Chainalysis

JUILLET 2024

Blanchiment d'argent et Crypto-monnaie

Tendances et nouvelles techniques de détection et d'investigation

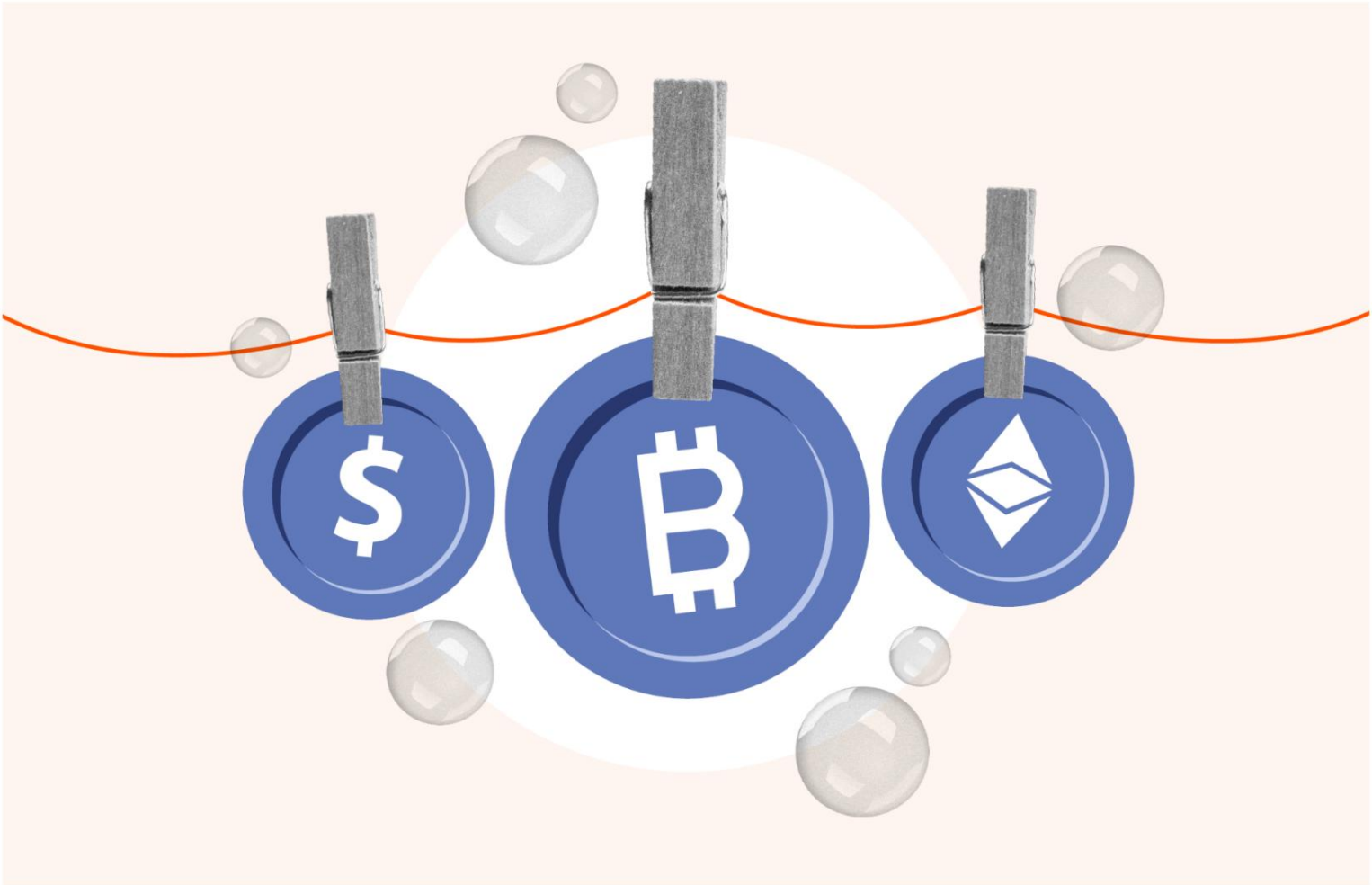


Table des matières

Blanchiment d'argent et crypto-monnaie

Bien que les blockchains publiques soient intrinsèquement transparentes et traçables, les acteurs illicites se tournent vers les cryptomonnaies pour blanchir leurs gains mal acquis pour les mêmes raisons que les gens les utilisent à des fins légitimes : elles sont transfrontalières, pratiquement instantanées et généralement peu coûteuses à effectuer. Le blanchiment d'argent dans le contexte des cryptomonnaies est généralement associé aux cybercriminels qui tentent de dissimuler le flux de fonds liés à des crimes sur la chaîne, tels que les opérations sur le marché du darknet et les ransomwares. Cependant, les cryptomonnaies sont de plus en plus utilisées pour blanchir des fonds provenant d'un éventail plus large d'activités illicites au-delà de la compréhension conventionnelle de la cryptocriminalité. L'omniprésence croissante des cryptomonnaies en a fait un outil de blanchiment des profits provenant de divers crimes hors chaîne, tels que le trafic de stupéfiants et la fraude. En 2024, le blanchiment d'argent en cryptomonnaies englobe tous les crimes, et pas seulement ceux qui sont intrinsèquement liés à l'écosystème des cryptomonnaies.

Cette évolution a des implications importantes pour les enquêteurs. Tout d'abord, l'expertise en cryptomonnaie doit s'étendre au-delà des unités spécialisées dans la cybercriminalité pour inclure les organismes chargés de l'application de la loi de toutes sortes. La cryptomonnaie est désormais l'un des moyens de paiement utilisés par les acteurs illicites dans le monde entier, et cette expertise doit donc englober à la fois le traçage des transactions par blockchain et une compréhension complète des tactiques traditionnelles de blanchiment d'argent. Ensuite, il y a un côté positif : avec les données et les outils appropriés, les enquêteurs des secteurs public et privé peuvent tirer parti de la transparence de la blockchain pour découvrir des activités illicites qui pourraient autrement passer inaperçues. L'analyse de la blockchain peut générer à la fois des signaux de renseignement pour la génération proactive de pistes et des preuves plus concrètes de flux illicites dans les enquêtes en cours, aidant ainsi un large éventail d'analystes et d'enquêteurs à démanteler des réseaux de blanchiment d'argent de plus en plus sophistiqués.

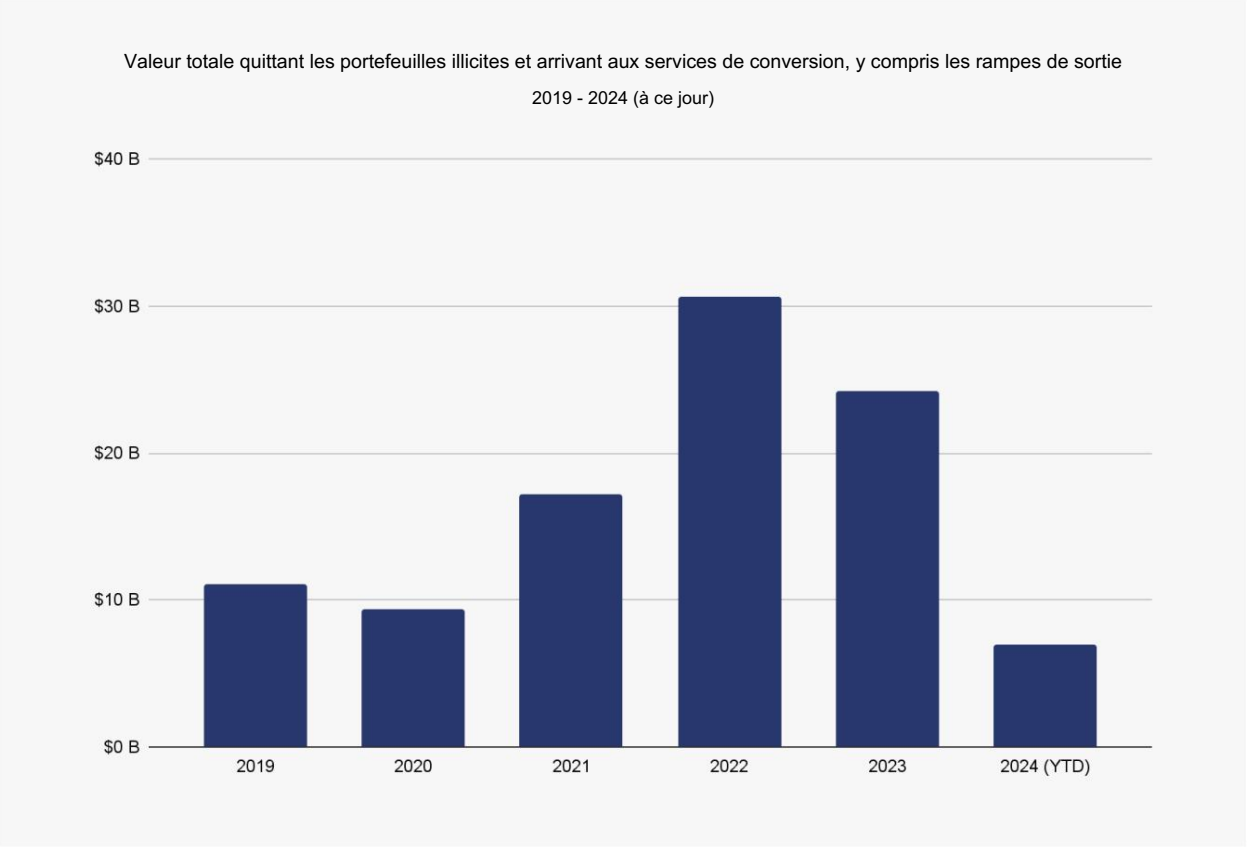
Qu'est-ce que le blanchiment d'argent ?

Le blanchiment d'argent est le processus qui consiste à dissimuler l'origine de l'argent obtenu à partir d'activités illégales afin que les fonds puissent être utilisés sans attirer l'attention sur leur source illicite. Il s'agit généralement de rendre légitimes d'importantes sommes d'argent générées par des activités criminelles, telles que le trafic de drogue ou le financement du terrorisme.

Le processus de blanchiment d'argent comprend généralement trois étapes : le placement, la superposition et l'intégration. Le placement est la première étape par laquelle l'argent illicite est introduit dans le système financier. L'empilement consiste à déplacer l'argent à travers une série de transactions financières pour masquer son origine. Enfin, l'intégration est le processus de réintroduction de l'argent dans l'économie légale, lui donnant l'apparence d'une source légale.

Chainalysis a publié des analyses sur le blanchiment d'argent Dans nos rapports annuels sur la criminalité cryptographique depuis plusieurs années, nous analysons le flux de fonds provenant de portefeuilles illicites connus pendant la phase de placement, vers des services de conversion qui représentent la phase de superposition du blanchiment. Les portefeuilles illicites connus contiennent des fonds liés à des activités criminelles crypto-natives confirmées telles que les vols d'échange, les escroqueries cryptographiques et les produits du marché sombre. Les services de conversion échangent des crypto-monnaies contre des monnaies fiduciaires, d'autres types de crypto-monnaies ou fournissent d'autres services. Les exemples de services de conversion incluent les échanges centralisés, les services DeFi, les sites de jeux d'argent, les mixeurs et les ponts. Étant donné que cette activité se déroule entièrement sur la chaîne, nous l'appelons blanchiment d'argent crypto-natif. Ce type de blanchiment d'argent peut être tracé et analysé avec un degré de précision et de rapidité supérieur par rapport aux systèmes financiers traditionnels grâce à la transparence inhérente à la blockchain.

Comme le montre le graphique ci-dessous, depuis 2019, près de 100 milliards de dollars de fonds ont été envoyés de portefeuilles illicites connus vers des services de conversion. Le montant le plus élevé enregistré a été enregistré en 2022, avec 30 milliards de dollars identifiés, dont une grande partie est attribuable à des transactions impliquant des services sanctionnés tels que la bourse russe Garantex.



Ces montants représentent la valeur en dollars des actifs au moment où ils quittent les portefeuilles associés à des acteurs illicites. Ces estimations n'incluent que les totaux transférés de sources illicites vers des services de cryptomonnaies, et n'incluent pas la valeur envoyée et reçue entre les intermédiaires – un processus décrit ci-dessous – qui peut inclure des dizaines ou des centaines de transactions individuelles. Cette estimation n'inclut pas non plus les transactions où

La cryptomonnaie est utilisée pour blanchir des fonds, mais la source de l'activité illicite n'est pas identifiée ou n'est pas en chaîne. Par exemple, prenons un cartel de la drogue qui vend des stupéfiants et paie un distributeur en utilisant une cryptomonnaie. Si cette transaction circule directement entre deux bourses connues, elle serait impossible à distinguer en chaîne des transferts légitimes de service à service sans informations de piste spécifiques. Cependant, les enquêteurs peuvent toujours suivre ces fonds en utilisant une combinaison de renseignements hors chaîne et d'analyses en chaîne, et les équipes de conformité peuvent signaler les transactions inhabituelles en dehors des activités commerciales de leurs clients.

Dans ce rapport, nous visons à élargir notre analyse du blanchiment d'argent pour englober non seulement le blanchiment d'argent natif des crypto-monnaies, mais également les modèles de transactions suspectes qui peuvent indiquer des activités de blanchiment d'argent liées à des crimes hors chaîne qui nécessiteraient une enquête plus approfondie pour confirmer

Tout d'abord, nous examinerons les tendances et les comportements dans le domaine du blanchiment d'argent crypto-natif, en identifiant les principaux modèles et méthodes utilisés par une gamme d'acteurs de la menace. Nous explorerons ensuite comment

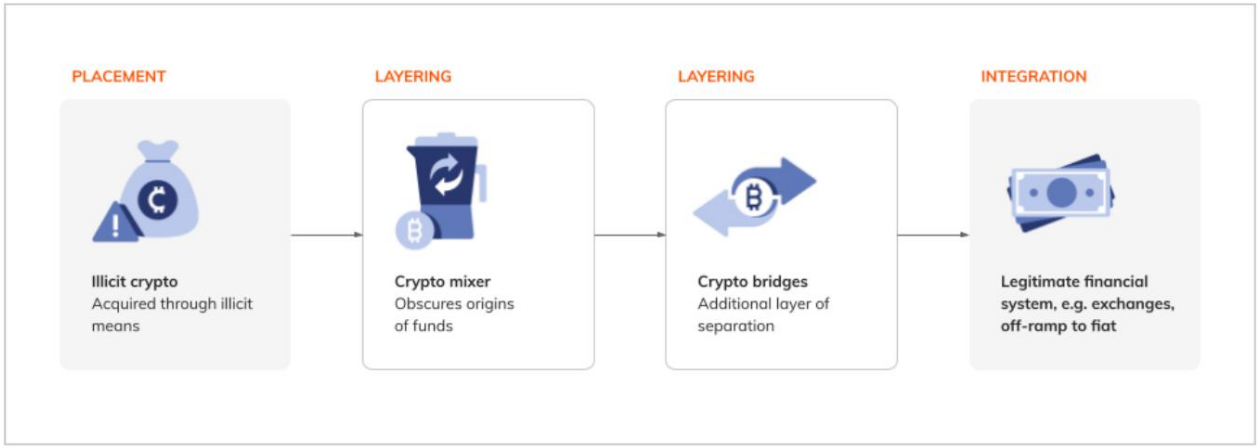
Les activités criminelles alimentées par la monnaie fiduciaire utilisent la crypto-monnaie pour le blanchiment d'argent, et comment l'analyse de la blockchain peut fournir des renseignements aux enquêteurs du gouvernement et de la conformité.

