Crypto-actifs et finance decentralisée

Quel impact sur les enquêtes de blanchiment de capitaux et de financement du terrorisme menées par les cellules de renseignement financier

Cofinancé par l'Union européenne

UNION EUROPÉENNE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Cofinancé et mis en œuvre par le Conseil de l'Europe

Cette publication a été élaborée dans le cadre du projet intitulé « Développement de l'expertise de la cellule française de renseignement financier axée sur la finance numérique et les actifs virtuels », cofinancé par l'Union européenne via l'Instrument d'appui technique (IAT), et mis en œuvre par le Conseil de l'Europe, en coopération avec la Commission européenne. Son contenu relève de la seule responsabilité des auteurs. Les opinions qui y sont exprimées ne sauraient en aucun cas être considérées comme reflétant l'opinion officielle de l'Union européenne ou du Conseil de l'Europe.

Couverture et mise en page : Division publications et identité visuelle, Conseil de l'Europe.

Photos : Shutterstock et Conseil de l'Europe.

Éditions du Conseil de l'Europe
F-67075 Strasbourg Cedex
www.coe.int

Imprimé dans les ateliers du Conseil de l'Europe.

Pour plus d'informations sur le sujet de cette publication, veuillez contacter :
Division de la coopération contre la criminalité économique
Département de la criminalité économique et de la corruption
Direction générale des droits humains et de l'état de droit
Conseil de l'Europe
Courriel : contact.econcrime@coe.int

Auteurs :
Guillaume LAMBOY
Edouard KLEIN

www.coe.int/econcrime

Table des matières

Avant-propos

On considère généralement la publication en novembre 2008 de « Bitcoin : A Peer-to-Peer Electronic Cash System » par l'énigmatique Satoshi Nakamoto comme le point de départ du phénomène des crypto-actifs. Ce dernier terme n'est pas neutre, car c'est bien cet usage du bitcoin, et tous ses successeurs, comme actifs financiers qui prime désormais largement auprès de nos concitoyens.

Pourtant, si l'on en revient à ce fameux « livre blanc », le bitcoin se voulait initialement une alternative aux systèmes financiers centralisés sur lesquels reposent traditionnellement une large partie de notre action de cellule de renseignement financier (CRF). Objectif que ses caractéristiques technologiques lui permettent potentiellement. Au-delà de ses perspectives, nous sommes donc face à un phénomène qui en se démocratisant aussi massivement offre à tout et à chacun un outil conçu défiant notre action, à nous comme aux superviseurs ou aux services répressifs. Nous sommes en conséquent face à un risque nouveau en matière de blanchiment des capitaux et de financement du terrorisme (BC/FT).

Savez-vous combien de fois le livre blanc mentionne les mot « pays » et « frontière » ? Aucune. Le sujet est par essence transnational, et c'est pourquoi Tracfin a sollicité l'appui du de la Commission européenne et du Conseil de l'Europe et via l'instrument d'appui technique.

Collectivement, nous avons ainsi pu mettre en place un ambitieux plan de formation : l'ensemble de nos 200 agents a été sensibilisé à la thématique, 130 ont été formés à un niveau intermédiaire axés sur les vulnérabilités BC/FT et 30 à un niveau avancé qui leur a permis d'utiliser concrètement les crypto-actifs comme moyen d'opacification mais aussi les outils à notre dispositif pour contrer ce mésusage. Car, encore une fois si la technologie intrinsèque des crypto-actifs présente des risques, elle offre dans le même temps des opportunités singulières en matière d'action des CRF.

Nous avons tiré de nombreuses leçons de cette tension entre risques et opportunités. La brochure que vous tenez dans les mains synthétisent une partie de ces enseignements, que nous sommes aujourd'hui fiers de partager avec vous. Car s'il ne faut retenir qu'un de ces enseignements, c'est que le partage nous rend collectivement plus forts, pour les crypto-actifs comme pour le reste.

Antoine MAGNANT

Directeur, Tracfin

Dans un contexte de transformation rapide de l'écosystème des crypto-actifs – qui redessine les dynamiques financières mondiales et crée de nouveaux défis pour l'État de droit –, il est essentiel de développer une compréhension solide des technologies émergentes, de leurs usages légitimes comme de leurs potentielles dérives, ainsi que des réponses stratégiques et opérationnelles les plus adaptées. Ces évolutions appellent des réponses éclairées, coordonnées et prospectives de la part des décideurs publics, des cellules de renseignement financier, des autorités répressives et des instances de régulation.

La présente brochure vise à offrir une synthèse claire et accessible des concepts fondamentaux qui sous-tendent la finance décentralisée et les crypto-actifs. Elle examine les caractéristiques propres à ces technologies, tout en abordant les risques de blanchiment de capitaux et de financement du terrorisme, les défis réglementaires, les typologies criminelles émergentes, ainsi que les outils d'analyse et d'enquête à la disposition des cellules de renseignement financier.

Ce travail s'inscrit dans la continuité de l'action de longue date du Conseil de l'Europe en faveur du renforcement de l'État de droit et de la lutte contre les menaces connexes, par le biais du développement institutionnel et de la coopération internationale dans la lutte contre la criminalité économique. Le Conseil de l'Europe est depuis longtemps à l'avant-garde dans ce domaine, notamment en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Il continue à soutenir ses États membres dans la mise en place ou le renforcement de leurs capacités institutionnelles pour faire face aux menaces émergentes.

En accompagnant les autorités nationales, cette publication contribue à l'élaboration de réponses efficaces, coordonnées et durables face aux risques financiers liés aux nouvelles technologies, en mettant particulièrement l'accent sur les besoins et les capacités des cellules de renseignement financier.

Cette publication est une initiative du Conseil de l'Europe, réalisée dans le cadre du projet « Développement de l'expertise de la cellule française de renseignement financier axée sur la finance numérique et les actifs virtuels » cofinancé par l'Union européenne via l'Instrument d'appui technique, et mis en œuvre par le Conseil de l'Europe en coopération avec la Commission européenne.

Nous adressons nos sincères remerciements à nos partenaires institutionnels pour leur confiance et leur collaboration, ainsi qu'aux auteurs pour leur expertise. C'est par une meilleure compréhension et une coopération renforcée que nous pourrons consolider la résilience des systèmes financiers des États et défendre l'État de droit dans une ère numérique en constante évolution.

Gianluca ESPOSITO

Directeur général des droits humains et de l'État de droit, Conseil de l'Europe

La période récente marquée par l'essor des crypto-actifs et de la finance décentralisée, entraine une multitude de défis pour la lutte contre le blanchiment d'argent et le financement du terrorisme. C'est dans ce contexte que Tracfin a sollicité la Commission Européenne pour un projet dans le cadre de l'Instrument d'appui technique, ici mis en œuvre en partenariat avec le Conseil de l'Europe, avec un double enjeu : premièrement, développer un programme de formation pionnier adapté aux agents de Tracfin et à leurs besoins spécifiques, visant à renforcer leurs compétences face aux risques de blanchiment d'argent et de financement du terrorisme qui découlent de l'utilisation croissante des crypto actifs et de la finance décentralisée; deuxièmement, et de façon tout aussi importante, partager les enseignements de ce projet avec l'ensemble des Cellules de renseignements financiers européennes et partenaires. C'est dans cet esprit de coopération que s'inscrit la présente brochure, élaborée dans le cadre de cette initiative, avec pour objectif de maximiser sa portée et son impact.

La Commission européenne est fière de soutenir Tracfin dans cette démarche de montée en compétence partagée qui s'inscrit dans la lignée d'autres projets soutenus par l'Instrument d'appui technique – et notamment dans la lignée du projet phare EU SDFA soutenant l'ensemble des superviseurs de la finance digitale dans les 27 États Membres, avec toujours un même objectif conjoint : soutenir et entretenir une communauté d'autorités compétentes dans un contexte d'innovations technologiques, faciliter l'adoption des technologies avancées et la mise en œuvre effective du cadre réglementaire de l'Union européenne en matière de finance numérique, en permettant aussi un échange de pratiques entre les différentes autorités sectorielles et au-delà des frontières.

Judit ROZSA

Directrice pour l'Instrument d'appui technique, SG REFORM, Commission européenne

Les crypto-actifs, le blanchiment de capitaux et le financement de terrorisme

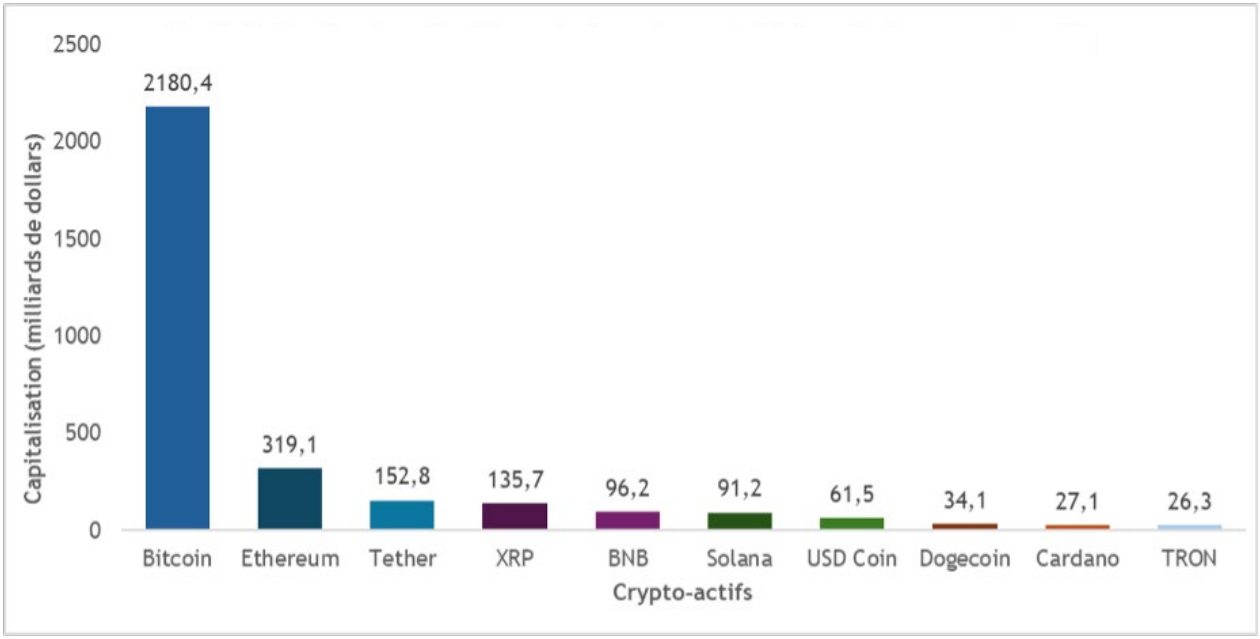
La chaîne de blocs (*blockchain*) est née il y a un peu plus de quinze ans. Depuis, les crypto-actifs se sont progressivement et largement répandus et ont commencé à être utilisés comme moyens de paiement. Cependant, malgré l'introduction récente d'une réglementation et d'un mécanisme de surveillance, le secteur – au-delà des opportunités qu'il offre – continue de présenter plusieurs risques, notamment en matière de blanchiment de capitaux et de financement du terrorisme (BC/FT).

Les risques persistants de BC/FT s'expliquent par plusieurs facteurs. D'une part, ils tiennent à un cadre réglementaire encore en phase d'harmonisation et de mise en œuvre effective (voir pp. 33-34). Des exigences clés telles que le renforcement de l'identification des utilisateurs (*Know Your Customer – KYC*) et la vérification de l'origine des fonds commencent tout juste à être appliquées de manière cohérente à l'échelle internationale.

D'autre part, il y a des facteurs liés aux particularités technologiques de la chaîne de blocs, qui en font un système infalsifiable, incensurable et largement en dehors du contrôle des autorités publiques (voir p. 18) :

- Le recours au pseudonymat comme principe de base : les utilisateurs sont identifiés par une adresse ou un pseudonyme sur la chaîne de blocs, plutôt que par leur identité réelle.
- L'absence de contrôle d'accès sur la plupart des plateformes de finance décentralisée (DeFi), l'unique condition étant la connexion à un portefeuille (*wallet*). Ceci rend la traçabilité techniquement possible, mais difficile et souvent limitée en pratique.
- Le recours à diverses techniques de dissimulation, telles que les ponts (*bridges*), les mixeurs (*mixers*), les sauts de chaîne (*chain-hopping*), et autres méthodes complexes de brouillage des flux financiers.

