

LES CRYPTO-ACTIFS : DU MIRAGE À LA RÉALITÉ

PENSER L'IMPACT FINANCIER, ÉCONOMIQUE, ÉCOLOGIQUE ET POLITIQUE DES CRYPTO-ACTIFS

Auteurs : Nicolas Dufrêne, Jean-Paul Delahaye, Jean-Michel Servet,
Pierre Krajewski, Clément Fabien, Paul Hannat

Préface d'Emmanuel MAUREL, député européen



Décembre 2022

À la demande du Groupe confédéral LA GAUCHE



Parlement européen
Emmanuel MAUREL
Rue Wiertz, 60
B-1047 Bruxelles, Belgique

emmanuel.maurel@europarl.europa.eu

Décembre 2022

Photo de couverture : © Mohamed Hassan - Pixabay

Les crypto-actifs : du mirage à la réalité

Penser l'impact financier, économique, écologique et politique des crypto-actifs

Auteurs : Nicolas Dufrêne (haut fonctionnaire, économiste et directeur de l'Institut Rousseau), Jean-Paul Delahaye (informaticien et spécialiste des questions relatives aux cryptoactifs), Jean-Michel Servet (économiste et spécialiste des questions monétaires), Pierre Krajewski (cadre dans une grande entreprise du numérique), Clément Fabien (cadre dans une grande institution financière publique), Paul Hannat (cadre dans une grande institution financière publique)

Table des matières

Préface.....	6
Introduction.....	9
Première partie : L'essor des crypto-actifs et leurs promesses.....	15
I. La nature polymorphe des crypto-actifs.....	15
A/ Une variété à croissance rapide de crypto-actifs, pour une multiplicité d'usages	15
B/ L'écosystème des crypto-actifs et sa hiérarchie : qui détient le pouvoir ?.....	22
C/ Un discours rôdé entre séduction de l'argument de la modernité et nouveau terrain de spéculation pour des acteurs financiers traditionnels.....	29
II. Une proposition monétaire aux allures de mirage	38
A/ La philosophie décentralisatrice et désintermédiée qui sous-tend les crypto-actifs : entre mythe et réalité	38
B/ Le bitcoin et le mirage d'une monnaie universelle	42
C/ L'illusion d'une souveraineté monétaire retrouvée	45
D/ Le risque du retour des monnaies privées et du libertarisme financier	49
Deuxième partie : Contenir l'impact des crypto-actifs sur la souveraineté monétaire et sur la stabilité financière	54
I. Une législation encore en construction qui doit s'adapter à des objets mouvants	54
A/ Les évolutions du droit européen relatif aux crypto-actifs	54
B/ Recension de quelques exemples étrangers	64
C/ Les travaux dans les différents forums internationaux	65
II. Aller plus loin dans la réglementation des crypto-actifs et adapter les institutions	66
A/ Aller plus loin dans la réglementation européenne	67
B/ Les risques pour le système financier traditionnel provoqués par les crypto-actifs	72
C/ Encourager la réflexion autour de monnaies numériques de banque centrale (MNBC) réellement accessibles aux citoyens et aux entreprises	79
D/ Le cas particulier des transferts internationaux d'argents (ou paiements transfrontières).....	84

Troisième partie : Intégrer les crypto-actifs dans la vie commune sans risque pour la société.....	89
I. Un environnement soumis à de nombreux risques techniques et technologiques, loin de la sûreté promise	89
A/ L'illusion de la décentralisation.....	89
B/ Les opérations sur des <i>blockchains</i> bien décentralisées	90
C/ Les risques criminels et sociaux majeurs liés à l'absence de réglementation adéquate des crypto-actifs.....	92
II. Réduire l'impact écologique et la consommation énergétique des crypto-actifs par l'interdiction progressive des protocoles dits « <i>proof of work</i> »	99
A/ La consommation électrique du minage.....	100
B/ L'impact écologique des crypto-actifs et l'interdiction progressive de la "preuve de travail"	100
C/ Sécurisation du fonctionnement du réseau	101
D/ Les comparaisons avec le système bancaire traditionnel n'ont pas de sens	103
Conclusion	105
Récapitulatif des propositions	106
Glossaire	108

Préface

Chers Lecteurs,

Seule une petite communauté de créateurs, développeurs, mathématiciens et informaticiens de très haut vol savent vraiment ce qu'est un cryptoactif.

Pour l'écrasante majorité des gens, y compris ces fameux « mineurs » qui fabriquent Bitcoins et autres cryptomonnaies dans d'immenses entrepôts bourrés de processeurs de calcul, y compris les banquiers de Wall Street qui ont pris le train en marche quand les cours ont explosé, y compris les responsables politiques appelés à réguler cette technologie, la chose demeure extrêmement opaque, voire carrément incompréhensible.

Même chose pour la « blockchain », ce programme qui permet d'effectuer les transactions et de comptabiliser les cryptoactifs. Depuis des années on nous vante ses vertus révolutionnaires - notamment le caractère sécurisé et décentralisé, mais on nous avertit aussi des risques de la blockchain, au premier rang desquels la consommation d'électricité faramineuse, insoutenable à long terme.

Après des années d'euphorie et pour paraphraser un ancien gouverneur de la Réserve Fédérale américaine, « d'exubérance irrationnelle », ces derniers mois semblent avoir remis les pendules à l'heure. Il n'y a rien de magique dans les cryptoactifs et ceux qui y voyaient la solution à tous les problèmes (on pense au Salvador, qui a adopté le Bitcoin comme devise officielle) sont nombreux à encaisser les pertes.

Nous sommes tous détenteurs de monnaie, consommateurs et épargnants. Et nous sommes tous citoyens, attachés à la démocratie, convaincus que seule la délibération collective est légitime à autoriser, promouvoir et encadrer tout procédé et toute pratique ayant un impact sur la société. Nous avons donc tous l'obligation non pas d'être spécialistes de A à Z des cryptoactifs et de la blockchain, mais d'en comprendre les principes, l'idéologie sous-jacente et les conséquences financières, juridiques, sociales et politiques.

Nicolas Dufrêne, directeur de l'Institut Rousseau, l'un des meilleurs « think-tanks » français, a rassemblé une équipe de cadres et chercheurs disposant des connaissances et de la pédagogie nécessaires à la compréhension des défis posés par les cryptoactifs.

Dans cette étude parfaitement documentée, ils nous aident à trouver notre chemin dans ce labyrinthe et sans jamais verser dans les slogans simplistes et les jugements à l'emporte-pièce, explorent les pistes techniques et juridiques à même d'intégrer les cryptoactifs dans la vie commune sans risque pour la société. Je les remercie vivement pour leur excellent travail.