Blanchiment d'argent crypto-natif

Chaque mois, des milliards de dollars circulent dans l'écosystème cryptographique, des portefeuilles illicites aux services de conversion. Le blanchiment d'argent cryptographique peut être particulièrement sophistiqué, car ces cybercriminels exploitent souvent des mixeurs, ponts à chaînes croisées, et les sauts entre les portefeuilles intermédiaires de leurs fonds. Une [1] pour masquer l'origine et le mouvement compréhension approfondie de ces mécanismes peut aider les acteurs natifs de la cryptographie à tenter d'échapper plus efficacement à la détection, ce qui constitue un défi persistant pour les services de cryptographie et les organismes chargés de l'application de la loi.

Nous pouvons voir cette complexité à l'œuvre dans l' exploit Atomic Wallet par le groupe de hackers affilié à la Corée du Nord TraderTraitor en juin 2023, comme détaillé dans notre rapport 2024 sur la crypto-criminalité. Cet incident illustre la complexité des strates impliquées dans le blanchiment sophistiqué des crypto-monnaies, démontrant les tactiques avancées utilisées par certains acteurs pour masquer les fonds obtenus illicitement.

Blanchiment en chaîne : une menace potentielle



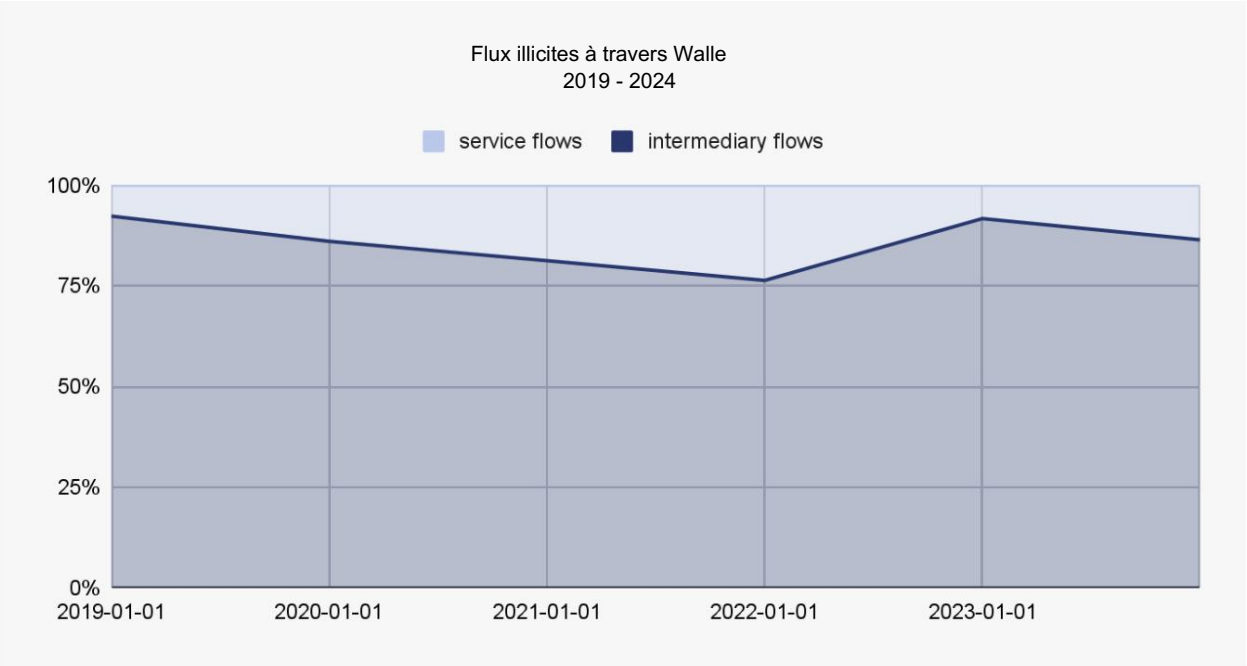
La technologie avancée d'analyse de la blockchain peut offrir des opportunités de détection et de perturbation tout au long de ce processus

Superposition de cryptomonnaies : portefeuilles intermédiaires

Les différentes étapes du blanchiment d'argent peuvent prendre de nombreuses formes. Dans le blanchiment traditionnel de monnaie fiduciaire, ce type de blanchiment consiste à envoyer des fonds via plusieurs comptes bancaires et sociétés écrans. Dans le domaine des cryptomonnaies, une méthode populaire de blanchiment consiste à envoyer des fonds via de nombreux portefeuilles personnels intermédiaires, appelés « hops ». Cette tactique vise à occulter le lien entre les fonds illicites au stade initial de placement et leur intégration éventuelle.

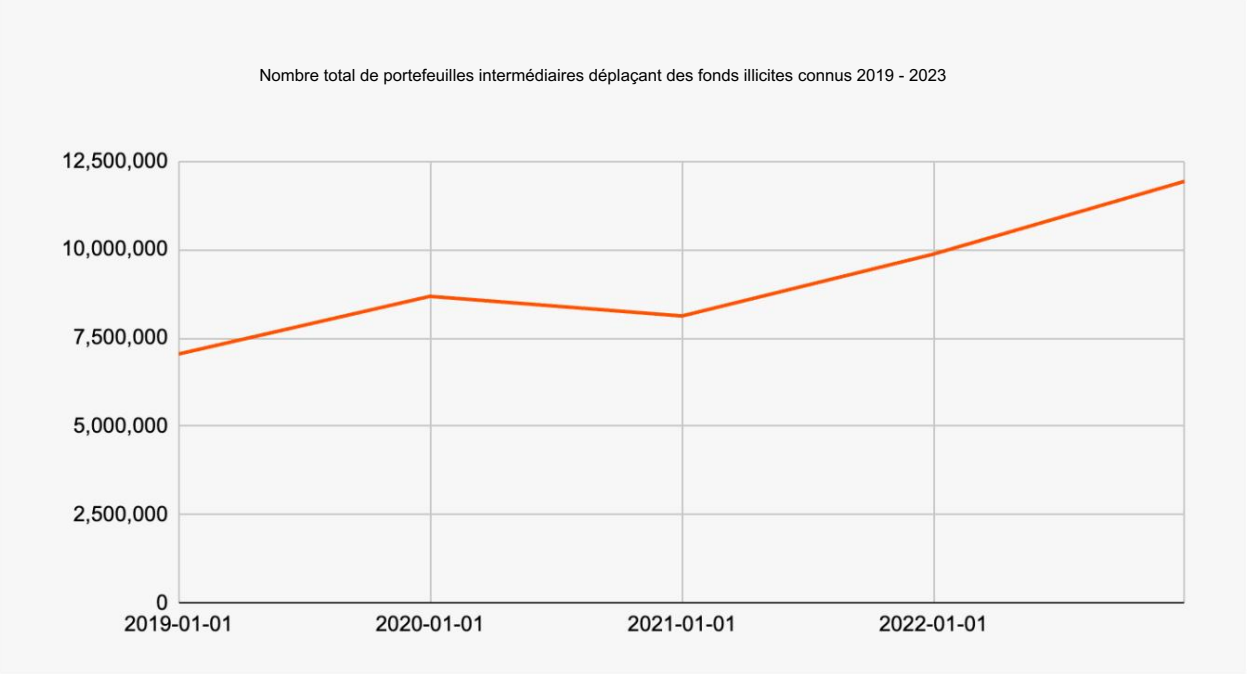
[1] D'un point de vue des données, nous définissons les intermédiaires comme des portefeuilles distincts non identifiés entre deux points de terminaison connus. Dans l'analyse du blanchiment d'argent, les intermédiaires se situent entre un portefeuille illicite et un service de conversion. Les transactions entre portefeuilles intermédiaires peuvent ou non représenter un changement de garde. En d'autres termes, la transaction peut impliquer un transfert d'un cybercriminel à un blanchisseur d'argent professionnel, ou il peut s'agir d'un individu envoyant des crypto-monnaies via de nombreux portefeuilles privés individuels qu'il contrôle. Dans l'analyse de ce rapport, nous soupçonnons que ces portefeuilles intermédiaires sont principalement des portefeuilles personnels, bien qu'ils puissent également inclure des services non identifiés. Tout au long de ce rapport, nous utilisons des techniques de science des données pour démontrer les tendances en matière de blanchiment d'argent, mais une enquête plus approfondie est nécessaire pour confirmer les cas individuels de blanchiment d'argent potentiel.

Dans le processus de blanchiment en chaîne, ces portefeuilles intermédiaires jouent un rôle important, représentant souvent plus de 80 % de la part de la valeur totale circulant à travers ces canaux de blanchiment, comme le montre le schéma ci-dessous.
[2]



De plus, la croissance du nombre de portefeuilles intermédiaires est le genre de chose à laquelle on s'attendrait si les acteurs illicites ajoutaient des sauts à leur processus de blanchiment afin d'augmenter la complexité de leurs opérations sur la chaîne.

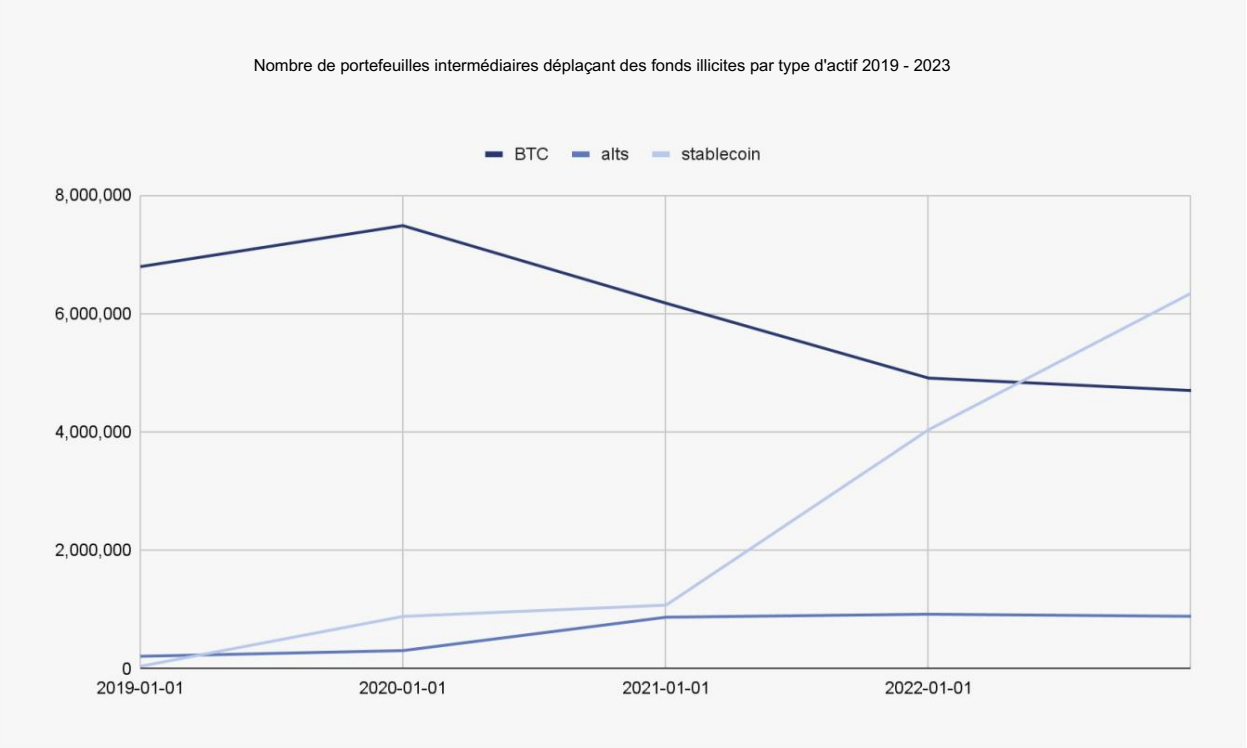
[2] Les « flux de services » tels qu'ils sont présentés ici sont définis comme le mouvement d'actifs d'un service à un autre, tandis que « l'intermédiaire » englobe les transactions entre portefeuilles intermédiaires, qui incluent les transactions de portefeuille à portefeuille ou les flux de portefeuilles illicites vers des portefeuilles intermédiaires.



Étant donné que chaque étape augmente les frais payés par les acteurs illicites, ces étapes supplémentaires peuvent être motivées, au moins en partie, par le désir d'éviter d'être détectées par les forces de l'ordre et les équipes de conformité des services de cryptographie.