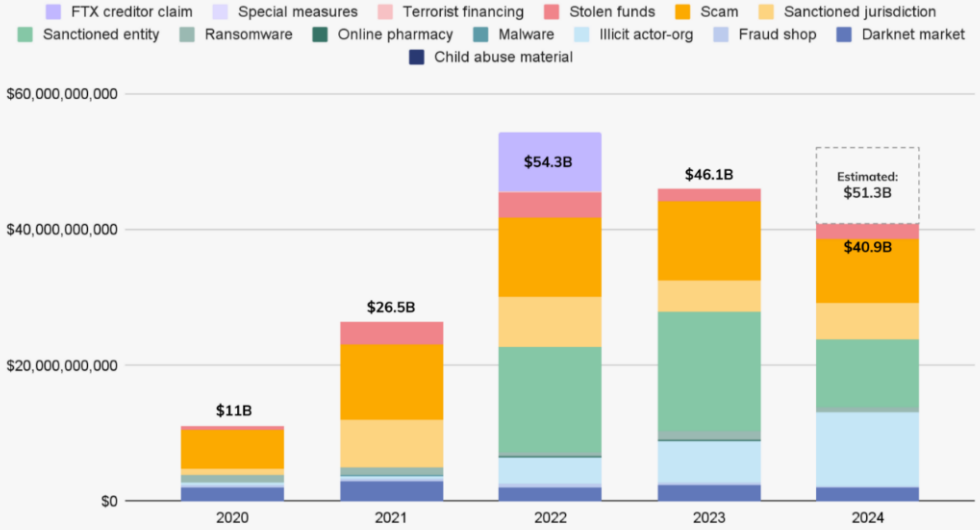
Capitalisation (nombre d'unités x prix de vente constaté) des principaux crypto-actifs



Source : Coinmarketcap.com, 31 mai 2025

Total cryptocurrency value received by illicit addresses

2020 - 2024



Source : Chainalysis (2025), Rapport 2025 sur la crypto-criminalité

L'utilisation des crypto-actifs à des fins de BC/FT connaît une évolution préoccupante selon les observations et analyses les plus récentes. En 2024, les adresses identifiées comme illicites ont reçu environ 40,9 milliards de dollars américains en crypto-actifs, un chiffre qui pourrait être révisé à la hausse jusqu'à 51 milliards de dollars américains (rapport Chainalysis 2025). Bien que cela ne représente que 0,14% du volume total des transactions crypto mondiales (à mettre en perspective avec les 2 à 5% de transactions illicites observées sur le produit intérieur brut (PIB) mondial [1]), ce pourcentage masque l'ampleur absolue du phénomène tant il est difficile d'obtenir des données exhaustives en la matière.

Les crypto-actifs présentent des caractéristiques intrinsèques qui en font un vecteur particulièrement attractif pour le blanchiment de capitaux en raison notamment de ce qui suit :

- Absence de barrière à l'entrée : l'accès à un simple logiciel et à une connexion Internet suffit pour effectuer des transactions ;
- Transactions rapides, peu onéreuses, et fiables ;
- Valeur reconnue à l'échelle mondiale, facilitant leur utilisation transfrontalière ;
- Existence d'un écosystème international en pleine expansion, où de nombreux acteurs demeurent peu ou non conformes en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB/FT) ;
- Diversité et disponibilité des moyens d'obfuscation, permettant de dissimuler la provenance, la nature, et la destination des fonds.

Une évolution notable réside dans l'utilisation des crypto-actifs stables (*stablecoins* – voir p. 11) notamment dans des mécanismes de compensation liés au blanchiment issu du trafic de stupéfiants (ex. l'affaire *Dark bank* [2]). Un autre phénomène émergent concerne la mise en rendement des fonds illicites via des protocoles de *staking* ou d'autres services offerts par la DeFi (voir pp. 18-23).

Malgré l'entrée en vigueur du Règlement européen sur les crypto-actifs (MiCA) (voir pp. 33-34), les crypto-actifs stables peuvent encore être facilement échangés contre des crypto-actifs confidentiels (*privacy coins* – voir p. 12), que ce soit via des plateformes d'échange centralisées (souvent hors d'Europe), ou par le biais d'infrastructures de la finance décentralisée (voir pp. 18-23), échappant à toute supervision ou régulation effective.

En 2025, le volume des transactions réalisées en crypto-actifs stables a dépassé, pour la première fois, celui des paiements en monnaie fiduciaire (fiat) traités par Visa : 27 600 milliards de dollars américains ont été réglés en crypto-actifs stables contre 13 200 milliards via Visa en 2024 [3].

L'utilisation des ponts qui permettent de transférer des actifs entre différentes chaînes de blocs a en effet doublé depuis 2022. Cette technique est désormais systématiquement utilisée par les réseaux criminels les plus sophistiqués pour complexifier la traçabilité des flux.

Enfin, le contournement de la règlementation par les crypto-actifs dépasse aujourd'hui le champ strictement criminel ou frauduleux, pour s'inscrire également dans des stratégies géopolitiques. Ainsi, des transactions en bitcoins auraient été observées entre des exportateurs de pétrole russes et leurs partenaires commerciaux en Asie [4]. Si les montants restent pour l'instant limités, l'intérêt stratégique de ces acteurs pour les technologies chaîne de blocs est manifeste.

LES CRYPO-ACTIFS STABLES

Les crypto-actifs stables sont des crypto-actifs conçus pour maintenir une valeur stable, généralement indexée sur une monnaie fiduciaire comme le dollar ou l'euro.

Bien que de légères fluctuations – de l'ordre de quelques pourcents – soient courantes, cette stabilité représente une exception notable dans l'univers hautement volatil des crypto-actifs.

Pour la troisième année consécutive, les crypto-actifs stables dominent les flux liés à des activités illicites, représentant 63% des transactions criminelles en 2024 [5]. Leur stabilité et leur facilité de conversion en monnaies fiat en font des instruments privilégiés pour les acteurs malveillants. Ils sont notamment utilisés par des entités placées sous sanctions cherchant à contourner les restrictions internationales [6].

La capacité technique du régulateur à contrôler un crypto-actif stable va grandement varier selon qu'il appartient à l'une ou l'autre des deux grandes catégories de crypto-actifs stables :

- Les **crypto-actifs stables centralisés** sont émis par une entité réglementée en échange d'un dépôt équivalent en monnaie fiduciaire ou en actifs traditionnels. Cette entité garantit le rachat des crypto-actifs émis à un taux proche de leur coût d'émission. Elle conserve également un contrôle technique sur les actifs, pouvant procéder à des gels ou saisies. Les crypto-actifs stables centralisés les plus répandus sont l'USDT (Tether) et l'USDC (Circle).
- Les **crypto-actifs stables décentralisés**, à l'inverse, sont plus complexes. Leur architecture sans autorité centrale rend leur contrôle, leur censure ou leur régulation particulièrement difficile (voir p. 21). Le plus emblématique de ces actifs est le DAI, émis via le protocole MakerDAO.

À ce stade, la règlementation européenne, et notamment le règlement MiCA ne couvre que les crypto-actifs stables centralisés, désignés comme « jetons référencés à un actif » ou « jetons de monnaie électronique ». Ces crypto-actifs stables doivent être émis par des entités agréées, soumises à des exigences strictes en matière de transparence, de constitution de réserves et de gestion des risques.

Tether (USDT)

Tether (USDT) est actuellement le crypto-actif stable centralisé le plus utilisé au monde. Il est émis par la société Tether Ltd., créée aux Îles Vierges britanniques, et désormais domiciliée au Salvador. En 2025 il y a environ 150 milliards d'USDT qui ont été émis.

L'émetteur affirme disposer d'un collatéral équivalent à la valeur des USDT émis, composé en grande partie (environ deux tiers) de bons du Trésor américain. Toutefois, la crédibilité de cette affirmation est sujette à controverse, notamment en raison de la qualité perçue de l'auditeur externe, BDO, dont la fiabilité n'est sans doute pas à la hauteur de l'enjeu (Foley, Stephen, 2024).

L'USDT évolue actuellement sur plus de 13 chaînes de blocs différentes.

PORTEFEUILLES ET ECHANGEURS

Pour interagir avec des crypto-actifs, les utilisateurs ont recours à deux types principaux de solutions de gestion :

Les portefeuilles non-dépositaires

Il s'agit de logiciels cryptographiques installés sur un ordinateur ou un téléphone portable. Ces portefeuilles offrent un haut degré d'anonymat, puisqu'ils ne nécessitent pas d'identification formelle. Toutefois, l'utilisateur est seul responsable de la sécurité de ses fonds et s'expose à un risque de piratage de sa clé privée stockée dans le portefeuille et utilisée pour signer les transactions et prouver la propriété du portefeuille ainsi que l'autorisation à effectuer des opérations.

Les portefeuilles dépositaires via des plateformes centralisées

Dans ce cas, les utilisateurs confient la gestion de leurs actifs à une institution tierce, à la manière d'une banque. Ces institutions offrent un large éventail de services : le gardiennage des fonds, l'échange entre crypto-actifs ou entre crypto-actifs et monnaies fiduciaires, l'accès à des produits financiers (futures, options, etc.), la participation à des protocoles décentralisés. Le niveau de régulation de ces institutions varie considérablement selon, notamment, leur lieu d'implantation.

LES CRYPTO-ACTIFS CONFIDENTIELS

Il est impossible de mesurer avec précision l'usage des crypto-actifs confidentiels, en raison de leur nature fondamentalement intraçables. Ces crypto-actifs intègrent des méthodes cryptographiques complexes et avancées à tous les niveaux de leur fonctionnement (voir p. 18), depuis la diffusion des données sur le réseau pair à pair (P2P), jusqu'au contenu même des transactions, qui reste chiffré et non accessible à l'analyse.

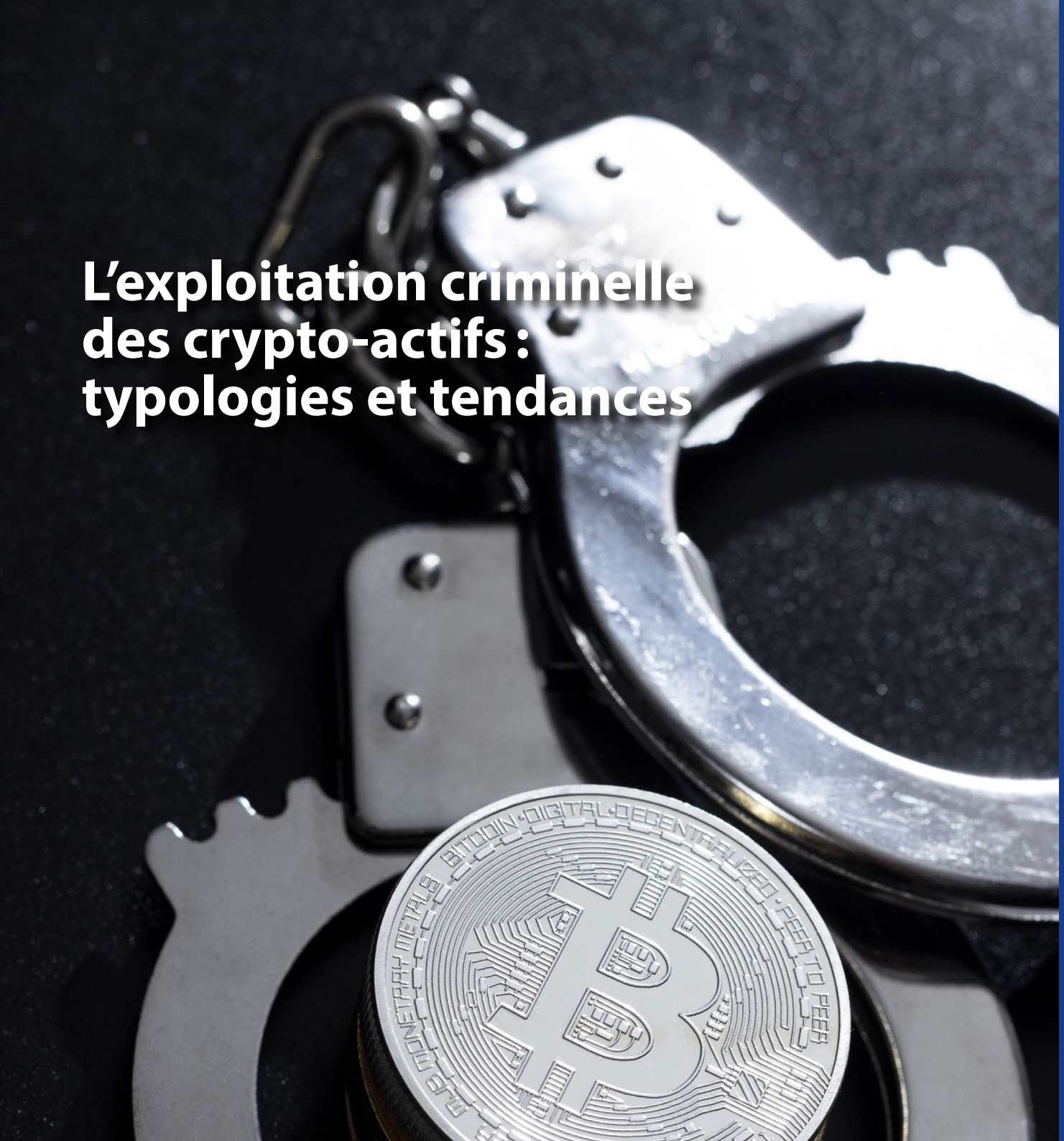
Néanmoins, malgré leur retrait des principales plateformes d'échange à la suite de l'entrée en vigueur du règlement MiCA (voir pp. 33-34), certains crypto-actifs confidentiels, en particulier Monero, continuent de faire l'objet d'échanges significatifs sur des plateformes moins regardantes, telles que KuCoin et HTX. Ainsi, en mai 2025, les volumes journaliers d'échange entre Monero et USDT demeurent élevés, avoisinant une centaine de millions d'euros par jour.