Emmanuel MAUREL

Député européen

Membre du groupe parlementaire LA GAUCHE

Gauche Républicaine et Socialiste

Introduction

En novembre 2021, le marché des crypto-actifs dépassait, pour la première fois de son histoire, la barre symbolique des 3000 milliards de dollars (Apple, première entreprise par sa capitalisation boursière, représente environ 2300 milliards de dollars en fin d'année 2022). À peine dix mois plus tard, il était redescendu à moins de 800 milliards de dollars. Depuis, les nombreux scandales, dont le dernier en date est celui de la faillite de la plateforme FTX en novembre 2022, ont conduit à prolonger l'« hiver » des crypto-actifs. Les promoteurs des crypto-actifs veulent ne voir dans ce retournement intense du marché qu'une crise de croissance, violente certes mais surmontable, tandis que ceux qui posent un regard critique sur le développement des crypto-actifs observent la concrétisation de craintes exprimées de longue date. Certaines institutions parlent même d'un « dernier souffle artificiellement induit avant la route vers l'insignifiance » pour décrire les mouvements récents du bitcoin¹. L'insuffisance, pour ne pas dire l'absence, de réglementation, les fraudes, les vols, les aventures personnelles, les manipulations de marché à grands renforts d'influenceurs, les problèmes de liquidité, de solvabilité et de transparence ont à ce jour largement entaché l'image et la confiance du public dans les crypto-actifs.

Ainsi, force est de constater que, jusqu'à présent, le marché des crypto-actifs a essentiellement pris les traits d'un vaste marché spéculatif, sans règles minimales de sécurité. Beaucoup de simples citoyens y ont perdu de l'argent : selon un rapport de la banque des règlements internationaux (BRI)², de 73 à 81 % des investisseurs particuliers à travers le monde ont perdu de l'argent sur leurs investissements dans le bitcoin entre 2015 et 2022. Si l'allégorie d'un « Far-west financier » n'est pas usurpée s'agissant du marché des crypto-actifs, la question des crypto-actifs ne peut pourtant pas se résumer à celle d'un « marché » financier balbutiant à propos duquel il suffirait de définir des paramètres adéquats de réglementation. En effet, les pratiques et l'idéologie qui accompagnent l'essor des crypto-actifs posent des questions – et des difficultés – bien plus profondes à l'ordre public, social et monétaire, à l'égalité des citoyens et à l'unité des systèmes économiques, qui demeurent trop souvent sous-estimées. En outre, les valeurs et les idéaux libertariens véhiculés par l'écosystème des crypto-actifs n'ont rien de neutre.

Plus encore que dans les autres marchés spécialisés, l'apparente technicité et le vernis de l'innovation conduisent cependant les personnes qui vivent de ce marché à en faire une promotion souvent trompeuse. Ainsi, les crypto-actifs auraient dû servir, selon leurs

¹ [Bitcoin's last stand, ECB Blog, 30 nov. 2022](#)

² [BIS Working Papers \(1049\), Crypto trading and Bitcoin prices: evidence from a new database of retail adoption, R. Auer & al., nov. 2022](#)

promoteurs, à rendre le système financier et monétaire non seulement plus efficient, plus inclusif et plus délibératif ; mais aussi plus transparent, plus rapide, plus simple et moins coûteux au niveau des paiements et des transferts de fond internationaux, et cela tout en facilitant le financement de l'innovation. Or, la quasi-totalité de ces promesses, à l'exception peut-être du financement de l'innovation via les *Initial coin offerings* (ICO, voir glossaire), se sont échouées sur le rivage de la réalité.

S'il est évident que les crypto-actifs ne remplissent pas, ou de manière très imparfaite, les fonctions d'une monnaie (ils ne sont ni une unité de compte permettant de libeller le prix des biens et services, ni un instrument de transaction puisqu'ils servent pour le moment assez peu à régler des achats de biens ou services dans l'économie réelle, ni une véritable réserve de valeur car leur cours contre les monnaies légales est encore trop volatil), leur plus-value sur le terrain des transferts de fonds n'est pas non plus probante. Le resserrement des politiques monétaires, qui a contraint les spéculateurs à davantage de prudence, s'est instantanément traduit par une chute du cours des principaux crypto-actifs, révélant par là leur nature d'actif spéculatif risqué, et non de refuge contre l'inflation ou de réserve de valeur comme ont voulu le faire croire certains de leurs promoteurs. Le pouvoir des citoyens sur la gouvernance des crypto-actifs est la plupart du temps complètement inexistant, exception faite de quelques expériences isolées dans le domaine de la finance décentralisée (« DeFi »). L'automatisme induite par des protocoles informatiques contraste avec la nécessaire délibération circonstanciée qui doit caractériser la gouvernance d'un bien commun tel que la monnaie. Quant à la transparence, elle est quasiment inexistante puisque la traçabilité des opérations sur la *blockchain* s'accompagne de mécanismes de pseudonymisation qui aboutissent *in fine* à une anonymisation bien réelle des transactions. Enfin, si le risque financier que constituent les crypto-actifs n'a pas encore provoqué de crise financière majeure, c'est que les marchés traditionnels ont longtemps évité de s'engouffrer dans ce marché très volatil. Mais ces digues pourraient bien céder à l'avenir si rien n'est fait pour prévenir cette contagion. Ce risque est d'autant plus prégnant à mesure que les autorités publiques et régulateurs semblent légitimer le fonctionnement des acteurs les plus opaques du secteur, comme en a récemment témoigné l'enregistrement de la plateforme chinoise Binance auprès de l'Autorité des marchés financiers française (AMF).

Au-delà de la question financière, la prolifération de crypto-actifs ayant une portée monétaire globale, comme le bitcoin, pose par ailleurs la question de la définition même de la monnaie et de l'organisation du système monétaire international. Ainsi les promoteurs des crypto-actifs prônent souvent, par conviction ou par ignorance, des systèmes monétaires organisés autour du principe de concurrence des monnaies, dans lequel toute politique monétaire autonome, centralisée et souveraine deviendrait impossible. À la différence des monnaies locales qui cherchent à établir une complémentarité avec l'ordre monétaire officiel, certains crypto-actifs

cherchent à s'émanciper de ce dernier, voire à le concurrencer. Or l'émergence de systèmes monétaires parallèles pose des questions fondamentales en matière de souveraineté des États, de solidarité nationale, de fiscalité et de cohésion des systèmes économiques. Ceux-ci ne peuvent pas en sortir gagnants, y compris pour des États en développement : l'exemple désastreux du Salvador faisant du bitcoin une monnaie officielle devrait servir d'avertissement. À l'intérieur des sociétés, une généralisation des crypto-actifs et une reconnaissance légale pourrait conduire à installer un système monétaire et financier parallèle dans lequel des transactions pourraient déroger au droit commun, favorisant les « *insiders* » au détriment de l'égalité entre les citoyens. Par ailleurs, l'irruption de grands groupes internationaux dans le monde des crypto-actifs ne va pas sans poser des enjeux de souveraineté pour les États. Le quasi-abandon du projet Libra porté par Facebook en 2019 ne doit ainsi pas faire oublier que plusieurs autres grands groupes internationaux cherchent à développer des monnaies privées pour accroître leur influence.

Il convient également de ne pas sous-estimer les risques posés par le marché des crypto-actifs en matière d'ordre public, dont de nombreuses institutions commencent à s'alarmer. En effet, ce « marché » offre de nombreuses possibilités de fraude, d'évasion fiscale, de blanchiment d'argent, de transactions illégales, de financement d'activités criminelles, de détournement d'argent et même de « racket numérique » à travers les « *ransomwares* »³(demandes de rançon payables en crypto-actifs) qui se multiplient au cours des dernières années, visant sans distinction des entreprises privées, mais aussi des hôpitaux, des prisons, des services publics. Il serait ainsi souhaitable et urgent de proposer l'interdiction de la diffusion et du commerce de crypto-actifs visant à garantir un anonymat complet en empêchant, par leur conception, toute procédure d'identification. C'est le cas d'un certain nombre de crypto-actifs (Monero, PIVX, DeepOnion, Zcash...) dont le but est de contourner toute possibilité d'identification des détenteurs. C'est aussi le cas d'applications de DeFi (ou *smart contracts*) comme Tornado Cash qui brise le lien entre destinataire et émetteur d'une transaction sur la *blockchain* et a été mis sur la liste noire de l'Office of Foreign Assets Control américain (OFAC)⁴. À ce jour, la régulation n'est malheureusement pas suffisamment contraignante.

