QU'EST-CE QUE LA CRYPTO-MONNAIE ET COMMENT ÇA MARCHE ?

Décryptage de cet actif crypté !

Bitcoin, ripple, ether, nem, litecoin, dash ...la digitalisation de l'économie a entraîné l'apparition de nouveaux actifs, les crypto-monnaies, qui pour certains constituent une façon nouvelle de stocker, d'échanger et de gérer de la valeur et pour d'autres s'apparentent à des barbarismes d'un autre monde ! En réalité, de quoi s'agit-il ? Qu'est-ce que la crypto-monnaie et comment fait-on pour se la transmettre ?

Contrairement aux apparences, la crypto-monnaie n'est pas une monnaie : Selon l'Autorité des marchés financiers (AMF), une crypto-monnaie ou un crypto-actif désigne « des actifs numériques virtuels qui reposent sur la technologie de la blockchain (chaine de bloc) à travers un registre décentralisé et un protocole informatique crypté ». Plus largement, les crypto-actifs représentent des actifs virtuels stockés sur un support électronique permettant à une communauté d'utilisateurs les acceptant en paiement de réaliser des transactions sans avoir à recourir à la monnaie légale. Sur le plan juridique, **une crypto-monnaie n'est pas une monnaie** : elle **ne dépend d'aucune institution, ne bénéficie d'aucun cours légal** dans aucun pays ce qui rend l'évaluation de sa valeur difficile et **ne peut être épargnée** donc constituer une valeur de réserve.

En définitive, **une crypto-monnaie est tout simplement un actif crypté et sa transmission repose sur la technique de la cryptographie**. En cela, le monde numérique n'a rien inventé de nouveau puisque le cryptage est connu depuis l'antiquité ; pour des exemples, on peut citer la scytale ou bâton de Plutarque des Spartiates permettant l'inscription d'un message chiffré sur une fine lanière de cuir pouvant être déchiffré à l'aide d'un bâton d'un diamètre identique à celui utilisé pour l'encodage ou encore la grille de Cardan inventée en 1550 par Jérôme Cardan pour le codage et le décodage de messages secrets. **Le transfert des crypto-monnaies va donc se faire au moyen du cryptage d'un message réalisé grâce à l'utilisation d'une double clé** appelée clé cryptée ou clé asymétrique associée à un portefeuille ou « wallet ».

Clé de cryptage privée. La première clé est strictement privée. Il s'agit d'une signature alphanumérique secrète, soit un chiffre de 256 bits auquel personne d'autre que le titulaire n'est censé avoir accès.

Elle est encodée de façon à en condenser l'écriture sur cinquante et un caractères et peut être représentée sous forme de QR code (exemple de clé privée :5jd4kDBTjnDmQwLv94gjWheWwsrmRMGfLj438BBLdRtw4axSAy). Cette clé privée ne doit pas être divulguée car elle permet à son titulaire d'accéder au portefeuille de crypto-actifs. Celui qui en a le contrôle a donc tous les pouvoirs sur les transactions et les dépenses liées aux fonds sur cette adresse.

Clé de cryptage publique. À partir de la clé privée, une deuxième signature est déduite, appelée clé publique. Celle-ci peut toujours être calculée en partant de la clé privée, tandis que l'inverse est impossible, d'où l'appellation de « cryptographie à clés asymétriques ». Elle fait l'objet d'opérations successives de « hachage » dont le résultat, toujours compris entre vingt sept et trente-quatre caractères, constitue une « adresse » (exemple de clé publique : 1BFW79d584dt2RXDBTsqBjnYe LWtgRjVhk).

Une comparaison pourrait être faite avec un coffre-fort : la clé publique qui est connue de tous correspond à l'adresse du lieu où se trouve le coffre-fort et la clé privée est celle qui permet de l'ouvrir.

Modalités d'un transfert. S'agissant des crypto-monnaies, la clé publique permet à des tiers d'effectuer des paiements à l'adresse du portefeuille tandis que la clé privée permet de dépenser à partir de cette adresse. Ainsi, le créancier communique son adresse, c'est-à-dire sa clé publique à son débiteur. Celui-ci initie alors, à l'aide de sa clé privée, le transfert que le créancier accepte avec sa propre clé privée. En définitive, le portefeuille ne détient pas des crypto-actifs mais uniquement des clés auxquelles les membres d'un réseau décentralisé reconnaissent le pouvoir d'associer un nombre donné d'unités. Ce réseau décentralisé permettant de retracer toutes les opérations réalisées et garantissant le stockage, l'émission, la transmission ou l'échange de l'actif est un grand registre sécurisé appelé blockchain.

Détention directe ou indirecte des clés. Il convient enfin de noter que ces clés peuvent être détenues de deux manières : par détention indirecte ou directe.

La détention indirecte se fait par le biais de plateformes dont les plus connues sont les plateformes Coinbase et Binance. Ces dernières détiennent les comptes crypto-monnaies de leurs clients, et donc les clés privées de ceux-ci. L'accès aux comptes se fait alors sur internet comme pour une banque classique avec un mot de passe. Ce système est risqué car les plateformes peuvent être piratées ou faire faillite comme dernièrement la faillite de la plateforme exchange FTX.

La détention directe peut se faire soit par le biais d'un portefeuille papier dans lequel les clés sont conservées (sur une simple feuille, dans un fichier ou sur une clé USB), soit par le biais d'un portefeuille froid se présentant sous la forme d'un mini-ordinateur (« hardware wallet » ou portefeuille électronique) de la taille d'une grosse clé USB qui, pour fonctionner, devra être raccordé à un ordinateur.

Ni une monnaie, ni un actif tangible, la crypto-monnaie est un actif crypté, émis et échangeable sur une blockchain et dont la valeur obéit aux règles immuables de l'offre et de la demande.

Gence & Associés
Notaires

Notaire

Étude de Rouen : 105 Rue Jeanne d'Arc, 76000 Rouen 02 35 07 82 90
Étude de Paris : 133 boulevard Haussmann, 75008 Paris 01 88 53 00 20
accueil@gence-associes.fr www.gence-associes.notaires.fr