité est l'échange entre les bureaux de communication nationaux, par exemple dans le cadre de l'*Egmont Group of Financial Intelligence Units*. Le MROS est la CRF suisse et, à ce titre, reçoit de la part de ses homologues de précieuses informations et des demandes relatives à l'utilisation d'AV à des fins de BA et de FT ayant un lien avec la Suisse. Le cas échéant, il peut transmettre ces informations à d'autres autorités ou offices suisses chargés de lutter contre le BA et le FT à des fins de renseignement. À l'inverse, le MROS envoie lui aussi des informations spontanées et des demandes d'information aux CRF étrangères pour sa propre analyse, ou parfois à titre d'assistance administrative pour d'autres autorités suisses. Les plates-formes d'échange mentionnées ici ont donné naissance à plusieurs projets et publications, comme des catalogues d'information sur les intermédiaires financiers exerçant une activité de PSAV établis dans différents pays, ou des guides avec les meilleures pratiques à l'intention des autorités de poursuite pénale, pour leurs enquêtes en lien avec des AV et pour la prise de contact avec des intermédiaires financiers exerçant une activité de PSAV dans un autre pays.

Les discussions avec les autorités de poursuite pénale à l'échelle cantonale ou fédérale ont montré que dans plusieurs cas, il a été possible de bloquer des AV se trouvant sur des plates-formes d'intermédiaires financiers étrangers exerçant une activité de PSAV et de les restituer aux victimes. Cela a pu se faire grâce à l'entraide judiciaire internationale ou à la faveur de la Convention de Budapest (cf. encadré n° 5).

Encadré n° 5

La Convention de Budapest

La Convention du 23 novembre 2001 sur la cybercriminalité (Convention de Budapest) est un traité international visant à lutter contre la cybercriminalité. Adoptée par le Conseil de l'Europe en 2001, cette convention compte aujourd'hui 65 pays signataires, dont la plupart des pays européens, les États-Unis et le Japon.

En Suisse, la Convention de Budapest est entrée en vigueur en 2012[223]. Les autorités de poursuite pénale peuvent profiter de cette convention pour avoir accès à des moyens de preuve électroniques se trouvant à l'étranger, y compris aux données conservées par des entreprises privées, sans avoir à passer par l'entraide judiciaire.

[223] RS **0.311.43** – *Convention du 23 novembre 2001 sur la cybercriminalité*, état le 14 septembre 2020

Ainsi, l'art. 32 de la Convention de Budapest prévoit que dans certaines circonstances, il est possible d'accéder à des données informatiques détenues par un autre État. Il peut s'agir également de données sur des relations d'affaires d'intermédiaires financiers exerçant une activité de PSAV qui sont domiciliés dans un pays signataire. Il est ainsi possible de déterminer rapidement à quel nom est établi un compte ouvert auprès d'un intermédiaire financier étranger exerçant une activité de PSAV, qui en est l'ayant droit économique, ou quelles transactions ont été effectuées sur ce compte et à quelles dates. Le BA et le FT au moyen d'AV étant souvent pratiqués au moyen de transactions transnationales effectuées en quelques secondes, la Convention de Budapest permet d'accélérer le travail des autorités de poursuite pénale, afin de parvenir à des taux d'élucidation plus élevés ainsi qu'à davantage de blocages et de confiscations d'AV. C'est un avantage de taille par rapport aux enquêtes usuelles, dont le succès dépend, d'une part, du temps de réaction des autorités étrangères pour exécuter les demandes d'entraide judiciaire internationale et, d'autre part, des délais de retenue des documents financiers par les banques, qui sont très variables en fonction de la juridiction.

L'analyse sectorielle du GCBF de 2018 faisait déjà référence à la Convention de Budapest, quand bien même on connaissait encore mal cette possibilité d'accès transfrontière à des moyens de preuve électroniques[224]. Selon les informations recueillies dans le cadre de la présente analyse de risques, les autorités de poursuite pénale suisses ont de l'expérience en matière d'application de la Convention de Budapest. Certaines semblent avoir fait plutôt de bonnes expériences, tandis que d'autres soulignent que la collaboration avec les entreprises privées étrangères s'avère difficile et imprévisible d'un cas à l'autre, si bien qu'on ne sait jamais si l'entreprise va accepter de transmettre ses données ou va au contraire refuser et renvoyer à la voie de l'entraide judiciaire, ce qui fait perdre un temps précieux pour l'enquête. Bon nombre d'entreprises choisissent une voie médiane, en transmettant leurs données, mais uniquement à des fins de "renseignement" et pas à des fins de preuve. Cela permet de continuer l'enquête, mais ces données ne peuvent être utilisées comme preuves qu'après avoir passé par l'étape de l'entraide judiciaire internationale.

5e vulnérabilité

Difficile répression du BA et du FT dans le domaine des AV (identifiée en 2018, inchangée en 2023)[225]

Le principe de l'anonymat ou de l'utilisation de pseudonymes dans le fonctionnement des AV, la décentralisation de leur architecture notamment dans le cadre de la FiDé et de la DAO, ainsi que les fortes imbrications internationales des relations d'affaires dans le domaine des AV, confrontent les autorités de poursuite pénale à de grandes difficultés pour identifier les interlocuteurs correspondants et prendre contact avec eux afin d'obtenir des informations utiles pour leurs enquêtes ou procédures. Lorsque les bons interlocuteurs sont identifiés, ils ne se trouvent généralement pas dans le même pays que l'autorité de poursuite pénale concernée. Si les informations visées ne peuvent pas être obtenues sur la base de la Convention de Budapest, les autorités de poursuite pénale doivent demander ces informations par le biais de l'entraide judiciaire internationale, ce qui prend en général du temps. Or, la perte de temps est déjà problématique dans les enquêtes et procédures sans lien avec des AV, lorsque les autorités de poursuite pénale doivent retracer des flux financiers. Le défi est d'autant plus grand dans le domaine des AV qui, par rapport au trafic de paiements traditionnel, est caractérisé par des transactions effectuées en quelques secondes et passant par plusieurs

[224] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowfunding*, octobre 2018, pp. 41 - 42
[225] Ibid., pp. 34 - 35

blockchains, intermédiaires financiers, plates-formes décentralisées et frontières nationales. Il est par conséquent plus compliqué d'élucider des infractions dans ce domaine en général, et de lutter contre le BA et le FT en particulier.

En comparaison internationale ainsi qu'au sein de chaque pays, de grandes différences apparaissent au niveau de l'expertise des autorités de poursuite pénale dans le domaine des AV. Tandis que certaines autorités ont investi très tôt dans le développement de connaissances et de capacités et disposent des outils nécessaires pour élucider les infractions, d'autres n'ont absolument rien entrepris, ce qui complique la coopération nationale et internationale, tant au plan de la communication qu'à celui de l'enquête et des procédures. Les approches de réglementation inégales voire absentes au niveau global, couplées à l'importance et à la priorité variables accordées aux cas du domaine des AV, augmentent les risques d'arbitrage réglementaire par les criminels, qui exploitent les vides juridiques à dessein afin d'empêcher que leurs activités ne soient découvertes et qu'ils ne soient poursuivis pénalement.

7.4.3 Jurisprudence

Selon les recherches effectuées dans le cadre de la présente analyse de risques, il n'y a pas encore en Suisse de jugements entrés en force relatifs au BA par l'utilisation d'AV, ni au niveau cantonal ni au niveau fédéral. Un jugement de ce type pourrait montrer de façon détaillée dans quelles conditions l'élément constitutif d'infraction de BA est réalisé en lien avec l'utilisation d'AV. Seul un arrêt du Tribunal pénal fédéral (TPF) de décembre 2022 contient plus d'informations à ce sujet. Il s'agissait du recours qui a été rejeté d'une personne qui voulait empêcher que le ministère public genevois ne transmette ses documents bancaires à un autre pays européen dans le cadre de l'entraide judiciaire internationale. Une autorité de poursuite pénale du pays concerné accuse cette personne (et d'autres) notamment de fraude fiscale et de BA en bande. L'arrêt spécifie que "le changement d'argent en cryptomonnaie [est une conduite propre] à entraver l'identification de l'origine, la découverte ou la confiscation de valeurs patrimoniales au sens de l'art. 305bis CP"[226]. Du point de vue du TPF, le "simple" changement de monnaie fiat en AV suffit déjà à réaliser l'élément constitutif d'infraction de BA.

7.5 Vulnérabilités des intermédiaires financiers dans le domaine des AV

La vulnérabilité des intermédiaires financiers à être exploités à des fins de BA ou de FT peut être atténuée notamment par une surveillance adéquate, même si cela ne suffit pas à la supprimer totalement. L'écrasante majorité (174) des intermédiaires financiers suisses exerçant une activité de PSAV sont affiliés à un OAR, qui veille à ce qu'ils respectent leurs obligations légales, tandis que les banques et les maisons de titres exerçant une activité de PSAV sont directement assujettis à la FINMA (environ 30)[227].

Il n'a pas été possible d'obtenir des informations consolidées sur la surveillance concrète exercée par les OAR sur les intermédiaires financiers exerçant une activité de PSAV. Un échange d'informations entre le MROS et un OAR en 2021 montrait toutefois que les membres affiliés ayant une activité de PSAV étaient soumis à des règles de surveillance plus strictes que les autres. Ils devaient par exemple passer un audit dans un délai de six mois (au lieu du délai habituel de douze mois) après leur admission dans l'OAR. C'est soit l'OAR, soit une

[226] RR.2022.45, *Arrêt du 20 décembre 2022*, arrêt du TPF, Bellinzone, 21 décembre 2022
[227] État à fin 2022

société d'audit accréditée par l'OAR qui contrôle que l'intermédiaire financier respecte les obligations de la LBA.

Typologie n° 5

Société anonyme suisse avec licence OAR acquise et payée en AV par des acheteurs anonymes

Un intermédiaire financier suisse exerçant une activité de PSAV a signalé une relation d'affaires avec un client commercial suisse qui s'est manifestement spécialisé dans la création de sociétés et de services fiduciaires suisses. Ce client proposait sur son site Internet de fonder des sociétés en Suisse pour le compte de personnes étrangères et de s'occuper de toute la "bureaucratie", à savoir créer un site Internet, un logo, une brochure de présentation et des cartes de visite, et mettre à disposition une boîte aux lettres domiciliée chez un tiers ainsi qu'un poste de travail entièrement équipé "temporaire". Pour un coût supplémentaire, il "vendait" également une domiciliation postale propre, vraisemblablement pour éviter de donner l'impression que la nouvelle société était une société boîte aux lettres. Enfin, sur les réseaux sociaux, il proposait aussi aux collaborateurs de ses clients commerciaux son assistance pour obtenir une licence OAR.

Le client précité a ouvert une relation d'affaires auprès de l'intermédiaire financier auteur de la communication au motif de pouvoir offrir à sa clientèle la possibilité de payer en cryptomonnaies. Quelque temps après l'ouverture de la relation d'affaires, l'intermédiaire financier a remarqué trois versements provenant d'une adresse crypto inconnue, effectués en l'espace de quelques minutes et qui additionnés représentaient un montant de l'ordre d'un demi-million de francs suisses. Chacun des trois versements était toutefois juste en dessous du montant limite autorisé par l'intermédiaire financier pour un tel versement, ce qui a paru suspect à l'intermédiaire financier (*smurfing*), si bien qu'il a pris contact avec le client afin de clarifier le contexte économique de ces transactions. Le client lui a répondu que ces versements étaient liés à la vente d'une de ses sociétés. En guise de preuve, il lui a fourni un acte de vente stipulant qu'il avait aliéné 100 % des actions d'une société suisse à deux acheteurs, dont il avait toutefois caviardé le nom sur l'acte. L'intermédiaire financier lui a alors demandé pour quel motif le paiement avait été subdivisé en trois, ce à quoi le client a répondu qu'il s'était conformé à la volonté des acheteurs d'avoir la possibilité de payer la facture à des dates différentes afin de pouvoir choisir des taux de change favorables. Cette réponse n'a pas paru plausible à l'intermédiaire financier, les trois versements ayant été effectués à quelques minutes d'intervalle, si bien qu'il a transmis une communication de soupçons au MROS. La société anonyme vendue était elle-même membre d'un OAR et, par conséquent, un intermédiaire financier régi par le droit suisse.

On a donc affaire ici à la vente d'un intermédiaire financier suisse à des acheteurs anonymes qui ont payé en AV.

11e menace

La *travel rule* n'est pas appliquée aux comptes marchands des intermédiaires financiers suisses exerçant une activité de PSAV (identifiée en 2023)

En Suisse, les personnes physiques et morales peuvent accepter des AV pour le paiement des services qu'ils fournissent. Les intermédiaires financiers suisses exerçant une activité de PSAV proposent des comptes marchands aux personnes morales dont le siège est en Suisse.

Selon le site Internet d'un intermédiaire financier suisse exerçant une activité de PSAV, les personnes morales précitées peuvent recevoir des versements en AV sur ces comptes. Le respect des obligations de diligence et de communication incombe à l'intermédiaire financier suisse qui propose ces comptes marchands. Contrairement aux dispositions de la *travel rule,* il ne semble pas dans ce cas que l'intermédiaire financier suisse exerçant une activité de PSAV recueille des informations sur l'expéditeur des AV (cf. fig. 9 au ch. 4.4.4). Il en résulte un risque accru que ce type d'offres proposées par des personnes morales suisses soient utilisées à mauvais escient pour blanchir des AV, notamment dans le cadre du BA basé sur des comptes marchands. Le MROS connaît en outre des cas où le montant limite de paiements en AV a été dépassé au moyen de *smurfing.*

Comme les OAR, la FINMA fait elle aussi appel à des sociétés d'audit pour contrôler les établissements qui lui sont assujettis en termes de risques et de respect de la LBA. En été 2021, la FINMA a précisé ce qu'elle attendait des sociétés d'audit lorsqu'elles contrôlent des établissements actifs dans le domaine des AV. Les sociétés d'audit utilisent un module de contrôle spécifique aux AV ou aux PSAV pour contrôler ces établissements.