Si ces dérives doivent appeler une réponse ferme et rapide, faut-il pour autant en conclure que rien n'est à sauver dans le système des crypto-actifs ? La réponse mérite d'être nuancée. Tout d'abord, le développement des crypto-actifs va de pair avec leur diversification croissante et l'on compte aujourd'hui plus de 20 000 crypto-actifs. Si les crypto-actifs de première génération, au premier rang desquels le bitcoin, dominent encore largement le marché, ils

³ Le rapport d'activité de TRACFIN (2021) précise ainsi qu'en « matière de rançongiciels, TRACFIN a transmis sept signalements à l'autorité judiciaire entre 2019 et 2020⁴⁵ dont les enjeux financiers vont de 11 000€ à 1,5M€, avec une moyenne de 240 000€ par dossier. »

⁴ <https://home.treasury.gov/news/press-releases/jy0916>

sont de plus en plus concurrencés par des crypto-actifs dont les usages, les objectifs, les modes d'émission, les possibilités d'échange ou encore les droits associés diffèrent. C'est pourquoi, si l'on reprend la définition du projet de règlement européen MiCA, donnée dans son article 3, un crypto-actif correspond plus largement à « la représentation numérique d'une valeur ou d'un droit qui peut être transféré et stocké électroniquement, en utilisant la technologie du grand livre distribué ou une technologie similaire ». Dans le détail, on retrouve ainsi les notions de « *stablecoins* » (crypto-actifs stables), de jetons de monnaie électronique, de jetons de service (« *utility tokens* »), de jetons non fongibles (« *non-fungible tokens* » ou « NFT »), d'instruments financiers numériques ou tokenisés (« *security tokens* ») ou encore de monnaie numérique de banque centrale (MNBC)⁵. Aborder la question des crypto-actifs en profondeur nécessite ainsi de faire preuve de discernement devant cette diversité que le droit peine encore à appréhender dans sa globalité. Des crypto-actifs visant à offrir de simples services financiers ou permettant de créer des organisations autonomes décentralisées (« DAO »), s'ils font l'objet d'une réglementation adaptée, peuvent certainement trouver leur place dans l'économie de demain.

Cette prudence ne doit pourtant pas se transformer en une forme d'inaction, justifiée au nom de l'innovation, face aux nombreuses dérives portées par ce marché émergent. C'est pourquoi il apparaît particulièrement urgent de « séparer le bon grain de l'ivraie » en matière de crypto-actifs, ainsi que l'avait récemment relevé un collectif de chercheurs, d'économistes et d'informaticiens⁶, dans l'intérêt même des innovations potentiellement utiles que pourraient receler ce secteur. Une réglementation suffisamment précise et ambitieuse pourrait ainsi aider cet écosystème à se débarrasser des usages les plus toxiques pour promouvoir les usages les plus intéressants, notamment en matière de désintermédiation et d'automatisation d'un certain nombre de tâches.

Pour cela, le projet de règlement européen sur les marchés de crypto-actifs (« Markets in Crypto-Assets » ou « MiCA ») ne suffira certainement pas. Celui-ci comporte certes plusieurs avancées importantes, telles qu'une obligation de déclaration et d'enregistrement concernant la mise sur le marché de nouveaux crypto-actifs ou des obligations de liquidité et de transparence concernant les plateformes, mais il fait l'impasse sur toute une série de sujets essentiels tels que la réglementation des crypto-actifs d'un point de vue écologique, le rôle des NFT, les garanties accordées au consommateur par les plateformes, la traçabilité des transactions et la lutte contre les usages criminels. La fiscalité demeure un trou noir, que pourrait par exemple en partie compenser une obligation de déclaration fiscale de la détention de crypto-actifs et non seulement des plus-values réalisées. À l'heure actuelle, le principe

⁵ Voir glossaire pour plus de détails.

⁶ « [La crainte de brider l'innovation ne doit pas freiner le besoin urgent de réglementation des cryptomonnaies](#) », Tribune, 10 fév. 2022

« même activité, même risque, même réglementation », auquel on pourrait rajouter « même taxation », est encore loin d'être pleinement appliqué à l'univers des crypto-actifs. C'est pourquoi de nombreux acteurs appellent d'ores et déjà à réfléchir à un « MiCA 2 ». Le présent rapport cherchera ainsi à formuler quelques principes et recommandations qui pourraient alimenter la réflexion en vue d'un second volet de réglementation.

Par ailleurs, si certains protocoles sont désormais moins énergivores, l'impact environnemental des technologies *blockchain* et des actifs numériques n'est pas négligeable dans le contexte du changement climatique. Ainsi, selon le cabinet spécialisé Digiconomist, le minage ou création d'un bitcoin, nécessite environ 1.150 kilowattheures, soit la consommation moyenne d'un foyer américain durant 40 jours. Un indice développé par l'université de Cambridge montre que ce 23 novembre, le minage de bitcoin consomme 90 térawattheures par an, soit près d'un quart de la consommation d'électricité française en 2019. Lors des périodes de forte hausse du prix du bitcoin, celui-ci consommait à lui tout seul plus d'électricité que la Belgique et la Suisse réunies. Il est néanmoins possible de ne pas passer par le minage et la « preuve de travail » : de nombreux réseaux de crypto-actifs ont recours à une validation par *proof of stake* ou « preuve d'enjeux » qui ne nécessite pas de réaliser des calculs avec des machines énergivores. Ethereum, deuxième crypto-actif le plus important en termes de capitalisation, a récemment adopté ce système et abandonné la « preuve de travail », ce que Bitcoin ne peut pas faire pour diverses raisons. La réglementation pourrait aller beaucoup plus loin sur ce sujet et aller jusqu'à interdire les protocoles de consensus trop consommateurs d'énergie, comme l'a récemment fait l'État de New-York aux États-Unis.

Sur ce sujet comme sur d'autres sujets liés aux crypto-actifs, le présent rapport cherchera à démontrer qu'il est important d'avoir conscience des risques et d'agir suffisamment tôt pour éviter leur matérialisation, avant que la logique dite de « bac à sable », c'est à dire une période de laissez-faire assumée au nom de l'épanouissement de l'innovation, ne conduise à installer des situations difficilement réversibles.

Le présent rapport traitera ainsi en premier lieu des raisons de l'essor des crypto-actifs, des acteurs de cet écosystème, de leur hiérarchie, du discours qu'il véhicule, pour mieux souligner les insuffisances actuelles de la réglementation et proposer des évolutions. La seconde partie sera davantage consacrée aux promesses et aux réalités de l'usage des crypto-actifs dans le domaine monétaire, en soulignant la continuité entre les valeurs revendiquées par les promoteurs des crypto-actifs et la vision libertaire et ultralibérale de la monnaie. Cela permettra de faire le point sur les « expériences » d'officialisation du bitcoin comme monnaie au Salvador et en République Centrafricaine. La dernière partie du présent document soulignera les difficultés posées par les crypto-actifs en termes d'ordre public et de sécurité nationale.

