OASIS INTERNATIONAL SCHOOL MODEL UNITED NATIONS

Conseil de Sécurité

Présidente: Sahar Nahid

Président Adjoint: Robin Tamer

Guide de recherche

Sujet N1: Le role des cryptomonais dans le financement du terrorisme pour contourner les sanctions bancairs internationals

XIX conférence annuel OISMUN
Octobre 2026

Table des matières

I. Abstrait **3**
II. Introduction **4**
III. Histoire du sujet **6**
IV. Définition des termes clés **8**
V. Implications des nations unies **9**
VI. Principaux pays et organisations impliquées **10**
VII. Solutions possibles **13**
VIII. Questions guides **14**
IX. Liens Utiles **15**
X. Bibliographie **16**

I. Abstrait



Les cryptomonnaies ont profondément transformé les systèmes financiers mondiaux en permettant des transactions rapides, décentralisées et accessibles à l'échelle internationale. Si ces technologies offrent des avantages pour l'innovation financière, elles présentent également de nouveaux défis pour la sécurité internationale. Parmi ces défis, leur utilisation croissante par certaines organisations terroristes afin de contourner les sanctions économiques imposées par les États et les organisations internationales.

Les sanctions bancaires internationales constituent l'un des principaux instruments utilisés pour limiter le financement des groupes terroristes. Elles visent à bloquer les avoirs, bloquer les transferts financiers et empêcher l'accès aux institutions bancaires traditionnelles. Cependant, les cryptomonnaies permettent d'effectuer des transactions sans passer par les banques centrales ou les institutions financières classiques, réduisant ainsi l'efficacité de ces sanctions.

Grâce à certaines caractéristiques comme la décentralisation, la rapidité des transferts, la possibilité d'utiliser des portefeuilles numériques anonymes ou pseudonymes et l'existence de plateformes d'échange peu réglementées dans certains États, les organisations terroristes peuvent recevoir des dons, transférer des fonds et financer leurs activités avec davantage de discrétion.

Toutefois, les cryptomonnaies ne sont pas entièrement anonymes. La technologie de la blockchain enregistre chaque transaction de manière permanente, ce qui permet aux autorités spécialisées d'effectuer des analyses financières complexes pour retracer certains flux de capitaux. Plusieurs gouvernements, entreprises spécialisées et organisations internationales développent aujourd'hui des outils permettant d'identifier les portefeuilles liés aux réseaux terroristes.

Le principal défi pour la communauté internationale consiste donc à trouver un équilibre entre la promotion de l'innovation financière, la protection de la vie privée des utilisateurs et le renforcement de la lutte contre le financement du terrorisme. Une coopération internationale plus étroite, une harmonisation des réglementations et le développement de nouvelles technologies de

surveillance financière apparaissent comme des pistes essentielles pour répondre à cette problématique.

II. Introduction

Les crypto-monnaies sont un type d'argent numérique n'ayant pas de format physique, elle repose sur une technologie qui sécurise et enregistre les transactions de manière transparente. Cette technologie appelée blockchain fonctionne comme un registre partagé entre des milliers d'ordinateurs à travers le monde, plutôt que stocker à un seul endroit comme dans une banque ce qui rend la transaction difficile à modifier. Depuis la création des Bitcoin en 2009, les crypto-monnaies se sont développées à une rapidité exponentielle connue par tous. Cependant, particulièrement depuis 2022, la communauté internationale observe une utilisation beaucoup plus préoccupante, notamment par plusieurs acteurs essayant de contourner les lois internationales et les systèmes financiers traditionnels reliés à des banques.



Pour le Conseil de sécurité, la mise en place de sanctions bancaires et financières représente un facteur clé pour préserver la paix et la sécurité internationales. L'apparition des technologies et des monnaies virtuelles crée un espace financier parallèle qui opère en dehors des systèmes bancaires classiques et des contrôles institutionnels. Afin d'aborder ce sujet de manière, il faut distinguer deux réalités au sein de la scène internationale. D'une première part, certains États soumis à des régimes de sanctions comme la Corée du Nord, l'Iran, la Russie ou le Venezuela ont recours à plusieurs mécanismes numériques, notamment le cyberpiratage à l'usage de stablecoins[1] pour maintenir leurs déplacements financiers et commerciaux. D'autre part, des organisations terroristes non gouvernementales comme le Hamas, Al-Qaïda, l'État islamique ou le

[1] *Qu'est-ce qu'une stablecoin ?* (n.d.). Retrieved August 12, 2026, from https://www.coinbase.com/fr-ca/learn/crypto-basics/what-is-a-stablecoin

Hezbollah exploitent indépendamment les réseaux virtuels pour lever des fonds et transférer des ressources. Ces pratiques ont [prix une grande ampleur globale et nécessitent une attention internationale immédiate.

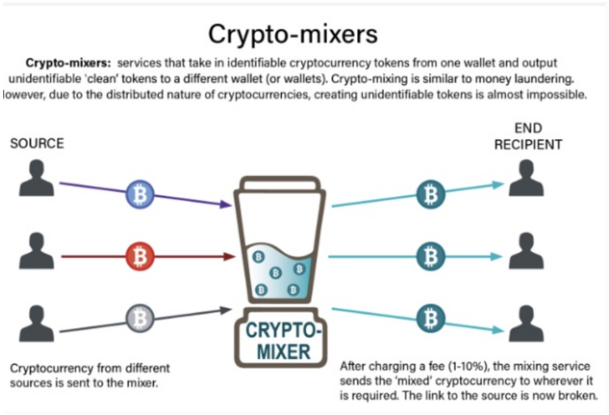
Contrairement aux systèmes bancaires traditionnels, ou chaque transaction passe par un intermédiaire capable de bloquer ou signaler, les cryptomonas permettent des transferts directe entre deux personnes n'importe où dans le monde sans vérification, ce qui réduit la capacité des autorités de vérifier ou identifier les virements.