La FINMA a en outre examiné chez plusieurs prestataires de services financiers qui lui sont assujettis comment ils mettaient en œuvre le contrôle de la justification économique de leurs clients pour avoir un portefeuille non hébergé. Une solution fréquente est que l'intermédiaire financier convienne le montant (micro-paiement par exemple) ainsi que la date du versement à l'avance avec son client. Une deuxième solution consiste à demander au client d'envoyer un message clair sur la blockchain dans un certain délai. Cette procédure est à effectuer lors du premier versement. Ensuite, l'adresse peut être ajoutée à une *white list*, laquelle rend le contrôle superflu lors de versements ultérieurs pourvus de la même adresse. Cette procédure est répétée à intervalles réguliers définis par l'établissement et par exemple suite à des transactions présentant des risques accrus, et ce, de manière à ce qu'il ne puisse y avoir aucun doute quant au pouvoir de disposition sur les portefeuilles externes. Elle est techniquement irréalisable lors des transactions où la contrepartie est représentée par un prestataire qui détient des portefeuilles collectifs. Dans de tels cas, la FINMA accepte la vérification du pouvoir de disposer au moyen d'une capture d'écran : l'intermédiaire financier bénéficiaire demande une capture d'écran de la transaction annoncée par le client ; le document fourni atteste que le client bénéficie du pouvoir de disposer sur le compte à débiter auprès du PSAV[228]. Un nouvel élément est venu s'ajouter aux méthodes de vérification usuelles : la procédure *time boxing*, où les clients effectuent une micro-transaction préalable en virant un montant directement. Ils doivent annoncer la transaction et le montant souhaité, puis l'intermédiaire financier leur indique l'adresse et une fenêtre temporelle courte (*time box*). La transaction convenue doit être effectuée suivant ces indications. La preuve du pouvoir de disposition est apportée par la vérification que ces indications ont été respectées. Une autre nouveauté est le *wallet-log-in* (connexion au portefeuille) des clients en présence de collaborateurs de l'intermédiaire financier. Pour autant que la procédure soit suffisamment documentée, il s'agit également d'une mesure judicieuse qui va dans le sens de la communication de la FINMA sur la surveillance 02/2019 "Trafic des paiements sur la blockchain".

Les investisseurs se montrent toujours très intéressés par les modèles d'affaires liés à la technologie de la blockchain, ce dont profitent aussi certains acteurs du marché qui ne sont pas sérieux et qui lancent des offres de ce type, souvent en faisant de la publicité sur Internet pour attirer les clients. Typiquement, ils tentent d'inciter les investisseurs à acheter des cryptomonnaies en leur faisant miroiter des entreprises et des produits qui n'existent pas. Dès qu'elle en a connaissance, la FINMA place ces acteurs du marché sur sa liste d'alerte et met en garde les investisseurs. En outre, elle se concerte avec les autorités de poursuite pénale suisses et les autorités de surveillance étrangères. Dans le domaine des Fintech, la FINMA a

[228] FINMA, Rapport annuel 2020, mars 2021, pp. 43 - 44

travaillé intensivement sur la question des ICO en Suisse. En raison du stade précoce de nombreuses ICO, beaucoup d'insécurités persistent quant aux projets à financer et à effectuer. La FINMA ne peut pas exclure que des activités liées à des ICO aient lieu dans un but frauduleux. Elle ne tolère pas de comportement frauduleux ou abusif, ni que le cadre réglementaire soit contourné, et peut, le cas échéant, prendre les mesures d'enforcement nécessaires.

Au total, environ 60 ICO ont fait l'objet de clarifications, dont plus de la moitié ont pu être clôturées. La FINMA a constaté une violation de la LBA dans une douzaine d'ICO et a déposé plainte contre les personnes responsables. Huit autres cas ont donné lieu à un placement sur la liste d'alerte. La FINMA a enfin mené une procédure d'enforcement contre trois sociétés, dont une a déjà pris fin. Dans l'une de ces procédures, la société a ignoré l'évaluation préalable de la FINMA en répondant à la demande d'assujettissement. Par ailleurs, la FINMA a ordonné des mesures visant à rétablir une situation conforme à la loi. Celles-ci comprenaient notamment le remboursement de dépôts du public acceptés illicitement selon la loi sur les banques ainsi que la suppression du mot "banque" et de la publicité mentionnant des autorisations de la FINMA non existantes. Récemment, on constate une nouvelle tendance à proposer des *stablecoins,* ce qui soulève des questions liées à l'applicabilité des lois sur le blanchiment d'argent, sur les banques et sur les placements collectifs.

Outre les activités de marché dans le domaine des ICO, la FINMA a aussi constaté que les prestataires suisses s'investissent de plus en plus dans les services financiers du marché secondaire dans le domaine de la cryptofinance. Il peut s'agir par exemple du négoce et de la conservation de jetons ou de l'exploitation de places de négoce et des activités connexes. Ces dernières années, la section chargée de l'enforcement a effectué des clarifications vis-à-vis de plusieurs de ces prestataires. Après avoir constaté des violations de la loi sur les banques et de la loi sur les bourses chez l'un d'entre eux, elle a ordonné des mesures de grande ampleur pour rétablir une situation conforme à la loi et a fait une dénonciation pénale. Elle mène en outre une procédure d'enforcement contre un prestataire de transmission de fonds (*money transmitting*) entre des crypto-bourses et leurs clients pour acceptation illicite de dépôts du public. Dans un autre cas, elle a ouvert une procédure d'enforcement pour négoce de titres en jetons non autorisé. Par ailleurs, la FINMA a aussi interdit divers prestataires de *coins* et, en mai 2023, achevé une procédure contre une fondation active dans la cryptofinance et contre son fondateur. Dans ce dernier cas, elle a conclu à une grave violation du droit de la surveillance sur plusieurs points. Une procédure de faillite avait été ouverte contre la fondation en mars 2023. La FINMA a prononcé une interdiction générale d'exercer à l'encontre du fondateur de la fondation, qu'elle a publiée sur son site Internet pour une durée de cinq ans[229]. Dans l'ensemble, la FINMA observe un nombre croissant de sites Internet frauduleux relatifs à des services d'AV qui proposent à leurs clients de prétendus investissements dans les cryptomonnaies et qui n'affectent pas les fonds versés aux fins prévues. Quand elle le peut, la FINMA met en garde contre ces offres sur sa liste d'alerte.

Dans le domaine des jeux d'argent illégaux, la CFMJ, qui exerce la surveillance sur les casinos, a traité deux cas d'établissements de jeu ayant installé un distributeur d'AV pour le paiement des gains aux joueurs. Dans l'un des cas, une plainte a été déposée et la procédure est pendante. Dans l'autre cas, on n'a pas pu apporter la preuve suffisante que le distributeur d'AV trouvé sur les lieux avait effectivement été utilisé pour le paiement des gains de jeu et on n'a pas pu établir non plus qui était l'exploitant réel de la plate-forme illégale. La CFMJ estime que les AV pourraient devenir un moyen de paiement apprécié en Suisse dans le domaine des offres de jeux de hasard illégaux.

[229] FINMA, La FINMA clôt une procédure à l'encontre d'une plate-forme cryptographique et son fondateur, mai 2023

7.5.1 Intermédiaires financiers auteurs de communications

L'analyse des communications de soupçons liés aux AV des années 2020 à 2022 montre que les intermédiaires financiers ont un comportement très différent selon qu'ils exercent une activité de PSAV ou non.

	2020		**2021**		**2022**		**2020-2022** (total)	
Communications de soupçons en lien avec des AV	312		499		1056		1867	
	avec PSAV	**sans PSAV**	**avec PSAV**	**sans PSAV**	**avec PSAV**	**sans PSAV**	**avec PSAV**	**sans PSAV**
Nombre d'intermédiaires financiers signalants	12	40	19	57	12	93	24	118
Nombre de communications en lien avec des AV	104	208	178	321	143	913	425	1442

Fig. 27 : Communications de soupçons en lien avec des AV et leur proportion par rapport à l'ensemble des communications (2020 - 2022), classées par activité de l'intermédiaire financier (avec ou sans PSAV).

Il est intéressant de noter que sur les 1867 (77 %) communications reçues dans la période analysée, 1442 provenaient de 118 intermédiaires financiers *sans* activité de PSAV.

Il s'agit généralement de communications dans lesquelles l'intermédiaire financier a attiré l'attention du MROS sur des transactions suspectes entre les comptes signalés et les comptes d'intermédiaires financiers exerçant une activité de PSAV en Suisse ou à l'étranger. Le nombre de communications de soupçons en lien avec des AV provenant de ce type d'intermédiaire financier n'a cessé de croître depuis 2020.

Typologie n° 6

Communication de soupçons en lien avec des AV d'un intermédiaire financier sans activité de PSAV

Une banque a transmis une communication de soupçons portant sur une relation d'affaires avec une personne physique, qui a reçu pendant plusieurs mois divers avis de crédit provenant de différents comptes bancaires, tous établis au nom de personnes physiques différentes. Les paiements reçus de ces tierces personnes étaient ensuite directement transférés du compte signalé sur le compte d'une bourse d'AV étrangère.
L'intermédiaire financier déclarant a soupçonné que ces tierces personnes, qui avaient viré de l'argent sur le compte signalé, étaient probablement lésées par une escroquerie. Le co-contractant signalé aurait joué le rôle de *money mule* en mettant, contre rémunération, son compte à disposition de donneurs d'ordre inconnus participant à l'escroquerie. Il transmettait ensuite ces montants en monnaie fiat à la bourse d'AV, où ils étaient convertis en AV puis transférés sur des portefeuilles non hébergés, qui étaient probablement contrôlés par les donneurs d'ordre inconnus.

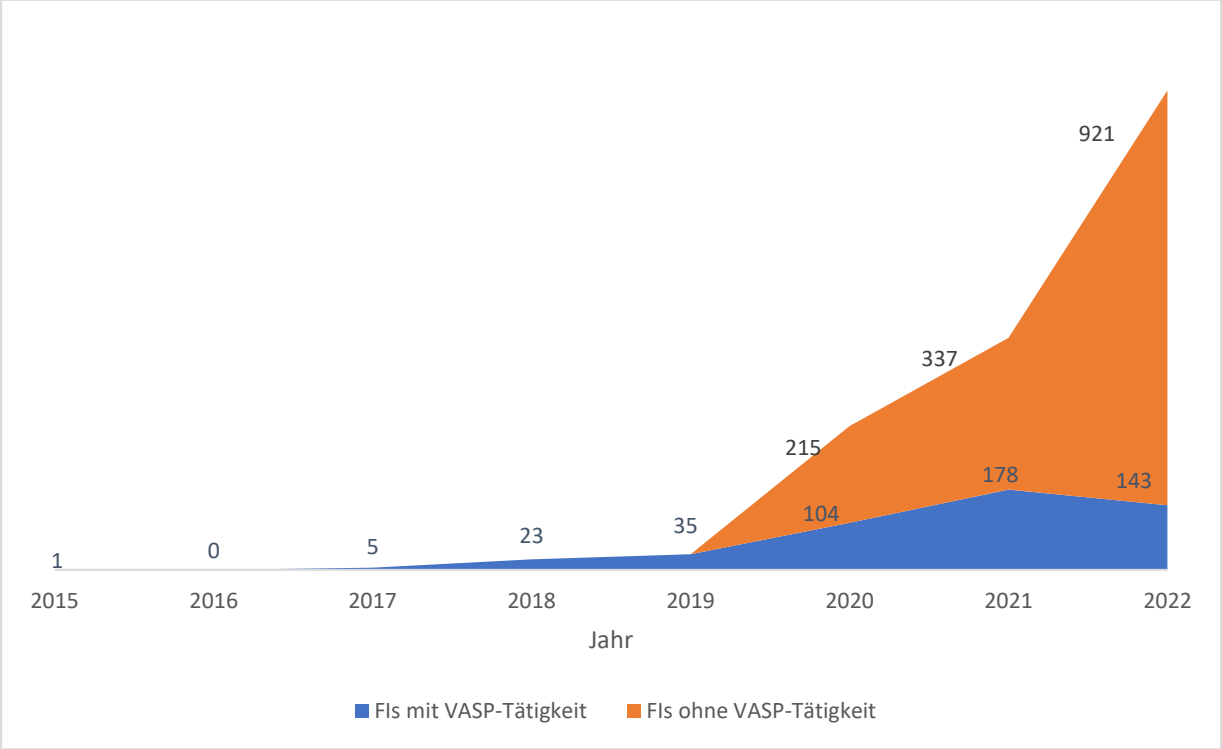

Fig. 28 : Les communications de soupçons en lien avec des AV provenant d'intermédiaires financiers sans activité de PSAV ont augmenté davantage que celles provenant d'intermédiaires financiers exerçant une activité de PSAV depuis 2020[230].