Première partie : L'essor des crypto-actifs et leurs promesses

L'écosystème des crypto-actifs se caractérise par une diversité croissante de jetons et d'applications. En 2019, on comptait ainsi près de 2000 crypto-actifs sur le site de référence Coinmarketcap.com. Trois années plus tard, ce chiffre est de près de 20 000 crypto-actifs. Pour comprendre les enjeux associés aux crypto-actifs, il est ainsi nécessaire d'expliquer les raisons de leur progression, d'identifier les acteurs qui les portent et d'analyser les ressorts du discours utilisé pour en faire la promotion.

I. La nature polymorphe des crypto-actifs

En 2008 apparaît la première mention de Bitcoin dans un groupe de discussion par *email*. Ce groupe, appelé Cypherpunk, est ostensiblement opposé à l'État et souhaite en minimiser le pouvoir. Son objectif est d'offrir au monde un actif monétaire hors de contrôle de tout État. Cette idée est reprise quelques années plus tard par un autre groupe souhaitant offrir au monde un ordinateur mondial, utilisable par tous et dont les programmes ne seraient pas censurables. La promesse évolue vers celle d'un Internet plus démocratique, moins centralisé, d'une émancipation des oligopoles qui contrôlent nos données. La *blockchain* promet alors décentralisation et anonymat. D'autres plus sceptiques cherchent encore « le problème à la solution » qu'est la blockchain, au sens où bien que la blockchain soit une nouvelle technique intéressante, il resterait à lui trouver des applications utiles dans la vie réelle. Il est ainsi nécessaire de confronter cette question de l'innovation technologique aux formes et usages qu'elle prend réellement dans la vie de la société.

A/ Une variété à croissance rapide de crypto-actifs, pour une multiplicité d'usages

En à peine plus d'une décennie, plusieurs millions de crypto-actifs ont été mis en circulation sur différentes blockchains. Selon le projet de règlement MiCA, notamment inspiré de la loi PACTE adoptée en France en 2019, est un crypto-actif toute représentation numérique « *of a value or a right which may be transferred and stored electronically, using distributed ledger technology or similar technology* », c'est-à-dire toute représentation numérique d'une valeur ou d'un droit qui peut être transféré et stocké électroniquement, en utilisant la technologie des registres distribués ou une technologie similaire.

Cette définition large et englobante recouvre une diversité d'usages et de situations. Si le droit européen commence à descendre dans des définitions plus précises (voir le détail dans la seconde partie), il est d'abord essentiel de comprendre cette diversité d'usages dans les faits. Ainsi, certains crypto-actifs assument un objectif purement spéculatif, tandis que d'autres essaient de servir des usages plus concrets. Comprendre l'histoire de la *blockchain*, ses acteurs, et ses diverses applications actuelles permet par ailleurs de relativiser le discours selon lequel *blockchain* et crypto-actif seraient indissociables, et de constater l'emploi croissant de *blockchains* en dehors du champ des crypto-actifs.

1/ De la naissance du bitcoin aux promesses technologiques de la blockchain

Si la *blockchain* est souvent associée aux crypto-actifs, une chaîne de blocs désigne à l'origine une structure de données spécifique dont l'objectif est de certifier, via des procédés cryptographiques, l'ordonnancement des blocs de données. Chaque ajout de bloc de données est identifié par une empreinte cryptographique⁷ qui certifie l'ensemble des blocs de données précédents ainsi que l'ordre de leur séquence.

Ce procédé a été appliqué à un contexte dans lequel des acteurs interagissant avec un même jeu de données ne peuvent pas se faire confiance. S'il n'est pas fait mention du terme « *blockchain* », les chercheurs Stuart Haber et W. Scott Stornetta publient dès 1991 un ensemble de techniques permettant d'arriver à assurer l'horodatage, et donc à la certification, d'un document en se passant d'une autorité centrale de certification⁸. Si cela ne permet pas encore de garantir une date et une heure précise, cela permet au moins de garantir l'ordre dans lequel les documents ont été répertoriés dans un registre partagé.

Alors que l'objectif était de limiter la confiance accordée à un tiers pour horodater un document, ce travail explorait déjà la voie permettant de se passer totalement d'un tel tiers. L'exercice de pensée s'est pourtant heurté à une limite : la conservation de l'anonymat. En effet, le système d'horodatage de Haber et Stornetta utilise des témoins, ce que signifie que chaque enregistrement doit être attesté par un grand nombre d'utilisateurs. Si ces utilisateurs sont anonymes, rien n'empêche pourtant un seul et unique acteur de se créer une infinité d'identités pour s'offrir la majorité des témoignages et ainsi pouvoir corrompre l'ensemble du système par ses faux témoignages. En informatique, cela est appelé une attaque Sybil, en référence au roman éponyme de 1973, sous la plume de Flora Rheta Schreiber, qui traite du trouble dissociatif de l'identité. Afin de pallier ce problème, les deux chercheurs ont suggéré de se référer à une autorité centrale chargée de répertorier les utilisateurs et leurs comptes.

⁷ Une empreinte ne permet pas de savoir quoi que ce soit sur un fichier mais permet de vérifier qu'il s'agit bien de celui que l'on attend. Par analogie, une empreinte digitale ne permet pas de savoir quoi que ce soit sur la personne à qui elle appartient, mais il est possible de vérifier qu'elle appartient bien à une personne donnée en comparant son empreinte à celle recherchée.

⁸ Haber, S., Stornetta, W., S. "How to time-stamp a digital document", *Journal of Cryptology*, 3, 99-111 (1991) (<https://doi.org/10.1007/BF00196791>).

Ainsi, les registres distribués étaient déjà largement répandus au tout début des années 2000. Le téléchargement en pair-à-pair (P2P) fonctionnait grâce à ces derniers, mais ces registres dépendaient encore d'annuaires centralisés. Dès 2001, des recherches ont été menées pour apporter de la décentralisation, mais sans jamais réussir à résoudre le problème de l'attaque Sybil en conservant l'anonymat. La méthode de décentralisation de ces annuaires de données consistait à les diviser en plusieurs parties de sorte que chacune soit hébergée un petit nombre de participants au réseau. Les réseaux P2P savaient donc déjà décentraliser les données et assurer leur redondance, mais il leur manquait un moyen de gérer les mises à jour de ces données. En 2008, quelqu'un ou un groupe se présentant sous le pseudonyme de Satoshi Nakamoto, dont l'identité reste inconnue à ce jour, publie les principes de fonctionnement de ce qu'il vise à être une monnaie électronique s'échangeant sans tiers de confiance sur Internet : le bitcoin. Sa principale innovation est de fournir un mécanisme de consensus qui s'affranchit de toute hiérarchie et de toute validation centralisée. Ce mécanisme, appelé preuve de travail (*Proof of Work*), permet de définir l'ordinateur qui validera les prochaines transactions. Il s'agit d'une sorte de « bingo » numérique dans lequel les utilisateurs cherchent à être le premier à trouver un nombre aléatoire en testant successivement toutes les combinaisons possibles. Cette astuce permet de distribuer le droit d'écriture dans le registre tout en s'assurant que chaque participant puisse héberger l'intégralité de celui-ci. Les données ne sont plus divisées afin d'être dispersées à travers le réseau, mais multipliées afin que chaque participant dispose de la dernière version. La *blockchain*, dans sa version moderne, était née.

