



Blockchain, crypto-actifs et les défis d'un monde décentralisé

par Yrieix Denis

HUBERT DE VAUPLANE



AVOCAT

Avocat chez Morgan Lewis et docteur en droit, Hubert de Vauplane est expert en blockchain et en crypto actifs, notamment auprès de la Banque Mondiale. Président du Think Tank Legal Blockchain & Cryptos Association, il enseigne par ailleurs à l'École de Droit de Sciences Po Paris.

Les crypto actifs, régulièrement associés aux affaires de fraude et de cybercriminalité, méritent-ils la mauvaise presse qu'on leur fait depuis leur création ?

Pour comprendre d'où leur vient cette mauvaise réputation, il faut distinguer deux phases dans l'histoire des cryptomonnaies. À leurs débuts, entre 2008 et 2018, elles étaient encore très confidentielles et restaient l'apanage des geeks, des libertariens et des activités illicites. C'est en quelque sorte leur « péché de jeunesse ». Les organes de police n'étaient pas encore familiers de la *blockchain* ou des cryptomonnaies, et encore moins outillés pour en faire la traque. Mais à partir de 2020, cette situation a complètement changé. Les polices

mondiales se sont formées et équipées. Aujourd'hui, si les cryptomonnaies sont encore utilisées dans le cadre des *ransomware* par exemple, elles sont de moins en moins utilisées par le crime organisé.

C'est ce qu'en effet ce que démontrent les études menées par Chainalysis : les transactions illicites en crypto ne représenteraient « plus que » 0,34 % du volume total des transactions en 2023, contre 0,42 % l'année précédente. La majorité de ces activités illicites sont par ailleurs liées à des entités déjà sanctionnées. En 2023, sur 186 000 signalements à Tracfin, seulement 1449 concernent les PSAN. Le Trésor américain a en outre publié un rapport qui met en évidence une plus grande proportion de blanchiment via les monnaies liquides que via les cryptos actifs.

Ce qui rejoint les études du Nasdaq : sur les 3 100 milliards de dollars qui ont transité illicitement dans le système financier mondial en 2023, seulement 24,2 milliards de dollars concernaient la *blockchain*.

L'actualité la plus récente vient renforcer ces observations. Dans la tragique affaire de la prise d'otage d'un des fondateurs de Ledger, comme dans la *hack* spectaculaire qui a frappé Bybite grâce à une intrusion d'une redoutable sophistication, les criminels ne sont pas parvenus, jusqu'à maintenant en tout cas, à écouler les cryptomonnaies qu'ils ont extorquées ou subtilisées. Pourquoi ? Parce que la très grande majorité des crypto-actifs ne garantissent pas un anonymat mais un pseudonymat. Ce qui permet une traçabilité propre au code alphanumérique spécifique à chaque adresse sur la *blockchain*. Il est possible de remonter la chaîne jusqu'aux détenteurs, d'autant plus que la grande majorité des plateformes collaborent activement avec les enquêteurs. Ce qui ne permet pas la monnaie traditionnelle. C'est là-dessus que les services de police se sont considérablement outillés. Ils font face cependant à de nouveaux obstacles avec les services de « mixer » et de VPN, qui freinent l'identification des détenteurs.

Comment expliquer la défiance persistante des États et de certaines institutions financières à l'égard des crypto-actifs ?

Il y a, dès le départ, une irréconciliable opposition philosophique. La *blockchain*, décentralisée par essence, va à l'encontre de la logique des États et des banques centrales dont la mission est de produire et contrôler la monnaie légale. Comme disait Hayek, l'idée même d'une « libre concurrence des monnaies » n'entre pas dans leur schéma de pensée. Du coup, pour une banque centrale, les crypto-monnaies sont perçues comme de potentielles concurrentes, et pour un État, ce sont des vecteurs de déstabilisation : on ne peut pas exercer de coercition directe à leur encontre ni leur imposer de surveillance stricte. C'est un espace de liberté totale, puisqu'il n'y a pas d'autorité centrale pour contrôler ou censurer les flux.

Il faut par ailleurs se rappeler les positions défendues par Satoshi Nakamoto en 2008, dans le contexte de la crise de 2007. Les banques centrales, pour faire face à la crise, ont inondé le marché de liquidités, générant plus de dettes et d'inflation monétaire.

Satoshi Nakamoto posait le Bitcoin en alternative : son émission est plafonnée à 21 millions, il est décentralisé, donc « non inflationniste ». On comprend qu'il soit difficile pour une banque centrale, dont la mission est de piloter la politique monétaire au nom de l'intérêt général, d'accepter cette forme de monnaie parallèle, à la fois autogérée et à l'abri de ses interventions.

Quant aux banques commerciales, elles aussi ont des réticences. Leurs modèles reposent sur la création de dette et sur le lien intime qu'elles entretiennent avec la monnaie des banques centrales. Les cryptomonnaies remettent potentiellement en cause ce schéma. Beaucoup de banques en sont encore au stade où elles associent les cryptos à des usages douteux et au trafic illicite, sans trop regarder les avancées technologiques de la *blockchain*. Pourtant, aux États-Unis, des établissements financiers ont déjà commencé à s'y intéresser sérieusement, et cette dynamique pourrait forcer les banques européennes à suivre le mouvement. Les lignes bougent vite, mais la crainte d'une concurrence sur le terrain monétaire reste un frein majeur, tant pour les États que pour de nombreuses institutions financières.

Quelles perspectives faites-vous de la conjonction entre l'intelligence artificielle et la blockchain ?

Dans la finance traditionnelle comme dans l'univers crypto, l'intelligence artificielle va remplacer une partie du travail humain, en particulier dans la gestion et le trading. Les crypto-actifs fonctionnent déjà via des *smart contracts*, un faux-ami qui désigne une « exécution automatisée d'un protocole informatique ». En couplant cette automatisation à l'intelligence artificielle, on peut imaginer beaucoup d'applications : exécutions ultra-rapides d'ordres de marché, détection en temps réel de fraudes ou d'anomalies, le tout sans intervention humaine. C'est à la fois fascinant et inquiétant : on sort l'humain de la boucle et on laisse un algorithme gérer la majorité des opérations. On gagne en efficacité, on réduit les coûts et le risque d'erreur, mais on touche à des questions plus philosophiques. Et si le code se trompe ? Peut-on revenir en arrière ? Le fameux *Code is Law* de Lawrence Lessig pose de vrais défis de gouvernance, auxquels l'IA ne fera que donner plus d'ampleur. ✨