La croissance du secteur des AV, l'utilisation de plus en plus généralisée des AV et l'imbrication accrue des intermédiaires financiers avec activité de PSAV et de ceux sans activité de PSAV semblent avoir pour effet que la vulnérabilité des intermédiaires financiers à la menace d'être exploités à des fins de BA et de FT grâce à l'utilisation d'AV ne se limite plus seulement aux intermédiaires financiers exerçant une activité de PSAV. Le grand nombre de communications de soupçons en lien avec des AV provenant d'intermédiaires financiers sans activité de PSAV en est un indice significatif. L'analyse de ces communications montre que les comptes ouverts auprès de ces intermédiaires financiers sont utilisés abusivement par exemple pour des transactions de passage, avec pour point de départ ou de destination un virement depuis ou vers un compte fiat d'une bourse d'AV, ou pour entasser des fortunes incriminées présumées, ayant auparavant été converties d'AV en monnaie fiat auprès d'un intermédiaire financier exerçant une activité de PSAV. En raison de l'utilisation généralisée et de l'établissement global du secteur des AV, les intermédiaires sans activité de PSAV sont beaucoup plus vulnérables qu'en 2018 au risque d'être exploités à des fins de BA et de FT grâce à l'utilisation d'AV, même si eux-mêmes n'exercent pas d'activité de PSAV. Les cas de ce type sont devenus plus fréquents et les montants concernés considérablement plus élevés. En outre, ce type d'intermédiaire financier est souvent tributaire d'expertises externes afin de déterminer, au moyen d'analyses de blockchain, la plausibilité de l'arrière-plan économique de la monnaie fiat déposée sur leurs comptes, qui a auparavant été convertie d'AV en fiat par le biais d'autres prestataires d'AV[231]. À cet égard, le MROS fait état de cas illustrant clairement que ces expertises ne peuvent apporter de "sécurité" que jusqu'à un certain degré par rapport à la plausibilité de l'origine des fonds. Si les intermédiaires financiers sans activité de PSAV ne peuvent pas comprendre et évaluer le degré de plausibilité par eux-mêmes, ils s'exposent au danger que les risques de BA se reportent sur eux. En particulier dans les cas où des

[230] Remarque: avant 2020, seules les communications de soupçons provenant d'intermédiaires financiers exerçant une activité de PSAV étaient comptabilisées, cf. ch. 11.1.1 en annexe.
[231] Cf. par ex. Gotham City, *L'enquête sur les pirates allemands de Movie2k passe par Genève*, N° 278, 25 janvier 2023.

entreprises[232] effectuent de telles expertises et gagnent de l'argent d'une manière ou d'une autre en mettant des clients en contact avec des intermédiaires financiers sans activité de PSAV, ces derniers doivent être conscients que les risques de BA se reportent sur eux.

6e vulnérabilité

Intermédiaires financiers effectuant des transactions en lien avec des AV (en AV ou en fiat) (identifiée en 2018, accrue en 2023)[233]

Dans l'analyse sectorielle de 2018, on a relevé la vulnérabilité à la menace de BA et de FT qui caractérise "les intermédiaires financiers actifs dans les transactions en crypto-assets"[234]. Même si ceux-ci respectent strictement leurs obligations de diligence, l'efficacité de ces mesures est forcément limitée, car les transactions en crypto-actifs sont transnationales et passent par des sociétés de services qui sont enregistrées dans de très nombreux pays. Les bureaux de change en ligne enregistrés en Suisse sont par exemple souvent chargés de changer des cryptomonnaies par des prestataires de portefeuilles hébergés étrangers qui agissent pour le compte de leurs clients. Dans ce cas, la plate-forme suisse n'a pas accès aux données KYC du client de la plate-forme étrangère pour laquelle elle effectue le change, si bien qu'elle ne connaît pas l'identité du client.

Le MROS a reçu depuis 2018 de nombreuses communications de soupçons de la part d'intermédiaires financiers sans activité de PSAV qui ont constaté des transactions suspectes en provenance ou à destination de plates-formes PSAV suisses ou étrangères sur les comptes qu'ils gèrent. En outre, le MROS a connaissance de plusieurs cas d'intermédiaires financiers suisses sans activité de PSAV qui ont mis des comptes marchands à la disposition d'intermédiaires financiers étrangers exerçant une activité de PSAV, comptes sur lesquels des transactions fiat ont été effectuées en lien avec l'achat ou la vente d'AV sur des plates-formes PSAV étrangères. Les intermédiaires financiers suisses ne semblent souvent pas en mesure de clarifier l'arrière-plan économique des valeurs patrimoniales transférées sur leurs comptes ni d'en établir l'ayant droit économique. En effet, seul l'intermédiaire financier étranger possède des informations sur les transactions effectuées sur ce compte et sur les personnes impliquées, et pas l'intermédiaire financier suisse. Ce dernier ne peut compter que sur le fait que l'intermédiaire financier étranger respecte ses obligations de diligence et de communiquer et n'est lui-même pas en mesure de garantir qu'aucun client à haut risque et aucune transaction dont l'arrière-plan économique est flou ne soient associés à ses comptes.

Le MROS fait état de plusieurs cas où des comptes marchands mis à disposition par la banque gérant le compte en Suisse ont été utilisés abusivement pour effectuer des virements en lien présumé avec des infractions commises à l'étranger. Dans certains cas, ce sont même les entreprises clientes d'un intermédiaire financier suisse ou les intermédiaires financiers étrangers exerçant une activité de PSAV qui ont été accusés d'avoir commis des infractions dans le cadre de procédures pénales à l'étranger. Le fait que l'intermédiaire financier gérant le compte en Suisse n'a que des informations lacunaires sur les transactions effectuées accroît le risque lié à ce type d'architecture commerciale du point de vue de la lutte contre le BA et le FT.

Cette évolution constitue un signal supplémentaire du brouillage des frontières entre les activités commerciales d'intermédiaires financiers avec activité de PSAV et celles

[232] Il peut s'agir d'intermédiaires financiers exerçant une activité de PSAV qui prélèvent des commissions pour changer des AV en monnaie fiat, ou d'entreprises sans activité de médiation financière qui se font payer pour effectuer des expertises et/ou pour mettre des clients en contact avec des intermédiaires financiers sans activité de PSAV.
[233] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowfunding*, octobre 2018, pp. 34 - 35
[234] Ibid., p. 34

d'intermédiaires financiers sans activité de PSAV (cf. infobox 1 au ch. 4.2). Elle débouche sur le fait que *tous* les intermédiaires financiers, qu'ils exercent une activité de PSAV ou non, sont vulnérables à la menace d'être utilisés comme point de passage ou comme destination finale de flux financiers illégaux (AV ou fiat) qui présentent des liens avec des AV.

Entre janvier 2020 et décembre 2022, le MROS a reçu entre trois et quatre fois plus de communications de soupçons en lien avec des AV de la part d'intermédiaires financiers sans activité de PSAV (1442) que de la part de ceux exerçant une activité de PSAV (425). Les communications de soupçons provenant de ces derniers ont également augmenté, mais de manière moins continue et moins marquée que celles provenant des premiers, et ce malgré le nombre croissant d'intermédiaires financiers exerçant une activité de PSAV et le volume probablement croissant de leurs activités commerciales.

Il est frappant de constater que les intermédiaires financiers sans activité de PSAV sont plus nombreux à avoir déposé des communications de soupçons en lien avec des AV que ceux qui exercent une activité de PSAV. Entre janvier 2020 et décembre 2022, 118 intermédiaires financiers différents sans activité de PSAV ont déposé au moins une communication de soupçons en lien avec des AV, tandis que seulement 24 intermédiaires financiers avec activité de PSAV en ont déposé au moins une au cours de la même période[235]. Par ailleurs, plus de trois quarts de ces communications (329 sur 425) proviennent des quatre mêmes intermédiaires financiers exerçant une activité de PSAV, qui ont déposé des communications régulièrement, tandis que les 20 autres l'ont fait de manière plus sporadique.

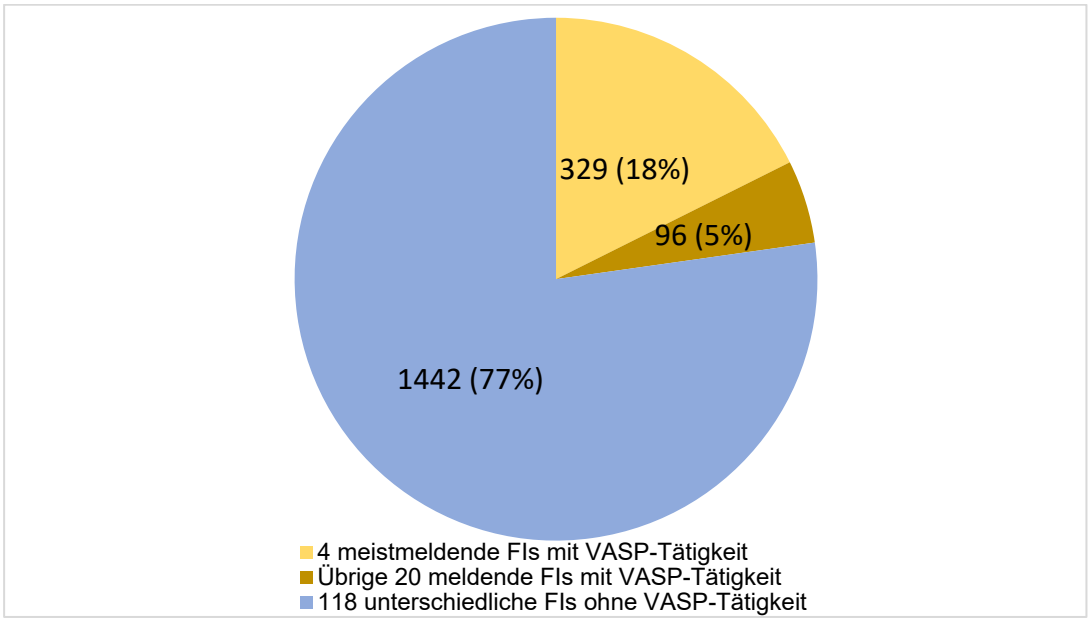

Fig. 29 : Intermédiaires financiers à l'origine des 1867 communications de soupçons en lien avec des AV déposées entre 2020 et 2022. Étonnamment, les intermédiaires financiers exerçant une activité de PSAV ont déposé un nombre bien inférieur de communications de soupçons en lien avec des AV, et beaucoup moins fréquemment, que les intermédiaires financiers sans activité de PSAV.

[235] On notera que les communications de soupçons en lien avec des AV ne constituent pas la *totalité* des communications déposées par les intermédiaires financiers exerçant une activité de PSAV dans cette période, car une partie d'entre elles concernent d'autres activités commerciales qui n'ont pas de lien avec des AV ou des PSAV (cf. ch. 4.2).

7e vulnérabilité

Absence de communications de la part d'intermédiaires financiers exerçant une activité de PSAV (identifiée en 2023)

À la fin de 2022, il existait en Suisse au moins 204 intermédiaires financiers exerçant une activité de PSAV qui étaient placés soit sous la surveillance directe de la FINMA, soit sous celle d'OAR. Au moins 180 d'entre eux n'ont déposé aucune communication de soupçons au MROS entre janvier 2020 et décembre 2022. La grande majorité de ces intermédiaires financiers sont affiliés à un OAR. Faute de données quantitatives sur les services proposés et les avoirs en AV gérés par les intermédiaires financiers suisses exerçant une activité de PSAV, il n'est pas possible d'examiner en détail si l'absence de communications de la part de l'écrasante majorité de ces intermédiaires financiers est due à une négligence de leurs obligations de diligence et de communiquer ou à une activité commerciale faible. Au regard de la croissance du secteur des AV suisse et de l'intensification flagrante des activités commerciales des intermédiaires financiers exerçant une activité de PSAV, il semble toutefois que le MROS ne reçoit pas toutes les communications de soupçons qu'il devrait de la part de ce type d'intermédiaire financier.

7.5.2 Éléments fondant le soupçon

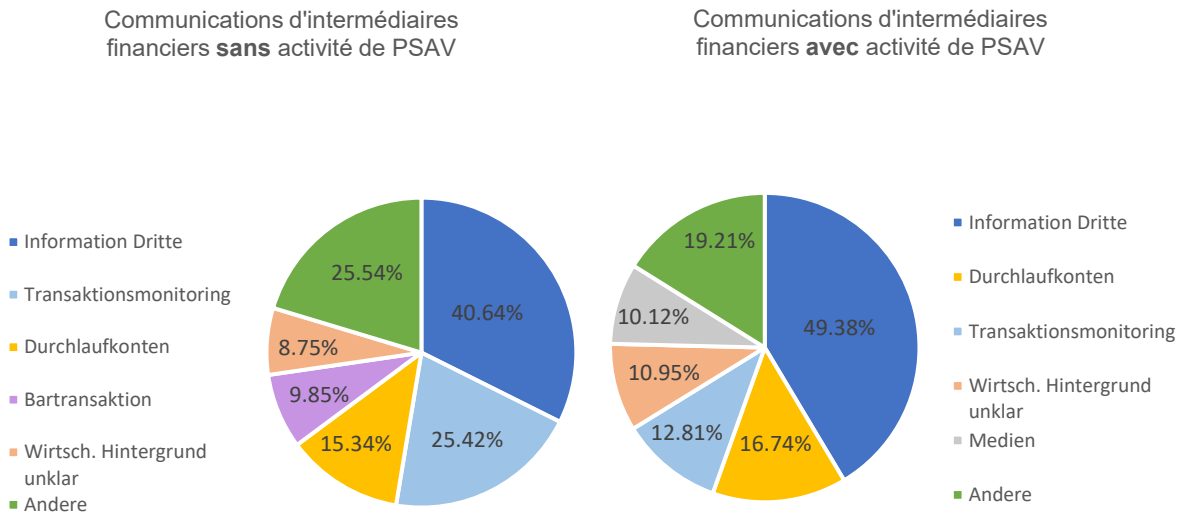

Fig. 30 : Les éléments fondant le soupçon varient selon que la communication a été déposée par un intermédiaire financier avec activité de PSAV ou par un intermédiaire financier sans activité de PSAV. Ceux qui n'exercent pas d'activité de PSAV émettent des communications plus souvent sur la base du monitoring interne des transactions, tandis que ceux qui exercent une activité de PSAV se fondent plus fréquemment sur l'information de tiers pour émettre une communication.