Les protocoles de consensus : *Proof of work* et *Proof of stake*

Le consensus *Proof of Work* peut être décrit de manière simplifiée ainsi : le registre le plus long et respectant les règles du protocole fait foi, et seul l'ordinateur ayant trouvé un nombre aléatoirement déterminé par la *blockchain* est autorisé à écrire la prochaine entrée.

Ainsi Satoshi Nakamoto, plutôt que de contourner le problème posé par l'anonymat dans les travaux de Haber et Stornetta en 1991, décide de le sanctuariser. En effet, plutôt que d'avoir à générer le plus rapidement possible et maintenir une liste infiniment croissante d'identités, les validateurs entrent en compétition pour deviner le plus rapidement possible un nombre aléatoire. Dans les deux cas, la puissance des machines utilisées dans le processus détermine leur influence sur le réseau. C'est pourtant l'innovation de Satoshi Nakamoto qui a donné naissance à ce qui est appelé aujourd'hui la *blockchain*, terme qui englobe bien plus de technologies que la simple chaîne de blocs. Il n'est effectivement plus question d'attaque Sybil, puisqu'il n'y a pas de multiplication des identités, mais cela ne change rien à l'influence qu'un acteur peut gagner sur le réseau.

Par la suite, d'autres mécanismes de consensus ont émergé tels que le *Proof of Burn* qui reprend l'idée du *Proof of Work* en l'affranchissant de la consommation énergétique associée, mais aussi le *Proof of Stake* (preuve d'enjeu), différent des deux premiers mais qui est aussi économe en énergie que le *Proof of Burn* (preuve de destruction), ou encore le *Proof of Authority* auquel seuls des membres identifiés et autorisés peuvent prendre part et disposent d'une influence équivalente – on parle alors parfois de « *blockchain* privée ». Cette dernière est ce qui ressemble le plus aux suggestions de Stuart Haber et W. Scott Stornetta dans les travaux susmentionnés, tout en s'affranchissant d'une autorité centrale. Dans ce type de consensus, l'autorisation à participer au consensus est délivrée par les pairs membres du réseau. Cela n'est pas sans rappeler le processus d'adhésion à l'Union Européenne. Notons tout de même que la majorité des *blockchains* actuelles se déploient cependant sur des dérivés du *Proof of Stake*.

Malgré la popularisation du terme « *blockchain* » par les crypto-actifs, cette dernière ne se limite désormais plus à cet usage et il existe de nombreuses *blockchains* indépendantes de tout crypto-actif. L'histoire de cette évolution technique permet donc également de comprendre les usages encore souvent disparates du terme. Dans une tentative de mettre un peu d'ordre, l'organisation internationale de normalisation (ISO) a proposé une définition de la *blockchain* : « un registre distribué sécurisé par un système cryptographique d'horodatage et disposant d'un mécanisme de consensus ». Cette définition officialise ce qui est à l'origine une métonymie et met sous un même chapeau l'ensemble des technologies rassemblées sous le terme *Distributed Ledger Technologies (DLT)*.

2/ Comment la blockchain s'est émancipée des crypto-actifs et peut servir à d'autres usages

Un des enjeux majeurs relatifs aux discussions tournant autour des crypto-actifs est de savoir si l'on a besoin de crypto-actif pour faire fonctionner une blockchain. À l'évidence, de nombreux exemples démontrent que ce n'est pas le cas, bien que la plupart des blockchains demeurent aujourd'hui encore associées à des crypto-actifs.

i. Les *smart contracts* et les applications décentralisées

Le protocole Bitcoin offre la possibilité de programmer certaines conditions sous lesquelles s'échangent les bitcoins sur son réseau, rendant ainsi possible l'établissement de "contrats numériques" entre plusieurs parties. On parle alors de *smart contract*. De façon plus générique, un *smart contract* est un programme informatique publié sur la *blockchain* et dont

le résultat d'exécution est également tracé sur celle-ci. Si Bitcoin a été le premier à permettre ce type de programmes, son hyperspécialisation a poussé d'autres développeurs à dépasser ces limites et permettre le développement de n'importe quel programme sur une *blockchain*. C'est précisément dans ce but que Ethereum a été créé, offrir un ordinateur virtuel mondial sur lequel on pourrait déployer des programmes exécutables et consultables par tous. Ainsi, plus qu'un contrat « intelligent », un *smart contract* est avant tout un contrat à exécution automatique dès lors qu'un certain nombre de conditions sont réunies.

Les motivations poussant à déployer de telles applications sont assez similaires à celles de l'adoption des DLT : immutabilité, résistance à la censure, transparence et possibilité d'exécuter des opérations sans tiers validateur. Il est ainsi possible de voir plusieurs *smart contracts* interconnectés les uns avec les autres de sorte qu'une interaction avec l'un d'entre eux active une cascade d'autres *smart contracts*. On parle alors d'une application décentralisée (Dapp). Certains *smart contracts* suivent ainsi des standards afin de les rendre facilement manipulables et interopérables avec plusieurs applications. L'interopérabilité est un caractère important afin que les objets qu'ils définissent puissent être manipulés depuis de nombreuses applications telles que des portefeuilles numériques matériels (hardware wallets, souvent sous forme de « clés » de type USB). Parmi ces standards, on retrouve par exemple ceux définissant les jetons fongibles et les jetons non-fongibles, les fameux NFT.

Avant la création du standard ERC-20 permettant de créer des jetons fongibles sur Ethereum, la plupart des crypto-actifs avaient leur *blockchain* dédiée. Depuis, la plupart repose sur une *blockchain* déjà bien établie afin de profiter d'une infrastructure déjà en place. Certains de ces jetons sont destinés à l'usage, d'autres à gagner un pouvoir supplémentaire dans l'orientation du projet sous-jacent. Cette facilité de création de nouveaux jetons a été utilisée comme un moyen de lever des fonds pour certaines organisations.

Ces levées de fonds se faisaient via une ICO (*Initial Coin Offering*). Le terme, tirée du sigle IPO (*Initial Public Offering*) utilisé pour désigner l'introduction en bourse d'une entreprise, signifie l'émission des premiers jetons d'un projet et leur attribution aux investisseurs décidant de les acheter. Alors que l'émission de titres financiers tels que des obligations ou des actions nécessite de passer par de nombreuses étapes légales, l'émission d'un jeton sur une *blockchain* ne nécessite, encore aujourd'hui dans de nombreux pays, aucune formalité. Il suffit de programmer un *smart contract* et mettre en vente les jetons ainsi créés sur au moins une place de marché dédiée à ce type d'investissement. Rien qu'en 2017 près de 2000 ICO ont permis de lever plus de 6 milliards de dollars américains. Peu de projets ont survécu, mais cela n'est pas propre aux projets dans les crypto-actifs. Ainsi, les ICO ressemblent à un type de financement participatif. Ce type d'utilisation des crypto-actifs figure parmi les applications les plus intéressantes de ces derniers, bien qu'il nécessite un encadrement très étroit pour

éviter les nombreux abus qui ont eu lieu, avec des ICO menés par des acteurs peu scrupuleux qui disparaissaient aussitôt après avoir levé des fonds.