Une fois les fonds volés, la phase de blanchiment et d'annonymasisation s'enclenche pour rompre la traçabilité du blockchain. Les organisations criminelles et non gouvernemental font rapidement circuler les bitcoins à travers des services de mixage (*crypto mixers*), qui mélangent les fonds de milliers d'utilisateurs pour en masquer l'origine et les rendre anonymes, ou utilisent des plateformes de finance décentralisée (DeFi) pour échanger en chaîne (*chain-hopping*) les jetons volés contre d'autres actifs moins traçables. Puis, ces sommes sont converties grace a des des plateformes d'échange non régulées ou auprès de courtiers de gré en gré [2](*OTC brokers*) opérant dans des juridictions tolérables. Ce processus permet d'injecter une liquidité propre sous forme de monnaie

[2] c'est un intermédiaire financier qui permet d'acheter ou de vendre des actifs directement entre deux parties, sans passer par une bourse publique



traditionnelle ou de jetons stables (*stable coins*), servant ensuite à financer des programmes militaires et à entretenir des actions terroristes sur le terrain.

III. Histoire du sujet

Depuis plusieurs décennies, les groupes terroristes dépendent de différentes sources de financement afin d'assurer leur fonctionnement. Historiquement, ces ressources provenaient du trafic d'armes, du trafic de drogues, des enlèvements contre rançon, des dons privés ou encore du commerce illégal de ressources naturelles.

Après les attentats du 11 septembre 2001, la lutte contre le financement du terrorisme est devenue une priorité mondiale. Les Nations Unies ont adopté plusieurs résolutions obligeant les États à renforcer leurs contrôles financiers, tandis que le Groupe d'action financière (GAFI/FATF) a développé des normes internationales destinées à prévenir le blanchiment d'argent et le financement du terrorisme.Cet interet du GAFI pour les monnaies virtuelles s'explique par les risques ineduite quelles oisauent pour un systenme de lutte contre le blqanchiment concu a lorigine pour les banques et des intermediaire indentifiables. Contrairement à un virement bancaire, les transactions en crypto peuvent être effectuées entre deux portefeuilles anonymes sans vérification d'identité, rendant les outils traditionnels d'identification inefficaces face à la nouvelle réalité.

L'apparition du bitcoin en 2009 a marqué le début d'une transformation profonde des finances internationales. La création progressive de mullier d'autres crypto monnaies, comme les bitcoins, ont offert aux utilisateurs des alternatives au système bancaire traditionnel. Il y a également eu l'émergence rapide des privacy coins conçue pour masquer l'historique des transactions, ou même les stable coins appuyées par des monnaies réelles, a vraiment complexifier la surveillance financière. Cette création de réseaux financiers parallèles est capable de contourner les contrôles appliqués par les banques, modifiant ainsi en profondeur l'efficacité des mécanismes de régulation et des sanctions.

En 2015, le GAFI publie ses premières directives obligées à suivre imposer sur tous les pays. Le GAFI demande simplement de surveiller les endroits ou on change les cryptomonas contre l'argent classique puisque elles sont encore nouvelles. Cependant entre 2015 et 2018, le bitcoin devient très populaire et de nouveaux sites d'échanges ouvrent sans aucun contrôle ni réglementation, ce qui crée de grands problèmes de sécurité. Les criminels et les terroristes n'ont plus besoin de repasser par l'argent classique, ils peuvent envoyer des fonds anonymes partout

dans le monde. En voyant que les conseils de 2015 ne suffisent plus, le GAFI décide de réagir en juin 2019, il crée la Travel Rule". Cette norme oblige désormais les prestataires d'actifs virtuels à identifier l'émetteur et le destinataire de chaque transaction, assimilant ainsi les plateformes crypto aux institutions financières traditionnelles.

Les sanctions financières internationales représentent aujourd'hui l'un des principaux moyens de pression contre les organisations terroristes. Elles consistent à :

- bloquer les comptes bancaires
- interdire les transferts internationaux
- limiter l'accès au système bancaire mondial
- sanctionner les personnes et entreprises qui soutiennent financièrement des groupes terroristes.

Ces mécanismes s'appuient notamment sur le régime mondial de sanctions du Conseil de sécurité, régi par la résolution 1267[3], qui impose le gel immédiat des avoirs des individus et entités associés à des groupes terroristes.

Les cryptomonnaies fonctionnent grâce à la technologie de la blockchain, un registre numérique distribué qui enregistre l'ensemble des transactions sans nécessiter l'intervention d'une banque ou d'un gouvernement. Chaque utilisateur possède un portefeuille numérique qui lui permet d'envoyer ou de recevoir de l'argent depuis n'importe quel endroit du monde. Cette décentralisation réduit la capacité des autorités à bloquer certaines transactions avant leur exécution.

Au cours des dernières années, plusieurs organisations terroristes ont commencé à expérimenter les crypto-monnaies comme moyen complémentaire de financement. D'abord limitées à des tests isolés entre 2014 et 2015 avec de simples transferts en Bitcoin, ces méthodes se sont progressivement structurées, notamment avec le développement des messageries cryptées et des plateformes décentralisées, les groupes armés sont passés de petites transactions expérimentales à de vraies campagnes de financement organisées. Des groupes comme Daech, Al-Qaïda ou les brigades Al-Qassam (Hamas) ont ainsi lancé des campagnes de collecte de dons en

[3] https://main.un.org/securitycouncil/en/sanctions/1267

Bitcoin sur Internet et les réseaux sociaux, souvent sous couvert de fausses causes caritatives. La réalité de ces opérations s'est confirmée en août 2020, lorsque le ministère de la Justice américain a procédé à la saisie de plus de 300 comptes virtuels et la confiscation de millions de dollars appartenant à ces réseaux. Cette opération a révélé des methodes tres variees, le Hamas gérait des site webs officiels générant des adresses de paiement unique pour chaque donateurs, alors que Al-Qaida utilisait des chaînes de télégramme pour gagner ses dons, et le Daech exploitait de faux sites marchands qui prétends vendre des equipement de protections médicales. Plus récemment, en octobre 2022, la « Déclaration de Delhi », adoptée en Inde par le Comité contre le terrorisme du Conseil de sécurité de l'ONU, a marqué une prise de conscience collective en plaçant la neutralisation de ces technologies financières parmi les priorités sécuritaires mondiales.

