Typologie juridique des infractions en matière de crypto-actifs

Fiche pratique publié le **01/01/2025**, vu **162 fois**, Auteur : Yanis MOUHOU

Cet article aborde les différentes méthodes de fraude et les réponses juridiques existantes, ainsi que les nouveaux défis de régulation.

Les crypto-monnaies ont radicalement transformé l'industrie financière, en apportant de nouvelles possibilités d'investissement et de transactions à l'échelle mondiale. Cependant, l'absence de régulation uniforme, la décentralisation et l'anonymat relatif des transactions ont également ouvert la voie à des pratiques frauduleuses. Les fraudes liées aux crypto-monnaies sont devenues un problème majeur pour les régulateurs et les investisseurs. Du piratage de plateformes d'échange aux escroqueries pyramidales, en passant par les faux ICO (Initial Coin Offering), les types de fraude sont multiples et variés.

1. Les Méthodes de Fraude les Plus Courantes en Matière de Crypto-monnaies

1.1. Phishing et Vol de Clés Privées

Le phishing est l'une des méthodes les plus courantes de fraude dans le secteur des crypto-monnaies. Cette technique consiste à tromper les utilisateurs pour qu'ils révèlent leurs informations de connexion ou leurs clés privées (qui permettent d'accéder à des portefeuilles de crypto-monnaies). Les fraudeurs créent des sites Web ou des emails semblant provenir de plateformes d'échange ou de portefeuilles de crypto-monnaies légitimes. L'utilisateur est incité à saisir ses informations personnelles, qui sont ensuite utilisées par les criminels pour transférer des fonds vers leurs propres portefeuilles.

Les attaques de phishing peuvent aussi concerner des smart contracts malveillants. En incitant les utilisateurs à interagir avec ces contrats (par exemple, en cliquant sur un lien malveillant), les fraudeurs peuvent accéder aux portefeuilles des victimes.

Réponse juridique : Le phishing est généralement considéré comme un crime lié à la fraude en vertu du droit pénal. Les législations sur les données personnelles, telles que le Règlement Général sur la Protection des Données (RGPD) en Europe, peuvent également s'appliquer en cas de vol de données personnelles sensibles.

1.2. Escroqueries par Ponzi et Schémas Pyramidaux

Les escroqueries par Ponzi et les schémas pyramidaux sont des pratiques frauduleuses classiques, qui se retrouvent dans le domaine des crypto-monnaies sous des formes variées. Ces escroqueries fonctionnent selon un modèle où les premiers investisseurs sont payés avec les fonds des nouveaux investisseurs, créant l'illusion de profits générés par un investissement légitime. Au fur et à mesure que le système se déstabilise, les investisseurs perdent leur argent.

Dans le domaine des crypto-monnaies, des ICO frauduleuses (Initial Coin Offering) ou des projets fictifs de tokenisation sont souvent utilisés pour attirer les fonds des investisseurs, en promettant des rendements élevés en échange d'investissements dans des projets qui n'existent pas réellement.

Réponse juridique : La fraude pyramidale est illégale dans de nombreuses juridictions, et les organismes de régulation comme la Securities and Exchange Commission (SEC) aux États-Unis et l'Autorité des Marchés Financiers (AMF) en France, poursuivent activement ces activités sous des lois sur les titres financiers et les escroqueries d'investissement.

1.3. Faux ICO (Initial Coin Offering) et Arnaques à l'ICO

Une ICO est une méthode de financement où une entreprise émet des crypto-monnaies ou des tokens en échange de fonds, souvent sous forme de cryptomonnaies telles que Bitcoin ou Ethereum. Les faux ICO ou les ICO frauduleuses sont des arnaques où une entreprise fictive propose des tokens qui n'ont aucune valeur réelle ou un produit non existant. Ces arnaques attirent généralement de grands nombres d'investisseurs en promettant des rendements élevés ou en utilisant des discours marketing agressifs.

Les scams ICO incluent souvent des sites Web qui imitent des projets légitimes, des bluffeurs qui font des promesses irréalistes, et des tokens qui ne sont jamais lancés ou qui n'ont aucune utilité dans le projet. En 2017, par exemple, des millions de dollars ont été perdus dans des ICO qui se sont avérées frauduleuses.