Toutefois, il n'est pas nécessaire d'avoir recours à ce type de financement pour émettre des jetons donnant le contrôle sur le protocole. Ethereum n'a pas réalisé d'ICO et pourtant, après avoir changé de protocole de consensus en 2022, dispose de jetons qui peuvent donner des droits de vote de manière analogue à des actions. Les crypto-actifs montrent ici leur nature protéiforme. Ils peuvent être utilisés tantôt comme moyen d'échange, parfois comme un simple droit de vote, souvent les deux à la fois. Rien que sur Ethereum, plus de 700 000 jetons fongibles différents coexistent. Certains de ces jetons servent uniquement de passerelle entre différentes *blockchains* comme le Wrapped Bitcoin (WBTC) qui permet de rendre les bitcoins échangeables sur les applications Ethereum – sans cela, il n'aurait pas été possible de l'échanger sur des plateformes de finance décentralisée de ce réseau – d'autres sont des crypto-actifs à part entière, sans aucun sous-jacent. À travers ces différents exemples, on saisit déjà la grande diversité d'usages des *blockchains* au sein de l'écosystème des crypto-actifs. Cette diversité d'emploi est également importante en dehors de cet éco-système.

ii. Les utilisations de la *blockchain* en dehors des crypto-actifs

Certains défenseurs des crypto-actifs répètent à outrance que les *blockchains* sans crypto-actifs ne sont pas possibles, sauf à ce qu'elles soient privées. Pour qu'une *blockchain* soit publique, il faudrait nécessairement avoir une incitation économique via l'émission de jetons. Cet argument ne tient pourtant pas l'épreuve de la réalité : pour les *blockchains* dont la sécurité dépend d'incitations économiques *via* l'émission d'un jeton, ce qui est le cas de la majorité des *blockchains*, la rémunération et le pouvoir sur le protocole est proportionnel au capital investi pour son fonctionnement. C'est tout le contraire de ce qui est entendu par "publique", c'est-à-dire accessible à tous. D'autres *blockchains* s'affranchissent pourtant de ces incitations économiques et distribuent l'influence plus équitablement.

Ainsi, avec la *Proof of Authority*, chaque acteur dispose d'une voix équivalente à celles de ses pairs. La seule contrainte est de pouvoir prouver l'identité de chaque acteur afin de garantir son unicité. L'identité numérique en étant tout juste à ses balbutiements, il n'y a pas encore d'expérimentation à grande échelle pour ce type d'infrastructure. Les freins ne sont pas tant techniques que d'ordre organisationnel. Les standards existent, mais il manque un cadre d'application commun pour la délivrance de preuves d'identité numérique. Cela pourrait évoluer dans les prochaines années avec un cadre européen d'identité auto-souveraine,

actuellement à l'étude au sein du projet eSSIF-Lab (*European Self-Sovereign Identity Framework Laboratory*)⁹.

Pour le moment, les expérimentations de *blockchains* sans crypto-actif ont donc été privilégiées dans des environnements au nombre d'acteurs restreints où chacun peut aisément valider la participation des autres. C'est ce qui tend à faire dire aux lobbyistes que les *blockchains* sans crypto-actifs sont forcément privées, le paragraphe précédent démontrant le contraire.

De nombreuses entreprises proposent de développer des *blockchains* qui seront support ou non de crypto-actifs. C'est le cas par exemple de Blockchain Partner¹⁰ ou d'IBM¹¹. Elles utilisent pour cela soit des logiciels propres, soit des logiciels open source, dont le fameux Hyperledger Fabric¹² qui est un logiciel libre dont le développement est coordonné par la fondation Hyperledger¹³. Des développements très importants ont été réalisés avec ce logiciel exceptionnel. Loin de la spéculation liée aux crypto-actifs, il y a par exemple l'application Tradelens¹⁴ qui permet le suivi des containers dans le monde entier : elle associe plus de 200 acteurs dont 10 armateurs, une centaine de ports et terminaux, des chargeurs, des transitaires, des douanes, des banques et assurances. Plus de 30 millions de containers ont été suivis grâce à plus d'un milliard d'enregistrements d'informations sur le fichier *blockchain* de Tradelens qui aujourd'hui concerne plus de 50 % du commerce mondial conteneurisé¹⁵. La plateforme n'ayant pas rencontré le succès commercial espéré, IBM et Maerks ont annoncé l'arrêt de sa commercialisation le 29 novembre 2022. Cet échec commercial n'est cependant pas à mettre sur le dos de la solution technique. Il s'agissait d'une nouvelle solution qui voulait gérer de bout en bout les processus logistiques alors que le secteur utilise plutôt des outils spécialisés pour chaque processus.

Une autre expérimentation est menée avec une *blockchain* utilisant le consensus *Proof of Authority* ; il s'agit du projet européen EBSI (*European Blockchain Services Infrastructure*)¹⁶. Parmi les cas d'usage envisagés, on peut citer celui de la délivrance de diplômes. La délivrance de certificats numériques n'a rien de nouveau, mais ces derniers ont une durée de validité pour des raisons de sécurité. Cette limite permet d'éviter à un fraudeur de retrouver la signature électronique de son émetteur et ainsi émettre de nouveaux faux diplômes au nom de l'établissement. Avec l'EBSI, chaque diplôme peut ainsi être immatriculé sur l'EBSI, associant ainsi la signature de l'établissement à l'horodatage de la *blockchain*. Chaque changement de signature de l'établissement étant lui-même consigné sur la *blockchain*, il

⁹ European Self Sovereign Identity Framework Laboratory, Horizon 2020 (<https://doi.org/10.3030/871932>)

¹⁰ <https://blockchainpartner.fr/services/>

¹¹ <https://www.ibm.com/blockchain>

¹² <https://www.hyperledger.org/use/fabric>

¹³ <https://www.hyperledger.org/>

¹⁴ <https://www.tradelens.com/>

¹⁵ "Blockchain : Tradelens révolutionne le suivi du fret maritime". L'Usine Nouvelle, 10 mai 2021

¹⁶ <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>

devient à présent possible de prouver que le diplôme a bien été certifié par une signature valide à l'époque de son émission. Actuellement, le réseau est hébergé sur 36 nœuds opérés par des universités de l'Union Européenne, de la Norvège et du Liechtenstein. Cette expérimentation ne compte pas se cantonner aux diplômes universitaires. Un autre cas d'usage envisagé, qui apparaît prometteur, serait la consignation des actes notariés qui sont soumis aux mêmes contraintes de sécurité.

Ainsi la blockchain permet de nombreux usages en dehors des crypto-actifs à visée financière. Pour comprendre qui en bénéficie le plus, il faut désormais s'intéresser à la question du pouvoir au sein de cet éco-système.

B/ L'écosystème des crypto-actifs et sa hiérarchie : qui détient le pouvoir ?

La question du pouvoir quand il s'agit des crypto-actifs les plus importants est assez simple. Sur le réseau Bitcoin la question du pouvoir revient à la question : qui décide de faire évoluer le protocole de fonctionnement ? Cette évolution concerne les mises à jour et corrections du programme qui fait fonctionner le réseau (appelé « client Bitcoin »), mais peut aussi concerner des problèmes plus profonds comme l'augmentation de la taille des pages ajoutées toutes les 10 minutes pour que le réseau Bitcoin puisse exécuter un plus grand nombre de transactions par seconde, ou le rythme d'émission de nouveaux jetons. Ce pouvoir dans le cas du bitcoin est principalement aux mains des mineurs.