Toutefois, les spécialistes estiment que les cryptomonnaies représentent encore une part faible de leurs ressources financières totales. Les espèces, les réseaux informels de transfert d'argent, les activités criminelles restent leurs principales sources de revenus. Les rapports spécialisés indiquent que l'ensemble des activités criminelles et illégales (fraude, piratage, trafic) représentent moins de 1 % du volume global des transactions en crypto-monnaies. Dans ce pourcentage deja faible, la part attribuee specifiquement au financement du terrorisme est encore plus minime. On observe toutefois un changement importante dans les usages : plus de 80 % des transferts suspects transitent désormais via des jetons stables (*stable coins*), privilégiés pour leur absence de volatilité par rapport aux autres cryptoactifs[4], utilisée par les groupes criminels et terroristes pour leur stabilité financière.

En même temps, les autorités internationales améliorent leurs capacités d'enquête. Les sociétés spécialisées dans l'analyse de blockchain permettent aujourd'hui d'identifier de nombreux portefeuilles suspects et de collaborer avec les forces de l'ordre pour saisir les actifs numériques liés au terrorisme. Ces outils d'analyse permettent de suivre la trace des fonds sur le registre public de la blockchain, facilitant des interventions coordonnées à l'échelle internationale menées par des organismes comme Europol.[5] Toutefois, ces outils sont victimes a plusieurs limites majeurs que les organisations terroristes exploitent activement:

[4] https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/
[5] https://www.europol.europa.eu/crime-areas/cyber-attacks

- Les monnaies axées sur la confidentialité (privacy coins): Des crypto monnaies comme Monero masquent l'adresse de l'expéditeur, du destinataire et le montant transféré ce qui rend la traçabilité impossible.
- Les mixeurs et la finance décentralisée (DéFi): l'usage de services de mixages comme Tornado Cash permettent de mélanger ou d'échanger rapidement les jetons pour effacer l'origine des fonds.
- La disparition de réglementation internationales: L'absence d'application uniforme des normes du GAFI crée des zones de refuge financier ou les changement d'actifs restent techniquement et juridiquement impossible.

La régulation des cryptomonnaies pose néanmoins de grands défis aux autorités internationales. La nature transfrontalière de la blockchain rend difficile l'application de règles uniformes à l'échelle mondiale. De plus, imposer un contrôle trop strict risquerait de pousser les utilisateurs vers des plateformes illégales. Le débat actuel ne porte donc pas uniquement sur l'interdiction des cryptomonnaies, mais plutôt sur la manière de réglementer leur utilisation tout en préservant leurs bénéfices économiques et technologiques.

Recapitulatif des dates	
2001	Attentats du 11 septembre. La lutte contre le financement du terrorisme devient une priorité mondiale, l'ONU multiplie les résolutions et le GAFI développe des normes internationales.
2009	Creation du BItcoin, ce uqi debute la transformation des fiances internationales
2014	Piratage de Sony Pictures par le groupe Lazarus, lié à la Corée du Nord. Premier grand coup d'éclat du groupe avant son virage vers le vol de cryptomonnaies
2014-2015	Premiers tests isolés de groupes terroristes utilisant de simples transferts en Bitcoin.
2015	Le GAFI publie ses premières directives, demandant la surveillance des lieux d'échange entre cryptomonnaie et argent classique.
2016	Le groupe Lazarus tente de dérober près d'un milliard de dollars à la banque du Bangladesh via le réseau SWIFT, une opération liée au contournement des sanctions nord-coréennes
2015-2018	Popularisation du Bitcoin. Ouverture de nombreuses plateformes d'échange sans contrôle ni réglementation.
Juin 2019	Le GAFI crée la Travel Rule, obligeant les prestataires d'actifs virtuels à identifier l'émetteur et le destinataire de chaque transaction
Aout 2020	Le ministère de la Justice américain saisit plus de 300 comptes virtuels liés au Hamas, à Al-Qaïda et à Daech
Mars 2022	Le groupe Lazarus dérobe environ 620 millions de dollars lors du piratage du réseau Ronin (jeu Axie Infinity), l'un des plus grands vols de cryptomonnaie de l'histoire
Octobre 2022	Adoption de la Déclaration de Delhi par le Comité contre le terrorisme du Conseil de sécurité, plaçant la neutralisation des technologies financières parmi les priorités sécuritaires mondiales
Fevrier 2025	Piratage de la plateforme By Bit, environ 1,5 milliard de dollars dérobés et attribué au groupe Lazarus, le plus important vol de cryptomonnaie jamais enregistré

IV. Causes du sujet

L'une des principales causes de ce phénomène est dans la facilité d'utilisation des cryptomonnaies, mais aussi dans leur nature pseudonyme et anonyme qu'elles offrent. Ces caractéristiques permettent de contourner le cadre légal international ainsi que les systèmes bancaires traditionnels. C'est exactement cette difficulté de régulation qui pousse certains cybercriminels et organisations à exploiter le système. L'exemple le plus frappant de cette exploitation est celui de la Corée du Nord. Ils ont commencer le piratage des cryptomonas vers 2017, entre 2021 et 2023, ils ont commencé leurs attaques a plus grande échelle, puis en 2024 ils ont dérobé plus de 1,3 milliards de dollars[6]. En 2025, ils ont passé un sommet historique en volant plus de 2,02 milliard de dollars en une seule année avec 1,5 milliard dérober seulement en février[7]. En 2026, de nombreuses poursuites d'attaques de haute précision visant des protocoles récents instaurés. À travers des groupes de cybercriminalité soutenus par l'État comme le *Lazarus Group*, Pyongyang a fait du piratage de plateformes de cryptomonnaies une véritable stratégie financière nationale. En exploitant les failles informatiques des services de change et des ponts inter-blockchains, le régime siphonne[8] des centaines de millions de dollars en actifs virtuels. Ces fonds sont ensuite blanchis pour financer directement le développement de ses programmes de missiles et d'armement nucléaire, contournant ainsi l'interdiction strict imposé par les Nations Unies.

