mon livret C

Formation crypto-actifs

Blanchiment et financement du terrorisme

Distinguer le vrai du faux

Novembre 2022

I - Wikileaks, Silk Road et l'émergence de Bitcoin

L'origine du débat sur le potentiel illégal des crypto-actifs remonte à la création de Bitcoin.

Le 31 octobre 2008, un dénommé Satoshi Nakamoto publie le livre blanc de ce qui sera plus tard la monnaie numérique de réference dans le monde. Entre autres considérations y est érigé **en priorité absolue le respect de la vie privée**, une notion de plus en plus bafouée par la généralisation d'Internet et la mainmise des États sur la monnaie.

Cette vision, sans surprise, trouve d'abord son écho parmi ceux qui recherchent le plus l'anonymat : les cypherpunks, groupe d'activistes numériques ayant fait de la protection de la vie privée un combat permanent… et les criminels.

En février 2011, Ross Ulbricht, jeune américain libertarien, met au point le sulfureux site Silk Road. Hébergé sur le darknet, celui-ci prend la forme d'un **marché noir permettant d'acheter et de vendre toute sorte de produits et services illégaux, avec pour seule et unique monnaie… Bitcoin.**

Le site connaît un gigantesque succès, et brasse l'équivalent de 183,9 millions de dollars de ventes entre 2011 et 2013. À son apogée, fin 2013, Silk Road représente près de 20% de l'activité économique totale générée par Bitcoin. La plateforme est fermée puis relancée plusieurs fois, et son propriétaire condamné en 2015 à la prison à perpétuité. Le sujet est alors clos mais le mal est fait : **Bitcoin est perçu comme la monnaie de l'illégal, et cette réputation lui restera attachée des années durant.**

En outre, un autre événement important vient alimenter l'opinion publique lorsque l'ONG WikiLeaks, fondée par le lanceur d'alertes Julian Assange, annonce le 15 juin 2011 accepter les dons en Bitcoin, contournant ainsi les sanctions américaines et les pressions exercées sur Visa, MasterCard et PayPal, qui bloquent alors tous les transferts de fonds de leurs utilisateurs vers la plateforme.

Bitcoin dévoile au monde entier la résistance de son protocole à la censure, et forcément, cette perspective soudaine de liberté monétaire ne plaît pas à tout le monde.

Enregistrée auprès de l'AMF en tant que Prestataire de Services sur Actifs Numériques n°E2022-035

II - Le fantasme de l'anonymat

Pour la première fois, les projecteurs du monde entier se braquent sur Bitcoin, sorte d'ovni financier porté par des geeks aux ambitions pas encore bien comprises. Très vite, d'autres crypto-monnaies se créent, démocratisant un peu plus encore la technologie blockchain et ses caractéristiques. Celles-ci, d'ailleurs, laissent encore le grand public perplexe. **Est-il réellement possible de cacher son identité en utilisant des crypto-monnaies ? Mais en fait, comment en acheter ? Et comment les utiliser ?**

Une notion fondamentale est alors peu à peu intégrée dans l'esprit des curieux : ce que la majorité des individus prennent pour de l'anonymat porte en fait un autre nom, celui de "pseudonymat". Une différence subtile mais qui change à peu près tout.

La blockchain, assimilable à un grand registre de données transparent et inaltérable, permet à tous ceux qui le souhaitent de consulter l'historique des transactions passées sur le réseau, avec les dates, les montants échangés et les différents protagonistes. **Ces derniers sont désignés par leur adresse publique, une suite de chiffres et de lettres donnant à leur portefeuille numérique une identité propre sur la blockchain.** Les noms de l'envoyeur et du récepteur n'apparaissent donc pas, mais leur adresse si, et celle-ci n'a de secret pour personne.

III - Les preuves Zero-Knowledge

Mais cette transparence méthodique ne convient pas à tous, et **peu à peu, des crypto-monnaies désignées comme complètement anonymes se développent.**

La plus connue d'entre elles se nomme Monero. Créée en 2014, elle utilise des systèmes cryptographiques très complexes de manière à ce qu'il soit impossible pour ses utilisateurs de connaître les montants envoyés dans chaque transaction, ainsi que les différentes parties prenantes. Arrivent également ZCash, Dash, ZCoin ou Verge, d'autres projets basés sur des protocoles dit "Zero Knowledge", permettant un anonymat optionnel ou complètement assumé.

À la question "certaines crypto-monnaies permettent-elles à leurs utilisateurs un anonymat total ?", il convient donc de répondre peut-être... mais.

Car ces crypto-monnaies se retrouvent de plus en plus esseulées et rendues interdites à la vente, déjà, et que **leur capacité à garantir l'anonymat de leurs utilisateurs, surtout, semble de moins en moins avérée.**
La société américaine spécialisée dans l'analyse et la traçabilité des flux blockchain, Chainalysis, a ainsi récemment affirmé pouvoir tracer les transactions passées sur les réseaux Zcash et Dash, en dépit de leur processus de fonctionnement opaque.