Monero

Parmi les crypto-actifs confidentiels, Monero s'impose comme le seul actif véritable et significatif en matière d'adoption, de robustesse technique et de protection de la vie privée. Contrairement à d'autres actifs similaires comme Zcash, dont les fonctionnalités d'anonymisation ne sont pas activées par défaut, celles de Monero sont intégrées nativement et demeurent non désactivables. Le protocole ne présente pas de failles techniques connues, et il bénéficie d'une communauté active et d'une adoption croissante. Les principales caractéristiques de son usage criminel sont les suivantes :

- Rançongiciels (*ransomwares*) : l'usage de Monero est en augmentation dans les demandes de rançon (Chainalysis Team, 2022). Certains groupes criminels offrent même une réduction aux victimes payant en Monero, afin d'encourager son usage.
- Internet clandestin (*Darknet*) : Monero est couramment utilisé sur les places de marché illicites de l'Internet clandestin. Certaines plateformes comme White House l'ont adopté comme unique moyen de paiement (Chainalysis Team, 2023).
- Contenus pédopornographiques : selon Chainalysis (2024) les services exploitant Monero dans ce domaine présentent une durée de vie plus longue que ceux utilisant d'autres crypto-actifs, en raison de la difficulté accrue de traçabilité.
- Usage étatique : On note un usage anecdotique par la Corée du Nord (United Nations Security Council, 2024) dont les méthodes de blanchiment reposent principalement sur les crypto-actifs stables.

L'exploitation criminelle des crypto-actifs : typologies et tendances



Cette dernière décennie, les piratages massifs des plateformes centralisées et des protocoles DeFi restent les plus spectaculaires en volume, avec des pertes estimées à 2,2 milliards de dollars américains en 2024 et 7,7 milliards de dollars entre 2022 et 2024 [7]. On assiste à une professionnalisation croissante des opérations, impliquant des groupes transnationaux, parfois étatiques, s'appuyant sur des infrastructures dédiées, des sociétés écrans et des outils de chiffrement pour opacifier les flux.

Parallèlement, certaines pratiques criminelles déclinent (comme les mixeurs ou les marchés de l'Internet clandestin), tandis que d'autres gagnent en popularité : notamment les ponts inter-chaînes, les services de blanchiment dans la chaîne (*on-chain*), ou encore l'utilisation de l'intelligence artificielle (IA) pour des escroqueries ciblées (voir p. 16). Ces dynamiques s'inscrivent dans un contexte de règlementation en transition (voir pp. 33-34), où l'adaptation des outils de lutte peine parfois à suivre le rythme de l'innovation criminelle (voir pp. 25-29).

POIDS DU PIRATAGE ET DE LA CYBERCRIMINALITE

Les dix dernières années démontrent l'importance écrasante du piratage (*hacking*) dans l'écosystème criminel lié aux chaînes de blocs avec un pic en 2022. Ces attaques, ciblant principalement les protocoles DeFi, les plateformes d'échange et l'infrastructure, ont représenté plus de 90% des montants détournés, pour un total supérieur à 11,6 milliards de dollars américains (DefiLlama – Piratages, juin 2025).

Parmi les incidents récents, l'attaque de Bybit en février 2025, avec 1,46 milliards de dollars américains détournés [8], illustre l'ampleur du phénomène. Les techniques les plus fréquentes incluent la compromission des clés privées ou signatures, l'hameçonnage, l'ingénierie sociale, les bugs de vérification et les attaques par le prêt éclair (*flash loan* – voir p. 22). Les retraits de tapis (*rug pulls*) demeurent fréquents. Enfin, la participation de groupes étatiques dans certaines de ces attaques souligne une évolution préoccupante, révélant des enjeux géopolitiques croissants liés à la sécurité des actifs numériques.

DIVERSIFICATION DES CRIMES UTILISANT LES CRYPTO-ACTIFS

Bien que la cybercriminalité demeure dominante, l'écosystème chaîne de blocs est de plus en plus utilisé pour faciliter des crimes traditionnels. Les groupes criminels organisés transnationaux se tournent en effet vers les crypto-actifs pour commettre ou blanchir le fruit de crimes traditionnels, tels que le trafic de drogue, les jeux d'argent, le vol de propriété intellectuelle, le blanchiment de capitaux, le trafic d'êtres humains et d'espèces sauvages et les crimes violents [5].

Les ventes de stupéfiants ont continué de croître et de s'étendre en dehors des écosystèmes du marché de l'internet clandestin, en se déplaçant vers des applications de messagerie chiffrée et des plateformes de réseaux sociaux, tels que Telegram et Signal [7].

Passent également par les chaînes de blocs le contournement des sanctions internationales (en hausse depuis le durcissement des sanctions), la fraude fiscale, les escroqueries, les marchés clandestins, les rançongiciels, etc.

En 2025, plusieurs affaires médiatiques d'enlèvement et de séquestration des personnalités néo-médiatiques avec demande de rançon en crypto-actifs ont mobilisé l'attention du public et des autorités [9].

PROFESSIONNALISATION ET ORGANISATION CROISSANTE

Même avec un niveau technique modeste et des compétences cryptographiques limitées, les groupes criminels démontrent une

professionnalisation croissante et une sophistication opérationnelle accrue. Face à la pression croissante des forces de l'ordre et à l'évolution du cadre réglementaire, les criminels adaptent continuellement leurs techniques.

La finance décentralisée est pleinement intégrée dans les schémas criminels (voir pp. 18-23). Ses caractéristiques – incensurabilité, absence de point de contrôle central, anonymat des parties – en font un terrain favorable à l'impunité. Les poursuites sont d'autant plus difficiles que les flux illicites se fragmentent entre multiples protocoles, souvent automatisés, opérant hors de tout cadre juridique clair.

DECLIN DE CERTAINES PRATIQUES

Certaines tendances criminelles sont en déclin, marquant une évolution des pratiques dans l'écosystème illicite des crypto-actifs.

- Les revenus générés par les marchés de l'Internet clandestin (tels que Kraken DNM, Mega, Blacksprut, OMG!OMG!, Abacus), ainsi que par les boutiques spécialisées (qui vendent des données volées et des informations personnelles identifiables), diminuent au fil des ans, en dépit de leur rôle historique dans les escroqueries, les vols d'identité et les campagnes de rançongiciels.
- L'utilisation des mixeurs décroît au profit des ponts inter-chaînes.
- Les volumes d'escroqueries et de fraudes diminuent, mais continuent de représenter une menace significative.

ADAPTATION DES CRIMINELS AUX EVOLUTIONS REGLEMENTAIRES

Les sanctions internationales, la mise en conformité progressive des principaux échangeurs centralisés (dont la concentration demeure élevée), l'émergence des normes internationales fortes et unifiées, ainsi que la montée en compétence technique des autorités, produisent des effets contrastés sur les comportements criminels.

D'une part, ces dynamiques poussent certains échangeurs vers les juridictions faiblement régulées, exploitant les lacunes ou l'absence de supervision adéquate. D'autre part, elles favorisent un basculement des activités illicites. Les criminels s'appuient ainsi sur un éventail d'outils difficilement contrôlables : échangeurs décentralisés, ponts inter-chaînes, crypto-actifs stables décentralisés, portefeuilles non-dépositaires, etc. Ces services, sont aujourd'hui employés de manière routinière, y compris par des criminels peu compétents. Ils sont utilisés en cascade de manière systématique par les groupes les plus sophistiqués. En outre, on observe l'intégration de sociétés écrans hors-chaîne (*off-chain*) [10], pratique issue des schémas traditionnels de blanchiment de capitaux et de financement du terrorisme, désormais articulée avec les nouveaux vecteurs crypto.

Le recours généralisé des groupes criminels à ces services décentralisés rend l'analyse encore plus difficile du fait du mélange des flux de crypto-actifs. Cette tendance est renforcée par l'explosion des volumes : en mai 2025, les échanges entre crypto-actifs réalisés via des protocoles décentralisés atteignent près d'un quart du volume total, contre moins de 10% en 2023. Ce glissement reflète directement l'effet de la pression réglementaire sur les plateformes centralisées.

UTILISATION DES MESSAGERIES CHIFFREES

L'écosystème de la criminalité liée aux crypto-actifs s'appuie de manière croissante sur des plateformes de messagerie chiffrée, en particulier Signal et Telegram, qui proposent leurs propres services liés aux crypto-actifs, et dont l'intégration avec des portefeuilles non-dépositaires est aisée.

Ces canaux sont utilisés pour :

- La mise en relation de prestataires de services criminels (attaques par déni de service distribué, piratage, blanchiment, etc.) ;
- Le commerce de bases de données compromises, d'identifiants volés et de malwares spécialisés ;
- Des discussions techniques entre cybercriminels ;
- Des activités de financement illicite, y compris celui du terrorisme.

UTILISATION DE L'IA GENERATIVE

L'essor récent de l'intelligence artificielle générative a été rapidement capitalisé par les cybercriminels, qui l'emploient pour industrialiser certaines pratiques frauduleuses. Ces outils permettent notamment :

- La création et l'animation de faux profils crédibles sur les réseaux sociaux ;
- La conduite en parallèle de multiples arnaques sentimentales par un seul opérateur ;
- La génération de l'hypertrucage (*deepfakes*) utilisés dans des campagnes d'extorsion sexuelle ciblée ;
- La production automatisée de contenus de *spear-phishing* (pêche au harpon).

Par ailleurs, l'IA facilite également la génération de campagnes massives de spam, notamment autour d'escroqueries à l'investissement. Ces dernières connaissent un pic d'activité en période de marché haussier des crypto-actifs, amplifiées par la médiatisation et l'euphorie spéculative.

Pig Butchering

Les arnaques sentimentales, également appelées *Pig Butchering*, consistent à gagner la confiance d'une victime sur une période prolongée, à travers de faux profils souvent animés via des outils d'IA générative, avant de l'inciter à investir dans des plateformes frauduleuses, généralement liées à des produits crypto.

Ce système est doublement punitif car les auteurs en contact avec les victimes sont eux-mêmes enfermés dans des camps de force en Asie.

L’utilisation abusive de la DeFi à des fins de BC/FT

LES COUCHES DE LA DEFI

Infrastructure réseau : la couche de communication

À la base, des ordinateurs communiquent et échangent des données grâce au protocole de contrôle de la transmission (*TCP*) quel que soit leur emplacement géographique ou topologique.

Ces ordinateurs forment ensuite un réseau pair à pair (*P2P*). Chaque nœud est connecté à plusieurs voisins, qui sont eux-mêmes connectés à d'autres, formant ainsi un maillage distribué et résilient. Ce réseau permet la diffusion d'informations entre tous les pairs sans point central de coordination.

La chaîne de blocs : technologie de registre distribué (DLT)

Sur ce réseau P2P, les nœuds exécutent un protocole cryptographique qui leur permet de se mettre d'accord sur le contenu d'un registre distribué (tous les nœuds en possèdent une copie) et infalsifiable (pas de retour en arrière possible), sans autorité centrale ni besoin de confiance mutuelle : ceci est la chaîne de blocs.

Le contenu de ce registre est contraint par les règles du protocole. Certains registres de blocs, comme Bitcoin, n'enregistrent que des transactions financières simples.

D'autres, comme Ethereum, recourent à des programmes autonomes qui sont déclenchés par des transactions et dont l'exécution est vérifiée par tous les nœuds avant d'être enregistrées dans le registre de blocs. Ces programmes sont les contrats intelligents.

Les contrats intelligents : la couche logique

Les contrats intelligents sont des logiciels déployés sur la chaîne de blocs. Ils définissent des règles et actions qui sont exécutées de manière automatique, transparente et infalsifiable.

La communauté se met d'accord sur des normes d'interprétation de ces contrats :

- Un contrat conforme à la norme ERC-20 est interprété comme un jeton fongible (par exemple, un jeton représentant un crypto-actif).
- Un contrat conforme à la norme ERC-721 définit un jeton non fongible, un actif unique et traçable individuellement.

La DeFi : l'automatisation des services

Des protocoles financiers automatisés sont ensuite construits à partir de ces contrats :

- Uniswap est un protocole d'échange décentralisé simulant un carnet d'ordre grâce à des fonctions algorithmiques.
- MakerDAO est un protocole décentralisé d'émission de crypto-actifs stables.

C'est cette couche qui constitue la DeFi : un écosystème d'applications permettant d'accéder à des services financiers (échange, emprunt, prêt, etc.) sans intermédiaire centralisé.

Les interfaces utilisateurs : l'accès aux services

Pour interagir avec ces protocoles, les utilisateurs disposent de portefeuilles, des logiciels qui gèrent leurs clés cryptographiques et leur permettent de signer des transactions. Certains s'intègrent directement dans les navigateurs web pour faciliter l'accès.

Au lieu de l'identification classique, les utilisateurs sont identifiés par une clef publique (des lettres et chiffres) sans gestion d'identité centralisée.

Des sites web ou interfaces décentralisées (dApps) exploitent ces portefeuilles pour proposer une interaction intuitive avec les protocoles DeFi. Ils exposent également les informations contenues dans la chaîne de blocs, comme les soldes, les transactions, ou les prix.

Cette couche visible représente la partie émergée du Web3.

Les passerelles vers le monde traditionnel : les échangeurs centralisés

Enfin, des acteurs centralisés (comme Binance ou Coinbase) permettent la conversion entre crypto-actifs et monnaies fiduciaires. Malgré la nature décentralisée des crypto-actifs, on observe une forte concentration des échanges autour de ces plateformes.

Ils agissent comme passerelles vers le système financier traditionnel et peuvent être sollicités pour fournir des informations (*KYC*, historique et autres).