Dans le système classique, chaque transaction est surveillée par une banque, tandis que des réseaux comme SWIFT servent à transmettre de manière sécurisée les messages et les instructions de paiement entre ces établissements. Cela permet aux gouvernements de bien surveiller les transactions et l'argent qui circule, de bloquer de comptes suspects et même d'empêcher certains transferts d'avoir lieu. C'est ce mécanisme que les sanctions bancaires utilisent pour réguler ou isoler un pays/groupe particulier. C'est précisément pour échapper à ce verrouillage que des États majeurs visés par des sanctions internationales se tournent vers ces technologies. La Russie, exclue du réseau SWIFT pour une grande partie de ses institutions, dès mars 2022[9] et utilise désormais

---

[6] https://www.bbc.com/news/articles/cwy3dz0614jo

[7] https://www.nbcnews.com/tech/crypto/north-korea-stole-billions-crypto-2025-new-research-says-rcna249738

[8] Ils liquident ou prennent

[9] https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/F

des paiements transfrontaliers en cryptomonnaies et en *stable coins* (transformer en dollar) pour maintenir son commerce extérieur. De manière similaire, le Venezuela a régulièrement exigé l'utilisation d'actifs numériques (notamment l'USDT[10]) pour le règlement des ventes internationales de son pétrole brut afin de contourner le blocus des banques correspondantes occidentales. Cependant, les crypto-monnaies ne passent par aucune banque. Les transactions se font directement entre deux personnes, similaire a un échange en mains propres, mais en ligne. Il n'y a donc personne au milieu pour arrêter la transaction ou la surveiller en temps réel. Une fois qu'un transfert est envoyé, il ne peut plus être annulé, même par un gouvernement. En plus de ça, les portefeuilles de crypto-monnaies ne demandent pas toujours de preuve d'identité. N'importe qui peut en créer un en quelques minutes, sans donner son vrai nom. Cela rend très difficile pour les autorités de savoir qui se cache derrière une transaction. Un autre problème vient du fait que les pays ne s'entendent pas tous sur les mêmes réglementations. Certains pays imposent des contrôles stricts sur les plateformes de crypto-monnaies, alors que d'autres n'en imposent presque aucun. Les acteurs qui veulent contourner les sanctions choisissent alors d'utiliser les plateformes situées dans les pays les moins stricts, ce qui rend la tâche encore plus difficile pour la communauté internationale. En outre les États, des organisations terroristes non étatiques telles que le Hamas (notamment via les brigades Al-Qassam), Al-Qaïda ou l'État islamique exploitent ces failles réglementaires pour contourner le système bancaire. N'ayant aucun accès aux banques traditionnelles, ces groupes lancent des campagnes de financement participatif en ligne via des réseaux sociaux et messageries cryptées. L'utilisation croissante de jetons stables leur permet de recevoir des micro-donations instantanées de sympathisants à travers le monde et de transférer ces fonds entre différentes cellules opérationnelles sans risquer l'interception par les autorités financières.

lagPost/2022/March/Exclusion_of_Russia_from_SWIFT#:~:text=FlagPost%2C%20March%2009%20March%202022.%20Russia's%20exclusion,economy%20and%20trade.%20*%20What%20is%20SWIFT%3F

[10] L'USDT est un dollar virtuel. C'est une cryptomonnaie stable qui vaut toujours 1 dollar américain.

V. Importance du sujet

Ce sujet revêt une importance particulière pour le Conseil de sécurité, car il touche directement à l'efficacité de l'un de ses outils les plus utilisés depuis des décennies pour maintenir la paix et la sécurité internationales, soit les sanctions financières. Les cryptomonnaies fragilisent cette efficacité en facilitant les transferts financiers transfrontaliers et en compliquant l'identification des bénéficiaires, ce qui permet à des acteurs non gouvernementaux d'exploiter de plus en plus cette faille avec facilité. Les chiffres récents montrent l'ampleur réelle du problème. La Corée du Nord, via ses groupes de piratage Lazarus Group et APT 38, aurait dérobé environ 2,2 milliards de dollars[11] en crypto monnaies seulement en 2025, sur les 3,4 milliards de dollars de crypto monnaies piratés dans le monde en 2025, près de 60 %[12] ont été détournés par les hackers nord-coréens. Des fonds qui servent directement à financer ses programmes d'armement nucléaire et balistique. L'Iran, à travers le Corps des Gardiens de la révolution islamique, utiliserait également des milliards de dollars en actifs numériques pour soutenir ses programmes militaires et des groupes alliés au Moyen-Orient. Ces stratégies permettent à des États isolés et sanctionnés de contourner l'influence financière exercée par les puissances occidentales, notamment via le dollar américain.

Du côté des organisations non étatiques[13]Des groupes comme Al-Qaïda et certaines branches du Hamas ont aussi recours aux crypto-monnaies, en particulier aux stable coins, faciles et rapides à transférer, pour collecter des dons, financer leurs opérations et recruter de nouveaux membres. Ce sujet est aussi important parce qu'il oblige la communauté internationale à repenser ses méthodes de régulation financière. Les instruments traditionnels, conçus pour un système bancaire centralisé, ne sont plus suffisants face à des technologies décentralisées qui évoluent plus vite que les lois destinées à les réguler. Sans une adaptation rapide des cadres juridiques internationaux, l'écart entre les capacités des acteurs malveillants et celles des régulateurs risque de continuer à se creuser et empirer la situation actuelle.