Un autre obstacle majeur vient se dresser sur la route des utilisateurs mal intentionnés : celui du processus d'achat. En effet, **pour acheter des crypto-monnaies, tout individu doit impérativement passer par une plateforme d'échange centralisée** (Centralized Exchange ou CEX en anglais), une structure régulée permettant d'échanger des monnaies traditionnelles contre des actifs numériques, ou bien par un intermédiaire (broker, gestionnaire d'actifs, bureau de change, etc.).

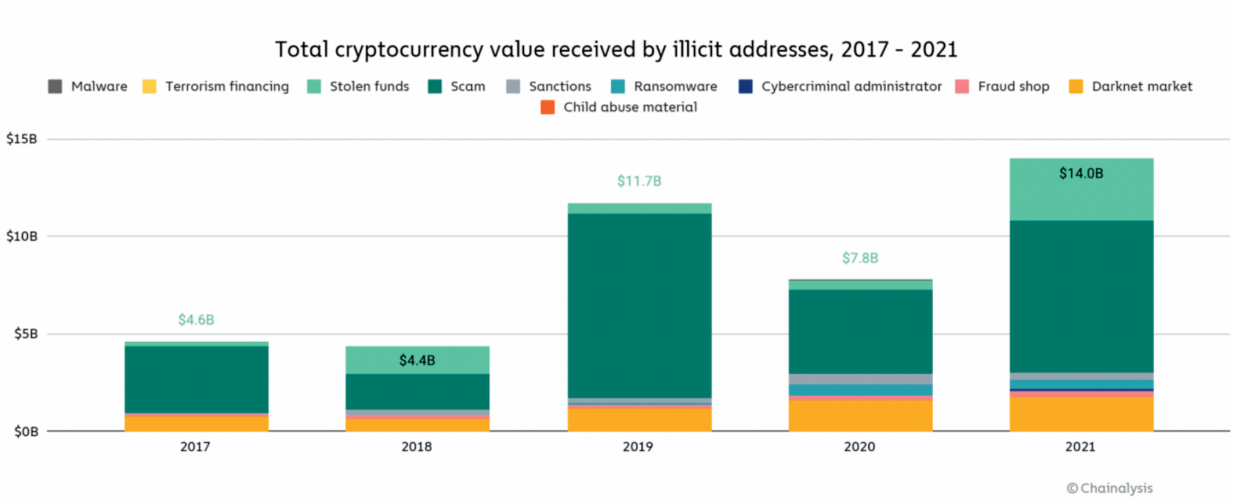
Quelle que soit l'option choisie, elle nécessite impérativement la réalisation d'une démarche de KYC, effectuée par le prestataire en question. Sont alors demandés : documents d'identité, adresses de contacts, preuves de domiciliation… et parfois même des justificatifs de provenance des fonds. **Personne ne peut donc légitimement acheter des crypto-actifs sans se soumettre à un processus de contrôle d'identité, ce qui, logiquement, limite les risques.**

Même chose pour les retraits. À moins de dépenser directement ses crypto-actifs dans des commerces, tout individu doit les convertir de nouveau en monnaie légale pour pouvoir profiter de ses éventuelles plus values. En d'autres termes, **s'il est effectivement possible d'utiliser des cryptomonnaies anonymisées pour effectuer des transactions masquées, celles-ci doivent être achetées, déjà, puis reconverties, ensuite. Et pour chacune de ces étapes, pas le choix : il faut être identifié.**

Enregistrée auprès de l'AMF en tant que Prestataire de Services sur Actifs Numériques n°E2022-035

IV - Qu'en disent les chiffres ?

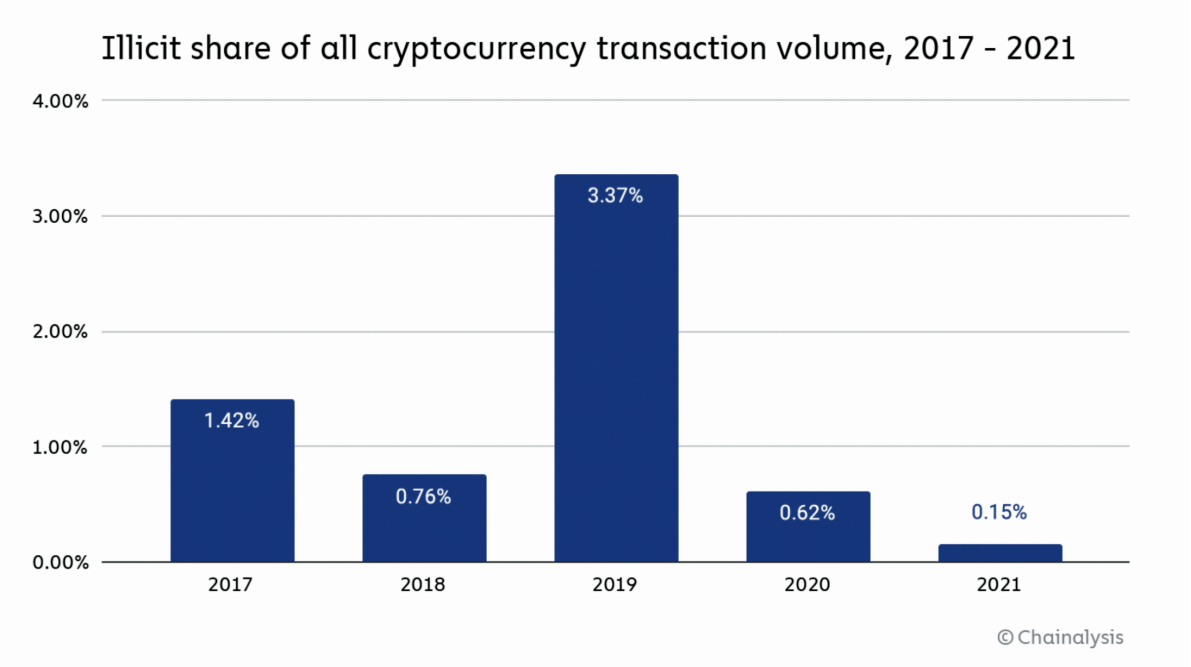
En 2021, selon Chainalysis, les adresses illicites, c'est-à-dire les adresses identifiées à des activités illégales comme le vol, la cybercriminalité ou les schémas de Ponzi, ont vues transiter **un total de 14 Mrds $, soit près de deux fois plus que l'année précédente. Un record.**