La finance décentralisée représente une évolution majeure et rapide de l'écosystème des crypto-actifs depuis son émergence dans les années 2010. Le nombre d'utilisateurs actifs de la DeFi est en constante hausse, illustrant une adoption et utilisation exponentielle.

Par ailleurs, la DeFi soulève des défis spécifiques en matière de LCB/FT. Les protocoles DeFi proposent des services financiers (prêt, emprunt, échange, ou autre) sans intermédiaire centralisé, uniquement gérés par des contrats intelligents hébergés sur la chaîne de blocs.

PRAGMATISME DANS L'APPROCHE REGLEMENTAIRE

L'infographie précédente illustre un fait subtil mais primordial : malgré leur mélange incessant et leur usage impropre dans la plupart des publications grand public, les termes tels que Bitcoin, crypto-actif stable, contrat intelligent, échangeur ou DeFi, font référence à des objets techniques bien différents, dont la capacité du régulateur à les contraindre varie du tout au tout, allant de l'assujettissement aux règles LCB/FT des échangeurs centralisés, à l'impossibilité technique absolue d'influencer les contrats d'échange (*swapping*) alors que ces acteurs rendent les mêmes services.

Il est notoire à présent que les systèmes automatisés présents sur la chaîne de blocs (la DeFi), ne sont pas réglementés dans le cadre de la LCB/FT en raison de plusieurs difficultés.

LES CONTRATS INTELLIGENTS

Si certaines chaînes de blocs comme Bitcoin ne permettent que l'échange d'avoirs, d'autres comme Ethereum permettent aux pairs de se mettre d'accord sur l'exécution de logiciels.

Ces logiciels, dont l'exécution est donc distribuée sur toute la planète et demeure cryptographiquement vérifiée, sont incensurables, et ils peuvent à leur tour émettre des transactions.

Cette invulnérabilité fait leur force compte tenu notamment de :

- la transparence (du point de vue de l'utilisateur, mais non nécessairement du régulateur),
- la fiabilité (dans la technologie au lieu des intermédiaires),
- la suppression des intermédiaires financiers, avec une interaction directe entre pairs,
- leur nature automatique et inter-opérationnelle sans barrière d'entrée.

Cependant leur utilisation a des effets pervers pour la lutte contre le blanchiment puisqu'elle ne permet pas la vérification de l'identité des utilisateurs. Par ailleurs, il est très difficile voire impossible de réguler un contrat une fois lancé (voir l'encart Tornado Cash, p. 23), sauf si le développeur a intégré dès l'origine des clauses de contrôle (ce qui est généralement perçu comme contraire à l'esprit de la DeFi, et dissuasif pour l'utilisateur). Par exemple, les crypto-actifs stables centralisés comme l'USDT ont une clause permettant à l'entité émettrice de geler les avoirs des adresses figurant sur des listes de sanctions (voir p. 11). Cela illustre bien le cas d'un contrat intelligent (*smart contract*) dont les fonctions sont étroitement contrôlées par son développeur. Dans ce type de configuration, la confiance des utilisateurs repose davantage sur l'institution émettrice que sur le fonctionnement autonome du contrat intelligent lui-même.

A l'inverse, les crypto-actifs stables décentralisés, tout comme d'autres protocoles DeFi, n'intègrent aucune autorité de contrôle.

On assiste via la finance décentralisée à une dérégulation en pratique du secteur financier des crypto-actifs.

Malgré cette puissance technique, le savoir-faire technique nécessaire à l'utilisation de la DeFi pousse la majorité des acteurs vers les plateformes régulées. En revanche, pour les groupes criminels

disposant des compétences nécessaires, l'usage de la DeFi est devenu à la fois routinier et stratégique. Cela a été illustré de manière emblématique par le piratage de la plateforme Bybit, qui a mis en évidence la maîtrise opérationnelle de ces acteurs dans l'exploitation des protocoles décentralisés [11].

JETONS

Une grande partie de l'écosystème DeFi repose sur l'utilisation de jetons (*tokens*), des crypto-actifs créés via des contrats intelligents déployés sur des chaînes de blocs existantes. Contrairement aux coins, qui sont les crypto-actifs natifs d'une chaîne de blocs (comme le Bitcoin pour la chaîne de blocs Bitcoin, ou Ether pour Ethereum) et servent notamment à payer les frais de transaction, les jetons ne nécessitent pas la création d'un écosystème chaîne de blocs propre.

Leur émission repose uniquement sur le déploiement d'un contrat intelligent conforme à une norme technique prédéfinie, la plus répandue étant la norme ERC-20 sur Ethereum. Cette norme définit les fonctions minimales qu'un contrat intelligent doit implémenter pour que l'écosystème DeFi puisse reconnaître l'actif comme un jeton interopérable.

Les jetons peuvent être comparés à des jetons de casino : ils n'ont de valeur que celle qui leur est attribuée, soit par leur émetteur, soit par la confiance des utilisateurs dans un usage, un projet ou une narration spéculative.

Les chaîne de blocs et les crypto-actifs

La première chaîne de blocs, Bitcoin, a été lancée en 2009. Depuis, l'écosystème s'est considérablement développé, avec plus de 350 chaînes de blocs recensées début 2025. Les chaîne de blocs les plus compétitives et durables à côté d'Ethereum, comprennent Solana, BSC, Tron, Base, Arbitrum, Avalanche, Aptos, Polygon et Cronos.

Sur ces chaînes de blocs, qui sont toutes des registres infalsifiables distribués, s'échangent différents avoirs. Ainsi par exemple l'USDT, émis par la société Tether, s'échange sur les chaînes de blocs Ethereum, Tron, Solana, Avalanche, et d'autres encore.

Chaque chaîne de blocs supporte un avoir natif, qui sert à payer les frais de transaction.

L'USDT est techniquement un jeton. Certains jetons sont liés à des plateformes de jeu en ligne, servent de contreparties pour des ressources rares (par exemple, des droits de reproductions d'animaux de race), ou n'ont qu'une valeur « réelle » très douteuse. Ils forment autant d'opportunités de blanchiment par l'arrangement de transactions crédibles à fort bénéfice, par le mélange des flux, et d'autres techniques.

LES JETONS NON FONGIBLES (JNF)

Les jetons non fongibles (*Non-Fungible Tokens*) reposent sur des normes telles que ERC-721 et ERC-1155, qui diffèrent de l'ERC-20 en ce que chaque jeton est unique et non interchangeable. Chaque JNF est donc traçable individuellement depuis sa création à travers toutes ses transactions.

Le parallèle avec le marché du luxe (certificat d'authenticité, réserve discrète de valeur) et de l'art (œuvre unique originale, prix subjectif, opacité des transactions) est évident, et les opportunités de blanchiment afférentes à l'un se retrouvent dans l'autre :

- *Achat à prix surévalué :* un JNF peut être acheté à un prix artificiellement élevé pour justifier un afflux de fonds illicites.
- *Fraude fiscale :* des dons de JNF à des institutions d'intérêt général peuvent être déclarés à une valeur gonflée pour réduire la base imposable,

ou pour optimiser la transmission de patrimoine (échappement aux droits de succession).

- *Thésaurisation :* certains acteurs achètent des JNF en masse pour constituer un portefeuille qui conserve sa valeur sans passer par le système bancaire classique.

La principale plateforme d'échange de JNF s'appelle *OpenSea*. Sur certaines collections, jusqu'à un quart du volume était dû à la pratique des « achetés-vendus » (*wash trading*) [12], tandis que sur d'autres plateformes plus petites (LooksRare, X2Y2 [13]), le volume de la pratique des « achetés-vendus » constitue la quasi-intégralité des transactions de la plateforme. Les JNF sont particulièrement adaptés aux pratiques des « achetés-vendus » en raison de la faible liquidité du marché, et de l'historique avéré de flambée des prix, attirant les spéculateurs.

Pratique des « achetés-vendus »

La pratique des « achetés-vendus » consiste à délibérément acheter et vendre un même actif entre des comptes contrôlés par une seule et même entité afin de créer une fausse apparence d'activité de marché légitime. L'objectif est de manipuler plusieurs indicateurs clé du marché : le volume d'échange, le prix, les signaux de demande.

En falsifiant ces signaux, l'auteur de la pratique des « achetés-vendus » induit les autres participants en erreur, leur faisant croire que l'actif est populaire ou a de la valeur. Cela peut inciter de véritables acheteurs à entrer sur le marché. Une fois cette demande artificielle créée, le fraudeur peut vendre à ces acheteurs réels avec un bénéfice, concluant ainsi sa manipulation.

Le problème est particulièrement répandu sur les chaînes de blocs à faible frais comme Solana.

LES CRYPTO-ACTIFS STABLES DECENTRALISES

Contrairement aux crypto-actifs stables centralisés (voir p.11) qui sont émis par une société en échange d'un collatéral financier souvent classique, les crypto-actifs stables décentralisés sont émis automatiquement par un contrat intelligent lorsque des investisseurs viennent bloquer sur celui-ci un collatéral lui aussi composé de crypto-actifs.

Les crypto-actifs stables décentralisés sont quasiment autonomes de leurs créateurs, ne maintiennent aucune *KYC*, ne peuvent techniquement pas être censurés, gelés, ou saisis.

Néanmoins il ne faut pas négliger les risques liés aux crypto-actifs stables centralisés, qui ne se sont tout simplement pas encore écroulés, et qui subissent parfois des variations jusqu'à 20% pendant quelques jours. Les fortes variations des prix des crypto-actifs, ainsi que les failles parfois présentes dans ces contrats complexes font courir aux porteurs un risque certain. Jusqu'à présent les plus gros évènements de décorrélation de la valeur du crypto-actif stable avec sa valeur cible (depeg) ont eu lieu sur des crypto-actifs stables décentralisés.

UST et LUNA

L'UST est un crypto-actif stable décentralisé qui s'est écroulé, effaçant 45 milliards de dollars américains de valorisation du marché des crypto-actifs. Lorsque l'UST tombait sous 1 dollar, les utilisateurs pouvaient l'acheter à bas prix, l'échanger via un contrat intelligent contre 1 dollar en LUNA, puis vendre ce LUNA pour réaliser un profit.

Mais la chute brutale de l'UST a amené un arbitrage massif, qui a fait générer au contrat beaucoup de LUNA. Cet afflux d'offre de LUNA a fait baisser son prix, ce qui a mécaniquement fait émettre encore plus de LUNA au contrat à chaque nouvelle apport d'UST par les arbitres, et ainsi de suite jusqu'à ce que la création de LUNA explose et son prix s'écroule, interdisant à l'UST de regagner son prix cible de 1 dollar.

LE PRET ECLAIR

Le prêt éclair, est une spécificité de la DeFi qui permet d'emprunter, sans fournir de collatéral des montants importants en crypto-actifs via un contrat intelligent. La seule condition est que l'emprunt et son remboursement – frais inclus – soient intégralement exécutés au sein d'une même transaction. Celle-ci peut comporter plusieurs sous-transactions, mais l'opération est atomique : soit toutes les étapes réussissent, soit la transaction est annulée dans son intégralité. Initialement conçus pour permettre des opérations d'arbitrage, les prêts éclair sont également détournés à des fins malveillantes, notamment dans le cadre d'attaques exploitant des vulnérabilités de contrats intelligents.

Par exemple, dans l'affaire Platypus, un attaquant a exploité une faille dans un protocole de crypto-actif stable décentralisé (USP), en combinant prêts éclair, manipulation de collatéral et bug dans le contrat pour détourner des fonds, provoquant une perte de valeur partielle de l'actif.

LES ECHANGEURS DECENTRALISES

Les exemples les plus connus des applications DeFi sont les échangeurs décentralisées (DEX) et les protocoles de liquidité. Ether Delta était le premier échangeur décentralisé (2017), surpassé depuis par Uniswap, et plus récemment (mai 2025) par PancakeSwap.

Ces contrats permettent à n'importe qui d'échanger un jeton pour un autre. Afin de rassurer les utilisateurs, les créateurs ne peuvent en modifier le comportement qu'à la marge (gestion des frais notamment), rendant techniquement impossible toute mesure de saisie, blocage, ou autre sanction.

UNISWAP

Protocole d'échange décentralisé simulant algorithmiquement un carnet d'ordre, les utilisateurs influent sur le taux de change en fonction des jetons qu'ils échangent, et les investisseurs participant à la gouvernance décident – par exemple des frais.

Maker DAO

C'est le premier protocole décentralisé d'émission de crypto-actifs stables. Les investisseurs peuvent décider des paramètres de l'algorithme de garantie équivalant aux monnaies fiat.

LES PONTS

Une autre fonctionnalité offerte par les prestataires de services sur crypto-actifs (PSCA) et qui est dupliquée par la DeFi est celle permettant d'échanger deux crypto-actifs non pas au sein d'une même chaîne de blocs comme les échangeurs décentralisés mais entre deux chaînes de blocs différentes (par exemple du Bitcoin contre de l'Ether).

Les ponts sont des systèmes autonomes et fonctionnent de manière sécurisée, et sans aucune exigence de *KYC*. Ils ont des usages légitimes, permettant notamment d'aller réaliser des échanges ou de gérer des produits complexes sur des chaînes de blocs plus rapides où les frais sont moindres. Mais ils sont également utilisés par des groupes criminels compétents pour retarder l'analyse des flux. La Corée du Nord (groupe « Lazarus ») utilise désormais cette technique [14].