---

[11] https://www.24heures.ca/2025/12/23/voici-comment-la-coree-du-nord-a-vole-un-record-de-22-milliards-de-dollars-en-2025

[12] https://cryptoactu.com/hackers-nord-coreens-21-md/

[13] Non gouvernemental ou administratif

VI. Terms clés

Hamas: Mouvement islamiste fondee en palestine en 1987, dans la bande de Gaza.Sa branche armée, Al-Qassam est financée en partie par des collectes de dons en cryptomonnaies auprès de sympathisants à travers le monde.

Al-Qaïda: Organisation terroriste islamiste fondée à la fin des années 1980, connue pour sa responsabilité des attentats du 11 septembre 2001. Ils prélèvent des fonds via des réseaux informels et via des plateformes numériques, donc leur cryptomonnaie.

Daech: C'est une organisation totalitaire islamiste cree en 2013, qui dirige la Syrie et l'Irak. Après la perte de son territoire, elle a maintenu certaines activités de financement en ligne, notamment via des crypto-monnaies.

GAFI (Groupe d'action financière): C'est une une organisation cree en 1989, chargée d'établir des normes internationales contre le blanchiment d'argent et le financement du terrorisme.

Lazarus Group: C'est un groupe de cybercriminalité nord-coréen lié aux services de renseignement de l'État, actif depuis les années 2010.

Blockchains: C'est un registre numérique qui garde une copie de toutes les transactions effectuées, réparti sur des milliers d'ordinateurs à travers le monde plutôt que stocké à un seul endroit comme dans une banque.

Ponts inter-blockchains (cross-chain bridges): Infrastructures technologiques qui permettent de transférer des actifs numériques d'une blockchain à une autre.

SWIFT: C'est un réseau mondial sécurisé utilisé par les banques pour faire des transferts internationaux.

Cryptomonnaie : Une forme de monnaie numérique ou virtuelle qui utilise la cryptographie pour sécuriser les transactions et fonctionne généralement sur une blockchain ou une technologie similaire. Bitcoin et Ethereum en sont des exemples.

Fournisseur de services d'actifs virtuels (PSAV) : Une personne ou une entreprise qui fournit des services liés aux actifs virtuels, tels que l'échange de crypto-monnaies, le transfert d'actifs virtuels ou les services de conservation/portefeuille électronique.

Règle de voyage : Une exigence de lutte contre le blanchiment d'argent et le financement du terrorisme (LCB-FT) qui impose la collecte et le partage de certaines informations concernant l'expéditeur et le destinataire d'un transfert de cryptomonnaies entre les PSAV concernés.

Stable Coins : Cryptomonnaies conçues pour maintenir une valeur stable, généralement en étant indexées sur un actif tel que le dollar américain ou une autre devise.

Pseudonymat : Situation où les utilisateurs sont identifiés par des adresses, des noms d'utilisateur ou d'autres identifiants plutôt que par leur véritable nom. Les transactions en cryptomonnaies peuvent être pseudonymes car les adresses blockchain ne révèlent pas automatiquement l'identité d'une personne.

Mixeurs de cryptomonnaies : Services qui combinent les cryptomonnaies de plusieurs utilisateurs et les redistribuent afin de rendre plus difficile le traçage de l'origine et de la destination des fonds.

Finance décentralisée (DeFi) : Services financiers tels que les prêts, les emprunts, le trading et l'échange d'actifs, proposés via des applications basées sur la blockchain et des contrats intelligents, en remplacement des institutions financières traditionnelles.

Ponts inter-chaînes : Technologies permettant le transfert d'actifs ou d'informations entre différentes blockchains, comme le transfert d'un actif d'Ethereum vers une autre blockchain.

(LCB-FT): Lutte contre le blanchiment d'argent et le financement du terrorisme.

Cadre international plus large de lois, de réglementations et de procédures visant à empêcher les criminels et les terroristes de dissimuler l'origine de fonds illicites. Les mesures LCB-FT visent à détecter et à signaler les activités financières suspectes, tandis que les mesures LCF-FT ciblent spécifiquement la perturbation des flux financiers vers les organisations terroristes.

VII. Implications des nations unies

Depuis les attentats du 11 septembre 2001, les Nations Unies ont placé la lutte contre le financement du terrorisme au cœur de leurs priorités en matière de sécurité internationale. La première réponse majeure fut l'adoption, le 28 septembre 2001, de la résolution 1373 du Conseil de sécurité, qui oblige l'ensemble des 193 États membres à criminaliser le financement du terrorisme, à geler les avoirs des personnes et organisations impliquées dans des activités terroristes et à renforcer leur coopération en matière de renseignement financier. Cette résolution a également créé le Comité contre le terrorisme (Counter-Terrorism Committee – CTC), chargé de suivre la mise en œuvre de ces obligations et d'évaluer les progrès réalisés par les États.

Afin de renforcer ce mécanisme, les Nations Unies ont créé en 2004 la Counter-Terrorism Committee Executive Directorate (CTED), une direction exécutive chargée d'apporter une assistance technique aux États. La CTED évalue les législations nationales, identifie les faiblesses des systèmes financiers et aide les gouvernements à améliorer leurs capacités de détection du financement du terrorisme. Avec l'apparition des cryptomonnaies et des actifs virtuels, cette assistance s'est progressivement élargie aux nouvelles technologies financières et aux méthodes d'investigation basées sur l'analyse de la blockchain.