Par rapport aux intermédiaires financiers n'exerçant pas d'activité de PSAV, ceux exerçant une activité de PSAV se sont plus rarement fondés sur leur monitoring des transactions pour établir leurs propres constats et émettre une communication en lien avec des AV (12,8 % contre 25,4 %).

S'agissant des communications en lien avec des AV provenant d'intermédiaires financiers exerçant une activité de PSAV, près d'une sur deux (49,4 %) invoquait comme motif un appel

au remboursement issu par une banque tierce pour des paiements déclenchés frauduleusement, ou une prise de contact par une autorité de poursuite pénale étrangère, ou encore une décision d'édition prononcée par une autorité de poursuite pénale suisse (les trois motifs sont résumés ci-après sous le terme "information de tiers"). Dans les communications en lien avec des AV provenant d'intermédiaires financiers sans activité de PSAV, les informations de tiers étaient plus rarement invoquées comme motif de dépôt d'une communication (40,6 %). Cependant, le pourcentage est élevé pour les deux types d'intermédiaires financiers, ce qui semble refléter une problématique générale dans le secteur des AV. Les intermédiaires financiers exerçant une activité de PSAV semblent toutefois nettement plus tributaires des informations de tiers pour détecter des opérations suspectes.

Dans les communications provenant de ces derniers, il ressort en outre qu'ils ont souvent été contactés directement par une autorité de poursuite pénale étrangère (principalement des ministères publics allemands), qui leur ont demandé de lui fournir des informations précises sur une de leurs relations d'affaires (par ex. le nom du détenteur du compte, le nom du bénéficiaire d'un paiement déclenché frauduleusement).

8e vulnérabilité

Le comportement en matière de communication des intermédiaires financiers exerçant une activité de PSAV semble souvent de type réactif et ne pas reposer sur des clarifications proactives (identifiée en 2023)

En rédigeant leurs communications de soupçons, les intermédiaires financiers décrivent le contenu des opérations suspectes et les motifs de dépôt d'une communication. Le MROS a constaté des différences entre ceux qui exercent une activité de PSAV et ceux qui n'exercent pas d'activité de PSAV au niveau des systèmes de détection, qui devraient tenir compte de différents motifs et sources de soupçons.

Les intermédiaires financiers exerçant une activité de PSAV ont été alertés d'opérations suspectes par le biais d'informations externes plus souvent que ceux sans activité de PSAV. Leurs soupçons les ont ensuite poussés à émettre une communication. Selon leurs dires, les informations de tiers étaient le plus fréquemment à l'origine des soupçons dans leurs communications émises entre 2020 et 2022 (49,4 % des communications d'intermédiaires financiers exerçant une activité de PSAV). Ceux-ci ont indiqué avoir été intrigués par la relation d'affaires signalée à la suite d'un appel au remboursement issu par une banque tierce pour des paiements déclenchés frauduleusement, d'une prise de contact par des victimes d'escroquerie présumées ou leurs mandataires, d'une demande d'une autorité de poursuite pénale étrangère, ou encore d'une décision d'édition prononcée par une autorité de poursuite pénale suisse. En revanche, les communications en lien avec des AV provenant d'intermédiaires financiers sans activité de PSAV n'ont été motivées et déclenchées par des informations de tiers que pour 40,7 % d'entre elles.

Dans les communications en lien avec des AV provenant d'intermédiaires financiers sans activité de PSAV, le monitoring des transactions était mentionné deux fois plus souvent (25,4 %) comme déclencheur de soupçons que dans celles provenant d'intermédiaires financiers exerçant une activité de PSAV (12,8 %). On peut en déduire que ces derniers semblent avoir des difficultés pour détecter les transactions et les opérations suspectes à l'aide de leur monitoring et clarifier leur arrière-plan économique de leur propre chef. Cela n'a pas l'air d'être une particularité suisse : un échange d'informations avec la CRF du Liechtenstein a révélé que celle-ci observe également un comportement plutôt réactif en matière de communication de la part des intermédiaires financiers exerçant une activité de PSAV. On peut dès lors supposer qu'il existe un nombre significatif de cas non découverts chez certains

intermédiaires financiers exerçant une activité de PSAV pour ce qui concerne les opérations de BA présumé. Si les clarifications internes ou les informations externes ne permettent pas à ces derniers de remarquer qu'il y a des opérations suspectes et devant donc être signalées, le MROS ne recevra pas de communication de soupçons.

8. Bilan et facteurs d'atténuation des risques

Dans ce qui précède, les menaces et les vulnérabilités déjà identifiées en 2018 ont été réévaluées et complétées à la lumière des changements et des variations considérables intervenues depuis 2018 dans le secteur des AV. Ces menaces et vulnérabilités sont résumées et mises en balance ci-après.

À l'instar de l'analyse sectorielle de 2018, le bilan de l'analyse de risques porte uniquement sur les changements dans les menaces et les vulnérabilités visant à donner un aperçu des risques bruts. Ce bilan est suivi d'une présentation des facteurs d'atténuation des risques identifiés. Faute d'informations disponibles, il n'est pas possible de procéder à l'examen et à l'appréciation quantitative des risques nets qui sont liés à l'exercice de l'intermédiation financière en Suisse dans le secteur des AV (cf. ch. 5.2). Ces chiffres seraient nécessaires pour effectuer une pondération précise des risques posés par les activités commerciales sur la base de leur intensité et de leur portée, afin de pouvoir dans un deuxième temps examiner dans quelle mesure ces activités commerciales sont touchées par les menaces et les vulnérabilités identifiées et quelle est l'influence exercée par les facteurs d'atténuation des risques.

8.1 Bilan de l'analyse de risques

Aucune des neuf menaces et deux vulnérabilités identifiées en 2018 ne se sont atténuées ou n'ont diminué au cours des cinq dernières années. Bien au contraire, elles ont généralement augmenté (7 sur 11), tandis que trois menaces et une vulnérabilité sont restées identiques. En outre, la présente analyse de risques a permis d'identifier deux nouvelles menaces et six nouvelles vulnérabilités.

	Menaces	**2018**	**2023**
1	Failles de sécurité des technologies sous-jacentes aux AV	identifiée	accrue
2	Rançongiciels et maliciels	identifiée	accrue
3	Les AV comme moyens de paiement de biens et services illégaux	identifiée	accrue
4	Blanchiment d'AV d'origine criminelle (en monnaie fiat)	identifiée	accrue
5	Blanchiment de monnaie fiat d'origine criminelle (en AV)	identifiée	inchangée
6	Menace liée à l'effet de nouveauté et à l'inexpérience des utilisateurs	identifiée	accrue
7	Recours aux AV lors d'attaques d'hameçonnage	identifiée	accrue
8	FT au moyen d'AV	identifiée	inchangée
9	Financement de la prolifération au moyen d'AV		accrue

10	Anonymat des transactions et difficulté d'identification des ayants droits économiques	identifiée	inchangée
11	La *travel rule* n'est pas appliquée aux comptes marchands des intermédiaires financiers suisses exerçant une activité de PSAV		accrue

Fig. 31 : Aperçu des menaces identifiés et de leur évolution depuis 2018

	Vulnérabilités	**2018**	**2023**
1	La perte tendancielle d'importance de l'intermédiation financière dans le secteur des AV pose des difficultés pour appliquer les approches réglementaires existantes concernant le BA et le FT		Identifiziert
2	Mise en œuvre et application internationales insuffisantes et inégales de la *travel rule* dans le secteur des AV		identifiée
3	Manque de ressources et de capacités des institutions chargées de lutter contre le BA et le FT compte tenu des développements fulgurants dans le secteur des AV		identifiée
4	Statistiques et chiffres insuffisants aux niveaux national et international		identifiée
5	Difficile répression du BA et du FT dans le domaine des AV	identifiée	inchangée
6	Intermédiaires financiers effectuant des transactions en lien avec des AV (en AV ou fiat)	identifiée	accrue
7	Absence de communications de la part d'intermédiaires financiers exerçant une activité de PSAV		identifiée
8	Le comportement en matière de communication des intermédiaires financiers exerçant une activité de PSAV semble souvent de type réactif et ne pas reposer sur des clarifications proactives		identifiée

Fig. 32 : Aperçu des vulnérabilités identifiées et de leur évolution depuis 2018

8.2 Facteurs d'atténuation des risques

Bien que les AV présentent à la fois des menaces et des vulnérabilités considérables, il existe plusieurs facteurs d'atténuation des risques. Ces facteurs peuvent prévenir les menaces et réduire les vulnérabilités. La plupart d'entre eux ont déjà été mentionnés dans le présent rapport et sont résumés brièvement ci-après. Certains existent à l'échelle globale, tandis que d'autres sont limités au contexte national, les éventuelles différences entre les deux plans sont soulignées ci-après.

	Facteurs d'atténuation des risques
1	Le focus renforcé du GAFI et l'attention politique accrue
2	Le renforcement de la coopération internationale qui produit déjà des résultats
3	La consolidation et l'augmentation du degré de maturité de compliance chez les grands acteurs de la branche
4	La transparence systématique de la plupart des blockchains
5	L'activité de surveillance et l'application de la *travel rule* en Suisse
6	La définition large de l'intermédiation financière dans la loi DLT (*distributed ledger technology*)

Fig. 33 : Aperçu des facteurs d'atténuation des risques identifiés

8.2.1 Le focus renforcé du GAFI et l'attention politique accrue

Au plan international, la mise en œuvre progressive des recommandations du GAFI relatives aux AV peut être considérée comme un facteur d'atténuation des risques. Le GAFI semble observer avec une grande attention cette mise en œuvre dans les différents pays et publie à intervalles réguliers des guides et des rapports sur son avancement.

Le redoublement d'attention du GAFI et de la communauté politique internationale accroît la pression sur les pays et les entreprises du secteur des AV pour qu'ils respectent les normes internationales de lutte contre le BA et le FT. Cette dynamique peut contribuer à accélérer la mise en œuvre de mesures visant à atténuer le risque d'utilisation abusive d'AV à des fins de BA et de FT. Elle peut aussi, dans un deuxième temps, conduire vers une meilleure identification et une meilleure surveillance des activités et des transactions suspectes, ce qui peut à son tour contribuer à réduire le risque de BA et de FT en lien avec des AV. Avec l'application de la *travel rule* par exemple, on parvient à effectuer une comparaison plus transparente des flux financiers entre les comptes d'intermédiaires financiers exerçant une activité de PSAV et entre l'indicateur de contrôle mesurant le respect des obligations de diligence dans les services d'AV et le trafic de paiements SWIFT. Une définition large du terme PSAV selon la recommandation n° 15 du GAFI permet en outre d'assurer que les dispositions relatives au BA et au FT déjà en vigueur dans l'intermédiation financière traditionnelle s'appliquent aussi au secteur des AV. Les intermédiaires financiers exerçant une activité de PSAV sont par exemple tenus de garantir qu'ils connaissent l'identité de leurs clients, qu'ils signalent les transactions suspectes et qu'ils mettent en place une gestion des risques efficace. Une réglementation et une surveillance globales plus poussées des intermédiaires financiers exerçant une activité de PSAV permettrait de garantir que ceux-ci parviennent à mieux détecter et à empêcher l'utilisation d'AV à des fins de BA et de FT, ce qui atténuerait les risques en conséquence.

8.2.2 Le renforcement de la coopération internationale produit déjà des résultats

Une coopération internationale renforcée à différents niveaux dans le secteur des AV, par exemple entre les autorités de régulation nationales, les autorités de poursuite pénale et les CRF, ainsi qu'entre les autorités de poursuite pénale et les entreprises privées pourrait permettre d'atténuer les risques de BA et de FT dans ce secteur. Les autorités ont approfondi leurs connaissances sur les AV, partagé leurs informations sur les cas suspects plus rapidement et plus efficacement, et intensifié la coopération avec des entreprises du domaine de l'analyse de blockchain, ce qui a déjà produit de premiers résultats positifs, par exemple en

relation avec le traçage, le blocage et la confiscation d'AV[236]. En partagent leurs pratiques éprouvées et leurs expériences, les pays et les institutions peuvent apprendre les uns des autres et améliorer leurs mesures, ce qui peut également contribuer à atténuer les risques car les activités de BA et de FT peuvent être plus rapidement identifiées et poursuivies pénalement. Une collaboration renforcée peut enfin contribuer à combler les lacunes et à supprimer les failles subsistantes dans l'instrumentaire de régulation afin d'améliorer la régulation et la surveillance d'une manière générale. Une collaboration plus étroite favorise aussi l'harmonisation de la mise en œuvre des normes internationales et peut ainsi augmenter l'efficacité des mesures de lutte contre le BA et le FT dans le secteur des AV[237].

8.2.3 Consolidation et augmentation du degré de maturité de compliance chez les grands acteurs de la branche

Une consolidation mondiale de l'offre dans le secteur des AV, concentrée autour d'un petit nombre de bourses de négoce d'AV majeures et centralisées qui possèdent des départements de compliance matures, peut contribuer à réduire les risques de BA et de FT. Si les PSAV sont moins nombreux, mais plus grands et mieux régulés, le nombre de risques est réduit d'autant et le contrôle et la surveillance des PSAV restants sont meilleurs. Sans compter que les grands PSAV sont en règle générale plus à même d'investir dans des départements de compliance et des technologies visant à surveiller les transactions, ce qui pourrait à son tour avoir pour effet d'empêcher les activités illégales en lien avec des AV. Les autorités de régulation peuvent interagir plus efficacement avec un nombre réduit de grands PSAV afin de leur imposer des normes de régulation et de surveillance. Contrôler si les normes anti-blanchiment et anti-terrorisme sont respectées est aussi plus facile, de même que les contraindre à prendre des mesures en cas de non-respect. Enfin, consolider le secteur des PSAV peut aussi aider à identifier plus rapidement l'utilisation d'AV à des fins de BA et de FT et à y mettre un terme, étant donné qu'il y a moins d'endroits où ces activités peuvent avoir lieu.