Les informaticiens développeurs qui conçoivent, détaillent et soumettent des modifications pour le programme faisant fonctionner le réseau Bitcoin jouent bien sûr un rôle de proposition et détiennent donc une parcelle de pouvoir. Les utilisateurs du réseau, simplement parce qu'ils gèrent des comptes et qu'ils peuvent mettre leur argent ailleurs si l'évolution du réseau leur déplaît, détiennent aussi une part du pouvoir sur le réseau. Il n'en reste pas moins que ce sont les mineurs du réseau Bitcoin, quand ils gagnent le concours de calcul, qui votent pour ou contre les propositions de modifications du client Bitcoin, et donc, que ce sont bien ces mêmes mineurs qui en dernier lieu détiennent le pouvoir décisionnel ultime sur le réseau Bitcoin et l'évolution de son protocole. Cette situation explique qu'il est difficile et parfois impossible de faire qu'un réseau qui fonctionne avec la *Preuve de travail* l'abandonne pour un autre protocole de consensus moins énergivore : ce serait contraire aux intérêts financiers directs des mineurs. Or ces mineurs sont de plus en plus regroupés dans des « pools » de minage très puissants qui se partagent le pouvoir, contrairement à la philosophie décentralisatrice et égalitaire prônée par les tenants des crypto-actifs (cf. *infra*).

Dans le cas des crypto-actifs autres que le bitcoin la gouvernance est conçue selon des modèles nombreux et variés construits par exemple sur des systèmes de votes plus ou moins difficiles à démêler. Elle se trouve finalement aux mains de quelques acteurs parfois

impossibles à identifier à cause de l'anonymat possible des acteurs, et il est souvent arrivé (par exemple pour Ripple ou Binance) qu'on soupçonne qu'elle était en grande partie sinon totalement contrôlée par un très petit nombre d'entre eux.

Précisons bien sûr que dans le cas des plateformes d'échange et de toutes les entreprises au sens habituel qui participent à l'écosystème des crypto-actifs, comme dans le cas des entreprises qui se financent par ICO, leur gouvernance est centralisée et aux mains de leurs dirigeants et actionnaires. Aussi est-il nécessaire de bien distinguer les *blockchains* et les crypto-actifs qui utilisent leurs infrastructures, de la même manière qu'il convient de distinguer les différents acteurs intervenant dans le processus.

1/ Les créateurs de crypto-actifs

On ne sait pas aujourd'hui qui se cache derrière le pseudonyme Satoshi Nakamoto l'inventeur en 2008 du protocole Bitcoin et le créateur du réseau correspondant. C'est pourtant lui le créateur du concept de « réseau *blockchain* » comme système de sécurisation décentralisé d'un registre à l'aide d'un réseau d'ordinateurs fonctionnant en pair-à-pair (c'est-à-dire sans autorité générale de contrôle). Il semble probable que derrière le pseudonyme de Nakamoto se cache une équipe, sans doute américaine, de 3, 4 ou 5 personnes déjà spécialistes des "monnaies numériques". Des noms circulent, mais aucune des personnes soupçonnées ne reconnaît être impliquée. Concernant le second crypto-actif en capitalisation (l'ether du réseau Ethereum) on sait en revanche qu'il a été créé par une équipe réunie autour de Vitalic Buterin, un jeune génie russo-canadien, et on la connaît.

Une multitude d'autres acteurs, en général informaticiens, sont à l'origine d'une multitude d'autres crypto-actifs : le site <https://coinmarketcap.com/> compte plus de 20 000 crypto-actifs en novembre 2022. Certains sont devenus des gloires internationales. Ils sont assez souvent millionnaires ou même milliardaires comme Changpeng Zao le créateur de la plateforme d'échange Binance, ou l'ont été un moment comme Sam Bankman-Fried le responsable de la plateforme FTX créateur du crypto-actif FTT et ruiné en quelques heures après la faillite de FTX en novembre 2022. Certains des créateurs de crypto-actifs sont issus du milieu universitaire comme une partie de l'équipe à l'origine de Cardano (parmi les dix plus importants crypto-actifs en capitalisation), mais ce n'est pas la règle et le monde académique n'est pas le moteur principal des nombreuses innovations dans l'écosystème des crypto-actifs. Parmi les entreprises créant des crypto-actifs, il faut distinguer celles qui émettent des *stablecoins* centralisés, chaque jeton émis valant par exemple exactement un dollar. Elles doivent en effet, pour assurer le maintien de la parité des jetons émis, garder en réserve une somme équivalente à celle émise, soit sous forme de dollars soit sous forme de produits financiers non risqués. Le modèle économique de telles entreprises s'appuie sur les

commissions qu'elles font payer lors des échanges de jetons contre de la monnaie officielle et de ce qu'elles gagnent en plaçant une partie des sommes qu'elles reçoivent en échange des jetons qu'elles mettent en circulation. La plus importante société de ce type est Tether Limited. Bien qu'elle ait émis plus de 130 milliards de jetons de un dollar (novembre 2022) des doutes sérieux existent concernant la contrepartie (aussi appelé collatéral) dont elle devrait disposer. Aux États-Unis, Tether Limited a d'ailleurs été condamnée pour « *making untrue or misleading statements* » concernant sa prétendue contrepartie. Elle a dû payer et a effectivement payé une amende de plus de 41 millions de dollars¹⁷.

2/ Les plateformes d'échanges et fonds spéculatifs

Les plateformes d'échange de crypto-actifs — souvent dénommées simplement « échanges » — sont des sortes de banques en ligne spécialisées dans les crypto-actifs. Chacun peut y ouvrir un compte, y déposer de l'argent en monnaie officielle, puis l'utiliser pour acheter des jetons de crypto-actifs et les gérer comme on gère un portefeuille d'actions, en en vendant certaines pour en acheter d'autres et en espérant tirer avantages de ces manœuvres au sein du monde des jetons de crypto-actifs. Les plateformes sont créées et gérées essentiellement par des informaticiens ou les entreprises qu'ils créent. En même temps qu'elles ouvrent et gèrent leurs services « bancaires », il est fréquent que les plateformes émettent aussi des crypto-actifs et offrent des produits divers liés aux crypto-actifs, dont des comptes de dépôts rémunérés. Elles proposent souvent aussi des services d'informations sur internet qui permettent par exemple de suivre les cours des crypto-actifs.

Binance est la plus importante plateforme de ce type : elle a introduit le crypto-actif BNB, et le *stablecoin* Binance-USD. Il existe plusieurs centaines de plateformes d'échange de crypto-actifs. Les plus importantes sont : Binance, Coinbase exchange, Kraken, Kucoin, Bitfinex, etc¹⁸.

La plateforme FTX était seconde en importance avant sa faillite en novembre 2022. Le gestionnaire chargé de la liquidation — John J. Ray III, qui s'était occupé de liquider Enron — a découvert le manque de sérieux et de rigueur déconcertant avec lequel était géré FTX. Beaucoup ont alors compris à quel point la réglementation trop peu exigeante imposée à ces plateformes était dangereuse¹⁹.

Signalons aussi l'existence de fonds spéculatifs (*Hedge funds*) proposant des produits à base de crypto-actifs. L'un d'eux, Three Arrows Capital, à la suite de la baisse générale des cours des crypto-actifs en juin 2022, a lui aussi fait faillite²⁰.