LES MIXEURS

Les criminels exploitent également les mixeurs de crypto-actifs. Ce sont des services qui mélangent les fonds de nombreux utilisateurs avant de les redistribuer, rendant la traçabilité très compliquée.

Ces services n'ont pas d'équivalent dans la finance officielle. Les autorités françaises ont pris conscience de ces risques. Ainsi en France, leur utilisation tombe explicitement sous le coup de l'article 324-1-1 du Code pénal sur la présomption de blanchiment, qui inverse la charge de preuve et présume que les fonds transitant par un mixeur proviennent d'un crime ou d'un délit.

Ces outils, bien qu'ayant des usages légitimes liés à la confidentialité financière, sont détournés de leur usage pour masquer la connexion entre des portefeuilles de collecte de fonds illicites et ceux utilisés pour transférer des fonds vers les plateformes d'échange.

Tornado Cash

Tornado Tornado Cash est un mixeur décentralisé, permettant depuis 2019 d'anonymiser les transactions sur la chaîne de blocs Ethereum en masquant automatiquement les liens entre les adresses d'envoi et de réception grâce à de la cryptographie avancée (Preuve à Divulgation Nulle de Connaissance ou *Zero-Knowlegde Proof*).

Une riposte judiciaire internationale en 2022-2023 permet l'arrestation des personnalités du projet, et la fermeture des comptes associés sur des plateformes techniques.

Cependant, d'une part, le contrat intelligent (voir p. 19) de Tornado Cash a continué, et continue encore de fonctionner, car il est impossible, même à des Etats, de le censurer. Et d'autre part les sanctions américaines contre Tornado Cash ont été levées par l'administration américaine.

Cet exemple illustre bien les défis posés par la finance décentralisée : malgré une action policière réussie et plusieurs arrestations, saisies et fermetures, le système de blanchiment fonctionne encore.

LA DEFI

Les risques systémiques, technologiques et de BC/FT sont évidents sur les plateformes de la DeFi. Par rapport aux exigences de LCB/FT, l'absence de procédures de vérification d'identité (*KYC*) dans les échanges décentralisés constitue une vulnérabilité majeure, permettant des transactions relativement confidentielles et difficiles à tracer. Dans ce contexte, il est important de souligner qu'il n'existe pas toujours de corrélation entre le niveau d'adoption des crypto-actifs dans un pays et la maturité de son cadre réglementaire. À titre d'exemple, plusieurs juridictions positionnées comme des hubs de la crypto-industrie – telles que Singapour, Hong Kong, les Émirats arabes unis ou la Suisse – présentent en réalité un taux d'adoption national relativement faible.

Récemment, un jugement a été rendu aux Etats-Unis sur l'utilisation d'une vulnérabilité sur une plateforme de DeFi (Mango Markets) qui a permis à un acteur mal intentionné de manipuler le cours du jeton utilisé par cette plateforme - le Mango (MNGO) – afin d'emprunter pour l'équivalent de 110 millions de dollars américains en crypto-actifs sans jamais les rembourser. Le jugement, qui fait date, donne raison à l'acteur, le juge indiquant qu'il n'avait fait qu'exploiter le code informatique et qu'il n'était pas responsable si celui-ci était mal codé. En d'autres termes et pour reprendre un dicton prisé dans le milieu des crypto-actifs : « *Code is Law* ».

Développement des outils et techniques d'enquête face à la criminalité crypto

Le succès des enquêtes repose sur une combinaison étroite entre une expertise technique pointue et un cadre juridique adéquat. Cette synergie permet de retracer les flux financiers, de lever partiellement l'anonymat de certains portefeuilles, et, le cas échéant, de procéder à la saisie des crypto-actifs.

Parmi les outils spécifiques à l'analyse des chaînes de blocs, on distingue principalement deux catégories. D'une part les explorateurs de blocs, qui offrent une interface graphique – plus ou moins évoluée – permettant d'explorer le contenu du registre des transactions. D'autre part, les outils d'analyse transactionnelle vont plus loin et capturent des informations supplémentaires, regroupent et désanonymisent certaines transactions entre autres.

Toutefois, ces outils ne suffisent pas, à eux seuls, à doter une cellule de renseignement financier (CRF) des capacités d'enquête dont elle a besoin. Ils doivent impérativement être combinés avec d'autres sources d'information : données issues des assujettis (déclarations de soupçon ou la suite au droit de la communication), renseignements collectés sur les réseaux sociaux, ou encore informations en source libre (voir p. 27).

LES EXPLORATEURS DE BLOCS

Un explorateur de chaîne de blocs est une interface web permettant de consulter, en temps réel ou de manière rétroactive, les données inscrites sur une chaîne de blocs : transactions, adresses, blocs, contrats intelligents, ou autres éléments.

Pour les enquêteurs, ces outils constituent un point d'entrée précieux. Ils permettent de retracer rapidement des flux simples entre adresses, de vérifier les détails d'une transaction (montant, horodatage, émetteur et destinataire), de suivre des interactions élémentaires avec un contrat intelligent – voire d'en consulter le code source –, ou encore identifier des schémas de mouvement ou d'interaction avec des entités connues. Ces observations peuvent ensuite être recoupées avec d'autres sources de renseignement ou outils d'analyse pour affiner l'enquête.

Les explorateurs mis à disposition gratuitement ne doivent donc pas être négligés. Certains, comme Etherscan, permettent d'accéder à des informations beaucoup plus complètes que les explorateurs commerciaux (par exemple, en ce qui concerne les données liées aux contrats intelligents et à leur code). Ils ont ainsi une vertu pédagogique et des capacités forensiques utiles pour les CRF et d'autres autorités compétentes.

ARBISCAN
Blockchain.com
BLOCKCHAIR
BscScan
Scan Original
Cardanoscan
Etherscan
polygonscan
SOLSCAN
SNOWTRACE
Tonviewer
TzKT
TRONSCAN

LES OUTILS D'ANALYSE TRANSACTIONNELLE DE CHAÎNE DE BLOCS

Les investigations sur les transactions en crypto-actifs s'appuient aujourd'hui sur des outils d'analyse transactionnelle de chaîne de blocs (OAT), qui constituent la principale innovation technique dans ce domaine. Ces outils exploitent un nœud d'une ou plusieurs chaîne(s) de blocs pour accéder aux données et suivre les transactions en temps réel.

Au-delà des fonctionnalités offertes par les explorateurs de blocs, les outils d'analyse transactionnelle permettent d'exploiter les données sur de longues périodes et à grande échelle. En combinant des techniques avancées de regroupement, ils établissent l'analyse comportementale d'une adresse liée

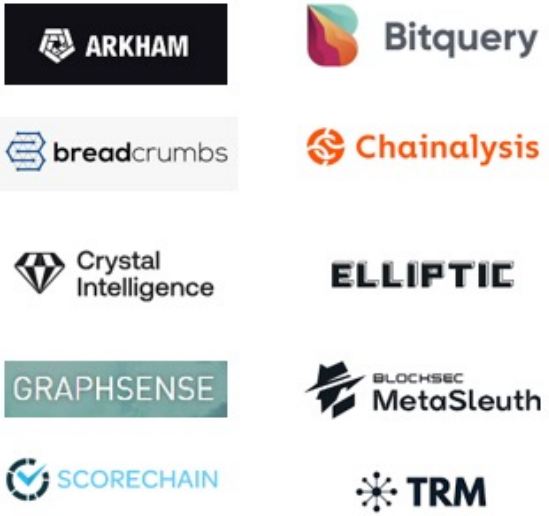
à un portefeuille de crypto-actifs. Ils permettent de regrouper des adresses entre elles (voir p. 28), d'identifier un portefeuille à risque, de générer des alertes et d'aider à retracer le parcours de fonds d'origine suspecte.

L'utilisation de ces outils est donc indispensable aujourd'hui pour les enquêtes sur les crypto-actifs. Ils constituent un chaînon critique dans la chaîne de renseignement, permettant aux analystes de passer d'un flux de transactions pseudonymes à des pistes concrètes exploitables.

Quelques exemples de solutions disponibles sur le marché sont presentés sur la page 27. Parmi celles-ci, GraphSense est la seule à être en source libre.

Outils commerciaux
Outils en source ouverte

Catégorie	+	Avantages	-	Inconvénients
Usage	✓	Accès libre et usage immédiat	☒	Agrément d'usage
Regroupement	✓	Regroupement des adresses, usage d'algorithmes de traitements par groupes ou par lots	☒	Pas de regroupement, identification faible suivant les explorateurs de blocs
Identification des services	✓	Identification des services	☒	Identification/regroupement pas exhaustifs (méthodes non publiées)
			☒	Capacités limitées d'analyse et d'identification
Complément d'information	✓	Rajout de données (OSINT, adresses IP…)	☒	Ne supporte pas toutes les chaînes de blocs existantes
			☒	Complément d'information manquant
Mise à jour	✓	Mises à jour régulières	☒	Mises à jour aléatoires
Interface	✓	Interface graphique	☒	Pas de suivi graphique sur la plupart des outils gratuits
Support client	✓	Support client	☒	Pas de support client
Service d'aide	✓	Services d'aide (enquête, technique.)	☒	Plutôt absence de tels services
Coût	✓	Plutôt gratuit par nature	☒	Coût élevé et couteux dans la mise en place (incluant souscription, personnalisation, intégration et support client complémentaire)
Fiabilité des données	✓	Fiabilité et précision élevées		
	✓	Fiabilité progressive des données des explorateurs de block		
Souveraineté des données	✓	Données en source ouverte et vérifiables par tout le monde	☒	Outil non souverain (données collectées par l'opérateur et à l'étranger, souvent aux Etats-Unis)



RENSEIGNEMENT DE SOURCES LIBRES

L'enquête ne peut se limiter aux seules données dans la chaîne. De nombreuses informations complémentaires, appelées métadonnées, sont essentielles pour enrichir l'analyse. Certaines sont collectées par les OAT qui les rendent exploitables via leurs interfaces. D'autres peuvent être obtenues en opérant un ou plusieurs nœuds du réseau P2P sous-jacent à la chaîne de blocs (voir p.18).

Ces données peuvent être croisées avec des attaques sur les réseaux d'anonymisation (comme TOR) ou à travers des demandes d'information adressées aux fournisseurs de réseaux privés virtuels (VPN), que les criminels utilisent quasi systématiquement.

Par ailleurs, les services spécialisés dans la lutte contre la cybercriminalité utilisent également des techniques comme le renseignement des sources libres (OSINT) et le regroupement ou clustering (technique d'analyse de données qui consiste à regrouper des ensembles d'objets similaires) afin d'identifier les utilisateurs derrière des portefeuilles pseudonymes. Ces méthodes sont particulièrement utiles lorsqu'il s'agit de reconstituer des chaînes de détention volontairement brouillées – par exemple, via des mixeurs ou le passage par des plateformes d'échange.

Un exemple concret d'analyse croisée des données en source libre et des données accessibles dans la chaîne consiste à exploiter la présence de noms ENS (Ethereum Name Service) sur les réseaux sociaux. De nombreux comptes Twitter mentionnent leur adresse ENS, ce qui permet, en recoupant les données issues de Twitter avec les transactions associées à ces adresses sur la chaîne de blocs, de faire émerger des pistes d'attribution voire d'identifier les bénéficiaires effectifs de certaines transactions.

ENS: Ethereum Name Service

Les noms de domaines sont gérés par des organisations centralisés, souvent étatiques (e.g. l'AFNIC en France pour gerer les domaines .fr).

A l'inverse l'ENS est un système de DeFi sur la chaîne de blocs Ethereum, qui permet d'attribuer des domaines (qui finissent en.eth) de manière autonome de toute autorité centrale.

De la même manière, certains malfaiteurs cherchent à transférer leur réputation d'une plateforme à l'autre en réutilisant un même pseudonyme ou une variation identifiable. Cette pratique est particulièrement répandue sur les places de marché de l'Internet clandestin. L'analyse croisée de ces alias peut permettre d'établir des liens entre plusieurs identités numériques, de cartographier des réseaux criminels, voire d'attribuer des activités à un même individu ou groupe.

LE REGROUPEMENT

L'une des plus importantes plus-values des outils d'analyse transactionnelle, au-delà de leur interface graphique intuitive, réside dans leur capacité à regrouper automatiquement les adresses contrôlées par une même entité.

Sur les chaînes de blocs reposant sur le modèle UTXO (comme Bitcoin et ses dérivés – voir encart), chaque transaction comporte une ou plusieurs sorties destinées au bénéficiaire, mais inclut souvent également une adresse de « change » , vers laquelle l'émetteur redirige le solde restant. Cette adresse, également contrôlée par l'émetteur, permet de récupérer l'excédent de la transaction

La capacité à identifier correctement l'adresse de change constitue une étape déterminante pour regrouper, avec un haut degré de probabilité, les adresses appartenant à un même utilisateur. Ce processus repose sur des techniques heuristiques, c'est-à-dire des règles d'analyse fondées sur des schémas de comportement typiques.

Certaines de ces techniques heuristiques, bien établies et considérées comme fiables, sont intégrées aux solutions commerciales. D'autres, plus incertaines, peuvent néanmoins s'avérer pertinentes lorsqu'elles sont croisées avec d'autres sources ou indices, permettant ainsi de suivre les flux avec un niveau de confiance élevé, même dans des situations complexes.