8.2.4 Transparence systématique de la plupart des blockchains

La transparence systématique des blockchains offre pour le moment l'opportunité d'observer les flux financiers dans le secteur des AV, ce qui serait impossible dans le trafic de paiement traditionnel[238]. Certains logiciels d'analyse de blockchain permettent de relier des informations numériques à des personnes et à des événements dans le monde analogique, ce qui offre des possibilités encore inexplorées de mener des analyses approfondies, étant précisé que la qualité de ces analyses dépend toujours de la qualité des données du monde analogique sur lesquelles elles se fondent. Il n'existe pas encore de normes uniformisées à cet égard. Ces solutions reposent sur le fait que les transactions en AV sont en général visibles par le public, si bien qu'il est plus facile de détecter et de tracer des activités suspectes. Cet avantage peut à son tour faciliter l'identification et le traçage des flux financiers en temps réel, ce qui est impossible dans le trafic de paiements traditionnel. Par ailleurs, comme la blockchain garde une mémoire durable et non modifiable des transactions, contrairement au trafic de paiements traditionnel, cela peut contribuer à réduire les risques généraux de fraude et de falsification à moyen et à long terme, car une fois la transaction effectuée, elle peut être vérifiée publiquement et ne peut plus être manipulée. Les protocoles de FiDé reposant en général sur des blockchains publiques, ils peuvent procurer une transparence plus grande. Cependant, il

[236] Pour des informations sur les confiscations d'AV pour une valeur de plusieurs milliards effectuées en 2022, cf. Chainalysis, *The Crypto Crime Report 2022*, février 2022, p. 23.
[237] Basel Institute On Governance and Europol, *Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering*, 2022, pp. 4 - 5
[238] Ibid., p. 3

existe aussi des applications de FiDé qui entravent ou empêchent la traçabilité des transactions, soit délibérément (par ex. Mixer, Tumbler, *privacy wallets*), soit comme effet collatéral de la fonctionnalité (Cross Chain Bridges, Lending Pools, Automated Market Makers). Si chaque transaction est bien enregistrée sur la blockchain en temps réel au sein d'un protocole de FiDé et devient publiquement visible, sa traçabilité et son attribution peuvent en revanche être rendues impossibles selon les circonstances. Par conséquent, le domaine de la FiDé pose aussi des risques considérables de BA et de FT en raison de l'anonymat de la plupart des utilisateurs. Il reste toujours aussi difficile d'identifier et de surveiller les transactions suspectes, notamment en raison de l'utilisation de technologies d'anonymisation. Cependant, les entreprises et les instituts de recherche qui se sont spécialisés dans l'analyse des données de blockchain constituent un domaine en plein essor. Cette branche professionnelle développe des outils et des technologies d'avant-garde pour analyser les transactions en AV et identifier les activités suspectes. Son apport peut aider les autorités de régulation et de poursuite pénale à détecter et à poursuivre les cas de BA ou de FT. Dans plusieurs cas déjà, les analyses de blockchain ont permis à ces autorités de détecter des cas de ce type, de bloquer et de confisquer des AV, et surtout, d'apporter la preuve des actes criminels et de poursuivre les coupables. Les plates-formes de FiCe en revanche reposent sur des bases de données et des systèmes centralisés qui manquent de transparence. L'accès aux données dépend donc du bon vouloir de l'exploitant à coopérer, ce qui peut compliquer la surveillance et l'analyse des transactions.

8.2.5 Activité de surveillance et application de la *travel rule* en Suisse

Eu égard au danger substantiel que fait peser le BA sur la Suisse, la FINMA attribue une priorité élevée à cette problématique, de manière générale mais aussi en ce qui concerne les PSAV. En conséquence, elle a introduit diverses mesures de surveillance et de contrôle dans ce domaine et effectue des clarifications et des procédures d'enforcement en cas de violations graves.

Depuis que des activités en lien avec les cryptomonnaies ont commencé à se développer sur les marchés financiers, la Suisse a appliqué le cadre légal existant (en matière de lutte contre le BA et le FT) à certaines cryptomonnaies et aux PSAV, qui sont clairement assimilés à des intermédiaires financiers traditionnels selon la définition de la FINMA. Selon ce cadre légal, toutes les activités d'intermédiation financière en relation avec des cryptomonnaies entrent dans le champ d'application de la LBA. Cela englobe notamment les services de change entre fournisseurs de cryptomonnaies et de monnaies fiat et/ou entre une ou plusieurs formes de cryptomonnaies, et toutes les activités en lien avec le transfert, la conservation et/ou la gestion de cryptomonnaies ou d'instruments de contrôle des cryptomonnaies. Pour de plus amples informations, il convient de se référer au deuxième rapport national d'octobre 2021[239].

En outre, la modification de l'OBA-FINMA en vigueur depuis le 1er janvier 2021 oblige tous les intermédiaires financiers suisses exerçant une activité de PSAV à identifier le cocontractant pour des opérations impliquant des AV, lorsqu'une transaction ou plusieurs transactions qui paraissent reliées entre elles atteignent ou dépassent la somme de 1000 francs, pour autant que ces transactions ne constituent pas de transmission de fonds et de valeurs et qu'elles ne soient liées à aucune relation d'affaires durable. Avec les exigences qui découlent de l'art. 10 de l'OBA-FINMA (Indications lors de virements), la Suisse contraint les intermédiaires financiers exerçant une activité de PSAV à remplir plus d'obligations que ce que prévoit la *travel rule* du GAFI, car cette règle est appliquée en Suisse aussi pour les transactions entre portefeuilles hébergés et portefeuilles non hébergés. Si ces exigences sont mises en œuvre correctement, il n'est aujourd'hui possible, sur les comptes de clients d'intermédiaires

[239] Cf. GCBF, *Deuxième rapport national sur les risques de blanchiment d'argent et de financement du terrorisme*, octobre 2021, ch. 3.8 Nouveautés relatives aux actifs virtuels et aux prestataires de services d'actifs virtuels, p. 42.

financiers suisses exerçant une activité de PSAV, de faire entrer ou sortir des AV que depuis ou vers des portefeuilles non-hébergés dont les clients concernés sont des ayants droits économiques. Cette limitation renforce le dispositif de lutte contre le BA et le FT des intermédiaires financiers. Toutefois, les possibilités de trouver par ce moyen les ayants droit économiques réels des valeurs patrimoniales d'un portefeuille non hébergé ainsi que de déterminer l'origine de ces fonds sont limitées par la conception technologique des AV. Cela dit, les possibilités sont aussi limitées en ce qui concerne les monnaies fiat et d'autres valeurs patrimoniales du domaine financier traditionnel. Il n'en reste pas moins qu'avec la mise en œuvre globale des recommandations du GAFI, l'anonymat ou le pseudonymat des transactions sera sévèrement limité à l'avenir, du moins en ce qui concerne les transactions entre portefeuilles hébergés, car les intermédiaires financiers exerçant une activité de PSAV devront échanger les indications sur le donneur d'ordre et le bénéficiaire de chaque paiement.

8.2.6 Définition large de l'intermédiation financière dans la loi DLT (*distributed ledger technology)*

La loi du Conseil fédéral sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués et l'ordonnance associée auront pour effet d'élargir le sens du terme "intermédiaire financier" à l'avenir, de sorte que le pouvoir de disposition sur des valeurs patrimoniales ne sera plus le seul critère pour qu'un intermédiaire financier entre dans le champ d'application de la LBA. L'élargissement de ce terme correspond aux dernières recommandations du GAFI d'interpréter le terme "PSAV" d'une manière aussi large que nécessaire afin qu'il ne subsiste aucune lacune dans le dispositif de lutte anti-blanchiment[240]. Dans le secteur des AV suisse, est considéré comme intermédiaire financier celui "qui permet le transfert de monnaies virtuelles à un tiers […], pour autant qu'il entretienne une relation d'affaires durable avec le cocontractant", ou qui exerce le pouvoir de disposition sur des monnaies virtuelles pour le compte du cocontractant, pour autant qu'il ne fournisse pas exclusivement cette prestation par rapport à des intermédiaires financiers surveillées de manière appropriée[241]. Par contre, les fournisseurs de portefeuilles non hébergés purs, "qui se contentent de mettre une seule fois un logiciel à disposition, ne sont pas soumis à la LBA"[242]. L'avenir dira si la différence entre une "relation d'affaires durable" et la simple "mise à disposition d'un logiciel" correspond à la réalité et constitue un critère pertinent à long terme dans le secteur des AV.

[240] Cf. GAFI, *Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers*, mars 2021, pp. 29 - 30.
[241] Cf. DFF: *Ordonnance du Conseil fédéral sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués*, rapport explicatif, 19 octobre 2020.
[242] Ibid.

9. Conclusions et recommandations

Le GCBF a publié sa première analyse de risques sectorielle sur la thématique des crpytomonnaies en 2018, estimant que les menaces et les vulnérabilités que celles-ci posaient pour la Suisse face au BA et au FT étaient "considérables"[243]. Dans le même temps, il établissait que les communications de soupçons reçues par le MROS dans ce domaine étaient encore peu nombreuses et ne permettaient pas d'en tirer des statistiques fiables. Le panorama des risques a beaucoup changé depuis 2018. Le MROS reçoit désormais *tous les jours* des communications de soupçons qui ont un lien avec les AV ou les PSAV. L'influence et l'importance des AV ont connu une évolution radicale. On peut identifier quatre développements significatifs :

Premièrement, on constate que le nombre d'intermédiaires financiers exerçant une activité de PSAV a explosé en Suisse en passant de moins de 10 en 2018 à 204 à la fin de 2022. Les quelques informations qu'on possède sur eux laissent supposer que leur activité commerciale s'est intensifiée ces dernières années. À la fin de 2021, ils géraient au moins 10 milliards d'avoirs en Suisse.

Deuxièmement, on observe que l'utilisation générale d'AV a fortement augmenté en Suisse au cours des cinq dernières années. Diverses études et enquêtes reflètent clairement cette tendance. Le nombre de personnes qui considèrent les AV comme un moyen de paiement légitime ne cesse de croître. Parallèlement, les possibilités d'utiliser des AV comme moyen de paiement se sont diversifiées et se généralisent peu à peu. L'imbrication croissante du secteur des AV et du secteur financier traditionnel, par exemple par l'intégration des AV sur les plates-formes de paiement établies, a provoqué une hausse probable du nombre de commerces et de prestataires suisses qui acceptent les AV comme moyen de paiement.

Troisièmement, l'utilisation criminelle des AV et les violations du droit de la surveillance ont également augmenté en Suisse. Les autorités de poursuite pénale suisses sont de plus en plus souvent confrontées à des procédures présentant des liens avec des AV. Même si l'on ne dispose que d'informations parcellaires, les données disponibles indiquent des montants de préjudice en hausse, aussi bien en valeur nominale qu'en pourcentage, qui se situent autour des dix millions en 2022. L'utilisation criminelle d'AV semble non seulement avoir augmenté, mais s'être aussi élargie et diversifiée. D'une part, il est désormais habituel d'utiliser des AV pour certaines infractions, parfois les auteurs en font même une condition essentielle pour réussir dans leur dessein criminel, par exemple pour se faire payer la rançon exigée lors d'une attaque par ransomware. Il y a quelques années encore, tous les flux financiers d'AV étaient libellés en bitcoins, mais les criminels ont adapté leur stratégie et utilisent désormais différents AV en fonction de leurs besoins, comme des *stablecoins*, des NFT, et surtout des *privacy coins* qui sont plus difficiles à retracer avec les outils de la poursuite pénale. Cela représente une difficulté croissante pour les autorités de poursuite pénale. S'y ajoute le fait que le danger n'est, depuis longtemps, plus cantonné seulement aux actes préalables dans le domaine de la cybercriminalité et aux infractions "crypto-spécifiques". Le spectre des faits qui sont portés à la connaissance des diverses autorités de poursuite pénale et du MROS et qui témoignent de l'utilisation d'AV s'est également élargi. Aujourd'hui, la menace émane aussi des infractions les plus diverses dans le monde "hors ligne", dont les formes les plus graves de criminalité économique et, enfin, l'utilisation d'AV par des réseaux de BA professionnels et des acteurs gouvernementaux. Dans plusieurs communications de soupçons en lien avec des AV reçues par le MROS, celui-ci a pu établir des liens avec des PPE, des affaires internationales de corruption, des groupes transnationaux de criminalité organisée ou encore des acteurs étatiques. Manifestement, les criminels ont découvert le potentiel des AV pour le BA, le FT et la prolifération, si bien que les AV font désormais partie des outils habituels de la

[243] GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowfunding*, octobre 2018, p. 4

criminalité financière. De son côté, la FINMA constate elle aussi une augmentation des cas et a mis en garde contre les risques liés aux AV et aux PSAV dans de nombreuses publications. Elle a aussi précisé ses attentes en matière de surveillance, et effectué diverses clarifications et procédures d'enforcement en conséquence.

Quatrièmement, la forte hausse des communications de soupçons en lien avec des AV qui ont été déposées auprès du MROS depuis 2020 révèle aussi que les intermédiaires financiers suisses constatent de plus en plus fréquemment sur les comptes qu'ils gèrent des opérations suspectes en termes de BA et de FT qui sont en relation avec l'utilisation d'AV. En 2022, près de 14 % des communications reçues par le MROS étaient en lien avec les AV.