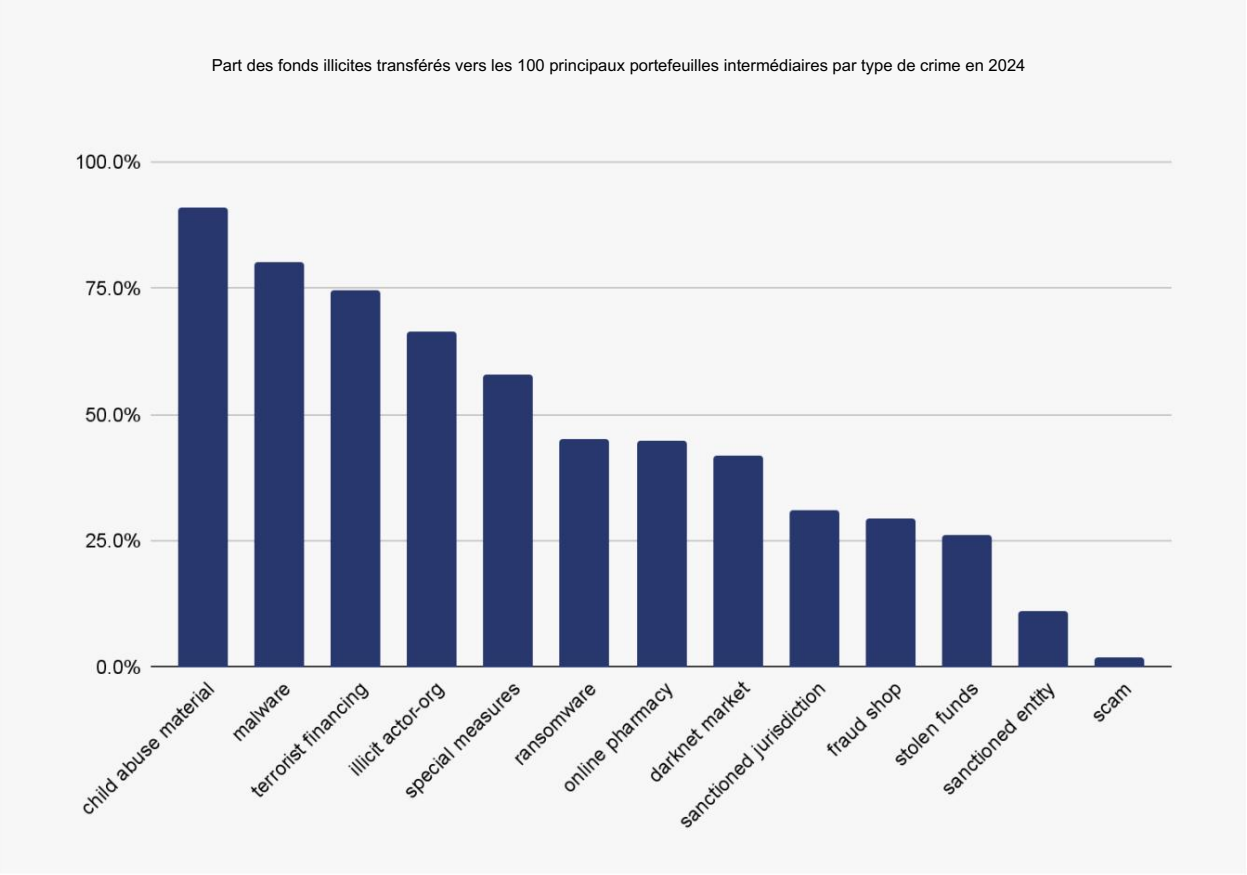
Dans le même temps, le nombre de portefeuilles intermédiaires entre les portefeuilles illicites et les services de conversion est généralement corrélé au montant total de l'activité illicite que nous observons à un moment donné. Par exemple, l'utilisation de portefeuilles intermédiaires impliquant des flux illicites a atteint un pic fin 2022, année où nous avons observé la plus grande valeur totale de cryptomonnaie reçue par des adresses illicites.

Une part croissante des fonds illicites transitant par des portefeuilles intermédiaires est représentée par des pièces stables, ce qui concorde avec notre constatation selon laquelle les pièces stables représentent désormais la majorité du volume total des transactions illicites.



Cette augmentation de l'utilisation des stablecoins reflète probablement l'augmentation globale de l'adoption des stablecoins au cours des cinq dernières années – après tout, les bons comme les mauvais acteurs préfèrent souvent détenir des fonds dans un actif dont la valeur ne changera pas en fonction des fluctuations du marché. Mais l'utilisation des stablecoins ajoute également un élément de risque pour les blanchisseurs : les émetteurs de stablecoins ont la possibilité de geler les fonds, ce que nous aborderons plus tard.

L'analyse des données peut aider à identifier les portefeuilles intermédiaires détenant une grande concentration de fonds liés à des activités criminelles liées aux crypto-monnaies. Ces portefeuilles agissent souvent comme des points de consolidation, contenant des crypto-monnaies déposées à partir de plusieurs autres portefeuilles intermédiaires.



Pour de nombreux types de crimes, seule une poignée de portefeuilles contient la grande majorité des fonds illicites, ce qui peut refléter le degré de concentration dans certaines parties du secteur illicite.

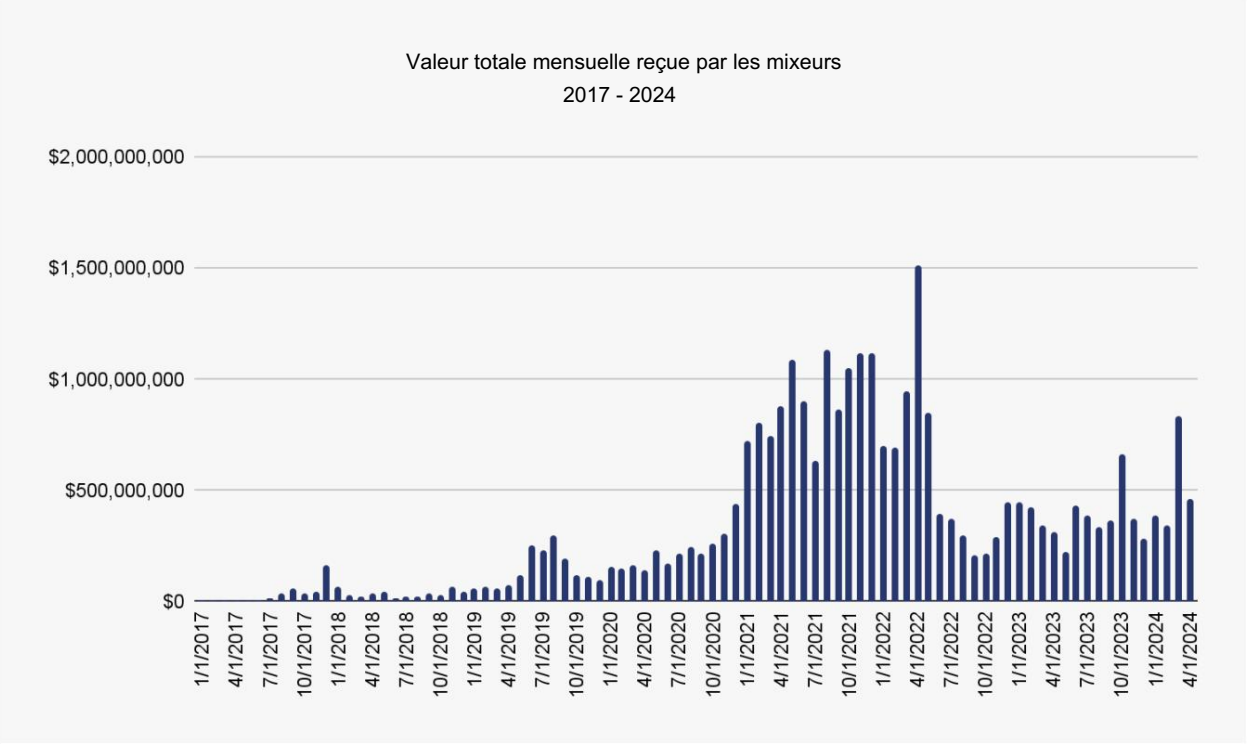
La tactique consistant à envoyer des fonds via de nombreux portefeuilles intermédiaires avant d'atteindre la destination finale complique le processus de traçage manuel pour les enquêteurs utilisant des explorateurs de blocs. Mais pour les enquêteurs et les professionnels de la conformité utilisant Chainalysis, la détection d'activités illicites et le traçage via des portefeuilles intermédiaires peuvent être relativement simples.

Services d'obscurcissement de crypto-monnaies

Étant donné que les enquêteurs équipés des bons outils peuvent facilement remonter jusqu'à la source illicite des fonds via des portefeuilles intermédiaires, de nombreux acteurs malveillants déploient des méthodes d'obscurcissement supplémentaires et des actifs cryptographiques spécialisés pour tenter de dissimuler davantage la source des fonds. Ces outils ont en commun de rompre le lien en chaîne entre la destination et l'origine des fonds, à moins que des techniques d'investigation avancées ne soient déployées. Nous examinerons plusieurs de ces méthodes d'obscurcissement ci-dessous.

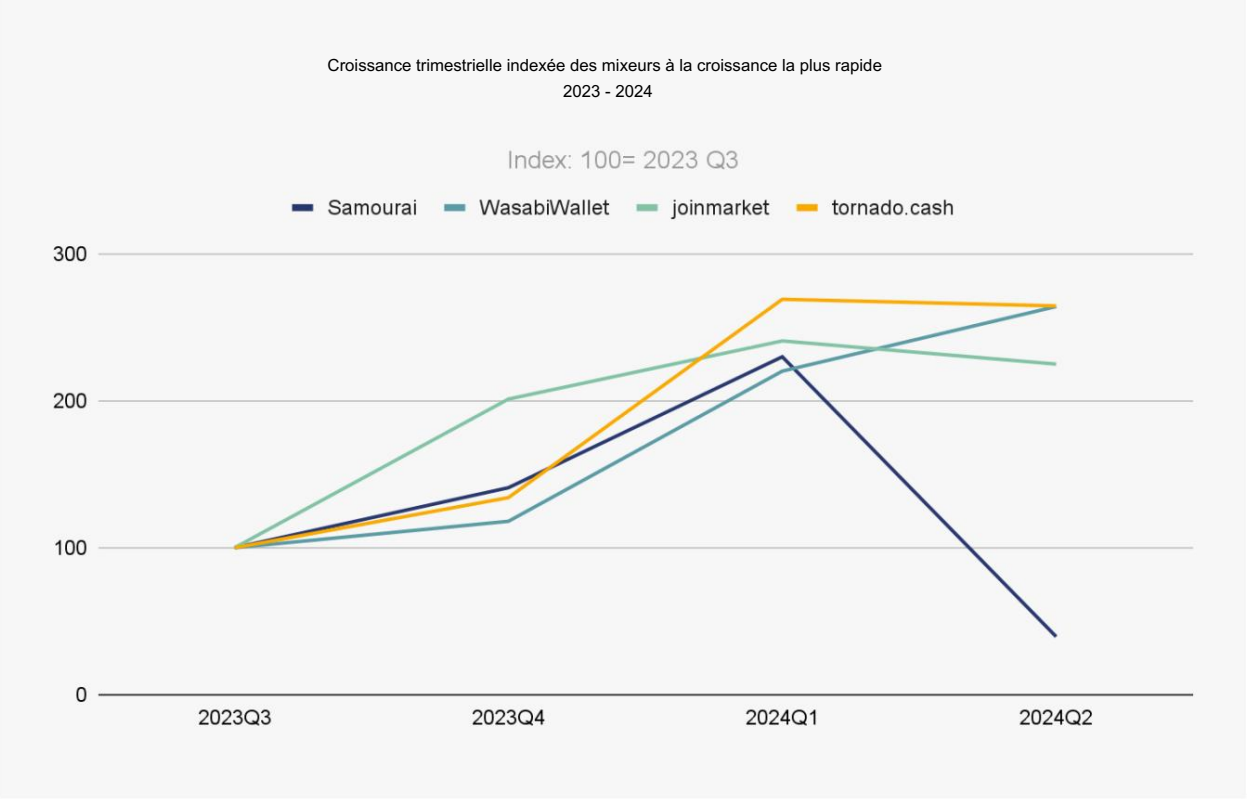
Les mixeurs de crypto-monnaies

Les mixeurs, également connus sous le nom de tumblers, sont des services qui mélangent les crypto-monnaies de nombreux utilisateurs afin de masquer les origines et les propriétaires des fonds. Bien que la fonction principale des mixeurs soit d'améliorer la confidentialité, il est important de reconnaître que toutes les transactions traitées via les mixeurs ne sont pas liées à des activités illicites. En 2022, les mixeurs ont atteint un pic de popularité, dépassant 1,5 milliard de dollars de valeur reçue en avril 2022.



Conformément à une hausse générale de l'activité du marché, les mélangeurs ont commencé à connaître une résurgence en 2024.

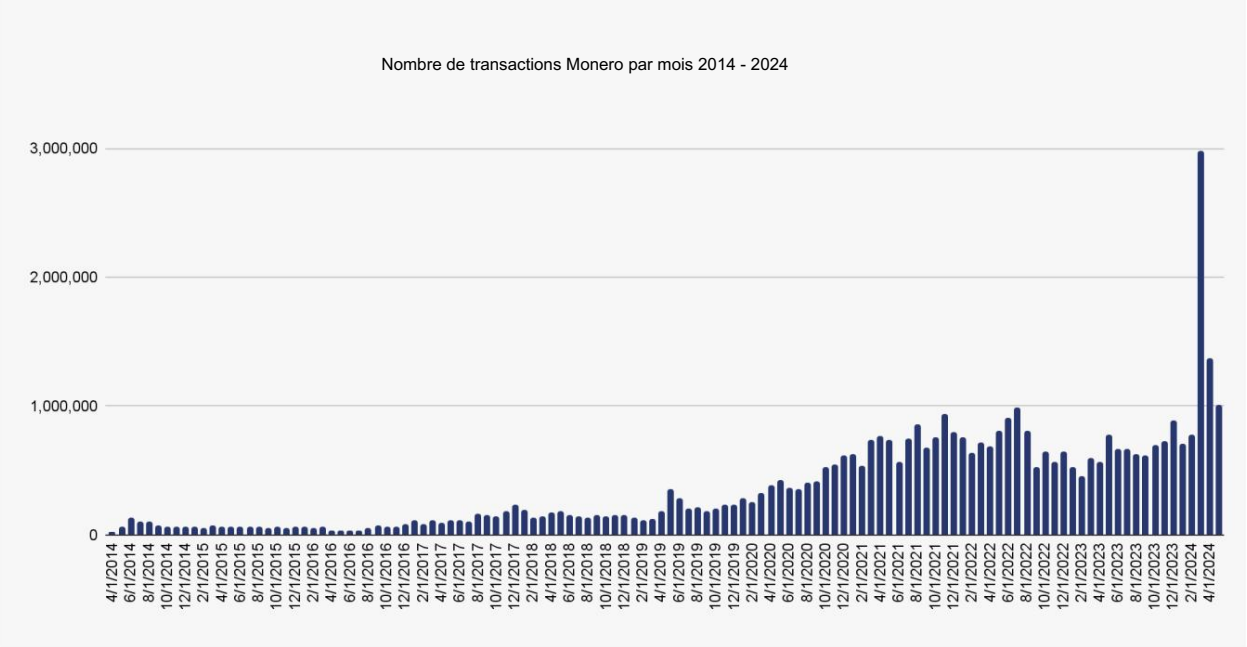
En examinant la croissance globale des services de mixage individuels, nous constatons que WasabiWallet, JoinMarket et Tornado Cash sont ceux qui ont connu la plus forte croissance.