Cette approche constitue la base du regroupement, une technique d'analyse fondamentale permettant de réduire considérablement la complexité des graphes de transaction. Elle facilite la reconstitution des trajectoires de fonds et l'identification des acteurs impliqués.

Il convient toutefois de noter que les fournisseurs de solutions commerciales ne publient pas les heuristiques du regroupement qu'ils utilisent, à la fois pour préserver leur avantage concurrentiel et pour éviter que des contremesures ne soient mises en place. Ce manque de transparence peut poser des problèmes en matière de preuve numérique, notamment dans un cadre pénal, si la validité de l'analyse est contestée.

Ce type d'analyse requiert donc une expertise technique poussée. Il est essentiel que les enquêteurs spécialisés soient formés à mobiliser ces heuristiques et capables, lorsque nécessaire, d'aller au-delà des capacités des outils commerciaux standard.

UTXO le modèle des transactions Bitcoin

Contrairement à Ethereum, Bitcoin n'utilise pas un système de compte avec un solde unique, comme un compte en banque. Au lieu de cela, il repose sur un modèle appelé UTXO (Unspent Transaction Output, ou « sortie de transaction non dépensée »).

Dans ce système, chaque transaction est composée :

- reçoit d'une ou plusieurs anciennes transactions,
- de sorties : les fonds que l'on envoie à une ou plusieurs adresses.

Les entrées doivent être entièrement dépensées dans une nouvelle transaction. Il n'est donc pas possible d'en dépenser une partie seulement. Lorsqu'un montant reçu dépasse la somme à transférer, la transaction doit comporter :

- une sortie vers le destinataire,
- une autre sortie vers une adresse contrôlée par l'expéditeur (souvent appelée adresse de « change»).

La différence entre le montant total des entrées et celui des sorties correspond aux frais de transaction payés aux mineurs.

L'IDENTIFICATION DES PLATE-FORMES D'ECHANGE

Un autre atout majeur des OAT réside dans leur base de données très étendue d'adresses associées à des plateformes d'échange.

Une technique d'enquête cruciale consiste à identifier, le plus tôt possible, les flux financiers entrant ou sortant d'un échangeur régulé. Lorsqu'un tel lien est établi, la plateforme concernée peut - selon le cadre juridique applicable – procéder à un gel des fonds, ou transmettre aux autorités compétentes des informations d'identification sur le titulaire du portefeuille (données *KYC*, historiques de transaction, adresses IP, etc.).

Toutefois, du seul point de vue des données accessibles dans la chaîne, rien ne permet de distinguer à priori une adresse créée par un utilisateur lambda de celle d'un échangeur centralisé (les motifs d'usage seront extrêmement différents). Il est donc très important d'arriver à identifier les adresses des échangeurs.

Les explorateurs de blocs publics référencent certaines de ces adresses, mais les OAT les plus avancés vont plus loin : ce sont désormais les plateformes régulées elles-mêmes qui communiquent directement leurs plages d'adresses aux OAT.

Impact, perspectives et orientations futures pour les CRF

L'émergence des crypto-actifs a profondément transformé l'environnement opérationnel des cellules de renseignement financier (CRF), en introduisant de nouveaux défis réglementaires, technologiques et humains. Ces enjeux nécessitent une révision continue des pratiques, des outils et des partenariats des CRF, afin de leur permettre de répondre efficacement à des menaces financières en constante évolution.

Un premier défi majeur a été d'obtenir l'assujettissement des plateformes d'échange à la législation LCB/FT. En France, cela s'est matérialisé dès 2019 par l'introduction du régime des prestataires de services sur crypto-actifs, suivi à l'échelle européenne par l'entrée en vigueur du règlement MiCA et la création du statut de PSCA. Ce cadre harmonisé constitue une avancée significative vers une meilleure supervision du secteur.

Un second enjeu, plus structurel, a consisté à amener ces acteurs à se faire agréer, à se conformer aux obligations réglementaires et à transmettre des déclarations de soupçon de qualité. Cet objectif s'est heurté à deux obstacles principaux :

- d'une part, l'absence de culture de conformité dans un secteur techniquement accessible sans autorisation préalable ;
- d'autre part, une idéologie fondatrice – le courant *cypherpunk* – historiquement hostile à toute forme de surveillance institutionnelle.

WSi ces résistances ont été partiellement levées dans l'Union européenne, certaines plateformes ont longtemps appliqué des procédures de *KYC* minimalistes, voire dissimulé leur localisation afin d'échapper aux régulateurs. Dans de nombreuses juridictions encore dépourvues de cadre spécifique, ces difficultés perdurent, entravant la capacité des CRF à collecter et exploiter efficacement les données financières.

Malgré les avancées réglementaires, les CRF doivent encore surmonter d'importants défis opérationnels. Elles dépendent largement d'outils commerciaux d'analyse de la chaîne de blocs, souvent coûteux et développés par des entreprises étrangères, ce qui soulève des préoccupations en matière de souveraineté et de sécurité. Par ailleurs, la spécialisation nécessaire à l'analyse des flux crypto exige des compétences rares et très recherchées, ce qui complique les efforts de recrutement, de formation et de fidélisation.

DEVELOPPEMENT DE L'ECO-SYSTEME CRYPTO

Évolution de l'environnement opérationnel des CRF

La part des transactions illicites dans les transactions en crypto-actifs tendrait à diminuer, mais la valeur absolue continue de croître. L'harmonisation de la règlementation européenne impose aux prestataires la collecte des données d'identification de leurs clients, et la forte concentration du marché conduit mécaniquement l'immense majorité d'entre eux à se conformer à ces exigences. Par ailleurs, la nature infalsifiable et pérenne du registre des transactions permet de conserver une trace publique exploitable de l'ensemble des flux, et l'offre commerciale d'outils permettant d'en tirer parti se développe rapidement.

La vision westphalienne de la souveraineté de l'état sur son territoire [15], trouve dans la chaîne de blocs et particulièrement dans la DeFi un contre-exemple définitif (voir encart Tornado Cash pour un exemple parlant, p. 23), où se réfugient en masse les utilisateurs chassés des plateformes régulées par l'obligation de *KYC*. Les paradis fiscaux et juridictions non conformes abritent également de nombreux opérateurs, qui échappent ainsi aux obligations réglementaires.

Les projets techniques portés par la chaîne de blocs se multiplient et se complexifient, tandis que l'information technique fiable à leur sujet demeure difficile à identifier et à interpréter. Cette difficulté est accentuée par le caractère intrinsèquement éphémère de cette information, en raison du rythme accéléré d'évolution des technologies.

Défis dans la collecte et l'exploitation des données

Les CRF peuvent difficilement faire l'impasse sur la dotation en outils d'analyse transactionnelle de la chaîne de blocs. Malheureusement ces outils sont coûteux, et surtout ne sont pas souverains, entraînant une dépendance forte et préoccupante à l'égard d'un petit nombre d'acteurs commerciaux, dont les allégeances sont parfois suspectées d'être liées aux services de renseignement des pays dans lesquels ils sont implantés. Il semble urgent que les Etats européens se dotent d'un outil souverain. Toutefois, cette ambition se heurte à de nombreuses difficultés dont parfois une absence de volonté politique, liée en grande partie à une mécompréhension persistante de la nature des chaînes de blocs au sein des plus hauts niveaux de l'exécutif.

Par ailleurs, il est complexe pour les CRF de profiter des saisies de données opérées par les forces de l'ordre. Ces saisies, par exemple celles de l'échangeur BTC-E à la fin des années 2010, permettent souvent de détricoter les transactions des mixeurs, permettant la résolution d'affaires en cascade, et portant des coups sévères à l'écosystème crapuleux. Il faudrait permettre davantage de coopération en ce sens. Les données d'enquêtes crypto partagées par les forces de l'ordre au niveau européen via la plateforme SIENA de l'Europol pourraient ainsi être d'une grande aide aux CRF.

Partenariats publics privés

La DeFi dans sa forme la plus pure restera, par essence, hors de portée des juridictions étatiques. La migration progressive des flux de blanchiment vers des opérateurs de la DeFi démontre l'efficacité de l'harmonisation européenne naissante de la réglementation. Néanmoins, des efforts supplémentaires peuvent et doivent être déployés pour accentuer cette pression sur les vecteurs centralisés encore accessibles.

Il est notamment crucial de fluidifier et d'accélérer les procédures de gels d'avoirs, en identifiant les interlocuteurs en mesure de les réaliser techniquement chez les échangeurs assujettis ou les opérateurs de crypto-actifs stables. Pour garantir une réelle efficacité, le délai entre la détection d'un flux criminel et l'exécution d'un gel devrait idéalement être réduit à quelques heures, voire quelques minutes, contre plusieurs jours – voire semaines – actuellement.

Par ailleurs, les CRF pourraient bénéficier d'un réseau de renseignement intégré incluant des contributions du secteur privé, dans une logique de co-construction et de mutualisation de l'intelligence financière.

Évolution du signalement et du partage d'information

Le volume des déclarations de soupçon liées aux crypto-actifs en Europe est en hausse constante. Toutefois, leur qualité reste hétérogène : les informations sont trop souvent peu normalisées, parfois incomplètes ou mal renseignées, ce qui en limite considérablement l'exploitation. Leur pertinence varie également en fonction des déclarants.

Les données transmises par les PSCA sont fréquemment mal calibrées, oscillant entre une granularité excessive et des déclarations trop lacunaires. Une meilleure formation des assujettis est donc indispensable pour renforcer leur capacité à détecter et signaler efficacement les comportements suspects.

La normalisation de ces déclarations au niveau européen, ainsi que l'utilisation d'un format commun pour le requêtage et le partage entre CRF sont des étapes indispensables à une coopération efficace. Cependant, il ne faut pas que cette normalisation se fasse au détriment des pratiques basées sur l'expérience mises en place par les CRF les plus avancées dans le domaine des crypto-actifs.

Détection automatique et détection de l'IA

Des outils d'apprentissage statistique peuvent être utilement déployés à partir des données chaîne de blocs brutes, des déclarations de soupçon, ou directement chez les opérateurs. Ce dernier cas

nécessite toutefois majoritairement l'établissement de partenariats publics-privés, ainsi qu'une définition claire des comportements cibles à détecter. Ces outils permettent de générer automatiquement des alertes sur la base de typologies de blanchiment connues.

Par ailleurs, les assujettis doivent se doter de solutions capables d'identifier les faux justificatifs d'identité générés par l'intelligence artificielle, de plus en plus crédibles, et déclencher en conséquence des signalements automatisés.

Formation, triage et priorisation

exhaustives, nettoyées et exploitables, et d'outils performants, l'ampleur du phénomène impose de gérer avec rigueur la contrainte humaine.

Il est essentiel de poursuivre et d'intensifier les efforts de formation des enquêteurs et de leurs équipes de soutien, tout en favorisant le recrutement ou la spécialisation interne d'agents sur les questions liées aux crypto-actifs. En parallèle, il convient de mettre en place des mécanismes de tri et de priorisation des cas à traiter, fondés sur des objectifs clairs et mesurables, afin de maximiser l'impact opérationnel des ressources disponibles.

RENFORCEMENT DU CADRE LCB/FT EUROPEEN

L'adoption du règlement MiCA constitue une étape clé dans la structuration du marché des crypto-actifs au sein de l'Union européenne. Ce cadre harmonisé encadre désormais les émetteurs de crypto-actifs, les PSCA et les marchés, en fixant des exigences en matière de transparence, de gouvernance et de protection des consommateurs.

Parallèlement, l'extension de la *Travel Rule* (la règle de voyage impliquant la transmission des informations relatives aux donneurs d'ordre et bénéficiaires) aux transferts de crypto-actifs renforce la traçabilité des transactions et la capacité des autorités compétentes à détecter les flux suspects.

Ces instruments sont complémentaires et visent à adapter l'arsenal LCB/FT aux spécificités du *Web3* (version décentralisée d'Internet basée sur la chaîne de blocs).

Toutefois, les applications décentralisées notamment restent à ce jour en dehors du champ de MiCA. La Commission européenne devra évaluer, dans les années à venir, l'opportunité de développer une régulation adaptée à ces nouveaux modèles. Contrairement à l'approche européenne, qui tend à envisager un cadre général de régulation de la DeFi (à définir : sur mesure, modulaire, ad hoc ou sectoriel), les autorités américaines privilégient une régulation au cas par cas, souvent par voie contentieuse.

Les méthodes traditionnelles de conformité – fondées sur l'identification d'un responsable juridique, la surveillance centralisée et des obligations ex ante – apparaissent mal adaptées aux architectures décentralisées. Une régulation efficace de la DeFi devra donc tenir compte de plusieurs paramètres :

- la nécessité d'une souplesse législative permettant d'anticiper l'évolution technologique ;
- la focalisation sur les interfaces utilisateurs et les opérations économiques, plutôt que sur le code lui-même ou les technologies et leur développement ;
- des mécanismes de gestion des risques couvrant les questions de gouvernance, de sécurité informatique, d'infrastructures, de services et d'oracles ;
- la mise en place éventuelle d'un système de certification ou d'enregistrement volontaire pour les protocoles à vocation financière.

Par ailleurs, la création de l'Autorité européenne de lutte contre le blanchiment de capitaux et le financement du terrorisme (AMLA) constitue une autre avancée décisive. Dotée d'un mandat supranational, capitaux et le financement du terrorisme (AMLA) constitue une autre avancée décisive.