Les quatre évolutions précitées ont eu pour effet que les menaces et vulnérabilités identifiées dans l'analyse de risques de 2018 se sont accrues et élargies. Aucune de ces neuf menaces et deux vulnérabilités ne se sont atténuées ces cinq dernières années. La majorité d'entre elles se sont au contraire accrues (7 sur 11), tandis que trois menaces et une vulnérabilité sont considérées être restées au même stade. En outre, deux nouvelles menaces et six nouvelles vulnérabilités ont été identifiées dans la présente analyse de risques. Celle-ci met ainsi en lumière le fait qu'en raison de leur valeur plus élevée et des risques inhérents de BA et de FT, les AV exigent une attention accrue de la part des autorités compétentes en matière de lutte anti-blanchiment.

Le secteur des AV se caractérise par une forte dynamique et des évolutions fulgurantes. Les nouvelles possibilités technologiques offertes par les AV sont vectrices autant d'opportunités que de risques pour la lutte anti-blanchiment. Déterminés en premier lieu par les propriétés des AV, ces opportunités et ces risques peuvent transformer le paysage des risques de manière décisive selon la direction dans laquelle ils évolueront.

Les AV forment des systèmes de paiement parallèles qui s'ajoutent au trafic de paiements traditionnel et qui permettent des transferts internationaux rapides. L'imbrication croissante des AV et du trafic de paiements traditionnel génère un nombre accru de points de croisement et d'intersection entre les systèmes de paiement. Cette évolution présente des risques de BA et de FT. D'abord, les autorités de poursuite pénale et les autres autorités et institutions chargées de la surveillance doivent consacrer davantage de temps aux investigations et au traçage des transactions, car elles doivent examiner plusieurs systèmes de paiement séparés. Cela exige d'une part des connaissances spécialisées supplémentaires et peut, d'autre part, compliquer les processus d'enquête actuels car il faut rajouter des étapes de travail et des ressources supplémentaires. Ensuite, l'intégration croissante des AV dans le trafic de paiements traditionnel facilite l'accès et l'utilisation des deux systèmes de paiement pour les criminels. Il en découle le risque que ces acteurs élargissent leur répertoire de techniques de BA en y ajoutant un outil supplémentaire. En outre, ils peuvent combiner l'utilisation d'AV avec les techniques de dissimulation usuelles ou utiliser des AV dans des secteurs déjà à risques, dans le but d'entraver encore davantage l'identification des activités suspectes. Enfin, le nombre croissant de points de contact et d'intersection entre les deux systèmes de paiement exacerbe la vulnérabilité de tous les intermédiaires financiers (avec ou sans activité de PSAV) face à la menace d'être utilisés comme point de passage ou de destination de flux financiers illégaux en lien avec des AV (en AV ou en fiat). Cette vulnérabilité ne fera qu'augmenter tant que la recommandation n° 16 du GAFI (*travel rule*) n'est pas mise en œuvre dans tous les pays.

Le volume mondial des flux financiers en AV reste encore relativement facile à appréhender par rapport à d'autres flux financiers. C'est pourquoi les risques de BA et de FT semblent encore limités dans le secteur des AV, contrairement à d'autres secteurs. Pour réussir à dissimuler des flux financiers en AV, il faut en outre une compréhension approfondie de la manière dont fonctionnent les AV. Or, on estime qu'il y a encore peu d'experts qui maîtrisent le sujet et que la majeure partie de leurs activités se limitent au domaine de la cybercriminalité et des infractions "crypto-spécifiques", comme le *rug pull*, l'hameçonnage de données de

portefeuille et le piratage de PSAV. Cependant, les AV ont un potentiel évident pour permettre à un "large public" de dissimuler des flux financiers, il pourrait par exemple s'agir de blanchisseurs professionnels implantés dans le secteur financier traditionnel ou de groupes de criminalité organisée transnationaux possédant des fonds d'origine criminelle provenant du monde "hors ligne". Cette évolution s'observe déjà par moments et nécessite une prise de conscience des dangers qui y sont associés. L'acceptation croissante des AV comme moyen de paiement, y compris pour des montants élevés, combinée à l'imbrication de plus en plus grande du secteur des AV et du secteur financier traditionnel, pourraient générer, à moyen et à long terme, des risques plus élevés de BA et de FT dans les deux secteurs.

Cela dit, la croissance du secteur des AV influence déjà une partie significative du monde économique et financier et exige la vigilance de nombreuses parties prenantes, dont les intermédiaires financiers, les autorités de poursuite pénale, et d'autres services et acteurs chargés de combattre le BA et le FT. Le présent rapport montre qu'il existe certaines lacunes et souligne l'importance d'acquérir des connaissances et d'y consacrer des ressources.

En effet, le manque de ressources et de capacités peut rendre la coopération très difficile entre les acteurs chargés de la lutte anti-blanchiment, que ce soit au plan national ou international, d'autant plus si ces derniers n'ont pas tous le même niveau de connaissances ni les mêmes capacités pour mener des enquêtes et des analyses dans le secteur des AV. Cette disparité peut sensiblement ralentir et freiner l'identification et la poursuite des cas de BA et de FT, quand bien même les cas de ce type ne seraient en soi peut-être pas si difficiles à détecter. Ce problème existe déjà au niveau national, mais s'aggrave encore plus au niveau international, car l'élucidation de ces cas dans le secteur des AV dépend presque toujours du bon fonctionnement de la coopération internationale entre les CRF, les autorités de poursuite pénale et les autres autorités. Il suffit d'un maillon faible dans cette chaîne pour ralentir ou paralyser l'élucidation transfrontalière des cas. À l'heure actuelle, le risque qu'il y a en Suisse (comme dans les autres pays) est que les acteurs chargés de la lutte anti-blanchiment ne soient pas toujours en mesure de détecter les cas de BA et de FT en lien avec des AV, ni de les poursuivre sur le plan pénal ou sur le plan des exigences prudentielles, car ils ne sont pas suffisamment armés pour faire face à ces nouveaux défis et manquent de ressources dans ce domaine.

La régulation du secteur suisse des AV est toutefois robuste en comparaison internationale et les recommandations du GAFI pour le secteur des AV ont toujours été mises en œuvre rapidement. Cependant, en plus des menaces et vulnérabilités d'ordre global, le présent rapport pointe aussi des problématiques spécifiques à la Suisse. La plupart d'entre elles sont dues à l'absence de données fiables sur le secteur suisse des AV.

Divers facteurs contribuent à réduire les risques liés aux AV. Le premier est que la coopération internationale a déjà enregistré des succès dans les enquêtes sur des AV, grâce au traçage, au blocage et à la confiscation renforcés d'AV, ce qui révèle que si elles sont suffisamment équipées, les autorités concernées peuvent lutter efficacement contre le BA et le FT dans le secteur des AV. La consolidation des prestataires dans le secteur des AV, qui a eu pour effet d'améliorer le degré de maturité des grands acteurs en ce qui concerne la compliance, constitue un autre facteur. Troisièmement, la transparence inhérente à la plupart des blockchains offre des possibilités uniques pour retracer les flux financiers, ce qui n'est pas possible avec les systèmes de paiement traditionnels. L'utilisation d'outils d'analyse de blockchain permet parfois d'identifier et de suivre plus facilement des activités suspectes. Un quatrième facteur est que la Suisse a communiqué et mis en œuvre, en amont et de manière transparente, un cadre législatif ainsi que des exigences prudentielles en matière d'AV et de PSAV. La *travel rule* du GAFI est mise en œuvre de manière intégrale, car elle concerne aussi les paiements en provenance et à destination de portefeuilles non hébergés, ce qui améliore le contrôle et la traçabilité des transactions. Enfin, l'élargissement de la définition de l'intermédiation financière a contribué à faire entrer un plus large éventail d'acteurs dans le

champ d'application de la LBA, afin de combler les lacunes dans les mesures de lutte anti-blanchiment.

Sur la base des menaces et vulnérabilités identifiées dans la présente analyse de risques, le GCBF propose les quatre mesures suivantes afin de renforcer le dispositif actuel :

1. **Améliorer l'état des données et des connaissances sur le secteur des AV en Suisse**
   Pour pouvoir identifier exactement, comprendre et évaluer les risques de BA et de FT en lien avec les AV ainsi que pour développer des mesures adéquates, il est indispensable de posséder des données sur le secteur des AV et sur l'utilisation criminelle d'AV en Suisse. Il s'agit par exemple d'informations sur la taille, les activités et les priorités du secteur, ou de données sur le nombre de procédures, les infractions qui ont fait l'objet d'une instruction et les montants concernés. Ces données sont d'une importance décisive pour garantir l'efficacité de la lutte contre le BA et le FT et protéger l'intégrité de la place financière. L'absence de données et d'informations complètes nationales et internationales nous empêche non seulement d'effectuer une appréciation générale des risques, mais peut aussi avoir pour effet que les évolutions sont sous-estimées et les mesures nécessaires ne sont pas prises, ou alors trop tard. Dans ce contexte, les principaux chiffres relatifs à ce secteur devraient être relevés de manière régulière et globale.

2. **Encourager un comportement proactif en matière de communication chez les intermédiaires financiers exerçant une activité de PSAV**
   Les chiffres relatifs aux communications de soupçons en lien avec des AV reçues par le MROS montrent qu'entre 2020 et 2022, moins d'un quart provenaient d'intermédiaires financiers exerçant une activité de PSAV. Il convient de noter que 4 d'entre eux sont responsables de la majorité de ces communications. Au total, seulement 24 intermédiaires financiers ont déposé au moins une communication de soupçons dans la période considérée, alors que la Suisse comptait déjà plus de 204 intermédiaires financiers exerçant une activité de PSAV à fin 2022. L'analyse des communications reçues de leur part témoigne donc d'un comportement de type plutôt réactif de ce secteur. Les autorités et institutions chargées de la surveillance devraient par conséquent informer leurs affiliés exerçant une activité de PSAV des résultats de cette analyse de risques, et les encourager à se montrer plus proactifs en matière de communication, éventuellement en contrôlant régulièrement leurs mesures de compliance et de monitoring.

3. **Mettre à disposition des capacités et des ressources suffisantes pour lutter contre le BA et le FT dans le secteur des AV**
   Une coopération renforcée entre les autorités compétentes est nécessaire pour répondre aux défis posés par la lutte anti-blanchiment dans le secteur des AV. Les chiffres et les données disponibles montrent que les AV sont utilisés à des fins criminelles de plus en plus fréquemment et de manière de plus en plus diversifiée. En outre, les techniques d'utilisation d'AV à de telles fins évoluent sans arrêt. Le développement de connaissances, de capacités et de ressources constitue par conséquent un aspect central du dispositif de lutte contre le BA et le FT. Les autorités de poursuite pénale ont comme principaux instruments d'abord leurs propres outils d'enquête (par ex. outils d'analyse de blockchain), puis la coopération nationale et internationale, l'entraide judiciaire et policière avec leurs partenaires étrangers ainsi que la Convention de Budapest. L'efficacité de ces instruments dépend toutefois de l'état des connaissances, des ressources et des capacités des acteurs concernés. C'est pourquoi les autorités chargées de la lutte anti-blanchiment en Suisse doivent être dotées de ressources et de capacités suffisantes pour pouvoir lutter efficacement contre le BA et le FT dans le secteur des AV.

4. **Renforcer la coopération internationale**

   La Suisse continue de s'engager au niveau international en faveur d'une lutte efficace contre les risques criminels dans le secteur financier. Cet engagement est important et peut contribuer à atténuer les risques de BA et de FT dans le secteur des AV. La Suisse continuera de s'investir afin que les normes développées au niveau international dans ce domaine soient rapidement mises en œuvre. Bon nombre des menaces et des vulnérabilités dues aux AV touchent tous les pays dans la même mesure, y compris la Suisse. Étant donné le caractère transnational des risques dans le secteur des AV, les principales mesures pour les atténuer doivent être coordonnées au plan international.

10. Bibliographie

22.3145 (postulat), *Poursuites pénales en matière de cybercriminalité. Efficacité des cantons*, déposé le 16 mars 2022 par le conseiller national Andri Silberschmid

22.3017 (postulat), *Renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies*, déposé le 15 février 2022 par la Commission de la politique de sécurité du Conseil national

Aktionariat, *Create a market for your shares*, consulté en mai 2023

AP News, *Mexican cartels turn to bitcoin, internet, e-commerce*, 10 mars 2022

Association suisse des banquiers (ASB), *Convention relative à l'obligation de diligence des banques*, 2020

Bank for International Settlements (BIS), *OTC foreign exchange turnover in April 2022*, octobre 2022

Banque centrale européenne (BCE), *Understanding the crypto-asset phenomenon, its risks and measurement issues*, mai 2019

Banque Migros, *Kryptowährungen bei jüngeren Generationen beliebter als Gold*, 27 février 2020

Barron's, *The Cryptocurrency Crash Could Lead to a Wave of M&A*, 23 juin 2022

Basel Institute On Governance, Europol, *Seizing the Opportunity: 5 recommendations for crypto-assets-related crime and money laundering*, 2022

BBC News, *Why the Central African Republic adopted Bitcoin*, 6 juin 2022

Bithome, *Buy and Sell Real Estate with Bitcoin or Cryptos*, consulté en mai 2023

Bloomberg, *Tesla Trails Only MicroStrategy in Treasury Bitcoin Allocation*, 8 février 2021

Cambridge Centre For Alternative Finance (CCAF), *3rd Global Cryptoasset Benchmark Study*, septembre 2020.