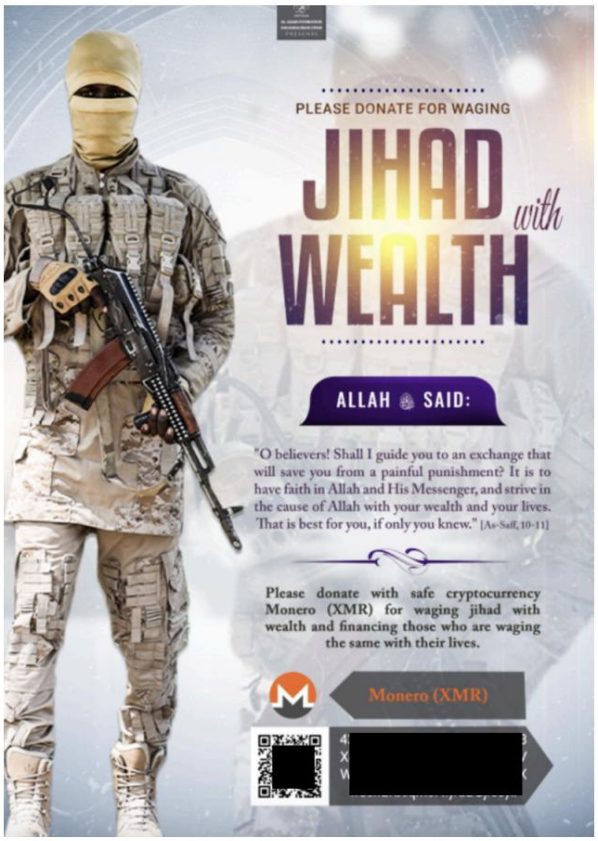
Il convient de noter que Tornado Cash en particulier affiche une croissance élevée et soutenue au cours de l'année écoulée, après une baisse spectaculaire de son utilisation après son approbation en 2022. Il s'agit d'une tendance que nous avons constatée pour la première fois dans notre rapport 2024 sur la crypto-criminalité, où nous avons détaillé comment le début de 2023 a marqué un point d'inflexion, lorsque l'afflux du mélangeur de contrats intelligents a commencé à augmenter à nouveau au fil du temps. À l'inverse, Samourai était en passe d'être l'un des meilleurs acteurs en termes de croissance cette année, mais cet élan a depuis chuté suite à l' action du ministère de la Justice d'avril 2024 contre les fondateurs et le PDG.

Pièces de
confidentialité Pièces de confidentialité, telles que Monero (XMR) et Zcash (ZEC), offrent des fonctionnalités d'anonymat améliorées, ce qui rend plus difficile le suivi des transactions sur ces chaînes. Monero utilise des techniques cryptographiques avancées telles que les signatures en anneau, les adresses furtives et les transactions confidentielles pour masquer l'expéditeur, le destinataire et le montant d'une transaction. Comme nous le voyons ci-dessous, les transactions Monero sont en hausse dans[3] l'ensemble

[3] Le pic anormal des transactions Monero de mars 2024 peut être attribué à un événement de spam appelé Black Marble.



Même si toutes les transactions Monero ne peuvent pas être attribuées à des activités illicites, ses fonctionnalités de confidentialité peuvent être particulièrement attrayantes pour les acteurs illicites. Par exemple, des organisations terroristes, comme la plateforme médiatique Al Azaim Media de l'État islamique au Khorasan, ont fait la publicité des adresses de don Monero.



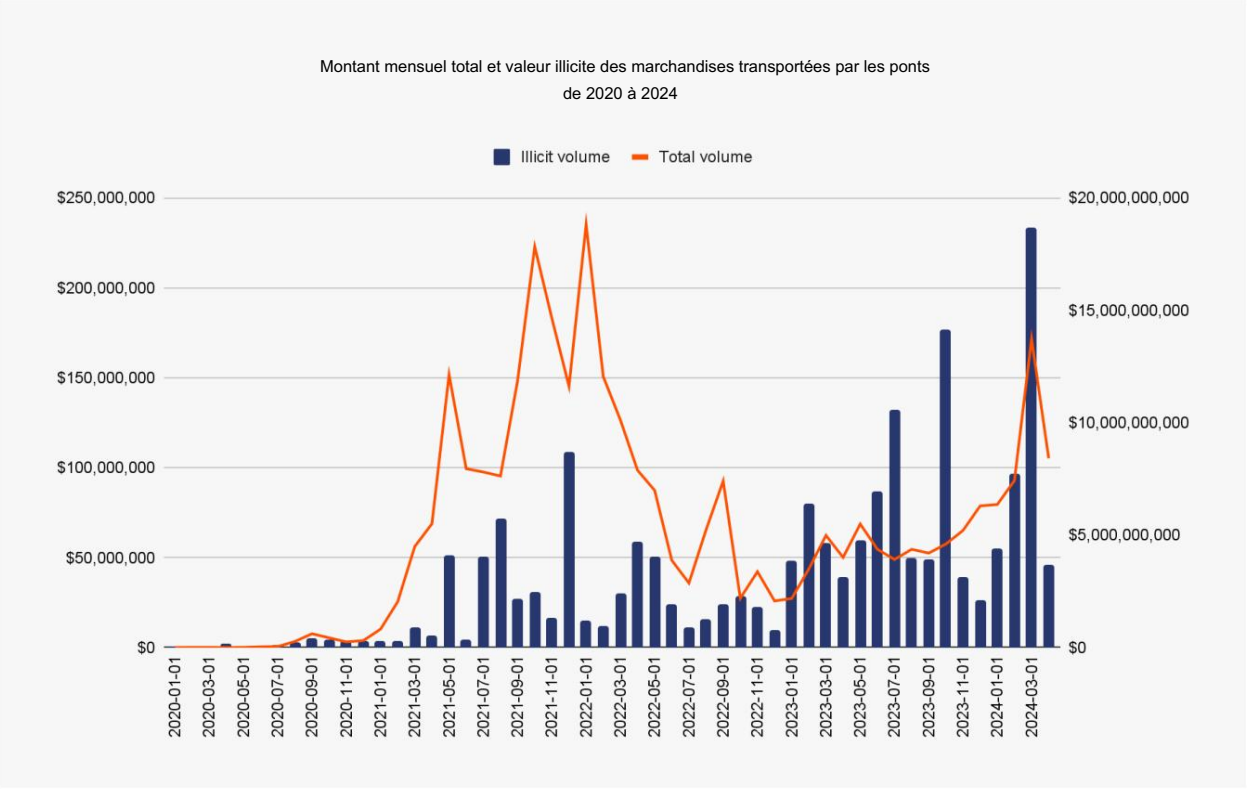
Étant donné que le niveau d'obscurcissement offert par les pièces de confidentialité cache les détails des transactions à la vue du public, les agences gouvernementales peuvent envisager d'investir dans des services d'analyse de blockchain spécialisés qui peuvent rendre possible le traçage de Monero et d'autres pièces de confidentialité.

Comme détaillé dans notre rapport 2024 sur la crypto-criminalité, le rôle de Monero dans les activités de blanchiment est particulièrement évident dans les échangeurs instantanés favorables à Monero, qui manquent souvent de mesures de conformité comme Know Your Customer (KYC). Ces échangeurs facilitent la conversion des crypto-monnaies en Monero, brisant ainsi efficacement la chaîne de traçabilité. Cependant, il est important de noter que certains régulateurs ont interdit les pièces de confidentialité et de nombreux échanges, plus récemment Binance, ont retiré Monero de la liste en raison de préoccupations concernant son potentiel illicite
utiliser.

Les ponts
cryptographiques , qui facilitent le transfert d'actifs entre différents réseaux blockchain, sont devenus des outils populaires qui améliorent l'interopérabilité entre les chaînes et les cas d'utilisation de certains actifs. À mesure que leur utilisation globale augmente, les acteurs malveillants tentent de plus en plus d'exploiter les ponts inter-chaînes pour masquer l'origine des fonds illicites en les déplaçant sur plusieurs blockchains.

Bien que les transactions de type « bridge » puissent être tracées par les enquêteurs dotés des outils adéquats, les blanchisseurs créent des réseaux complexes de transactions en divisant les fonds en montants plus petits et en les transférant sur différentes chaînes, ce qui rend le démêlage plus long pour les enquêteurs.

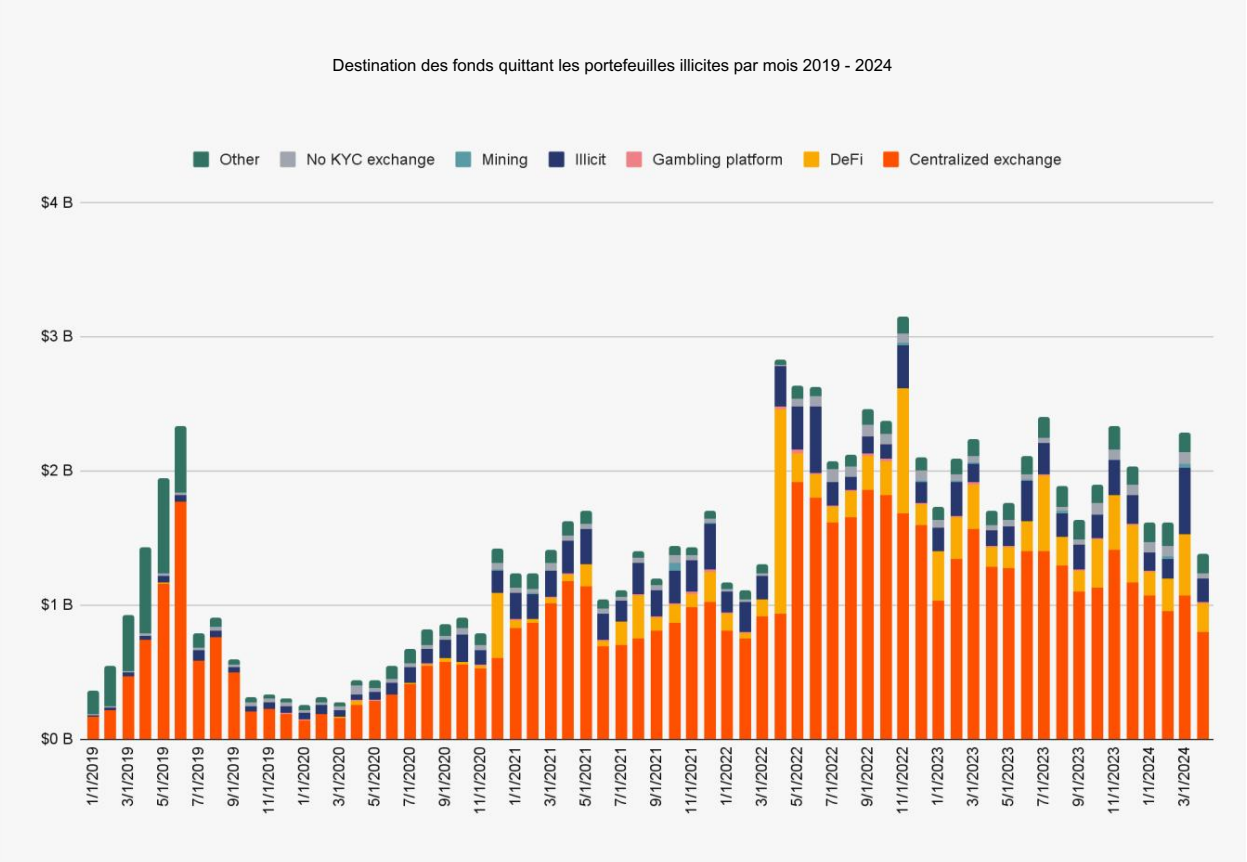
En examinant les flux illicites vers les ponts, nous pouvons constater que la valeur a augmenté régulièrement au fil du temps, poursuivant la tendance que nous avons observée dans notre rapport 2024 sur la crypto-criminalité.



On observe une augmentation prononcée de la valeur illicite à partir de fin 2023, avec près de 234 millions de dollars d'entrées illicites enregistrées en janvier 2024 - la valeur la plus élevée à ce jour, en grande partie due aux fonds circulant de Tornado Ca vers les ponts.

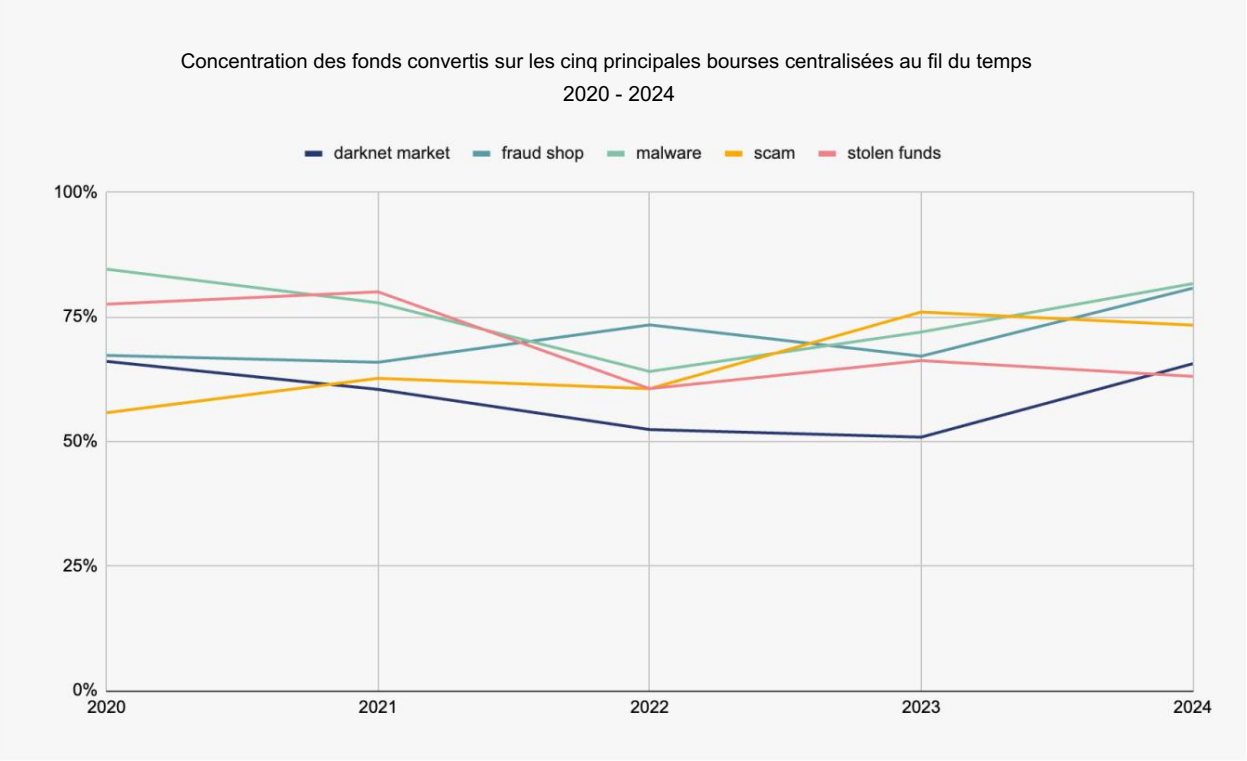
Destination des fonds illicites

Si certains cybercriminels peuvent conserver leurs gains mal acquis dans leurs portefeuilles personnels pendant des années – sans doute dans l'espoir que les autorités détourneront leur attention – la plupart des acteurs malveillants cherchent à transférer des fonds des crypto-monnaies vers des espèces. Plus de 50 % des fonds illicites finissent sur des plateformes d'échange centralisées, directement ou indirectement après l'utilisation de techniques d'obfuscation.