Dotée d'un mandat supranational, cette autorité indépendante sera chargée de garantir l'application cohérente des règles LCB/FT à travers l'Union et jouera un rôle central dans la coordination des CRF et des superviseurs nationaux. Elle contribuera également à faciliter la coopération transfrontalière et à superviser directement certains acteurs à haut risque, y compris ceux opérant dans le secteur des crypto-actifs.

RENFORCEMENT DE LA COOPERATION AVEC LES PRESTATAIRES DE SERVICES SUR CRYPTO-ACTIFS

Au-delà des outils juridiques et institutionnels, le renforcement de la coopération avec les prestataires de services sur crypto-actifs constitue un pilier fondamental pour une lutte efficace contre le BC/FT. La sensibilisation de ces acteurs aux typologies de blanchiment, aux méthodes de fraude fiscale et aux attentes des CRF vise à améliorer la qualité et la pertinence des déclarations de soupçon, tout en facilitant l'établissement d'un dialogue constructif avec le secteur privé.

Cette coopération est d'autant plus essentielle que de nombreuses professions assujetties disposent encore d'une marge de progression importante dans leur compréhension des risques liés aux crypto-actifs. Certaines institutions financières éprouvent des difficultés à identifier les opérations associées à ces actifs dans leurs propres systèmes, notamment dans les cas où :

- un client alimente un compte ouvert auprès d'un PSCA via une carte bancaire ;
- un virement bancaire est effectué à destination d'un PSCA, parfois via un prestataire de paiement tiers intercalé entre la banque et la plateforme.

Ce manque de visibilité rend difficile la détection des flux liés aux crypto-actifs et nuit à la qualité des dispositifs de vigilance.

Cependant, on observe l'émergence de prestataires spécialisés dans les services de paiement à destination de l'industrie crypto, comme ceux fournissant des IBAN virtuels à des PSCA. L'identification de ces acteurs, et l'établissement de canaux de coopération spécifiques avec eux, peut constituer un levier opérationnel précieux pour renforcer la chaîne de détection et de signalement.

LA COOPERATION INTERNATIONALE : UN IMPERATIF FACE AUX ENJEUX CRYPTO EN MATIERE DE BC/FT

En matière de coopération internationale, l'un des principaux défis réside dans la difficulté de rattacher des flux en crypto-actifs à une juridiction précise.

Contrairement à un compte bancaire, qui est intrinsèquement lié à une juridiction - celle ayant délivré la licence à l'établissement teneur du compte – une adresse en crypto-actifs, visible sur une chaîne de blocs, peut être associée à n'importe quel pays. Cette problématique se pose même dans le cas d'adresses liées à des plateformes d'échange ou, plus largement, à des entités réglementées. En effet, si des enquêteurs parviennent à établir un lien entre une infraction et un prestataire de services sur crypto-actifs, mais que ce dernier dispose d'autorisations d'exercice dans plusieurs juridictions, il ne sera pas évident de déterminer à quelle CRF partenaire s'adresser en priorité.

Cette complexité est accentuée par le fait que le siège ou le lieu d'implantation de certaines plateformes reste parfois flou ou volontairement obscurci.

Dans ce contexte, la coopération internationale joue un rôle essentiel pour permettre une réponse coordonnée à ces enjeux. Elle pourrait notamment favoriser un échange systématique d'informations sur les juridictions d'établissement des principaux acteurs du secteur et sur leur périmètre d'activité réglementée.

La nature transfrontalière des crypto-actifs exige en effet une coopération renforcée entre les CRF. À l'échelle européenne, cette coopération prend désormais une forme plus structurée, grâce au nouveau cadre réglementaire en matière de LCB/FT, qui vise à renforcer la collaboration entre États membres tout en intégrant les spécificités propres aux crypto-actifs. Cette coordination est d'autant plus cruciale que les flux financiers associés à ces actifs dépassent très largement les frontières nationales.

Des goulots d'étranglement techniques

L'échange de renseignements, l'accès à une expertise technique spécialisée et le partage d'expériences entre CRF sont des éléments essentiels pour suivre l'évolution rapide des typologies de BC/FT impliquant les crypto-actifs. Pourtant, plusieurs obstacles techniques entravent encore cette coopération.

L'un des problèmes majeurs tient à l'hétérogénéité des formats dans lesquels les informations relatives aux crypto-actifs sont reçues. À ce jour, une minorité des entités déclarantes utilisent les systèmes de déclaration numérique mis en place par les CRF. Dans de nombreux cas, les déclarations sont encore transmises par email, voire sur support papier, ce qui complique leur traitement, nuit à l'exploitabilité des données et freine les capacités d'analyse automatisée.

Ce manque d'uniformisation freine également l'interopérabilité entre les CRF, limite les possibilités de croisement d'informations transfrontalières, et nuit à la réactivité dans le traitement des flux financiers suspects. Des efforts accrus en matière de normalisation des formats, d'outillage technique et d'investissement dans des solutions d'analyse avancée sont nécessaires pour remédier à ces goulots d'étranglement.

Les attaques étatiques

La menace ne provient pas uniquement de groupes criminels ou d'acteurs privés. Certains États ou entités soutenues par des gouvernements adoptent des comportements activement hostiles à l'ordre financier international.

Le piratage de la plateforme Bybit attribué à des acteurs affiliés à la Corée du Nord [16], ainsi que l'utilisation de certaines plateformes russes comme véritables blanchisseries d'actifs numériques [17], illustrent cette évolution inquiétante. Ces activités ne relèvent pas seulement d'une absence de coopération, mais d'une stratégie délibérée visant à financer des activités illicites – comme les programmes de développement d'armes – ou à contourner les sanctions internationales.

Face à cette réalité, les CRF et les autorités compétentes doivent adapter leur posture en considérant que certains risques relèvent de la menace étatique. Cela suppose un renforcement de la coordination internationale, un soutien aux mécanismes de cyberdéfense financière, et une vigilance accrue dans l'identification des flux crypto associés à des acteurs étatiques hostiles.

CONCLUSION

L'écosystème de la finance décentralisée évolue rapidement et présente une complexité technique qui rend sa régulation particulièrement difficile. Alors que certains acteurs centralisés peuvent être soumis à des contrôles et contraintes réglementaires, les contrats intelligents – autonomes et incensurables – échappent en grande partie à toute forme de contrôle traditionnel. La maîtrise de ces systèmes exige des compétences pointues, ce qui confère un avantage aux groupes criminels sophistiqués, tandis que les autorités peinent à imposer des mesures de conformité efficaces, renforçant ainsi les défis liés à la surveillance et au contrôle de cet univers financier en constante mutation.

Dans ce contexte mouvant, les CRF se retrouvent confrontées à une multitude de défis à la fois technologiques, organisationnels et humains. L'accès aux données pertinentes, leur interprétation, la

formation des agents, le développement d'outils souverains ou encore la coopération avec les prestataires de services sur crypto-actifs deviennent autant d'exigences incontournables. La qualité des déclarations de soupçon, la capacité à exploiter les signaux faibles issus des chaînes de blocs et l'aptitude à agir rapidement pour geler des avoirs sont autant de facteurs déterminants pour garantir l'efficacité de la lutte contre les flux financiers illicites. Ces exigences imposent une transformation profonde des méthodes de travail des CRF, une densification de leurs partenariats – publics comme privés – et une reconnaissance claire de leur rôle stratégique dans l'écosystème de sécurité financière.

Face à l'ampleur et à la nature transnationale des menaces, l'avenir de la lutte contre le blanchiment de capitaux et le financement du terrorisme liés aux crypto-actifs repose sur une intensification de la coopération entre CRF, au niveau européen comme international. L'uniformisation des formats d'échange, le partage d'expertises techniques, la réponse coordonnée aux menaces étatiques ou l'accès mutualisé à des outils performants sont des leviers essentiels pour faire face collectivement à des flux financiers qui ignorent les frontières. Si des progrès notables ont été réalisés, notamment grâce au cadre MiCA et à la montée en puissance de l'AMLA, la consolidation de cette architecture reste tributaire d'une volonté politique forte et d'un investissement soutenu. Car seule une mobilisation durable permettra de préserver l'intégrité du système financier face aux mutations profondes introduites par les technologies chaîne de blocs.

Annexes

GLOSSARY

Attaques par déni de service distribué *(DDoS)*: attaque informatique visant à rendre un site web, un serveur ou un réseau indisponible en surchargeant leur capacité avec une quantité massive de trafic provenant de multiples sources. L'objectif est de saturer le serveur cible pour qu'il ne puisse plus répondre aux requêtes légitimes, ce qui rend le service inaccessible. Les échanges de cryptomonnaies sont particulièrement vulnérables aux attaques DDoS, car ils sont souvent les cibles privilégiées des pirates qui cherchent à voler des fonds ou à perturber le marché.

L'abattage du cochon / *Pig butchering*: Il s'agit d'un type de fraude à l'investissement (arnaque) où les escrocs créent une fausse identité pour tromper et attirer leurs victimes en ligne. Ils utilisent des techniques d'ingénierie sociale, l'intelligence artificielle et la technologie pour gagner la confiance des gens, manipuler les émotions et exploiter leurs vulnérabilités financières afin de dérober de l'argent.

Chaîne de blocs / *Blockchain*: Une chaîne de blocs est un registre distribué décentralisé qui conserve les blocs et leurs enregistrements en mode chronologique ajout uniquement. Le nouveau bloc faisant référence au bloc précédent (hash) est ajouté à la chaîne de blocs par consensus entre les nœuds. Inventée en 1991 par Haber et Stornetta, elle constitue la technologie sur laquelle reposent les crypto-actifs. L'historique du registre est immuable (impossible à modifier ou falsifier), visible et de source libre.

Contrat intelligent / *Smart Contract*: Un contrat intelligent est un programme informatique ou un accord d'opérations avec des actions codées stocké sur une chaîne de blocs qui est exécuté de façon automatique sans l'intervention d'un tiers lorsque les clauses du contrat ou un ensemble de conditions établies par les parties sont remplies.

Crypto-actif / *Crypto-asset*: Un crypto-actif est un actif numérique sécurisé par cryptographie et enregistré sur une chaîne de blocs et où les transactions sont distribuées et validées par des participants décentralisés, notamment des crypto-monnaies, des jetons non-fongibles, des cryptomonnaies stables et des jetons de sécurité.

Crypto-actifs confidentiels / *Privacy coins*: Un type de crypto-actif qui ne divulgue pas publiquement la totalité ou la plupart des détails des opérations, en masquant les flux des opérations, les expéditeurs, les destinataires, les montants et les soldes des comptes.

Crypto-actif stable / *Stablecoin*: Crypto-actifs conçus pour maintenir une parité avec une valeur de référence par une garantie (une monnaie fiduciaire telle que le dollar en USDC ou des crypto-actifs comme le DAI) ou sans garantie par autorégulation (AMPL et ESD).

Dans la chaîne / *On-chain*: « Dans la chaîne » désigne l'état des transactions enregistrées sur la chaîne de blocs, vérifiées et authentifiées, ce qui les rend immuables et permanentes. En revanche, les transactions hors chaîne se produisent en dehors de la chaîne de blocs principale et peuvent présenter des failles de sécurité.

Dépositaire / non-dépositaire / *Custodial* / *non-custodial*: Un service dépositaire est celui dans lequel un portefeuille conserve et stocke les clés privées des clients afin d'éviter leur vol ou leur perte, en autorisant l'accès via un identifiant et un mot de passe. Il offre également sécurité et sauvegarde des actifs des utilisateurs. Les plateformes d'échange centralisées de cryptomonnaies sont un type courant de service de garde.

L'utilisation et la gestion non-dépositaires correspondent généralement au contexte dans lequel l'utilisateur est directement propriétaire et gestionnaire des clés privées, sans l'aide d'un prestataire tiers.

Echange / *Swapping* : Le processus par lequel les utilisateurs échangent un jeton contre un autre.

Empiler / Staking : Le fait d'empiler des crypto-actifs consiste à bloquer ou à détenir une certaine quantité de crypto-actifs pour participer à la validation des transactions sur un réseau de chaîne de blocs avec un effet de récompense. Cette quantité peut être « supprimée » (« brûlée » et mise hors circulation) en cas de comportement malveillant de leur validateur ou de non-respect des exigences de performance.

Hypertrucage / *Deepfake* : Il s'agit de contenus vidéo, audio et autres contenus trompeurs manipulés par l'intelligence artificielle pour usurper l'identité de personnes et d'événements. Grâce à leur capacité à se substituer à l'apparence et à la voix d'une personne, ils constituent un potentiel d'utilisation abusive pour diffuser de la désinformation et des fausses nouvelles, commettre des fraudes et d'autres activités malveillantes telles que le vol de propriété intellectuelle, les atteintes à la vie privée, l'usurpation d'identité et autres.

Internet clandestin / *Darknet* : Internet clandestin est une partie d'Internet non indexée par les moteurs de recherche et dont l'accès nécessite l'utilisation de navigateurs anonymisants (identité et localisation) comme Tor. La plupart des places de marché de l'Internet clandestin effectuent des transactions en Bitcoin ou autres crypto-actifs.