Canton de Zoug, *Kanton Zug akzeptiert ab 2021 Kryptowährungen für Steuerzahlungen* (communiqué de presse), 3 septembre 2020

Cash, *Handelsvolumen an der SIX 2022 rückläufig*, 3 janvier 2023

Center for Philanthropy Studies (CEPS), Universität Basel SwissFoundations, Verband der Schweizer Förderstiftungen Zentrum für Stiftungsrecht, Universität Zürich, *Der Schweizer Stiftungsreport 2022*, mai 2022

Center for Philanthropy Studies (CEPS), Universität Basel SwissFoundations, Verband der Schweizer Förderstiftungen Zentrum für Stiftungsrecht, Universität Zürich, *Der Schweizer Stiftungsreport 2023*, juin 2023

Chainalysis, *The 2020 Crypto Crime Report*, janvier 2020

Chainalysis, *The 2021 Crypto Crime Report*, février 2021

Chainalysis, *The 2021 Geography of Cryptocurrency Report*, octobre 2021

Chainalysis, *Cryptocurrency Exchanges in 2021*, novembre 2021

Chainalysis, *North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High*, 13 janvier 2022

Chainalysis, *The Crypto Crime Report 2022*, février 2022

Chainalysis, *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class*, 2 février 2022

Chainalysis, *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, 5 avril 2022

Chainalysis, *DeFi-Driven Speculation Pushes Decentralized Exchanges' On-Chain Transaction Volumes Past Centralized Platforms*, 6 juin 2022

Chainalysis, *The State of Web3*, juin 2022

Chainalysis, *The 2022 Geography of Cryptocurrency Report*, septembre 2022

Chainalysis, *2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking*, 12 janvier 2023

Chainalysis, *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, 26 janvier 2023

Chainalysis, *The 2023 Crypto Crime Report*, février 2023

Chemins de fer fédéraux suisses CFF, *Achetez votre portefeuille papier bitcoin en tout temps aux distributeurs de billets CFF*, consulté en mai 2023

Ciphertrace, *Cryptocurrency crime and anti-money laundering*, juin 2022

City of Lugano, Tether, *Lugano's Plan B*, consulté en mai 2023

CNET, *Ransomware rises as a national security threat as bigger targets fall*, 18 octobre 2021

Coin ATM Radar, *Bitcoin ATM Map*, consulté en mai 2023

Coindesk, *'Ship-to-Ship' Trade and Other Secrets of North Korea's Illicit $1.5B Crypto Stash*, 7 avril 2020

Coinmap, *Crypto ATMs & merchants of the world*, consulté en mai 2023

CoinMarketCap, *Global Cryptocurrency Market Charts*, consulté en mai 2023

Conseil de sécurité des Nations Unies, *S/2021/211 Rapport final présenté par le Groupe d'experts en application de la résolution 2515 (2020)*, mars 2021

Conseil de sécurité des Nations Unies, *S/2022/132 Rapport final présenté par le Groupe d'experts en application de la résolution 2569 (2021)*, mars 2022

Conseil de sécurité des Nations Unies, *S/2022/668 Rapport de mi-mandat présenté par le Groupe d'experts en application de la résolution 2627 (2022)*, septembre 2022

Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), *Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France*, septembre 2019

Conseil fédéral, *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070)*, 25 juin 2014

Conseil fédéral *Leadership mondial, ancrage en Suisse: Politique pour une place financière suisse tournée vers l'avenir*, décembre 2020

Curry David, *Coinbase Revenue and Usage Statistics (2023)*, 28 mars 2023

Département fédéral des finances (DFF), *Ordonnance du Conseil fédéral sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués, rapport explicatif en vue de l'ouverture de la procédure de consultation*, octobre 2020

Department of Justice (USA), *Two Chinese Intelligence Officers Charged with Obstruction of Justice in Scheme to Bribe U.S. Government Employee and Steal Documents Related to the Federal Prosecution of a PRC-Based Company*, 24 octobre 2022

Department of the Treasury (USA), *National Money Laundering Risk Assessment*, février 2022

Elliptic, *NFTs and Financial Crime*, août 2022

Europol Spotlight, *Cryptocurrencies – Tracing the Evolution of Criminal Finances*, décembre 2021

Europol, *Bitzlato: senior management arrested*, 23 janvier 2023

Europol, *Underground drug-money bank laundering EUR 180 million liquidated by law enforcement*, 13 avril 2023

FF 2020 7559, *Loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués*, octobre 2020

FF 2023 84 – *Message relatif à la modification de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques)* du 2 décembre 2022, janvier 2023

Financial Crimes Enforcement Network (FinCEN), *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, 10. August 2021

Financial Crimes Enforcement Network (FinCEN), *Advisory on Illicit Activity Involving Convertible Virtual Currency*, Mai 2019, pp. 1 - 2

Financial Intelligence Unit (Deutschland), *Jahresbericht 2019*, juin 2020

Financial Intelligence Unit (Deutschland), *Jahresbericht 2021*, août 2022

Financial Intelligence Unit (Estland), *Yearbook 2019*, 2020

Financial Intelligence Unit (Estland), *The Risks related to Virtual Asset Service Providers in Estonia*, janvier 2022

Financial Intelligence Unit (Liechtenstein), *Jahresbericht 2020*, mars 2021

Financial Intelligence Unit (Liechtenstein), *Jahresbericht 2021*, avril 2022

Financial Intelligence Unit (Niederlande), *Annual Review 2019*, juin 2020

Financial Intelligence Unit (Niederlande), *Annual Review 2021*, juin 2022

Financial Stability Board (FSB), *FSB Chair's letter to G20 Finance Ministers and Central Bank Governors*, mars 2018

Financial Stability Board (FSB), *Assessment of Risks to Financial Stability from Crypto-assets*, février 2022

Financial Stability Institute, *Supervising cryptoassets for anti-money laundering*, avril 2021

Financial Times, *How North Korea became a crypto crime hub*, 14 novembre 2022

Finews, *Tessiner dürfen ihre Steuern jetzt in Bitcoin zahlen*, 7 juillet 2022

Finews, *1 Milliarde Krypto-Nutzer bis ins Jahr 2030*, 25 juillet 2022

Finews, *Chainalysis: Crypto Hacks Reach Record $3 Billion*, 13 octobre 2022

Finews, *EU erhält europaweite Krypto-Regulierung*, 21 avril 2023

FINMA, *Rapport annuel 2016*, mars 2017

FINMA, *Guide pratique ICO pour les questions d'assujettissement concernant les initial coin offerings*, février 2018

FINMA, *Communication FINMA sur la surveillance 02/2019, Trafic des paiements sur la blockchain*, août 2019

FINMA, *Complément au guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO)*, septembre 2019

FINMA, *Rapport annuel 2020*, mars 2021

FINMA, *Rapport annuel 2021*, mars 2022

FINMA, *Monitorage FINMA des risques 2022*, novembre 2022

FINMA, *Rapport annuel 2022*, mars 2023

FINMA, *La FINMA clôt une procédure à l'encontre d'une plate-forme cryptographique et son fondateur*, mai 2023

Forbes, *Scandals And Mafia Allegations May Force Malta To Reconsider Its Reliance On Online Betting*, 13 mars 2021

GAFI, *Monnaies virtuelles: Définitions clés et risques potentiels en matière de LBC/FT*, juin 2014

GAFI, *Guidance for a Risk-Based Approach to Virtual Currencies*, juin 2015

GAFI, *Outcomes FATF Plenary, 17-19 October 2018*, octobre 2018

GAFI, *Lignes directrices de l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels*, juin 2019

GAFI, *Les progrès de la Suisse dans le renforcement des mesures de lutte contre le blanchiment d'argent et le financement du terrorisme*, janvier 2020

GAFI, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, juin 2020

GAFI, *Actifs virtuels: indicateurs de blanchiment de capitaux et de financement du terrorisme*, septembre 2020

GAFI, *Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers*, mars 2021

GAFI, *Actualisation du Guide "Approche fondée sur les risques des actifs virtuels et des prestataires de services d'actifs virtuels"*, octobre 2021

GAFI, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, juin 2022

GAFI, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, juin 2023

GAFI, *Recommandations du GAFI*, février 2023

GAFI, *Lutte contre le financement des rançongiciels*, mars 2023

GAFI, *Press Release - Virtual Assets Contact Group (VACG)*, 14 avril 2023

GCBF, *Rapport sur l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme en Suisse* , juin 2015

GCBF, *Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowfunding*, octobre 2018

GCBF, *Deuxième rapport national sur les risques de blanchiment d'argent et de financement du terrorisme*, octobre 2021

Gotham City, *L'enquête sur les pirates allemands de Movie2k passe par Genève*, N° 278, 26 janvier 2023

Government Of The Grand Duchy Of Luxembourg, *ML/TF Vertical Risk Assessment: Virtual Asset Service Providers*, décembre 2020

Handelszeitung, *6000 Kunden kaufen bei der SBB Bitcoins | Handelszeitung*, 1er novembre 2017

Handelszeitung, *Krypto lockt: Studie zeigt grosses Interesse in der Schweiz*, 22 juin 2021

Handelszeitung, *85'000 Händler in der Schweiz können nun Zahlungen mit Bitcoin und Ether annehmen*, 19 août 2021

HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, décembre 2020

Home of Blockchain, *Swiss Digital Asset Market Report 2022*, mai 2022

Institute of Financial Services Zug IFZ (Hochschule Luzern), *Crypto Assets Study 2021*

Institute of Financial Services Zug IFZ (Hochschule Luzern), *Crypto Assets Study 2022*

Institute of Financial Services Zug IFZ (Hochschule Luzern), *Fintech Study 2023*

International Monetary Fund (IMF), *Treatment of Crypto Assets in Macroeconomic Statistics*, 2019

International Monetary Fund (IMF), *F.18 Recording of Crypto Assets in Macroeconomic Statistics*, mars 2022

Jimenez Alison, *3 Misconceptions about Cryptocurrency Crime Estimates*, 11 janvier 2022

Journal officiel de l'Union européenne, *Règlement (UE) 2023/1113 du Parlement européen et du Conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (UE) 2015/849, JO L 150,* 9 juin 2023

La banque mondiale, *PIB ($ US courants) – World*, consulté en mai 2023

La banque mondiale, *Virtual Assets and Virtual Asset Service Providers ML/TF Risk Assessment Tool*, juin 2022

L'avvenire di Calabria, *Boom delle scommesse online, ma per la Dia c'è l'ombra dei clan*, 23 janvier 2020

Malta Gaming Authority, *Annual Report 2021*, septembre 2022

McGuire Michael, *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy*, avril 2018

Monetary Authority of Singapore, *Guidelines to Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism - Digital Payment Token Service*, mars 2020

Moneyland, *Wie legen Schweizer ihr Geld an?*, 22 avril 2020

Moneyland, *So investieren Schweizerinnen und Schweizer ihr Geld*, 19 juillet 2022

Monroe Brian, *FinCEN, OFAC fine crypto exchange Bittrex nearly $30 million on AML, sanctions failings, missed SARs, links to darknet markets, mixers, ransomware gangs*, 11 octobre 2022

MROS, *Rapport annuel 2020*, mai 2021

Nasdaq, *Blockware Estimates 10% Global Bitcoin Adoption By 2030: Report*, 9 juin 2022

National Coordinating Committee on Combating Money Laundering and Funding of Terrorism (Malta), *Key Results of the Sectoral Risk Assessment on Virtual Financial Assets*, février 2020

New York Times, *In Global First, El Salvador Adopts Bitcoin as Currency*, 7 septembre 2021

New York Times, *Banks Tried to Kill Crypto and Failed. Now They're Embracing It (Slowly)*, 1 novembre 2021

New York Times, *Coinbase Reaches $100 Million Settlement With New York Regulators*, 4 janvier 2023

New York Times, *Government Cracks Down on Crypto Industry With Flurry of Actions*, 18 février 2023

Office des Nations Unies contre la drogue et le crime (ONUDC), *Blanchiment d'argent*, consulté en mai 2023

Office fédéral de la cybersécurité (OFCS), *Rapport semestriel 2022/II (juillet-décembre)*, mai 2023

Office fédéral de la statistique (OFS), *Statistique policière de la criminalité (SPC) - Rapport annuel 2021*, mars 2022

Office fédéral de la statistique (OFS), *Statistique policière de la criminalité (SPC) - Rapport annuel 2022*, mars 2023

Organized Crime & Corruption Reporting Project (OCCRP), *Italian Mafia Bets on Illegal Online Gambling*, 4 mars 2021

Parlement européen, *Crypto-actifs: feu vert à de nouvelles règles de traçabilité des transferts*, avril 2023

Prestige Business, *Cyber-Attacken in der Schweiz nehmen auch 2023 zu*, 3 mai 2023

Prévention suisse de la criminalité, *Money Mules*, consulté en mai 2023

Reuters, *Crypto exchange Bittrex to pay $29-mln penalty to U.S. Treasury Department*, 11 octobre 2022

Reuters, *Dutch central bank fines cryptocurrency exchange Coinbase 3.3 mln euros*, 26 janvier 2023

Reuters, *Dutch central bank fines Binance 3.3 million euros*, 18 juillet 2022

RR.2022.45, *Arrêt du 20 décembre 2022 – Cour des plaintes*, Urteil des Bundesstrafgerichts, Bellinzone, 21 décembre 2022

RS *0.311.43* – *Convention du 23 novembre 2001 sur la cybercriminalité*, état le 14 septembre 2020

RS *935.51* – *Loi fédérale sur les jeux d'argent* (LJAr), état le 1er janvier 202

RS *935.511* – *Ordonnance sur les jeux d'argent* (OJAr), état le 1er janvier 2021