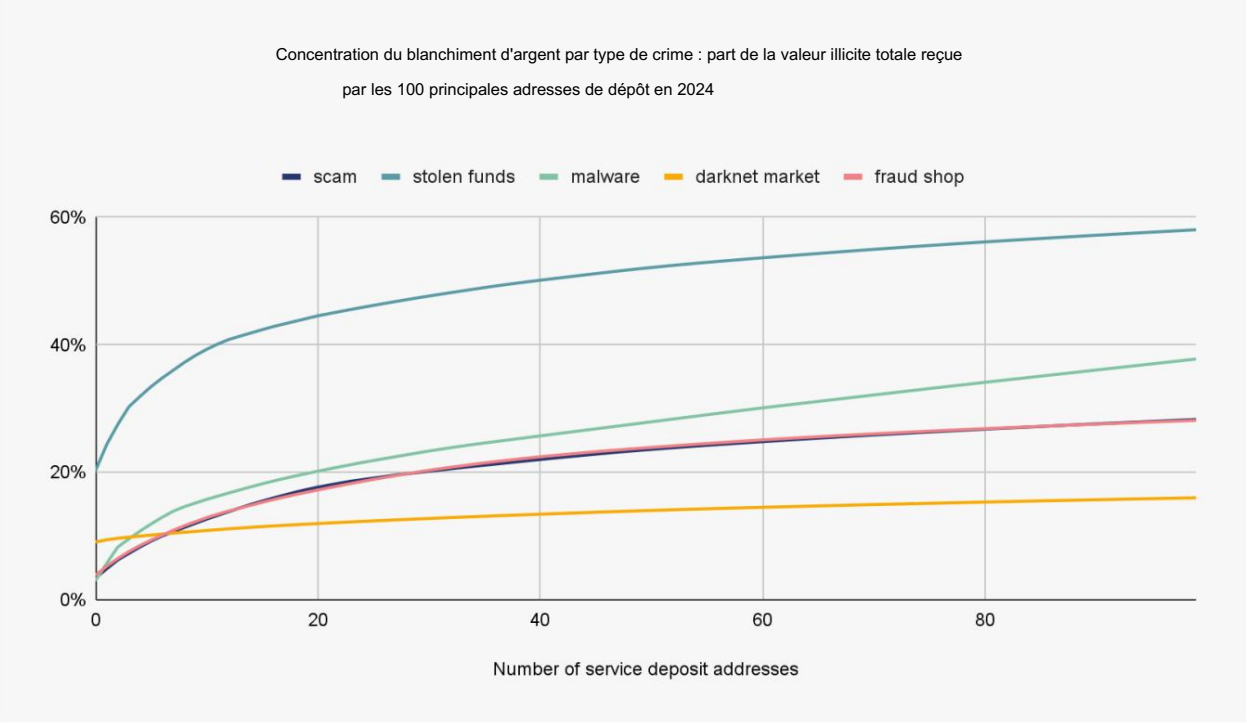
Les acteurs illicites peuvent se tourner vers les plateformes d'échange centralisées pour blanchir de l'argent en raison de leur grande liquidité, de la facilité de conversion des cryptomonnaies en monnaie fiduciaire et de leur intégration avec les services financiers traditionnels qui permettent de combiner les fonds illicites avec des activités légitimes. Il existe actuellement des centaines de services centralisés qui reçoivent chaque année plus d'un million de dollars de fonds illicites. Cependant, une tendance à la baisse notable du volume reçu par les plateformes d'échange centralisées – de près de 2 milliards de dollars par mois au plus fort à environ 780 millions de dollars par mois – suggère une efficacité accrue des programmes de lutte contre le blanchiment d'argent des plateformes d'échange centralisées pour détecter et atténuer les activités de blanchiment.

Concentration des points de retrait Malgré une dispersion entre de nombreux services, il existe une forte concentration de fonds illicites qui circulent uniquement vers les échanges centralisés. Jusqu'à présent en 2024, on a constaté une augmentation particulière de l'utilisation de quelques services de conversion de fonds provenant des marchés du darknet, des boutiques frauduleuses et des logiciels malveillants.



Chainalysis peut non seulement analyser les types de services qui reçoivent des fonds illicites, mais également les adresses de dépôt exactes qui reçoivent les fonds. Une adresse de dépôt est similaire à un compte bancaire dans la mesure où chacune d'entre elles tend à correspondre à un compte individuel du service.

Une tendance intéressante se dégage lorsque l'on examine la part des fonds allant aux cent premières adresses de dépôt recevant la plus grande valeur illicite en 2024. Les acteurs qui tentent de retirer des fonds volés ont tendance à utiliser moins d'adresses de dépôt que les autres types de crimes, en raison de quelques piratages aberrants de plus grande envergure. En revanche, les revenus des marchés du darknet affichent la plus faible concentration parmi les cent premières adresses de dépôt, ce qui témoigne du grand nombre de vendeurs qui les utilisent.



Cependant, dans toutes les catégories présentées ci-dessus, les cent premières adresses de dépôt reçoivent au moins 15 % de tous les fonds illicites de cette catégorie, ce qui indique que la communauté de la cybercriminalité est peut-être plus petite que beaucoup ne le pensent.

Courtiers de gré à gré

Les courtiers en cryptomonnaies de gré à gré (OTC) facilitent les transactions importantes entre deux parties, garantissant la confidentialité et souvent de meilleurs prix pour les transactions à volume élevé. Ces courtiers connectent les acheteurs et les vendeurs directement via un réseau de courtiers-négociants ou des bureaux de négociation OTC, contournant ainsi les carnets d'ordres publics.

Si la plupart des OTC sont des services légitimes, certains ont émergé qui ne nécessitent pas de procédures KYC appropriées pour les clients et s'adressent souvent spécifiquement à la diffusion de fonds illicites. Ces OTC peuvent être présents partout dans le monde et peuvent être difficiles à identifier, nécessitant souvent une combinaison de renseignements hors chaîne et sur chaîne.

La société de cybersécurité Cloudburst analyse les chaînes Telegram et recherche des publicités provenant de ces OTC Ils ont récemment identifié de nombreux OTC opérant en Chine et proposant des services de conversion en monnaie fiduciaire directement via les canaux Telegram.

Vous trouverez ci-dessous un exemple de publicité pour un de ces courtiers OTC qui fait la promotion d'un « échange en libre-service 24 heures sur 24 via Telegram ». Leur site Web, qui fait de la publicité en mandarin, se vante : « Nous avons vendu une grande quantité d'USDT volés à l'étranger. » Selon Cloudburst, ce service affirme avoir expédié plus de trois millions d'USDT par jour en 2024. Une fois la connexion établie sur Telegram, les clients reçoivent une adresse de dépôt numérique pour faciliter les transactions.

Certains de ces OTC ont une empreinte illicite sur la chaîne qui peut aider à profiler le service en plus de la publicité sur Telegram. Nous pouvons voir un autre OTC basé en Chine sortir directement des fonds illicites, comme le montre le graphique Reactor ci-dessous.

Bien que les médicaments en vente libre constituent en général une part importante du marché réglementé, certains éléments les rendent attrayants pour les criminels, en particulier lorsque les exigences réglementaires ne sont pas respectées.

Le lien entre les crypto-monnaies et le blanchiment d'argent non natif des crypto-monnaies

Le blanchiment d'argent non natif des crypto-monnaies fait référence au blanchiment de fonds provenant d'activités criminelles hors chaîne, plutôt que de fonds provenant directement de crimes spécifiques aux crypto-monnaies comme les piratages ou les escroqueries. Comme de plus en plus de transactions financières se font globalement sur la chaîne, les blanchisseurs d'argent traditionnels se tournent vers les crypto-monnaies pour faciliter leurs opérations. Le suivi du blanchiment d'argent non natif des crypto-monnaies peut être difficile à grande échelle en dehors du contexte d'enquêtes spécifiques, car les preuves concrètes reliant les fonds à des activités illicites sont souvent rares. Mais ci-dessous, nous exploitons les techniques de la science des données pour examiner certains indicateurs qui pourraient indiquer que cette activité se produit.

Typologies d'activités suspectes sur la chaîne et exemples d'heuristiques pouvant aider à les identifier

La relation entre les méthodes traditionnelles de blanchiment d'argent et la blockchain a élargi la boîte à outils à disposition des blanchisseurs d'argent – et de leurs traceurs. La surveillance des flux financiers pour détecter toute activité suspecte repose souvent sur des heuristiques et des seuils, comme dans le guide Red Flag du Groupe d'action financière (GAFI) pour décrire un comportement qui pourrait être suspect. En outre, des conseils du Financial Crimes Enforcement Network (FinCEN) suggère que le blanchiment d'argent potentiel et l'évasion des sanctions liés à la Russie peuvent être signalés par des augmentations inexpliquées des flux de valeur et d'autres modèles transactionnels inhabituels

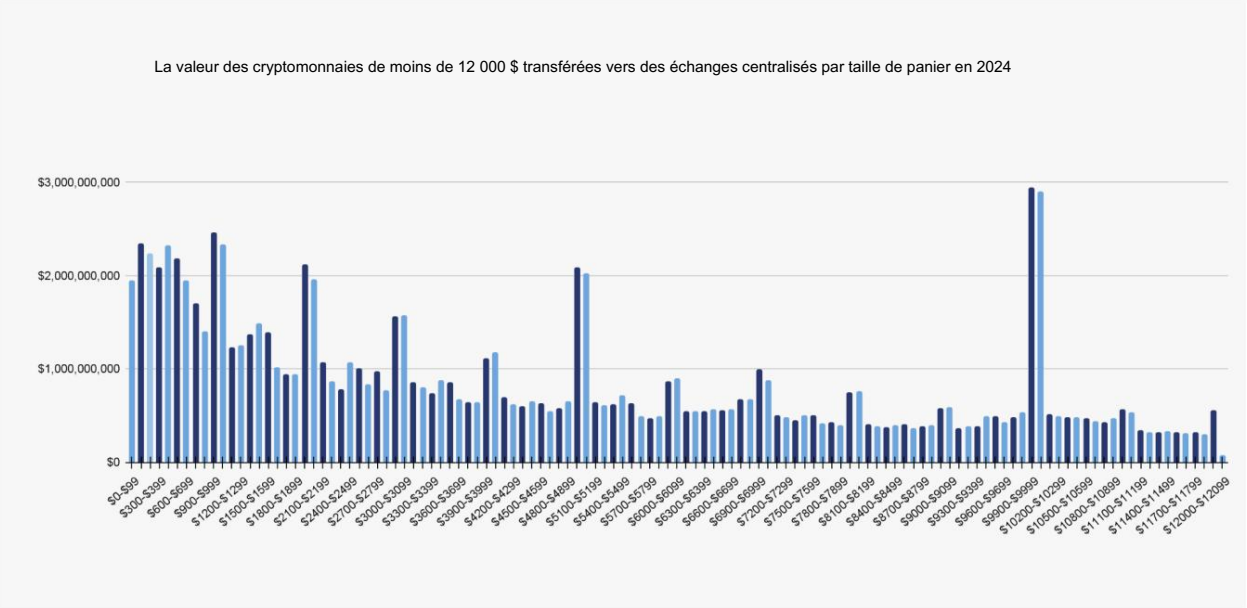
L'utilisation d'heuristiques basées sur les données de la blockchain peut améliorer les flux de travail existants des équipes de conformité et des enquêteurs pour aider à identifier les activités potentiellement suspectes sur la chaîne. Il est important de noter que dans tous ces cas, les modèles identifiés ne constituent pas, à eux seuls, une confirmation d'actes répréhensibles.

Transferts répétés juste en dessous des seuils de déclaration

Bien que le seuil varie selon les pays, le GAFI recommande que les transactions en cryptomonnaie dépassant 1 000 USD/EUR soient soumises à la Travel Rule, Les États-Unis ont fixé cette valeur à 3 000 USD. De plus, la loi américaine sur le secret bancaire (BSA) exige la déclaration des transactions en espèces supérieures à 10 000 USD.

Les transactions supérieures à ces valeurs déclenchent un examen plus approfondi, tandis que les transactions inférieures à ces seuils, même d'un seul dollar, ne font pas l'objet du même niveau d'inspection.

Le graphique ci-dessous présente la valeur des fonds transférés vers les bourses centralisées par taille de transfert pour l'année 2024 à ce jour. Il révèle une augmentation notable des transferts juste en dessous des seuils de 1 000 $, 3 000 $ et 10 000 $, ainsi que juste au-dessus. Les transferts légèrement supérieurs à ces seuils pourraient potentiellement être attribués aux différences d'arrondi des taux de change. Ces augmentations sont des schémas typiques qui sont identifiés lorsque des acteurs malveillants structurent des paiements pour éviter de déclencher des exigences de déclaration. Les transactions juste en dessous des exigences de déclaration sont l'un des indicateurs d'alerte que le GAFI a mis en évidence dans les directives des fournisseurs de services d'actifs virtuels (VASP) pour aider à identifier les comportements suspects.

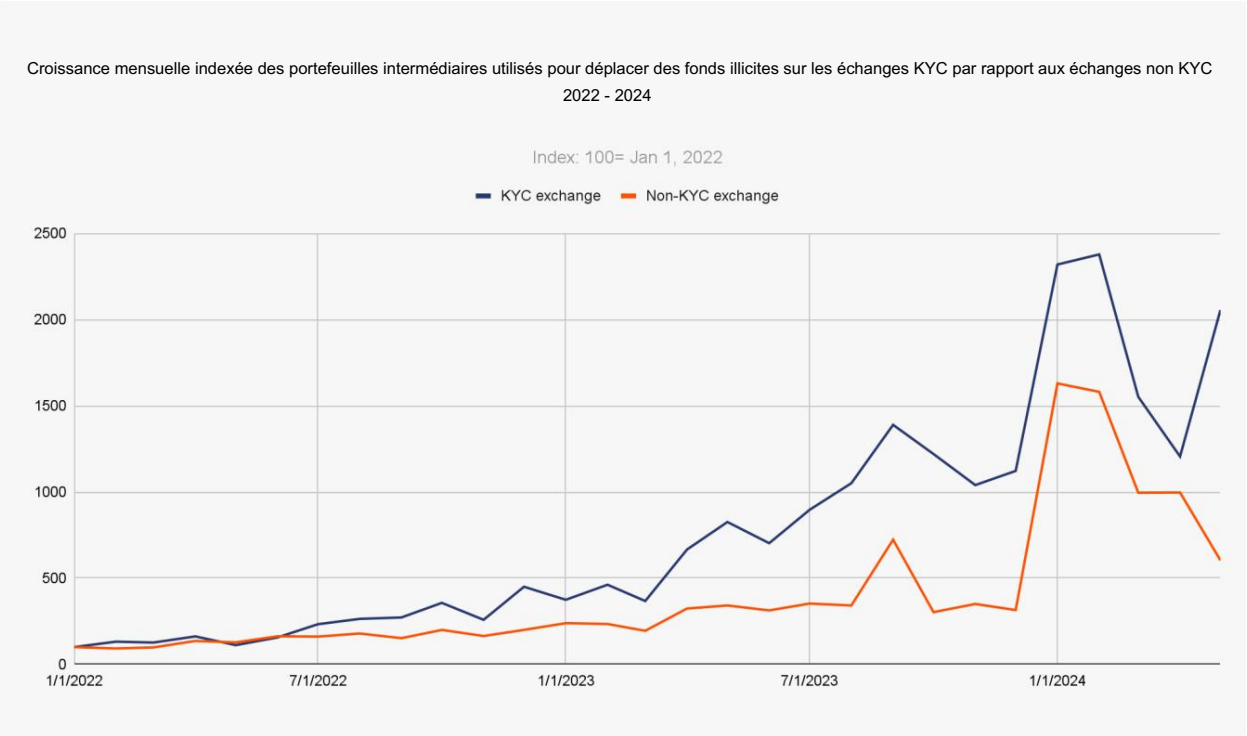


Cela suggère que les exigences de déclaration sont susceptibles d'accroître l'activité à la marge, juste en dessous et légèrement au-dessus des seuils de déclaration, dans le but d'éviter de déclencher un examen supplémentaire.