Une étape importante a ensuite été franchie en 2006, lorsque l'Assemblée générale des Nations Unies a adopté la Stratégie antiterroriste mondiale des Nations Unies, premier cadre international approuvé par consensus par tous les États membres. Cette stratégie vise à renforcer la coopération internationale, à développer les capacités nationales de lutte contre le terrorisme et à garantir que les mesures de sécurité respectent les droits de l'homme. Révisée tous les deux ans, elle a progressivement intégré les défis posés par la numérisation des services financiers et par le développement rapide des crypto-monnaies.

Face à l'utilisation croissante des actifs virtuels dans certaines activités criminelles, le Conseil de sécurité a adopté le 28 mars 2019 la résolution 2462, qui constitue la première résolution consacrée presque exclusivement au financement du terrorisme. Ce texte reconnaît que les nouvelles technologies financières, notamment les cryptomonnaies, peuvent être exploitées pour contourner les sanctions bancaires internationales et demande aux États de mettre en place

des cadres réglementaires adaptés. La résolution encourage également les gouvernements à appliquer les recommandations du Groupe d'action financière (GAFI/FATF) relatives aux fournisseurs de services sur actifs virtuels afin d'améliorer la transparence des transactions et la coopération internationale.

VIII. Principaux pays et organisations impliquées

A. Principaux pays concernés :

- ***Les Etats Unis d'Amérique:*** Ce pays joue un rôle crucial dans la lutte contre l'utilisation des cryptomonas à des fins de financement terroriste et du contournement des sanctions. Leurs principaux intérêts est de préserver l'intégrité du système financier international et de maintenir l'efficacité de leurs sanctions économiques pour empêcher les organisations terroristes d'exploiter les actifs numériques. Washington considere que les transactions doivent etre soumises aux meme obligations de lutte contre le blanchiment d'argent et le financement du terrorisme que les autres acrtivitees fiancieres, et a meme deja sancrtuonne des olatformes et certaines adresses de portefeuilles numeriques associes a des acteurs de sanctions. Leurs objectifs sont d'améliorer la traçabilité des transactions, de renforcer les réglementations des fournisseurs de services d'actifs virtuels (VASP) et de développer les coopérations internationales.



- ***La république isalmique d'Iran:*** L'Iran est particulièrement important pour ce sujet en raison de leurs nombreuses restrictions financières auxquelles il est confronté et de leurs accusations portées contre plusieurs institutions iraniennes concernant le financement de groupes armés au Moyen Orient. Leur intérêt national est de préserver leur accès aux échanges internationaux et de réduire leur dépendance aux systèmes financiers qui peuvent possiblement être affectés par des sanctions étrangères. Téhéran rejette en particulier toutes les sanctions américaines qu'ils considèrent comme une atteinte a leur souveraineté économique. En même temps, le GAFI continue de considérer l'Iran comme une juridiction à haut risque.



- ***La République populaire democratique de la Corée du Nord:*** Elle constitue un des cas les plus importants de ce sujet puisqu'ils sont reconnus comme un des pionniers du hacking crypto à l'échelle international, notamment grâce au groupe Lazarus. Les fonds volés pendant les piratages de plateformes d'échanges servent a financer le programme nucléaire et balistique du pays, contournant les sanctions de l'ONU qui visent justement à ralentir ce programme. C'est un cas particulier car il ne sahit pas de financement de groupes terroristes au sens classique, mais d'un usage gouvernemental de la cybercriminalité crypto à des fins militaires. La capitale cherche avant tout de préserver son accès à ses ressources financières extérieures, le gouvernement nord coreen rejette les accusations concernant leurs activités financières.



- ***Fédération de Russie:*** La Russie est devenue particulièrement importante dans les discussions sur les cryptomonas et les systèmes financiers depuis l'expansion des sanctions occidentales. Leur principale intérêt est de préserver leur capacité à commercer et effectuer des transactions internationales malgré les restrictions imposées par les etats unies, l'Union européenne et tout leurs partenariats, tout en réduisant leur dependance a d'autres infrastructures financières dominée par les puissances occidentales. Moscou affirme qu'ils soutiennent la lutte contre le terrorismemais rejettent à leurs tours les sanctions occidentales. La russie veut soutenir des mesures ciblant le financement du terrorisme, mais elle s'oppose aux mesures qui permettraient aux pays occidentaux d'imposer leurs sanctions a d'autre etats. Les sanctions qui touchent les banques et les entreprises russes compliquent leurs echangenets a letranger, ce qui pousse la capitale à chercher d'autres moyens de paiement et de réduire sa dépendance sur les systèmes financiers occidentaux.



- ***République populaire de Chine:*** La chine est un acteur important a cause de leurs poids économique ainsi que leurs statut de membre permanent du Conseil de sécurité, en plus de



leurs contrôle stricte de l'utilisation des cryptomonnaies sur leur territoire. Leur principale intérêt est de protéger la stabilité de leur système financier d'empecher que les cryptomonnaies soient utilisées pour le blanchiment d'argent, la fraude et les financement terroristes. La Chine soutient alors la coopération internationale pour lutter contre les transactions illégales. Donc Pékin a totalement interdit les transactions, le minage et les plateformes d'échange de crypto-monnaies privées sur son territoire. Toutefois, la Chine développe parallèlement sa propre monnaie numérique d'État (le yuan numérique ou e-CNY. Cet outil permet au gouvernement de maintenir une surveillance totale sur les flux financiers tout en créant un réseau de paiement international alternatif capable de contourner le système bancaire SWIFT et d'échapper aux sanctions financières occidentales.