Jeton / *Token* : Un jeton est construit sur une chaîne de blocs existante et sert à représenter un intérêt dans un actif et à faciliter les opérations sur la chaîne de blocs. Les jetons de la chaîne de blocs incluent les jetons de récompense, d'utilité, de sécurité, de gouvernance et d'actifs. Cependant, ils se distinguent de l'actif natif, qui est le crypto-actif créé par le protocole et utilisé pour payer les frais. Un crypto-actif possède sa propre chaîne de blocs et constitue son actif natif, le crypto-actif le plus populaire étant le Bitcoin.

Jeton non fongible / *Non-fungible token* : Un jeton non fongible est un crypto-actif unique qui n'est pas interchangeable avec un autre pour diverses raisons telles que la qualité, la valeur ou d'autres caractéristiques. En revanche, les crypto-actifs sont fongibles par nature.

Mixeur / *Mixer* : Service qui mélange les crypto-actifs provenant de divers utilisateurs afin d'en brouiller l'origine et le propriétaire des fonds.

Oracle : Dans l'écosystème des crypto-actifs et de la chaîne de blocs, un oracle est un agent ou un service tiers qui achemine des données externes vers une chaîne de blocs ou des contrats intelligents. Ces entités intermédiaires sont nécessaires car les chaînes de blocs ne peuvent pas accéder aux données extérieures de manière native en raison de leur conception sécurisée et décentralisée.

La pêche au harpon / *Spear Fishing* : La soi-disante « pêche au harpon » est une attaque d'hameçonnage ciblée qui incite la personne intéressée à cliquer sur un lien malveillant dans un courriel.

Perte de parité / *Depeg* : Une perte de parité est un phénomène qui se produit lorsqu'un crypto-actif stable, dont la valeur est indexée sur une autre devise, diminue ou augmente en valeur par rapport à l'actif auquel il est indexé.

Piratage / *hacking* : Tentative illégale d'accéder à des portefeuilles de crypto-actifs ou à des échanges de crypto-actifs pour détourner des fonds.

Pont / *Bridge* : Outil conçu pour transférer des crypto-actifs et des données entre chaînes de blocs sans intervention d'un tiers (de façon unidirectionnelle ou bidirectionnelle).

Pont inter-chaînes / *Cross-chain* : Il s'agit de l'interconnexion de deux ou plusieurs chaînes de blocs totalement distinctes pour permettre l'échange d'informations et de données. Parmi les différents cas d'utilisation, on peut citer le transfert d'actifs via des ponts inter-chaînes, des oracles inter-chaînes et des contrats intelligents inter-chaînes.

Portefeuille / *Wallet* : Un portefeuille est une application permettant de générer, gérer, stocker ou utiliser des clés cryptographiques privées et publiques. Un portefeuille peut être logiciel ou matériel et peut être utilisé en ligne (portefeuille chaud) ou hors ligne (portefeuille froid). Un portefeuille hébergé est géré par un tiers sous contrat, tandis qu'un portefeuille non hébergé (ou auto-hébergé) est géré par les utilisateurs eux-mêmes.

Pratique des « achetés-vendus » / *Wash Trading* : Une forme de manipulation du marché (de cours) dans laquelle les investisseurs créent une activité artificielle sur le marché en vendant et en achetant simultanément les mêmes crypto-actifs.

Prêt éclair / *Flash loan* : Le prêt éclair permet d'emprunter auprès d'un pool de contrats intelligents sans fournir de garantie. Le prêt n'est valable que pour une opération Ethereum et est remboursé à son terme ou ramené à son statut initial. Sans risque de contrepartie pour le prêteur et sans durée, les prêts éclair sont principalement utilisés pour le refinancement et l'arbitrage.

Preuve à Divulgation Nulle de Connaissance / *Zero-Knowledge Proof* : protocole permettant à un utilisateur de prouver qu'une situation est réelle sans avoir à révéler d'information relative à cette dernière. Il s'agirait par exemple pour une personne de prouver son identité sans avoir à la révéler.

Règle de voyage / *Travel Rule* : La règle de voyage exige que les PSCA obtiennent, conservent et échangent des informations sur les initiateurs (expéditeurs) et les bénéficiaires (destinataires) des opérations en crypto-actifs initiées par leurs utilisateurs dès que le montant dépasse un certain montant. Cependant, cette règle ne s'applique qu'aux opérations impliquant un PSCA ou une autre entité soumise à la LCB/FT et ne s'applique pas explicitement aux opérations pair-à-pair non médiatisées via des portefeuilles non hébergés.

Regroupement / *Clustering* : Technique d'analyse de données qui consiste à regrouper des ensembles d'objets similaires. L'objectif principal est de segmenter un ensemble de données en sous-groupes appelés clusters, où les objets au sein d'un même cluster partagent des caractéristiques communes. Ainsi, le clustering permet de relier plusieurs portefeuilles cryptographiques à une seule entité.

Renseignement de source libre / *Open Source Intelligence* : L'OSINT dans l'écosystème des crypto-actifs est une branche des techniques et outils de source libre qui permettent d'enquêter sur les crypto-actifs et leurs opérations entre les adresses en identifiant et en traçant les modèles d'activité suspects.

Réseau privé virtuel / *Virtual Private Network* : Un réseau privé virtuel est une technologie qui crée un réseau sécurisé et crypté à partir d'une connexion Internet publique, offrant anonymat et confidentialité (comme le masquage de l'activité de navigation, de l'identité et de l'emplacement/IP).

Retrait de tapis / *Rug Pull* : A l'instar d'un schéma de Ponzi traditionnel, il s'agit d'une fraude dans laquelle les créateurs d'un jeton, après avoir levé des fonds par une série de stratagèmes frauduleux, disparaissent avec les fonds de leurs investisseurs, retirant ainsi le tapis sous les pieds des investisseurs.

Saut de chaîne / *Chain-hopping* : Processus de conversions successives de différents crypto-actifs par l'envoi des fonds d'une chaîne de bloc à l'autre pour masquer leurs flux financiers illicites, souvent via des ponts, des échanges décentralisés (DEX) ou des protocoles d'échange.

Sortie de transaction non dépensée / *Unspent Transaction Output (UTXO)* : terme utilisé pour décrire une sortie de transaction non dépensée. Toutes les chaînes de blocs n'utilisent pas le système UTXO mais c'est le cas de Bitcoin notamment. Sur ce dernier, chaque transaction est composée d'une ou plusieurs entrées et sorties, chaque entrée étant la sortie d'une autre transaction, hormis pour

le cas très spécifique de la création des nouveaux bitcoins à chaque bloc.

Service d'appellation Ethereum / *Ethereum Name Service* : Il s'agit d'un système de dénomination décentralisé, ouvert et extensible pour améliorer la facilité et la précision des transactions au sein de la chaîne de blocks Ethereum qui remplace les adresses de portefeuille longues et complexes (longue chaîne de chiffres et de lettres) par des noms simples, conviviaux et mémorables (par exemple kathe.eth).

Technologie de registre distribué / *Distributed Ledger Technologies (DLT)* : Une technologie de registre distribué est simplement une base de données décentralisée gérée par plusieurs participants. Elle enregistre l'historique des transactions sur des nœuds de manière décentralisée. Chaque nœud valide et enregistre les transactions simultanément. Les enregistrements ont chacun un horodatage unique et doivent faire l'objet d'une signature cryptographique, gage de la sécurité et de l'incorruptibilité du réseau. Une chaîne de blocs, ou *blockchain*, est un type particulier de DLT.

BIBLIOGRAPHIE

1. ONUDC (Office des Nations unies contre la drogue et le crime), Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes, ONUDC, Vienne, 2011 : www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf, consulté le 10 juin 2025.
2. Abdelhak El Idrissi, « La chute de Dark Bank, le « banquier » du crime organisé qui aurait aidé à blanchir plus de 1 milliard d'euros », Le Monde : www.lemonde.fr/les-decodeurs/article/2025/01/10/la-chute-de-dark-bank-le-banquier-du-crime-organise-qui-aurait-aide-a-blanchir-plus-d-un-milliard-d-euros_6490703_4355770.html, janvier 2025, consulté le 10 juin 2025.
3. Stephen Katte, « Crypto : Des « dark stablecoins » pourraient émerger face au durcissement des régulations », Cointelegraph : https://fr.cointelegraph.com/news/regulations-spark-censorship-resistant-dark-stablecoins, mai 2025, consulté le 10 juin 2025.
4. Anna Hirtenstein et Chen Aizhu, « Russia leans on cryptocurrencies for oil trade, sources say», Reuters : www.reuters.com/business/energy/russia-leans-cryptocurrencies-oil-trade-sources-say-2025-03-14/, mars 2025, consulté le 10 juin 2025.
5. Chainalysis, The Chainalysis 2025 Crypto Crime Report, Chainalysis, 2025 : www.chainalysis.com/blog/2025-crypto-crime-report-introduction/, consulté le 10 juin 2025.
6. Timothy G. Massad, « Stablecoins et sécurité nationale : tirer les leçons des eurodollars », Brookings.edu : www.brookings.edu/articles/stablecoins-and-national-security-learning-the-lessons-of-eurodollars/, avril 2025, consulté le 10 juin 2025.
7. TRM Labs (2025), 2025 Crypto Crime Report. Key trends that shaped the illicit crypto market in 2024, TRM Labs, 2025: www.trmlabs.com/resources/reports/2025-crypto-crime-report, consulté le 10 juin 2025.
8. Elliptic, «The largest theft in history - following the money trail from the Bybit Hack », Elliptic Research: www.elliptic.co/blog/bybit-hack-largest-in-history, février 2025, consulté le 10 juin 2025.
9. Antoine Albertini, « Enlèvements dans le secteur des cryptomonnaies : une nouvelle vague d'interpellations », Le Monde : www.lemonde.fr/societe/article/2025/05/27/nouvelle-vague-d-interpellations-dans-des-enquetes-sur-les-enlevements-du-secteur-des-cryptomonnaies_6608781_3224.html, mai 2025, consulté le 10 juin 2025.
10. US DoJ (Département de la Justice des États-Unis), « Foreign National Pleads

Guilty to Laundering Millions in Proceeds from Cryptocurrency Investment Scams » : www.justice.gov/archives/opa/pr/foreign-national-pleads-guilty-laundering-millions-proceeds-cryptocurrency-investment-scams, novembre 2024, consulté le 10 juin 2025.

11. TRM Labs, « Le piratage de Bybit : Suivre le plus grand exploit de la Corée du Nord », Blog TRM. Perspectives : www.trmlabs.com/fr/resources/blog/the-bybit-hack-following-north-koreas-largest-exploit, février 2025, consulté le 10 juin 2025.
12. Aleksandar Tošić, Jernej Vičič et Niki Hrovatin, « Beyond the surface: advanced wash-trading detection in decentralized NFT markets », Financ Innov 11, no. 86: https://rdcu.be/eqh6Q, février 2025, consulté le 10 juin 2025.
13. Yuanzheng Niu et al., « Unveiling Wash Trading in Popular NFT Markets », Cornell University: www.arxiv.org/abs/2403.10361,mars 2025, consulté le 10 juin 2025.
14. Elliptic, « North Korean hackers return to Tornado Cash despite sanctions », Elliptic Research: www.elliptic.co/blog/north-korean-hackers-return-to-tornado-cash-despite-sanctions, mars 2024, consulté le 10 juin 2025.
15. Benjamin H. Bratton, « The Stack : On Software and Sovereignty », MIT Press Direct : www.direct.mit.edu/books/monograph/3504/The-StackOn-Software-and-Sovereignty, Février 2016, consulté le 10 juin 2025.
16. Challenges, « Corée du Nord : le casse crypto à 1,5 milliard qui alimente la machine de guerre de Pyongyang », Challenges : www.challenges.fr/la-verticale-cyber/coree-du-nord-le-casse-crypto-a-15-milliard-qui-alimente-la-machine-de-guerre-de-pyongyang_601303, avril 2025, consulté le 10 juin 2025.
17. Greg Otto, « Russian crypto exchange Garantex seized in international law enforcement operation », Cyberscoop: www.cyberscoop.com/garantex-seized-secret-service-doj-russia-crypto-sanctions/, mars 2025, consulté le 10 juin 2025.

Cette publication a été élaborée dans le cadre du projet intitulé « Développement de l'expertise de la cellule française de renseignement financier axée sur la finance numérique et les actifs virtuels » , cofinancé par l'Union européenne via l'Instrument d'appui technique (IAT), et mis en œuvre par le Conseil de l'Europe, en coopération avec la Commission européenne. Dans le cadre de cette initiative, la Commission européenne et le Conseil de l'Europe ont apporté leur soutien à la cellule française de renseignement financier – Tracfin – en vue de renforcer ses capacités et ses connaissances dans le domaine des crypto-actifs et de la finance numérique décentralisée, permettant ainsi d'améliorer la qualité de ses fonctions d'analyse stratégique et opérationnelle.

PREMS 087425

FRA

Les États membres de l'Union européenne ont décidé d'unir leurs savoir-faire, leurs ressources et leurs destins. Ensemble, ils ont construit une zone de stabilité, de démocratie et de développement durable, tout en préservant la diversité culturelle, la tolérance et les libertés individuelles. L'Union européenne s'engage à partager ses réalisations et ses valeurs avec les pays et les peuples au-delà de ses frontières.

http: //europa.eu

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

www.coe.int

Cofinancé par l'Union européenne

UNION EUROPÉENNE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Cofinancé et mis en œuvre par le Conseil de l'Europe