Utilisation de plusieurs portefeuilles intermédiaires avant les retraits

Comme indiqué ci-dessus, une méthode populaire de blanchiment d'argent crypto-natif consiste à envoyer des fonds via de nombreux portefeuilles personnels intermédiaires. Bien sûr, l'utilisation de portefeuilles personnels n'est pas intrinsèquement suspecte, mais nous pouvons utiliser les données pour répondre à des questions sur des comportements potentiellement suspects.

Par exemple : les utilisateurs envoient-ils des fonds via davantage de portefeuilles intermédiaires avant de convertir des fonds sur des plateformes d'échange qui ont une vérification KYC par rapport à celles qui n'en ont pas ?



C'est le cas. Le graphique ci-dessus montre que le nombre de portefeuilles intermédiaires utilisés par les acteurs malveillants augmente plus rapidement sur les échanges KYC que sur les échanges non KYC. Cela peut suggérer que la connaissance des obligations AML/KYC pourrait inciter à cette utilisation accrue de portefeuilles intermédiaires pour tenter d'éviter la détection d'activités illicites. Bien qu'il existe de nombreuses raisons légitimes pour lesquelles des fonds transitent par plusieurs portefeuilles, les échanges peuvent considérer le nombre de portefeuilles intermédiaires comme un indicateur potentiel de signal d'alarme dans le cadre de leur évaluation globale des risques d'un utilisateur.

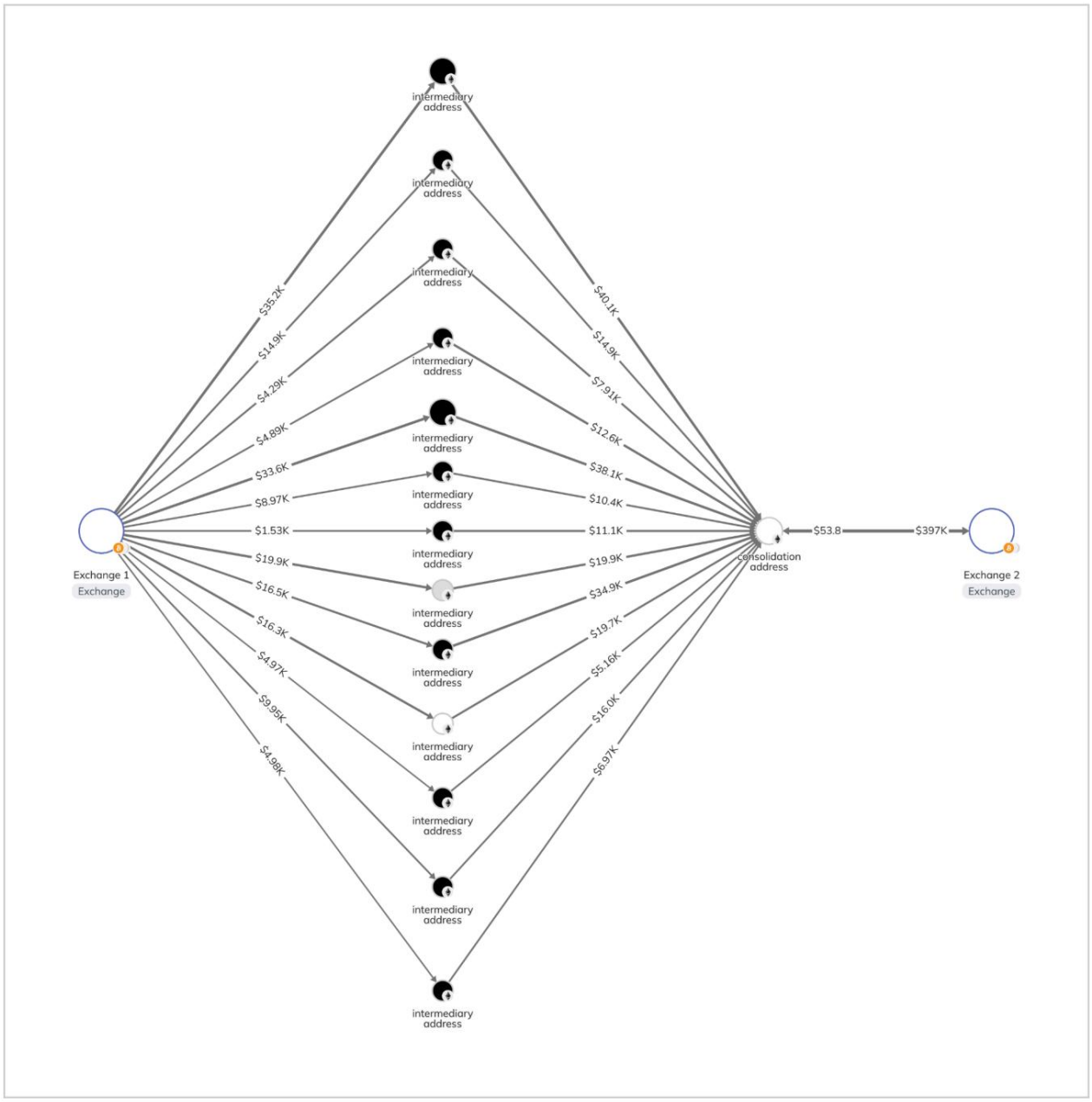
Utilisation des portefeuilles de consolidation

Les plateformes d'échange pourraient également bénéficier de la surveillance des portefeuilles de consolidation qui interagissent avec leur service. Lorsque les blanchisseurs superposent des fonds à de nombreux portefeuilles intermédiaires, les flux de transactions ne sont souvent pas simples et linéaires. Au contraire, le blanchisseur peut répartir les fonds dans plusieurs portefeuilles, puis reconsolider les fonds plus tard, après plusieurs transactions.

Un portefeuille de consolidation reçoit et combine des fonds provenant de plusieurs portefeuilles ou sources. Si les fonds transitent par plusieurs portefeuilles intermédiaires distincts, puis se consolident à une seule adresse, cela peut suggérer une tentative d'éviter la détection.

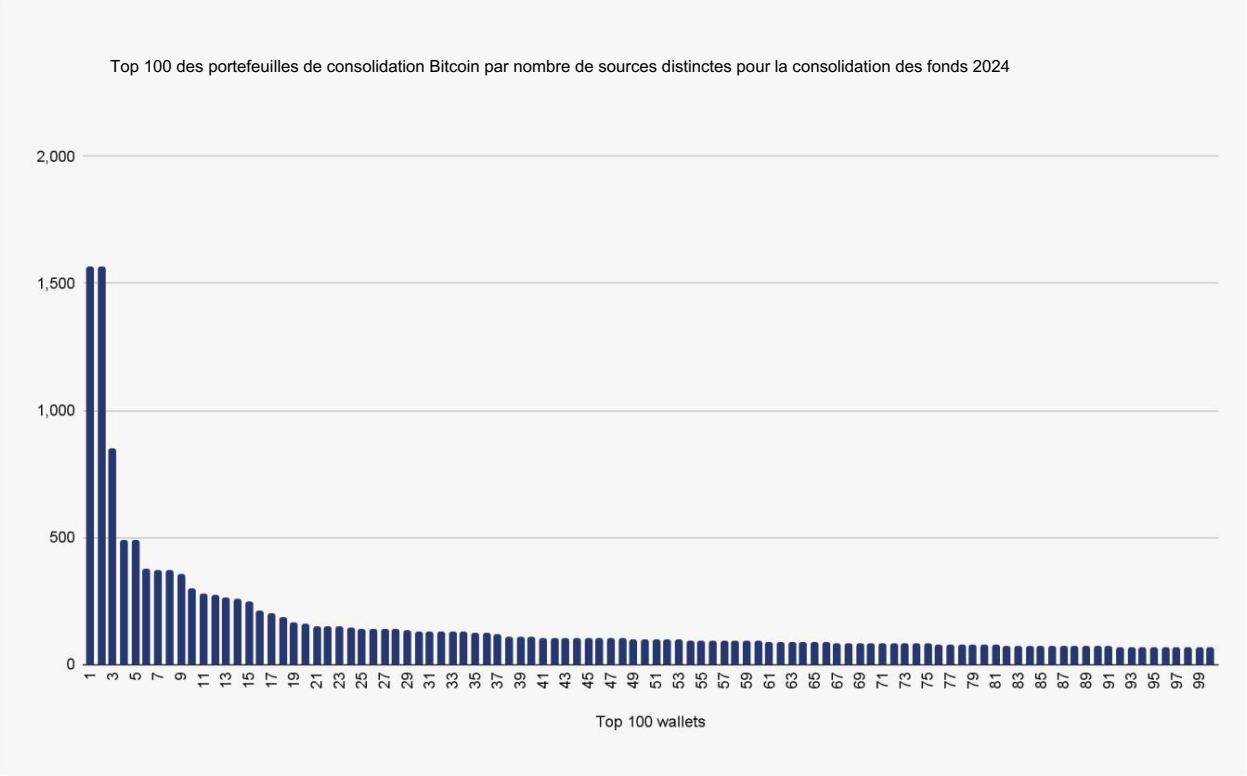
Les enquêtes de Chainalysis sur les crypto-monnaies Le graphique ci-dessous illustre ce type de comportement dans un groupe d'escroqueries connu ciblant les personnes âgées. Dans ce scénario, l'escroc a probablement demandé à ses victimes d'utiliser un service spécifique, Exchange 1, pour acheter des actifs cryptographiques. Chaque victime a ensuite été invitée à envoyer des fonds à un autre

portefeuille contrôlé par l'escroc. L'escroc a ensuite regroupé ces fonds dans un seul portefeuille avant de les encaisser sur Exchange 2.



Les équipes de conformité d'Exchange 1 auraient du mal à relier directement les victimes à l'arnaque, en particulier si les adresses intermédiaires sont à usage unique et n'ont aucun lien préalable avec une activité illicite, à moins qu'elles n'aient retracé les transactions jusqu'au portefeuille de consolidation. Le recours à de nombreux intermédiaires avant la consolidation est une stratégie visant à empêcher l'équipe de conformité d'Exchange 1 de comprendre le lien entre toutes les victimes qui envoyaient des fonds.

Bien que l'exemple ci-dessus soit relativement simple, les réseaux de blanchiment d'argent plus complexes comportent des portefeuilles de consolidation qui regroupent des fonds provenant de dizaines, voire de centaines de portefeuilles intermédiaires. L'interrogation des données de Chainalysis peut orienter les enquêteurs vers les principaux portefeuilles de consolidation, qui peuvent servir de pistes utiles. Par exemple, jusqu'à présent cette année, les cent principaux portefeuilles de consolidation de bitcoins en 2024 – qui ont tous effectué des transactions à deux sauts d'une bourse – ont reçu pour 968 millions de dollars de bitcoins provenant de plus de 14 970 adresses distinctes.



En élargissant encore l'ouverture, nous pouvons identifier plus de 1 500 portefeuilles de consolidation qui ont reçu un total de 2,6 milliards de dollars de bitcoins en 2024 ; chacun d'entre eux a reçu des fonds d'au moins dix portefeuilles différents. Encore une fois, nous ne pouvons pas affirmer avec certitude qu'il s'agit d'une activité de blanchiment d'argent – en fait, une grande partie de cette activité représente probablement des flux économiques légitimes. Mais cette activité peut justifier un examen plus approfondi

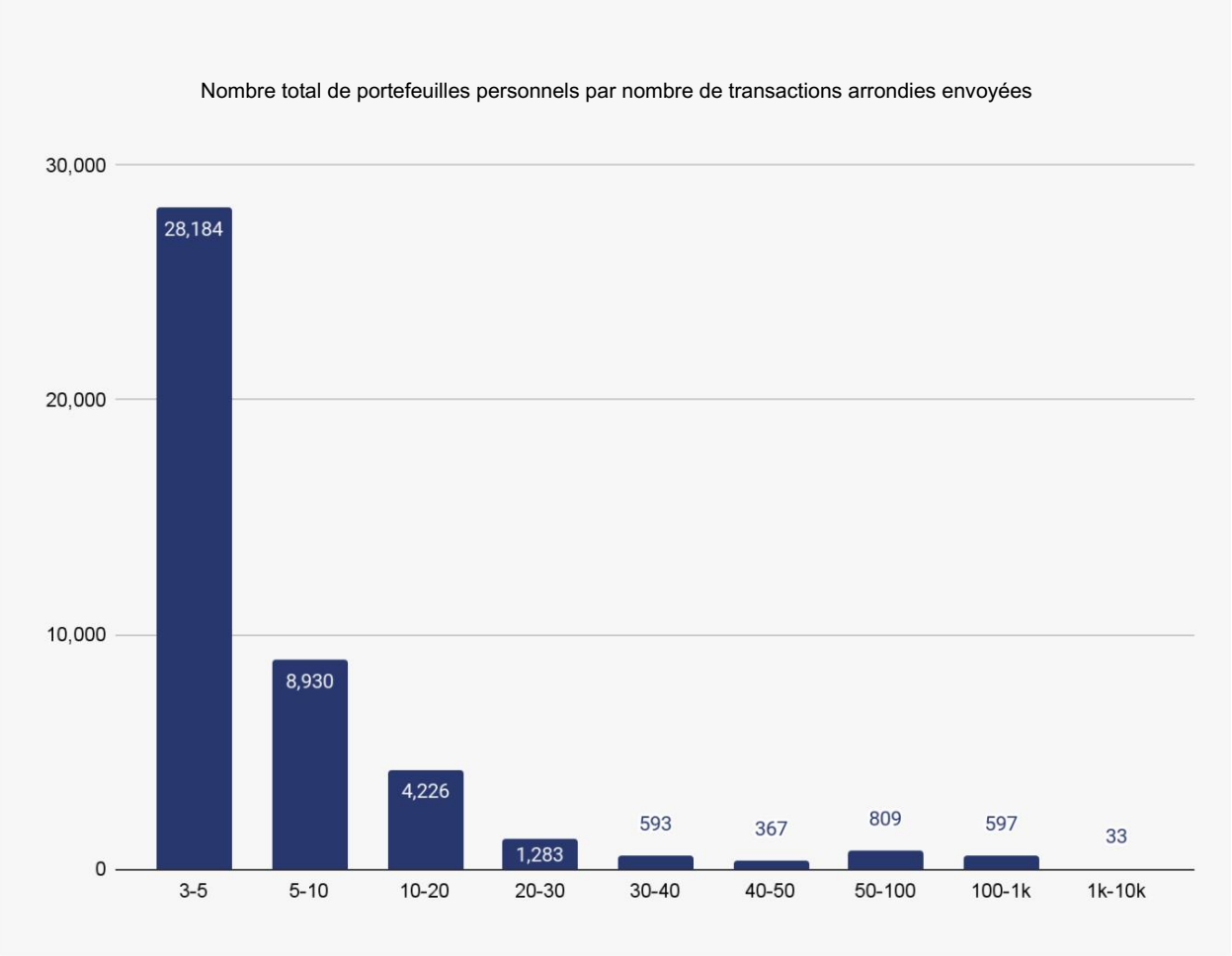
Paiements effectués en montants arrondis

Il existe de nombreuses raisons légitimes pour lesquelles les utilisateurs de cryptomonnaies transfèrent fréquemment des montants arrondis vers des services de conversion. Par exemple, les gens s'efforcent souvent de devenir un « coiner complet » ou d'atteindre un nombre arrondi dans un actif donné pour des raisons psychologiques.