Montant total attribué aux activités illicites sur la blockchain, de 2017 à 2021

Mais il serait peu pertinent de s'arrêter sur celui-ci, puisque **dans le même temps, les transactions totales enregistrées sur les blockchains ont grossi de… 567%.** Étant donnée l'adoption massive des crypto-monnaies, voir les volumes de transactions illégales augmenter est tout sauf une surprise. Les voir augmenter infiniment moins rapidement que l'ensemble du marché, en revanche, en est une grosse.

S'il fallait retenir un seul chiffre, donc, ce serait plutôt celui-ci : **la part des transactions définies comme illégales sur le marché des cryptos s'élève à 0,15% en 2021, soit près de 4x moins qu'en 2020.**



Par des transactions en crypto-actifs définie comme illégale, de 2017 à 2021

Encore une fois, la blockchain possède l'immense avantage d'une traçabilité totale là où notre système financier actuel est structurellement plus opaque, et donc plus difficile à déchiffrer.

Néanmoins, les dernières recherches de l'Office des Nations Unies contre la drogue et le crime tablent sur un **montant total d'activités illicites sur le marché financier traditionnel, en 2020, de 2 100 milliards de dollars, soit environ 3,6% du PIB mondial.** Plus du double de la capitalisation totale du marché des crypto-actifs...

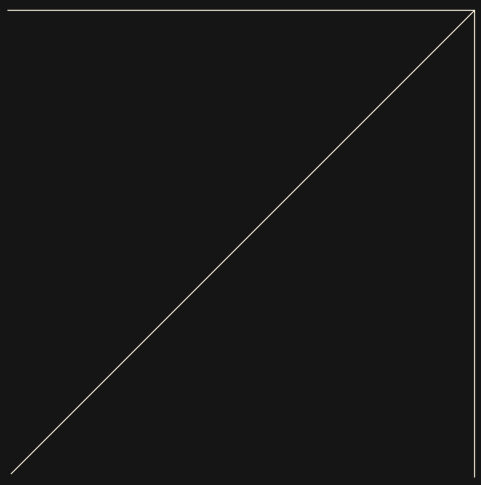
Tout n'est donc pas idéal sur les secteur des crypto-monnaies, et il est en partie vrai d'affirmer que certains projets favorisent le développement d'activités illégales.

Cependant, il convient de noter que ces projets sont très peu développés, de plus en plus esseulés et facilement identifiables. **Il revient donc à tout acteur intègre et honnête d'exclure ces quelques projets douteux de son champ d'investissement, et de continuer à traiter directement avec l'immense majorité des crypto-actifs dont l'usage est parfaitement légal.**

EN BREF

- Le sulfureux site Silk Road, très utilisé entre 2011 et 2013, a écorné l'image de Bitcoin ;
- La plupart des crypto-actifs sont pseudonymes, et non pas anonymes. Chaque utilisateur est donc identifiable par une adresse publique, dont les informations sont partagées à tous sur la blockchain ;
- Quelques rares crypto-actifs, créés sur des mécanismes Zero Knowledge, ont fait en sorte de rendre leurs transactions difficilement traçables ;
- Néanmoins, ces derniers se retrouvent souvent rendus indisponibles à l'achat, tandis que leur mécanisme d'anonymisation est régulièrement décodé ;
- En outre, toute action de vente/achat de crypto-actif doit auparavant faire l'objet d'un processus KYC sur une plateforme centralisée ;
- Si le volume de transactions illégales en crypto-actifs, parallèlement à l'essor du secteur, a augmenté en 2021, leur part sur l'ensemble des transactions ne cesse de diminuer ;
- 0,15% des transactions en crypto-actifs étaient reliées à des activités illicites en 2021, un chiffre bien inférieur à la part d'activité illicite estimée sur le marché financier traditionnel.

Enregistrée auprès de l'AMF en tant que Prestataire de Services sur Actifs Numériques n°E2022-035



mon
livret C

monlivretc.com

contact@monlivretc.com