- ***Etat d'Israël:*** Le gouvernement israélien utilise des technologies permettant de suivre les transactions sur les blockchains et a procédé au gel ou à la saisie de portefeuilles numériques qu'il affirme être liés à des organisations armées. Cependant ces interventions font l'objet de nombreuses critiques concernant leur manque de transparence, parce que ces saisies d'actifs virtuels sont souvent effectuées sans preuves publiques ni procédures judiciaires claires et empêche les personnes ciblées de se défendre. De plus, ce blocage massif touche également des citoyens ordinaires, des commerçants et des associations caritatives sans aucun lien avec des activités illégales. Dans les territoires palestiniens, où le système bancaire classique est fortement dégradé, de nombreux civils dépendent des cryptomonnaies pour recevoir de l'aide ou de l'argent de leurs proches à l'étranger et donc ces interruptions financières répétées sont ainsi dénoncées comme une forme de punition collective qui aggrave directement la crise économique locale.



B. Principaux organisations concernée

- **Les Nations Unies** demeurent l'acteur central de la coopération internationale contre le financement du terrorisme grâce au Conseil de sécurité, au Comité contre le terrorisme (CTC), à la CTED et à l'Office des Nations Unies contre la drogue et le crime (ONUDC). Depuis l'adoption de la résolution 1373 en 2001, ces organes coordonnent les efforts des États, élaborent des recommandations et fournissent une assistance technique afin d'améliorer les capacités nationales de prévention, de détection et de répression du financement des groupes terroristes, y compris lorsque celui-ci implique des crypto-monnaies.

- **Le Groupe d'action financière (GAFI/FATF)**, créé en 1989, joue un rôle essentiel dans l'élaboration des normes internationales relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme. Composé de 40 membres, il a publié en 2019 ses premières recommandations spécifiques concernant les fournisseurs de services liés aux actifs virtuels. Parmi celles-ci figure la Travel Rule, qui impose aux plateformes d'échange de transmettre certaines informations sur les expéditeurs et les bénéficiaires des transactions afin de limiter l'anonymat des transferts et de faciliter les enquêtes internationales.

- **INTERPOL**, qui regroupe 196 pays membres, soutient les enquêtes transfrontalières portant sur les réseaux criminels et terroristes utilisant les cryptomonnaies. L'organisation coordonne l'échange d'informations entre les services de police nationaux, organise des formations spécialisées sur les enquêtes liées aux actifs numériques et participe à plusieurs opérations internationales visant à identifier les portefeuilles numériques utilisés à des fins criminelles.

- **Europol:** Au niveau européen, il apporte son expertise aux 27 États membres de l'Union européenne dans la lutte contre la criminalité financière. En 2020, l'agence a créé le European Financial and Economic Crime Centre (EFECC) afin de renforcer les enquêtes portant sur les cryptomonnaies, le blanchiment d'argent et le financement du terrorisme. Ses analyses permettent d'identifier les nouvelles tendances criminelles et d'améliorer la coopération entre les autorités judiciaires et policières européennes.

- **L'Office des Nations Unies contre la drogue et le crime (ONUDC)** intervient dans plus de 150 pays en fournissant une assistance technique aux gouvernements. Ses programmes comprennent la formation des magistrats, des procureurs et des enquêteurs spécialisés,

ainsi que le développement des cellules de renseignement financier et des capacités nationales d'analyse de la blockchain. L'ONUDC participe également à l'élaboration de cadres juridiques permettant aux États de mieux réglementer les actifs virtuels.

- **Egmont Group**, fondé en 1995, rassemble aujourd'hui plus de 170 cellules de renseignement financier (Financial Intelligence Units FIU). Cette organisation facilite l'échange rapide d'informations financières entre ses membres afin de détecter les flux financiers suspects, de soutenir les enquêtes internationales et d'empêcher les organisations terroristes d'exploiter les différences entre les systèmes juridiques nationaux pour contourner les sanctions bancaires internationales.

IX. Liens utiles

1. *Les cryptomonnaies, nouvelle arme des groupes terroristes? - France 24*. (n.d.). Retrieved August 10, 2026, from https://www.france24.com/fr/20190822-bitcoin-cryptomonnaie-jihadistes-terrorisme-brigade

2. Simplearn. (2019, February 27). *La blockchain en 7 minutes | Qu'est-ce que la blockchain ? | La blockchain expliquée | Fonctionne...* [Video recording]. https://www.youtube.com/watch?v=yubzJw0uiE4

3. *La cryptomonnaie peut-elle financer le terrorisme ? - RTBF Actus*. (n.d.). RTBF. Retrieved August 12, 2026, from https://www.rtbf.be/article/la-cryptomonnaie-peut-elle-financer-le-terrorisme-10988221

4. *Comment les groupes terroristes exploitent les cryptoactifs et les apps numériques pour se financer*. (2026, May 21). clubic.com. https://www.clubic.com/actualite-613666-ce-que-70-pays-ont-decide-a-paris-pour-couper-les-cryptofinancements-du-terrorisme.html

5. Faculté Droit, Économie, Management - Paris-Saclay. (2024, October 18). *Dans quelles mesures la Russie a su contourner les sanctions ?* [Video recording]. https://www.youtube.com/watch?v=qaW7b7YR-oc

6. Crypto Mindset Podcast. (2025, March 3). *Lazarus Group: Pourquoi Personne ne Peut Stopper Ces Hackers De Corée Du Nord* [Video recording]. https://www.youtube.com/watch?v=aroZMIZ7tGU

X. Solutions possibles

Il est nécessaire de bien comprendre que le système de surveillance financière actuel présente des lacunes considérables à l'échelle mondiale. Selon le rapport annuel du GAFI, 69 %[14] des juridictions évaluées présentent des déficiences majeures dans leurs capacités à enquêter, poursuivre et condamner les financeurs du terrorisme.

De plus, la réglementation des crypto actifs reste largement insuffisante malgré les appels répétés des organismes internationaux. Le GAFI a constaté qu'à peine 30 %[15] des pays évalués ont mis en place une réglementation satisfaisante concernant les crypto-monnaies, ce qui laisse aux acteurs malveillants une large marge de manœuvre pour se réfugier dans les juridictions les moins strictes.