Il est néanmoins important de prendre en compte la façon dont les montants de paiement arrondis sont souvent retrouvés dans les schémas de blanchiment d'argent des acteurs illicites connus. Par exemple, dans les activités de blanchiment d'acteurs liés à la République populaire démocratique de Corée (RPDC), les blanchisseurs sont connus pour diviser une grande quantité de fonds en montants plus petits et arrondis et les envoyer à des fréquences élevées à des services de conversion. Nous voyons ci-dessous que

des acteurs soupçonnés d'être affiliés à la RPDC ont envoyé quatre transactions totalisant 308 BTC en montants arrondis à une adresse de dépôt sur un échange centralisé sur quatre jours, vraisemblablement pour accéder à la FIA

Les données de Chainalysis montrent que la plupart des portefeuilles personnels effectuent des transferts de montants arrondis de seulement trois à cinq fois. Notamment, seuls trente-trois portefeuilles personnels ont envoyé plus d'un millier de montants arrondis à une adresse de dépôt. Ce comportement peut être révélateur d'un blanchiment d'argent méthodique et professionnel ou d'un service qui verse des montants arrondis, ce qui incite à une enquête plus approfondie.

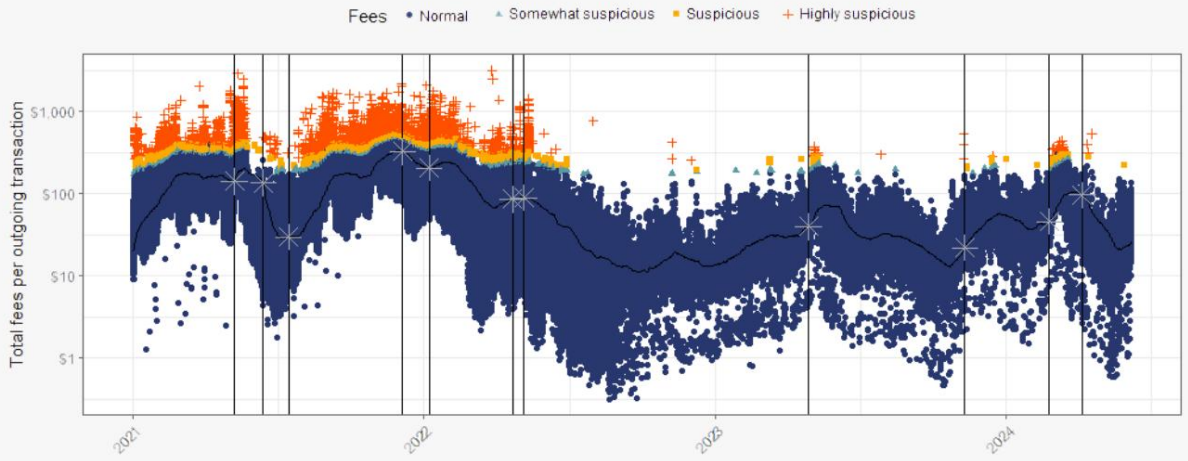


L'envoi de montants arrondis peut s'expliquer par le fait qu'il est plus facile de trouver des acheteurs sur les plateformes d'échange P2P, les courtiers de gré à gré (OT) ou d'autres services informels lorsqu'il s'agit d'unités entières. Pour les acteurs illicites qui cherchent à encaisser, le temps est souvent plus important que l'obtention du meilleur prix, ce qui fait de la rapidité une priorité plus élevée à ce stade du processus de blanchiment. Quelle que soit l'intention, les enquêteurs signalent souvent de nombreux montants arrondis au cours d'une enquête comme une tendance notable.

Frais suspects liés aux mixeurs Comme nous
l'avons vu plus haut, les services tels que les mixeurs sont conçus pour brouiller les pistes entre les points d'origine et de destination. Cependant, l'enregistrement détaillé des événements sur la chaîne peut toujours aider à identifier les activités suspectes.

Le graphique ci-dessous montre les frais de transaction du mixeur de contrats intelligents approuvé Tornado Cash. En examinant la moyenne mobile des frais sur 30 jours, nous pouvons identifier si une transaction paie des frais anormalement élevés. Par exemple, si les frais moyens au cours des 30 derniers jours sont de 1 $, des frais de 100 $ seraient anormalement élevés, tandis que des frais de 1,01 $ ne le seraient pas. Dans le même temps, payer 1,01 $ pourrait être anormal si les frais se situent autour de 10 cents.

Frais de sortie de Tornado Cash anormalement élevés associés aux entrées de fonds volés dans le mix



Cette méthode catégorise clairement les transactions qui privilégient la rapidité (via des frais plus élevés) par rapport à l'efficacité économique. Bien que les transactions avec des frais anormalement élevés ne soient pas nécessairement illicites ou révélatrices d'un blanchiment d'argent, il convient de noter que les augmentations de frais importantes coïncident souvent avec les entrées de fonds dans les portefeuilles Tornado Cash contenant des fonds volés (indiqués par les lignes noires dans le graphique, chacune représentant une date de piratage ou de vol important). L'analyse des frais peut suggérer des efforts pour éliminer rapidement les fonds, facilitant potentiellement le processus de blanchiment et le faisant passer de la phase de superposition à la phase d'intégration.

Appliquer les techniques traditionnelles de détection du blanchiment d'argent à la blockchain À bien des égards, l'identification de nouveaux modèles sur la chaîne qui pourraient indiquer un blanchiment est similaire à la détection de ces activités dans la monnaie fiduciaire, où l'accent est mis sur l'analyse des modèles de transaction et des activités anormales. Les blanchisseurs d'argent conventionnels se tournent vers la cryptographie, avec des méthodes qui ressemblent à leurs stratégies basées sur la monnaie fiduciaire. Bien qu'il puisse être difficile de faire la distinction entre le blanchiment d'argent et les transactions légitimes sur la chaîne, les informations fournies par des outils de renseignement sur la blockchain comme Chainalysis sont plus puissantes en raison de la nature transparente et immuable de la blockchain. La finance traditionnelle (TradFi) s'appuie fortement sur des procédures de conformité pour retracer les sources de fonds, tandis que la blockchain offre une visibilité claire.
Malgré cela, les acteurs malveillants appliquent des techniques de blanchiment traditionnelles aux écosystèmes blockchain afin de tenter d'échapper à la détection. À mesure que l' acceptation mondiale des crypto-monnaies À mesure que le blanchiment d'argent se développe et que les barrières à l'entrée diminuent, Chainalysis s'attend à ce que ce type de blanchiment d'argent devienne plus important, car les acteurs illicites s'approprient historiquement les nouvelles technologies à leurs propres fins.

Les autorités doivent utiliser ces heuristiques avec précaution, en s'assurant de disposer de preuves solides pour étayer leurs affirmations sans perturber indûment les opérations financières légitimes.

Lutte contre le blanchiment d'argent (LBC) : politiques et stratégies de prévention

Une prévention efficace du blanchiment d'argent, qu'il s'agisse de cryptomonnaies natives ou non, nécessite une approche multidimensionnelle. Cela comprend des mesures réglementaires, des innovations technologiques et une coopération mondiale. Les stratégies doivent être adaptées pour tenir compte des caractéristiques uniques des cryptomonnaies tout en renforçant les mesures traditionnelles de lutte contre le blanchiment d'argent (AML).

Aperçu de la réglementation existante

À mesure que les crypto-actifs deviennent monnaie courante, les pays du monde entier ont progressivement introduit des réglementations portant sur diverses propriétés des crypto-monnaies, notamment des mesures de lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CFT), le financement de la prolifération (CPF), les mesures de protection des consommateurs, les politiques de conduite du marché et les exigences prudentielles. À cette fin, le Groupe d'action financière intergouvernemental (GAFI) a publié des orientations établir un cadre global que les pays doivent mettre en œuvre pour lutter contre les activités de blanchiment d'argent.

Exigences en matière de lutte contre le blanchiment d'argent

(LBA) Les exigences en matière de LBA, notamment les règles de connaissance du client (KYC), sont des réglementations fondamentales qui obligent les institutions financières, y compris les VASP, à prendre un certain nombre de mesures pour prévenir le blanchiment d'argent. Cela comprend la vérification de l'identité de leurs clients et la surveillance de leurs transactions pour détecter toute activité suspecte.

Règle de voyage

La Travel Rule impose aux institutions financières, y compris les VASP, d'obtenir et, dans de nombreux cas, de partager des informations sur l'initiateur et le bénéficiaire des transactions au-delà d'un certain seuil, garantissant ainsi la transparence et la traçabilité.

Bien que les blockchains publiques offrent une visibilité inégalée sur les flux de transactions, leur nature pseudonyme nécessite une approche différente pour se conformer à la Travel Rule. À cette fin, les technologies réglementaires, telles que le partenariat de Chainalysis avec Notabene et VerifyVAS — permettent aux VASP d'améliorer leurs stratégies de conformité.

Émetteurs de stablecoins et capacités de gel

La plupart des stablecoins, comme l'USDT (Tether) et l'USDC (USD Coin), sont émis par des entités centralisées qui ont le pouvoir de contrôler et de gérer leurs contrats intelligents. Ainsi, ces émetteurs peuvent surveiller de manière proactive les transactions pour détecter toute activité suspecte et geler les fonds si nécessaire. Cette capacité permet aux émetteurs de répondre rapidement aux demandes des forces de l'ordre.

Par exemple, Tether (USDT) et Circle (USDC) ont tous deux indiqué précédemment avoir gelé des adresses associées à des activités illicites. Tether a déclaré à Chainalysis avoir gelé environ 1 600 adresses détenant des fonds d'une valeur d'environ 1 500 000 000 USDT.

Cadres réglementaires de premier plan

En 2019, le Groupe d'action financière intergouvernemental (GAFI) a publié des orientations détaillées sur l' application des normes de LBC/FT dans le secteur des actifs virtuels. Pour lutter contre les activités financières illicites, les régulateurs du monde entier s'efforcent d'intégrer les normes mondiales du GAFI dans leurs propres cadres réglementaires, dans le but de parvenir à une approche cohérente et unifiée de la réglementation de la lutte contre le blanchiment d'argent sur les actifs numériques à l'échelle mondiale.

Union européenne

En 2018, l'Union européenne (UE) a adopté la cinquième directive anti-blanchiment d'argent (5AMLD), pour lutter contre le blanchiment d'argent et le financement du terrorisme liés aux actifs numériques. Cette directive a nécessité une transposition nationale par les États membres de l'UE et est entrée en vigueur en janvier 2020, étendant les exigences de lutte contre le blanchiment d'argent aux PSAV. En outre, le règlement sur les transferts de fonds (TFR) existant — la mise en œuvre de la Travel Rule par l'UE — a été mise à jour pour inclure également les transactions d'actifs cryptographiques par les VASP, à compter de décembre 2024, parallèlement aux dispositions relatives aux fournisseurs de services d'actifs cryptographiques en vertu du règlement sur les marchés d'actifs cryptographiques (MiCA).

- La 5AMLD exige une plus grande transparence dans les transactions financières et les crypto-actifs et bénéficie
  - La TFR exige que les institutions financières, y compris les VASP, obtiennent et vérifient partiellement les informations sur les clients et les transactions à haut risque, notamment en identifiant et en vérifiant l'identité des clients impliqués dans des transactions complexes ou à grande échelle. Elle encourage également la coopération et le partage d'informations entre les États membres et les cellules de renseignement financier (CRF) afin de lutter efficacement contre le blanchiment d'argent et le financement du terrorisme à plus grande échelle.

    Les VASP destinataires doivent vérifier l'exactitude des informations reçues avant de mettre des cryptoactifs à la disposition des clients.

- En 2023, afin d'harmoniser davantage l'approche de la surveillance de la lutte contre le blanchiment de capitaux entre les États membres de l'UE, l'UE a également adopté un ensemble de trois nouveaux règlements de lutte contre le blanchiment de capitaux, collectivement connus sous le nom de « paquet AML ».
  - Règlement anti-blanchiment (AMLR) : en remplacement de certaines parties de la 5e directive anti-blanchiment, l'AMLR introduit le premier « recueil unique de règles anti-blanchiment » de l'UE pour les entités assujetties, applicable à partir de juillet 202. • Autorité de régulation de la lutte contre le blanchiment d'argent (AMLAR) : établit la première autorité de régulation de l'UE en matière de blanchiment d'argent.
    - Directive 6 sur la lutte contre le blanchiment d'argent (6AMLD) : abroge la 5AMLD qui ordonne aux États membres de l'UE de mettre en œuvre des changements dans leurs législations nationales dans un délai de trois ans, en se concentrant sur l'organisation de la surveillance nationale de la LBC/FT, comme les cellules de renseignement financier (CRF)

Singapour

Singapour est connue pour son cadre réglementaire solide. L'Autorité monétaire de Singapour (MAS) administre le régime réglementaire de lutte contre le blanchiment de capitaux et le financement du terrorisme pour les institutions financières, y compris les entreprises de crypto-monnaies.

