De l'application du droit pénal aux crypto-actifs

Actualité législative publié le **25/01/2025**, vu **40 fois**, Auteur : Yanis MOUHOU

La multiplication des vols et séquestrations dans le monde des crypto-actifs soulève des enjeux de sécurité et de réponse juridique nouvelle. Voici un panorama des principales infractions pénales.

Les infractions pénales en matière de crypto-monnaies : enjeux juridiques et techniques

Introduction

Les crypto-monnaies, telles que le Bitcoin, Ethereum ou Ripple, représentent une évolution significative des systèmes financiers traditionnels. Toutefois, leur nature décentralisée et leur anonymat apparent les rendent également attrayantes pour des activités illicites. En conséquence, le droit pénal a été confronté à de nouveaux défis pour identifier, réglementer et sanctionner les infractions liées à ces actifs numériques. Cet article explore les principales infractions pénales en matière de crypto-monnaies, leurs spécificités techniques et les outils juridiques disponibles pour les combattre.

---

1. Les typologies des infractions liées aux crypto-monnaies

Les infractions pénales liées aux crypto-monnaies se regroupent en plusieurs catégories majeures :

1.1 **Le blanchiment d’argent**

Le caractère pseudonyme des transactions sur les blockchain favorise leur utilisation pour le blanchiment de fonds. Les criminels utilisent souvent des techniques comme le "mixing" ou le "tumbling" pour dissimuler l'origine des fonds.

Exemple : L’utilisation de services comme Tornado Cash pour fragmenter les transactions afin de les rendre inexploitables par les outils d’analyse blockchain.

Références juridiques :

- Directive (UE) 2015/849 relative à la prévention de l’utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (Directive AMLD4).
- En France, l’article 324-1 du Code pénal punit de cinq ans d’emprisonnement et de 375 000

euros d’amende le fait de faciliter la justification mensongère de l’origine de biens ou de revenus.

1.2 **La fraude et l’escroquerie**

Les escroqueries en matière de crypto-monnaies incluent les schémas Ponzi, les ICO frauduleuses (Initial Coin Offering) et les "rug pulls", où les développeurs abandonnent un projet après avoir collecté des fonds.

Exemple : BitConnect, un schéma Ponzi mondial ayant entraîné des pertes de milliards de dollars.

Références juridiques :

- Article L313-1 du Code pénal : « L’escroquerie est le fait, soit par l’usage d’un faux nom ou d’une fausse qualité, soit par l’abus d’une qualité vraie, soit par l’emploi de manoeuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d’un tiers, à remettre des fonds, des valeurs ou un bien quelconque ».
- Les peines prévues incluent jusqu’à cinq ans d’emprisonnement et 375 000 euros d’amende.

1.3 **Les cyberattaques**

Les vols de crypto-monnaies par piratage informatique, comme les attaques contre des plateformes d’échange (Mt. Gox, FTX), représentent une autre forme d’infraction. Les ransomwares, tels que WannaCry, exigent souvent des paiements en Bitcoin.

Références juridiques :

- Article 323-3 du Code pénal : Punit d’une peine de cinq ans d’emprisonnement et de 150 000 euros d’amende le fait d’accéder frauduleusement à un système de traitement automatisé de données.

1.4 **Le financement du terrorisme**

Des groupes terroristes utilisent les crypto-monnaies pour financer leurs activités, profitant de l’absence de surveillance centralisée.

Références juridiques :

- Article 421-2-2 du Code pénal : Le financement du terrorisme est puni de dix ans d’emprisonnement et de 225 000 euros d’amende.

---

2. Les spécificités techniques des infractions en crypto-monnaies

2.1 **Anonymat et pseudonymat**

Bien que les transactions sur la blockchain soient enregistrées publiquement, l’absence d’identités liées aux adresses complique la traçabilité. L’utilisation de monnaies privées comme Monero ou Zcash accentue ces défis.

2.2 **Irréversibilité des transactions**

Une fois qu'une transaction est validée, elle ne peut être annulée, ce qui favorise les escroqueries et rend difficile la restitution des fonds volés.

2.3 **Outils de dissimulation**

Des mécanismes comme les échanges pair à pair (P2P), les wallets non custodial et les mécanismes de mélange (“tumblers”) complètent l’arsenal des criminels.

---

3. Les cadres juridiques et les réponses pénales

3.1 **Réglementation internationale**

Des organisations comme le Groupe d’action financière (GAFI) ont publié des recommandations pour la lutte contre le blanchiment et le financement du terrorisme en crypto-monnaies. La règle du « travel rule » impose la transmission des informations sur les expéditeurs et bénéficiaires des transactions.

Référence juridique :

- Recommandation 16 du GAFI sur la transparence des transferts électroniques.

3.2 **Législations nationales**

Dans l’Union européenne, le règlement MiCA (Markets in Crypto-Assets) cherche à harmoniser les lois et renforcer la transparence. En France, le Code monétaire et financier impose l’enregistrement des prestataires de services sur actifs numériques (PSAN) auprès de l’AMF.

Références juridiques :

- Article L54-10-3 du Code monétaire et financier : Cet article impose aux prestataires de services sur actifs numériques d’être enregistrés et conformes aux réglementations en matière de lutte contre le blanchiment.

3.3 **Sanctions pénales**

Les lois nationales prévoient des sanctions pénales pour les infractions liées aux crypto-monnaies.

Exemples :

- Escroquerie (Article L313-1 du Code pénal) : Peine maximale de cinq ans d’emprisonnement et 375 000 euros d’amende.

- Blanchiment (Article 324-1 du Code pénal) : Puni de cinq ans d’emprisonnement et de 375 000 euros d’amende.

---

4. Les outils d’enquête et de prévention

4.1 **Analyse blockchain**

Des entreprises comme Chainalysis ou Elliptic développent des outils pour analyser les transactions et identifier les schémas suspects.

4.2 **Collaboration internationale**

Les forces de l’ordre collaborent à l’échelle internationale (Interpol, Europol) pour lutter contre les crimes transfrontaliers impliquant des crypto-monnaies.

4.3 **Education et sensibilisation**

Les institutions publiques et privées mettent en place des programmes de formation pour sensibiliser les utilisateurs aux risques liés aux crypto-monnaies.