RS *941.31* – *Loi fédérale sur le contrôle du commerce des métaux précieux et des ouvrages en métaux précieux* (loi sur le contrôle des métaux précieux, LCMP), état le 1er janvier 2023

RS *955.0* – *Loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme*, (loi sur le blanchiment d'argent, LBA), état le 23 janvier 2023

RS *955.01* – *Ordonnance sur la lutte contre le blanchiment d'argent et le financement du terrorisme* (ordonnance sur le blanchiment d'argent, OBA), état le 1er janvier 2016

RS *955.01* – *Ordonnance sur la lutte contre le blanchiment d'argent et le financement du terrorisme* (ordonnance sur le blanchiment d'argent, OBA), état le 1er août 2021

RS *955.033.0* – *Ordonnance de l'Autorité fédérale de surveillance des marchés financiers sur la lutte contre le blanchiment d'argent et le financement du terrorisme* (ordonnance de la FINMA sur le blanchiment d'argent, OBA-FINMA), état le 1er janvier 2021

RS *958.1* – *Loi fédérale sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés* (loi sur l'infrastructure des marchés financiers, LIMF)

RS *958.11* – *Ordonnance sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés* (ordonnance sur l'infrastructure des marchés financiers, OIMF

Schurter Daniel, *Das ist die gefährlichste Hackerbande, die auch in der Schweiz wütet*, 23 janvier 2023

Schweizer Radio und Fernsehen (SRF), *Die Schweiz tut sich schwer mit Gesetzesverschärfungen zum Gold*, 10 mai 2022

Secrétariat d'État aux questions financières internationales (SFI), *Mandat du groupe de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme*, institué par la décision du Conseil fédéral du 17 novembre 2021

Secrétariat d'État aux questions financières internationales (SFI), *Feuille d'information crypto*, janvier 2022

Secrétariat d'État aux questions financières internationales (SFI), *Place financière suisse Chiffres-clés 2023,* avril 2023

Secrétariat d'État aux questions financières internationales (SFI), *Blockchain/DLT*, consulté en mai 2023

Stalinsky Steven, *The Coming Storm – Terrorists Using Cryptocurrency*, 21 août 2019

State Financial Service of Ukraine, *Report on the National Risk Assessment*, 2019

Süddeutsche Zeitung, *Wieso die Mafia Fan von Maltas Online-Casinos ist*, 18 décembre 2022

Swedish Police Authority, *The Financial Intelligence Unit Annual Report 2021*, mai 2022

Swiss Foundations, *Rapport sur les fondations en Suisse,* CEPS Forschung und Praxis, volume 30, juin 2023

Swissinfo, *L'ONU se penche sur les importations d'or en Suisse*, 3 octobre 2022

Tages Anzeiger, *Schweizer Online-Drogenversand – «Hippe Kleider, Typ Studentin, und das Täschli voller Drogen»*, 18 mars 2021

Triple-A, *Global Cryptocurrency Ownership Data*, consulté en mai 2023

TRM Labs, *Ensuring Responsible Development of Digital Assets; Request for Comment*, novembre 2022

United Nations Data Retrieval System, *Democratic People's Republic of Korea*, consulté en mai 2023

Vedrenne Gabriel, *In Europe, Suspicious Payments Triple Thanks to VASPs, Cryptocurrency*, 25 octobre 2022

Von Luckner, Reinhart & Rogoff, *Decrypting New Age International Capital Flows, NBER Working Paper No. 29337*, octobre 2021, p. 1, note de bas de page n° 2

Wired Magazine, *Most Criminal Cryptocurrency Funnels Through Just 5 Exchanges*, 26 janvier 2023

11. Annexe

11.1 Méthodologie utilisée pour analyser les communications de soupçons du MROS

L'introduction du système goAML a offert de nouvelles possibilités au MROS pour analyser les données qu'il reçoit des intermédiaires financiers, des autorités nationales et de ses homologues étrangers. Toutes les données sont désormais stockées dans un système de traitement des données relationnel et peuvent être analysées plus en profondeur par divers processus de recherche. Dans le cadre du présent rapport, le MROS a pu appliquer ces nouvelles méthodes d'analyse avec succès. Elles sont expliquées schématiquement ci-dessous :

S'agissant des résultats présentés au ch. 7 issus de l'analyse des communications de soupçons déposées entre 2020 et 2022, nous avons examiné lesquelles d'entre elles présentent un lien avec des AV. Afin d'être catégorisée comme communication "en lien avec des AV", une communication de soupçons doit remplir au moins un des critères suivants :

1. Identification des communications pertinentes au moyen d'informations sur les transactions, le compte et le détenteur du compte : une communication de soupçons devait mentionner des transactions entre les comptes signalés et les comptes (formellement identifiés par le MROS) d'intermédiaires financiers suisses ou étrangers exerçant une activité de PSAV. Ce critère englobe de fait les communications déposées par les intermédiaires financiers suisses exerçant une activité de PSAV, pour autant qu'elles comprennent des transactions suspectes ou des faits en lien avec des AV[244]. Par ailleurs, cela comprend aussi les communications déposées par des intermédiaires financiers *sans* activité de PSAV dont les transactions signalées ont comme contrepartie (bénéficiaire ou donneur d'ordre) un intermédiaire financier (formellement identifié par le MROS) exerçant une activité de PSAV en Suisse ou à l'étranger.

2. Identification des communications pertinentes à l'aide d'une liste de mots clés en lien avec les AV[245]: chaque communication de soupçons remise au MROS contient une description des faits par l'intermédiaire financier signalant. Celle-ci devait inclure au moins un des 50 mots clés (par ex. "bitcoin" ou "crypto") afin d'être classée dans les dossiers devant être analysés plus en profondeur. Nous avons pris soin de ne compter ces communications identifiées par des mots clés comme ayant un lien avec des AV que si elles ne présentaient pas de faux positifs (par ex. FIAT pour la marque automobile ou "mining" au sens de l'extraction minière).

Au total, 1867 communications émises entre 2020 et 2022 remplissaient au moins l'un de ces critères. Et il s'agit d'une estimation plutôt conservatrice. En effet, nous ne pouvons pas exclure que parmi les 18 937 communications reçues pendant cette période, il y en ait d'autres qui présentent des liens avec des AV. Premièrement, il est possible que d'autres communications comportent des transactions entre les comptes signalés et les comptes d'intermédiaires financiers exerçant une activité de PSAV suisses ou étrangers, mais que ces transactions

[244] Les communications de soupçons provenant d'intermédiaires financiers exerçant une activité de PSAV ne doivent pas nécessairement avoir un lien avec des AV, car ce type d'intermédiaire financier propose parfois aussi des services financiers traditionnels sans rapport avec les AV; cf. fig. 4 au ch. 4.2.
[245] Les mots clés ont été sélectionnés et réunis par le MROS au cours de l'élaboration de la présente analyse. Tous ont été utilisés dans les différentes langues (allemand, italien, français et anglais) et graphies lors de la recherche textuelle.

n'ont pas été signalées par les intermédiaires financiers[246], ou que ces comptes n'étaient pas connus du MROS et que les communications concernées n'ont donc pas pu être identifiées. Deuxièmement, il est aussi possible qu'une communication de soupçons présente effectivement un lien avec des AV ou des PSAV, mais que ce lien n'a pas pu être identifié avec la recherche par mots clés. Cette méthode implique par conséquent qu'ont été identifiées seulement les communications dans lesquelles l'intermédiaire financier signalant a déjà constaté un lien avec des AV et qu'il l'a mentionné explicitement dans sa description des faits, et que la liste de mots clés a fait mouche. En outre, les informations supplémentaires demandées par le MROS pour analyser une communication (demandes d'information visées à l'art. 11*a* LBA) n'ont pas été prises en compte dans l'analyse. Par conséquent, les chiffres sur les communications de soupçons en lien avec des AV constituent des indications minimales.

La sélection obtenue par cette méthode a été classée en deux catégories : communication déposée par un intermédiaire financier exerçant une activité de PSAV, ou communication déposée par un intermédiaire financier sans activité de PSAV, car nous avons constaté que les flux financiers et les typologies n'étaient pas les mêmes dans chaque catégorie. Dans les communications émanant d'intermédiaires financiers sans activité de PSAV, les flux financiers prenaient uniquement la forme de monnaie fiat, tandis que les communications émanant d'intermédiaires financiers exerçant une activité de PSAV pouvaient contenir des transactions aussi bien en fiat qu'en AV. Il convient en outre de noter que ces dernières communications ne représentaient qu'*une partie* des communications déposées par ce type d'intermédiaires financiers, car ils en ont aussi déposé d'autres qui n'avaient pas de lien avec des AV ou des PSAV, par exemple lorsqu'il s'agit de banques qui proposent à leurs clients également des services financiers traditionnels sans rapport avec des AV (cf. fig. 4 au ch. 4.2). Les 1867 communications ont été analysées sur le plan de la quantité et de la qualité à l'aide d'une liste d'indicateurs. Les éléments principaux étaient les informations sur les intermédiaires financiers signalants, les actes préalables soupçonnés par l'intermédiaire financier signalant, les éléments fondant le soupçon, les cocontractants signalés, les flux financiers constatés et les sommes concernées.

11.1.1 Communications d'intermédiaires financiers exerçant une activité de PSAV avant 2020

Même si la présente analyse de risques se concentre en priorité sur la période après 2020, nous avons également cherché à déterminer le nombre de communications de soupçons reçues par le MROS entre 2015 et 2019 provenant d'intermédiaires financiers exerçant une activité de PSAV. Cela a permis de mettre en lumière la hausse des communications et le comportement de ces intermédiaires financiers en matière de communication sur une longue période.

Pour comprendre la comparaison des chiffres d'après 2020 avec ceux des années antérieures, quelques explications s'imposent : avant 2020, le MROS comptait chaque relation d'affaires signalée comme une communication. Depuis l'introduction du système goAML à la fin de 2019, la façon de compter les communications de soupçons reçues par le MROS a changé[247]. À partir de cette date, l'intermédiaire financier peut désormais signaler plusieurs relations d'affaires au sein de la même communication de soupçons, lorsqu'elles sont signalées dans le même contexte ou par rapport aux mêmes faits suspects. Depuis le 1er janvier 2020, le MROS compte le nombre de communications et non plus, comme auparavant, le nombre de relations d'affaires signalées. C'est pourquoi il s'avère difficile de comparer avec exactitude les

[246] Les communications remises au MROS contiennent des indications sous une forme structurée, conformément aux prescriptions du MROS, sur les transactions suspectes signalées par l'intermédiaire financier.
[247] MROS, *Rapport annuel 2020*, mai 2021, p. 16

chiffres d'avant 2020 avec ceux d'après 2020. Pour donner néanmoins une idée de l'évolution, nous avons analysé les 185 relations d'affaires signalées entre 2015 et 2019 et plusieurs d'entre elles ont été comptées comme une seule communication parce qu'elles avaient été signalées par le même intermédiaire financier à la même date et pour les mêmes faits[248]. Cette méthode a permis de regrouper les 185 relations d'affaires dans 53 communications de soupçons.

11.2 Explications relatives à la fig. 22

Fig. 22, ch. 7.3.2
La catégorie "Autres" comprend les actes préalables suivants soupçonnés par les intermédiaires financiers :

- Abus de confiance (art. 138 CP)
- Accès indu à un système informatique (art. 143 CP)
- Actes d'ordre sexuel avec des enfants (art. 187, ch. 1, 189, 190, 191, 195 et 197, al. 4, CP)
- Assassinat (art. 112 CP)
- Autres infractions
- Autres infractions contre le patrimoine (art. 140, 144bis, ch. 2, 148, 157 et 160 CP)
- Banqueroute frauduleuse et fraude dans la saisie (art. 163, ch. 1, 164, ch. 1, 165 et 171, al. 1, CP)
- Crimes ou délits contre l'État (art. 265, art. 266bis, 266*b*, 267, ch. 1 et 2, et 271, ch. 1, al. 4, ch. 2 et 3, CP)
- Escroquerie en matière de prestations et de contributions (art. 14, ch. 4, DPA, art. 51 LAP)
- Exploitation d'informations d'initiés ou manipulation de cours (art. 154, al. 2, et 155, al. 2, LIMF)
- Extorsion et chantage (art. 156 CP)
- Fabrication de fausse monnaie et falsification de la monnaie (art. 240, al. 1, CP)
- Falsification de marchandises (art. 155, al. 2, CP)
- Faux dans les titres (art. 251, ch. 1, 253, 254 et 317, ch. 1, CP)
- Gestion déloyale (art. 158, ch. 1 et 2, CP)
- Gestion déloyale des intérêts publics (art. 314 CP)
- Importation, acquisition et prise en dépôt de fausse monnaie (art. 244, al. 2, CP)
- Loi du 13 décembre 1996 sur le contrôle des biens (art. 14, al. 2, LCB)
- Loi du 17 juin 2011 sur l'encouragement du sport (art. 22, al. 2 et 3, LESp)
- Loi du 22 mars 2002 sur les embargos (art. 9, al. 2, LEmb)
- Loi du 9 octobre 1992 sur le droit d'auteur (art. 67, al. 2, et 69, al. 2, LDA)
- Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (art. 116, al. 3, et 118, al. 3, LEI)
- Loi fédérale du 29 septembre 2017 sur les jeux d'argent (art. 130, al. 2, LJAr)
- Loi fédérale du 8 novembre 1934 sur les banques (art. 47, al. 1bis, LB)
- Loi sur les produits thérapeutiques (art. 86, al. 2, LPTh)
- Meurtre (art. 111 CP)
- Vol (art. 139 CP)

[248] Par ex., sur ces 185 relations d'affaires, plus de 100 ont été signalées au MROS par le même intermédiaire financier sur la base des mêmes opérations suspectes.