Réponse juridique : Selon les juridictions, les ICO frauduleuses peuvent être poursuivies sous les lois de la fraude, des titres financiers ou de la protection des consommateurs. Aux États-Unis, la SEC a introduit des actions contre plusieurs ICOs pour non-enregistrement des titres. Dans l'UE, des actions similaires sont entreprises sous l'égide des lois sur les abus de marché.

1.4. Manipulation de Marché et Pump and Dump

La manipulation de marché en crypto-monnaies, souvent appelée "Pump and Dump"
, consiste à manipuler artificiellement le prix d'un actif (généralement un altcoin ou un token) pour inciter les autres investisseurs à acheter en masse, gonflant ainsi son prix. Une fois que la valeur est artificiellement augmentée, les fraudeurs vendent leurs actifs à un prix élevé, laissant les autres investisseurs avec des actifs dont la valeur chute rapidement.

Les groupes organisés de traders peuvent également organiser des pumps via des plateformes de messagerie et des réseaux sociaux, créant des vagues d'achats spéculatifs.

Réponse juridique : La manipulation de marché est illégale dans la plupart des juridictions et est régie par les lois sur l'abus de marché. La Commodity Futures Trading Commission (CFTC) aux États-Unis et l'Autorité des Marchés Financiers (AMF) en France ont ouvert des enquêtes sur les manipulations de marché dans le secteur des crypto-monnaies.

1.5. Hacking et Piratage de Plateformes d'Échange

Les piratages de plateformes d'échange de crypto-monnaies constituent l'une des méthodes de fraude les plus médiatisées et souvent les plus dommageables. Les

hackers exploitent des failles de sécurité dans les systèmes de sécurité des plateformes d'échange pour voler des fonds des utilisateurs. Ces attaques peuvent viser des exchanges centralisés ou des portefeuilles numériques. Par exemple, le piratage de Mt. Gox en 2014 a entraîné la perte de plus de 450 millions de dollars en crypto-monnaies.

Les attaques par ransomware sont également fréquentes, où les fraudeurs exigent des paiements en crypto-monnaies, sous menace de publier des données sensibles ou de perturber des services.

Réponse juridique : Le piratage est une infraction criminelle en vertu des lois sur la cybercriminalité . Les victimes de piratages peuvent porter plainte sous des juridictions locales, et les autorités collaborent souvent au niveau international pour traquer les cybercriminels.

2. Réponses Juridiques aux Fraudes en Matière de Crypto-monnaies

2.1. Régulation et Sécurisation des Plateformes d’Échange

Pour contrer les fraudes, de nombreuses juridictions ont renforcé les régulations des plateformes d’échange de crypto-monnaies. Par exemple, des régulations imposent aux plateformes d’échange d'être enregistrées auprès des autorités financières et de respecter des normes de sécurité élevées, telles que la mise en place de mécanismes de double authentification (2FA), de cryptage des données des utilisateurs et des procédures de vérification de l'identité (KYC - Know Your Customer).

2.2. Réglementation des ICO et des Cryptomonnaies

Les régulateurs, en particulier dans des pays comme les États-Unis, le Royaume-Uni et la France , ont intensifié leur surveillance des ICO et des crypto-monnaies en exigeant des entreprises qu'elles respectent les régulations relatives aux titres financiers, aux abus de marché, et à la protection des consommateurs. L’action de la SEC contre certaines ICO frauduleuses a marqué un tournant dans la régulation des crypto-actifs.

2.3. Enquêtes et Collaborations Internationales

La lutte contre la fraude dans le domaine des crypto-monnaies nécessite une coopération internationale. Des organismes de régulation, comme l'Interpol et l'EUROPOL, ainsi que des agences nationales comme la FBI aux États-Unis, mènent des enquêtes sur des fraudes internationales liées aux crypto-monnaies. Des arrangements de coopération transfrontalière sont essentiels pour traquer et poursuivre les fraudeurs opérant à l'échelle mondiale.

3. Défis à surmonter pour la Régulation de la Fraude Crypto

Les principaux défis pour la régulation des fraudes en matière de crypto-monnaies résident dans la nature décentralisée de nombreuses plateformes de crypto-monnaies et le manque de régulations harmonisées à l’échelle mondiale. De plus, la difficulté à tracer les transactions sur les blockchains anonymes, telles que Monero ou Zcash, complique la tâche des autorités pour identifier les fraudeurs.