Ce manque de coordination a des conséquences concrètes sur le terrain. Rien qu'en 2025, la Corée du Nord aurait dérobé environ 2,2 milliards de dollars en crypto-monnaies, des fonds qui servent directement à financer ses programmes de missiles et d'armement nucléaire.

Pour cela, voici quelques solutions possibles,

Encourage les États membres à adopter et appliquer sans délai la recommandation 15 du GAFI sur l'enregistrement et la supervision des fournisseurs de services d'actifs virtuels

Invite les États membres à renforcer les capacités techniques de leurs cellules de renseignement financier, notamment par des partenariats avec des entreprises spécialisées en analyse de blockchain

Appelle à l'adoption de sanctions ciblées contre les plateformes d'échange, mixeurs et courtiers de gré à gré opérant sciemment dans des juridictions à faible régulation

Demande à la CTED et à l'ONUDC de développer des programmes de formation spécifiques à l'analyse des crypto actifs pour les pays disposant de capacités limitées

---

[14]Canton, B. (2024, April 1). Régulation des cryptomonnaies: Le GAFI lance un « appel à l'action » ! *Journal du Coin*. https://journalducoin.com/actualites/regulation-des-cryptomonnaies-le-gafi-lance-un-appel-a-laction/

[15]*Actifs virtuels*. (n.d.). Retrieved August 12, 2026, from https://www.fatf-gafi.org/fr/Sujets/actifs-virtuels.html

XI. Questions guides

1. Dans quelle mesure les cryptomonnaies facilitent-elles réellement le financement du terrorisme par rapport aux méthodes traditionnelles de financement ?

2. Les sanctions financières internationales demeurent-elles efficaces face au développement rapide des actifs virtuels ?

3. Comment renforcer la coopération internationale afin de mieux suivre les transactions en crypto-monnaies tout en respectant la souveraineté des États ?

4. Les plateformes d'échange de crypto-monnaies devraient-elles être soumises à des réglementations internationales plus strictes et harmonisées ?

5. Comment protéger le droit à la vie privée des utilisateurs légitimes sans créer des failles exploitables par les organisations terroristes ?

6. Les technologies d'analyse de la blockchain sont-elles suffisamment performantes pour identifier les réseaux terroristes utilisant les actifs numériques ?

7. Quel rôle les organisations internationales, telles que l'ONU, le GAFI, INTERPOL et Europol, devraient-elles jouer dans le renforcement de la lutte contre le financement du terrorisme numérique ?

8. Les États devraient-ils instaurer des obligations communes concernant l'identification des détenteurs de portefeuilles numériques ?

XII. Bibliographie

Cybermonnaies et terrorisme—Droit. (n.d.). Retrieved August 6, 2026, from https://droit.univ-cotedazur.fr/dl4t/cybermonnaies-et-terrorisme

The role of cryptocurrency in financing terrorist organizations | PBS News Weekend. (n.d.). Retrieved August 12, 2026, from https://www.pbs.org/newshour/show/the-role-of-cryptocurrency-in-financing-terrorist-organizations

2025 Crypto Theft Reaches $3.4 Billion. (n.d.). Retrieved August 12, 2026, from https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/

Security Council Committee pursuant to resolutions 1267 (1999) 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities | Security Council. (n.d.). Retrieved August 12, 2026, from https://main.un.org/securitycouncil/en/sanctions/1267

2022 National Terrorist Financing Risk Assessment. (2022). https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf

2024 Crypto Crime Trends from Chainalysis. (n.d.). Retrieved August 12, 2026, from https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

Canton, B. (2024, April 1). Régulation des cryptomonnaies: Le GAFI lance un « appel à l'action » ! *Journal du Coin*. https://journalducoin.com/actualites/regulation-des-cryptomonnaies-le-gafi-lance-un-appel-a-laction/

Actifs virtuels. (n.d.). Retrieved August 12, 2026, from https://www.fatf-gafi.org/fr/Sujets/actifs-virtuels.html

Les cryptomonnaies, nouvelle arme des groupes terroristes? - France 24. (n.d.). Retrieved August 10, 2026, from https://www.france24.com/fr/20190822-bitcoin-cryptomonnaie-jihadistes-terrorisme-brigade

Simplearn. (2019, February 27). *La blockchain en 7 minutes | Qu'est-ce que la blockchain ? | La blockchain expliquée | Fonctionne...* [Video recording]. https://www.youtube.com/watch?v=yubzJw0uiE4

La cryptomonnaie peut-elle financer le terrorisme ? - RTBF Actus. (n.d.). RTBF. Retrieved August 12, 2026, from https://www.rtbf.be/article/la-cryptomonnaie-peut-elle-financer-le-terrorisme-10988221

Comment les groupes terroristes exploitent les cryptoactifs et les apps numériques pour se financer. (2026, May 21). clubic.com. https://www.clubic.com/actualite-613666-ce-que-70-pays-ont-decide-a-paris-pour-couper-les-cryptofinancements-du-terrorisme.html

Faculté Droit, Économie, Management - Paris-Saclay. (2024, October 18). *Dans quelles mesures la Russie a su contourner les sanctions ?* [Video recording]. https://www.youtube.com/watch?v=qaW7b7YR-oc

Crypto Mindset Podcast. (2025, March 3). *Lazarus Group: Pourquoi Personne ne Peut Stopper Ces Hackers De Corée Du Nord* [Video recording]. https://www.youtube.com/watch?v=aroZMlZ7tGU

Qu'est-ce qu'une stablecoin ? (n.d.). Retrieved August 12, 2026, from https://www.coinbase.com/fr-ca/learn/crypto-basics/what-is-a-stablecoin

Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. (n.d.). Retrieved August 12, 2026, from https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html

"Cryptocurrency and Blockchain - Everything You Need to Know | Specbee." January 21, 2020. https://www.specbee.com/blogs/cryptocurrency-and-blockchain.