- Entreprises de cryptographie opérant à Singapour (connues localement sous le nom de service de jetons de paiement numérique)

  Les prestataires de services de paiement (PSA) sont réglementés par la Loi sur les services de paiement (PSA), qui est entrée en vigueur pour la première fois

Janvier 2020. Les exigences en matière de LBC/FT pour les entreprises de cryptographie sont définies dans l'avis PSN02 de la MAS, et sont complétées par des conseils détaillés. •

La MAS continue d'améliorer son cadre réglementaire pour les entreprises de crypto-monnaie, plus récemment

• Singapour a récemment publié une évaluation nationale mise à jour des risques de blanchiment d'argent, car elle a élargi la portée de la réglementation en mettant en vigueur la loi de 2021 portant modification de la loi sur les services de paiement. Cette loi a élargi la gamme des entreprises de crypto-monnaie soumises à la réglementation AML/CFT et à d'autres réglementations pour couvrir les prestataires de services de garde, ainsi que les entreprises facilitant la transmission ou l'échange

de crypto-monnaie, même lorsque ces dernières n'entrent pas en possession des actifs des clients.

se prépare à sa prochaine évaluation mutuelle du GAFI.

Hong Kong

Les autorités de Hong Kong sont connues pour leur supervision rigoureuse dans différents domaines à risque, notamment la lutte contre le blanchiment d'argent et le financement du terrorisme. À Hong Kong, la Securities and Futures Commission (SFC) est le principal régulateur des plateformes de négociation d'actifs virtuels (VATP), tandis que l'Autorité monétaire de Hong Kong supervise les activités des banques et supervisera à terme les émetteurs de stablecoins.

• En décembre 2022, le Bureau de lutte contre le blanchiment d'argent et le financement du terrorisme de Hong Kong

L'ordonnance (AMLO) a été modifiée pour couvrir officiellement l'exploitation des entreprises d'actifs virtuels. Le nouveau régime réglementaire des VATP est entré en vigueur le 1er juin 2023.

• Des exigences strictes et détaillées en matière de LBC/FT pour les VATP sont définies dans un chapitre autonome • En outre, en février 2024, les autorités de Hong Kong ont publié des propositions pour la réglementation des fournisseurs de services de crypto-monnaie OTC. En vertu de ces propositions, les plateformes OTC devraient être agréées par le Département des douanes

et accises et devraient se conformer aux obligations de LBC/FT.

Le Royaume-Uni a pris des

mesures proactives pour perturber les opérations de blanchiment d'argent avec des mesures d'application nationales proactives et une forte emphase sur l'éducation des entreprises et du public sur les risques de LBC et les obligations de conformité.

• La Financial Conduct Authority (FCA) du Royaume-Uni est le superviseur AML/CFT des entreprises de crypto-monnaie (fournisseurs et dépositaires d'échange de crypto-monnaie) en vertu du règlement de 2017 sur le blanchiment d'argent, le financement du terrorisme et le transfert de fonds (informations sur le payeur). Cela signifie que depuis janvier 2020, les entreprises sont tenues de s'enregistrer pour obtenir une licence de crypto-monnaie et sont ensuite soumises à la supervision de la FCA et de se conformer aux mêmes exigences AML/CFT que les institutions financières.

• Les forces de l'ordre britanniques ont le pouvoir de saisir les actifs cryptographiques soupçonnés d'être

• Le Royaume-Uni a mis en place des unités spécialisées au sein du National Economic Crime Centre (NECC) et du Metropolitan Police Service (MPS) qui se concentrent sur les

enquêtes et les poursuites en matière de blanchiment d'argent et de crimes financiers. Ces unités exploitent la technologie et l'analyse de la blockchain pour suivre et traquer les fonds financiers illicites.

- La collaboration entre les secteurs public et privé est la pierre angulaire de la stratégie de LBC/FT du Royaume-Uni.
  Des initiatives telles que le Joint Money Laundering Intelligence Taskforce (JMLIT) facilitent le partage d'informations et la coopération entre le secteur privé et les organismes chargés de l'application de la loi. Alors que le JMLIT a été à l'origine de succès dans de nombreuses enquêtes, le Joint Money Laundering Steering Group (JMLSG), un autre partenariat public-privé, s'est avéré fondamental pour produire des orientations officiellement reconnues pour aider les entreprises, y compris les prestataires de services de lutte contre le blanchiment d'argent, à comprendre et à respecter les obligations en matière de LBC/FT.

Les Émirats arabes unis

Les Émirats arabes unis ont introduit des obligations de LBC/FT pour les fournisseurs de services d'actifs virtuels (VASP) par le biais d'amendements à leur principale législation LBC/FT, le décret-loi fédéral n° (20) de 2018. À la suite de ces modifications, diverses autorités de régulation, dont la Financial Services Regulatory Authority (FSRA) à ADGM, la Virtual Assets Regulatory Authority (VARA) à Dubaï, et la Dubai Financial Services Authority (DFSA) au sein du DIFC, ont prévu des exigences en matière de LBC/FT pour les VASP dans leurs juridictions respectives.

- En 2023, la Banque centrale des Émirats arabes unis (CBUAE) a publié des orientations pour les institutions financières agréées qui gèrent les risques de LBC/FT liés aux actifs virtuels et aux VASP. En 2024, la CBUAE a publié le Règlement sur les services de jetons de paiement. • Conformément à l'approche fondée sur les risques, les prestataires de services de paiement virtuels sont tenus de procéder à des évaluations des risques dans une perspective de blanchiment de capitaux
et de financement du terrorisme. Cela implique d'identifier les risques spécifiques auxquels le prestataire de services de paiement virtuel est exposé et de mettre en œuvre des contrôles appropriés pour atténuer ces risques.

- Les VASP sont également tenus de surveiller les transactions et de signaler les activités suspectes au Financial
  Unité de renseignement financier (FIU) utilisant la plateforme goAML.

États-Unis Bien que le

paysage réglementaire plus large spécifique aux cryptomonnaies aux États-Unis soit encore en évolution, il est clair depuis plus d'une décennie que les entreprises de cryptomonnaies sont soumises aux exigences de lutte contre le blanchiment d'argent et doivent surveiller leurs plateformes pour détecter toute activité illicite. En 2013, le Financial Crimes Enforcement Network (FinCEN) a expliqué que les échanges de cryptomonnaies constituent des entreprises de services monétaires (ESM) soumises à la réglementation en vertu du Bank Secrecy Act. En 2019, le FinCEN a fourni des orientations supplémentaires clarifiant quelles autres entreprises de cryptomonnaies répondaient à la définition d'ESM et abordant d'autres problèmes de conformité uniques liés aux cryptomonnaies.

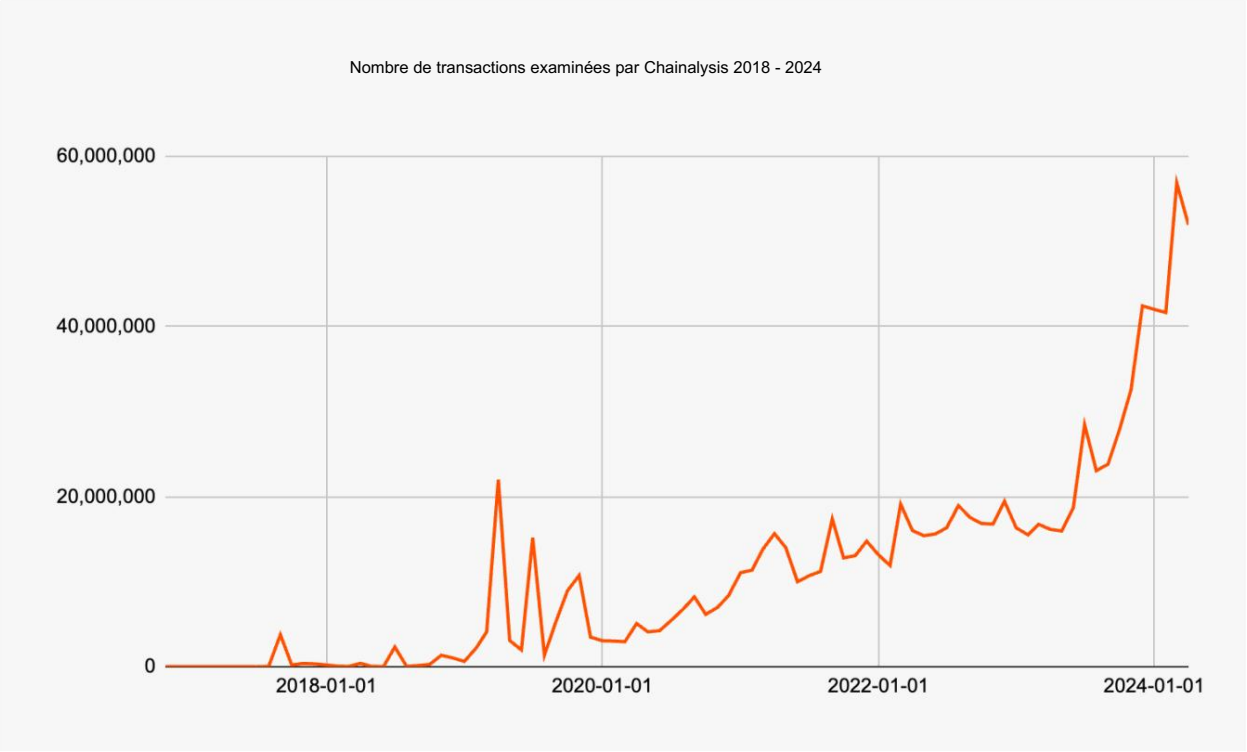
- Le Bank Secrecy Act (BSA) est le principal cadre juridique régissant la réglementation AML aux États-Unis
  La BSA exige que les institutions financières, y compris les entreprises de crypto-monnaie, aident les gouvernements à identifier et à arrêter les activités de blanchiment d'argent. • Le FinCEN est chargé de créer et
d'appliquer les réglementations AML, en fournissant des conseils pour
  Conformité et collecte de données sur les transactions financières au moyen de rapports tels que les rapports sur les transactions en devises (CTR) et les rapports sur les activités suspectes (SAR).
- La BSA exige que les institutions financières, y compris les MSB, mettent en œuvre un programme de lutte contre le blanchiment d'argent basé sur les risques et collectent et vérifient l'identité de leurs clients, connue sous le nom de Know Your Customer (KYC).

Stratégies pour les scénarios crypto-natifs et non-crypto-natifs

Le blanchiment d'argent touche tous les aspects des activités illicites, ce qui nécessite une approche globale et adaptative de la lutte contre le blanchiment d'argent (LBC) et de la gestion des risques. À mesure que la technologie blockchain évolue, les stratégies de LBC doivent également évoluer pour contrer les nouvelles tactiques et garantir que la réglementation suive le rythme des développements technologiques.

Protocoles KYC et AML renforcés Il est impératif
de garantir des mesures strictes de connaissance du client (KYC) et de lutte contre le blanchiment d'argent (AML) pour les échanges de crypto-monnaies et les institutions financières traditionnelles. Cela comprend la vérification des identités, la surveillance des transactions et le signalement des activités suspectes.

Systèmes de surveillance des transactions
Les institutions financières traditionnelles et les échanges de crypto-monnaies mettent de plus en plus en œuvre des systèmes avancés de surveillance des transactions qui utilisent l'apprentissage automatique et l'intelligence artificielle pour détecter des modèles inhabituels indiquant un blanchiment d'argent. Solutions de conformité cryptographique Chainalysis sont de plus en plus utilisés par les entreprises de cryptographie et les institutions financières pour signaler les activités suspectes en temps réel



Le nombre de transactions contrôlées par des produits de conformité tels que Chainalysis est en augmentation, ce qui indique un engagement croissant des entreprises à empêcher les fonds illicites de sortir de l'écosystème.

Collaboration transfrontalière et partenariats public-privé La coopération
internationale est essentielle dans la lutte contre le blanchiment d'argent. Les criminels exploitent souvent les conflits réglementaires entre les juridictions, ce qui rend les efforts internationaux coordonnés absolument essentiels. Cela comprend

Il s'agit d'harmoniser les réglementations, de partager les renseignements et de mener des opérations conjointes. Il convient d'encourager la collaboration entre les secteurs public et privé pour partager les informations et les meilleures pratiques en matière de lutte contre le blanchiment d'argent.

L'absence de mise en œuvre de programmes de conformité rigoureux peut avoir des conséquences irréparables, notamment des sanctions réglementaires, une perte de confiance des consommateurs et une exclusion complète du système financier. Les institutions financières traditionnelles et natives de la cryptographie doivent donner la priorité à des mesures anti-blanchiment solides pour éviter ces risques et garantir l'intégrité de leurs opérations.

Le rôle de la technologie et de l'innovation dans la prévention du blanchiment d'argent

L'avenir des enquêtes et de la conformité en matière de cryptomonnaies repose essentiellement sur l'intelligence de la blockchain et sur la capacité des données sous-jacentes à identifier les activités suspectes pour générer des prospects. L'analyse des données joue un rôle crucial dans l'identification et la neutralisation des menaces les plus pressantes dans l'écosystème cryptographique, un domaine dans lequel une seule adresse de portefeuille peut mettre en lumière de vastes réseaux d'abus criminels.

Il est essentiel de trouver un équilibre entre confidentialité et sécurité pour protéger les utilisateurs légitimes tout en empêchant les abus. La gestion des coûts de conformité est également essentielle pour éviter d'impacter de manière disproportionnée les petites entreprises et les startups, en favorisant l'innovation tout en préservant l'intégrité réglementaire. À mesure que l'écosystème évolue, la formation continue et le développement des compétences sont également impératifs pour garder une longueur d'avance sur les menaces émergentes. Une compréhension approfondie de la technologie blockchain et de ses intersections avec l'activité criminelle permet aux institutions de mettre en œuvre des contrôles précis adaptés à leur profil de risque spécifique.

La technologie permet aux institutions d'améliorer leur efficacité et leurs résultats tout en réduisant la dépendance à des exigences de reporting fastidieuses. Les systèmes automatisés peuvent analyser rapidement de grands volumes de données, identifier les risques et générer des informations exploitables, améliorant ainsi l'efficacité globale de la lutte contre le blanchiment d'argent.

L'interaction entre l'intelligence de la blockchain et les informations basées sur les données est la pierre angulaire de l'enquête et de la conformité en matière de cryptographie. En tirant parti des technologies avancées, en gérant la conformité et en investissant dans l'éducation, l'écosystème crypto peut parvenir à un cadre durable et sécurisé qui favorise l'innovation tout en protégeant contre les activités illicites.

Chainalysis

Bâtir la confiance dans les blockchains

À propos de Chainalysis

Chainalysis, leader de l'intelligence blockchain, facilite la connexion des mouvements d'actifs numériques aux services du monde réel. Les organisations peuvent suivre les activités illicites, gérer l'exposition aux risques et développer des solutions innovantes des solutions de marché avec des informations client intelligentes. Notre mission est de renforcer la confiance dans les blockchains, en combinant sécurité et la sûreté avec un engagement indéfectible envers la croissance et l'innovation. Pour plus d'informations, visitez www.chainalysis.com.

POUR PLUS D'INFORMATIONS
chainalysis.com/blog

SUIVEZ-NOUS SUR X
@chainalysis

ENTRER EN CONTACT
info@chainalysis.com

SUIVEZ-NOUS SUR LINKEDIN
linkedin.com/company/chainalysis