¹⁷ "Tether Fined \$41M over 'Misleading Statements'", Alexandria, 2021

¹⁸ Voir : <https://coinmarketcap.com/rankings/exchanges/>

¹⁹ Declaration of John Jay Ray — FTX is worse than Enron, D. Gerard, 17 nov. 2022

²⁰ Cryptomonnaies : un hedge fund de premier plan en défaut de paiement, L'Usine digitale, 28 juin 2022

3/ Les utilisateurs et détenteurs de crypto-actifs

Les utilisateurs et détenteurs de crypto-actifs occupent bien évidemment un rôle central dans le développement de l'écosystème des crypto-actifs : ce sont eux principalement qui introduisent de l'argent dans cet univers. Après une courte période (2009-2012) où seuls quelques spécialistes informaticiens cryptologues détenaient des crypto-actifs, rapidement d'autres utilisateurs non nécessairement informaticiens s'y sont intéressés, alléchés par la montée des cours du bitcoin, ou sensibles à l'idéologie libertarienne qui présente les « cryptomonnaies » comme la solution définitive aux problèmes monétaires et en particulier aux risques liés à l'inflation. L'économiste d'origine autrichienne Friedrich Hayek (1899-1992) est souvent évoqué par ces idéologues des « cryptomonnaies » qui reprennent à leur compte l'idée qu'une monnaie saine ne peut exister que si « elle est retirée des mains de l'État », et qui soutiennent que les “cryptomonnaies” sont le moyen moderne d'y arriver²¹ (ce point sera détaillé dans le II. ci-dessous).

Petit à petit, grâce à la création des plateformes d'échange qui sont plus faciles à utiliser que la détention directe permise sans passer par elles pour celui qui gère lui-même les clefs de ses comptes sur les *blockchains* émettrices, tout le monde a été concerné et a pu facilement détenir des crypto-actifs ou des produits dérivés incorporant des crypto-actifs. Il est difficile d'évaluer combien de gens dans le monde détiennent des crypto-actifs. La raison principale en est que ceux qui gèrent eux-mêmes anonymement et directement leurs comptes possèdent en général plusieurs comptes, voire plusieurs dizaines (cela ne coûte rien d'en créer beaucoup) sans que l'on puisse savoir que ces comptes sont sous le contrôle d'un même acteur. Il ne fait cependant aucun doute que plusieurs dizaines de millions d'acteurs détiennent aujourd'hui des crypto-actifs. Certains sondages indiquent par exemple que plus de 10 % des Américains détiendraient des crypto-actifs²².

S'ajoutant aux détenteurs privés, des entreprises puis des investisseurs institutionnels ont acquis des crypto-actifs dans le but le plus souvent, non pas de les utiliser pour commercer, mais seulement de spéculer, ou pour les plus optimistes, dans le but de constituer des « réserves de valeur ». Aujourd'hui après la baisse considérable de la capitalisation totale des crypto-actifs passée de 3000 milliards de dollars en décembre 2021, à moins de 800 milliards de dollars un an plus tard, l'idée longtemps soutenue par les défenseurs des crypto-actifs que les crypto-actifs constituent des réserves de valeurs et un outil pour échapper à l'inflation fait sourire. Parmi les institutionnels piégés citons le fonds de pension canadien CDPQ (Caisse

²¹ [“Bitcoin, totem & tabou - Que présage l'essor des cryptomonnaies ?”, Institut Sapiens, fév. 2018](#)

²² [“États-Unis : 11% des Américains auraient investi dans les cryptomonnaies selon un sondage”, Cryptoast, 26 août 2021](#)

de dépôt et placement du Québec) qui a perdu 200 millions de dollars à la suite de la faillite, en août 2022, de la société Celsius Network LLC qui opérait des prêts en crypto-actifs²³.

4/ Les validateurs et les “mineurs”

Certains protocoles de crypto-actifs, dont les plus importants comme le bitcoin, et l'ether du réseau Ethereum, offrent une récompense à ceux, que nous appellerons *validateurs*, qui participent au fonctionnement et à la surveillance des réseaux permettant aux crypto-actifs d'exister et de circuler. Puisque, par nature, il n'y a pas d'autorité centrale chargée de surveiller et de faire circuler les crypto-actifs des réseaux de *blockchains* publics (comme les réseaux du Bitcoin ou Ethereum) ce sont ces validateurs dispersés et si possible indépendants les uns des autres qui font fonctionner les réseaux et assurent qu'aucune fraude ne se produit. Leur coordination s'opère en utilisant des protocoles de consensus qui maintiennent en continu leur accord général sur ce que chaque compte détient. Ces acteurs validateurs sont bien souvent des informaticiens ou des entreprises spécialisées. Dans le cas des plus « libéraux » des réseaux de crypto-actifs, tout le monde peut être validateur et même l'être en restant anonyme (Bitcoin). Dans le cas des réseaux moins ouverts (par exemple les réseaux entre banques) appelés « réseau de consortium » seuls quelques acteurs bien précis et connus jouent ce rôle de mise en fonctionnement et de surveillance décentralisée.

Dans le cas des crypto-actifs fonctionnant avec le protocole de *Preuve de travail (Proof of work)* comme Bitcoin ou Ethereum jusqu'au 15 septembre 2022, pour gagner les récompenses distribuées pour rémunérer les validateurs, le protocole met en œuvre un concours de calcul renouvelé périodiquement. Pour Bitcoin ce concours recommence toutes les 10 minutes. Le gagnant du concours de calcul se voit attribuer de nouvelles unités du crypto-actif créées *ex nihilo* : 6,25 bitcoins toutes les 10 minutes aujourd'hui pour le réseau Bitcoin. Cette participation aux concours de calcul se nomme « le minage » et ses acteurs « les mineurs ». Il est important de distinguer les calculs faits pour le fonctionnement du réseau et sa surveillance, et les calculs faits pour participer aux concours de calculs et accroître ses chances d'être gagnant. Nous reviendrons plus loin sur cette distinction essentielle pour comprendre le problème de la dépense électrique considérable de certains réseaux de *blockchain*.

Au cours des années s'est développée une industrie du minage qui a fini par devenir monstrueuse. Elle fait fonctionner aujourd'hui plusieurs millions de machines, chacune très énergivore (souvent de l'ordre de 3000 W). De nombreuses entreprises se sont développées en se spécialisant dans l'activité de minage ou la conception et la production de machines de minage. Il y a par exemple Bitmain en Chine, Bitfarm au Canada, Bigblock Datacenter en

²³ [“La CDPQ dit avoir perdu les 200 millions investis dans Celsius Network”, Le Devoir, 18 août 2022](#)

France. Pour améliorer leurs performances (c'est-à-dire pour augmenter la probabilité de gagner chacune des occurrences du concours de calcul) certaines de ses sociétés de minage fabriquent les machines spécialisées, appelées « rigs de minage ». Elles ont même conçu et fabriqué des circuits spécialisés ASIC (pour *Application specific integrated circuit*) améliorant encore leurs performances. La firme INTEL elle-même s'est mise à concevoir, fabriquer et vendre des circuits ASIC pour le minage. Les entreprises de minage ont installé leurs machines partout dans le monde, mais plus spécialement dans des endroits où elles peuvent se procurer de l'électricité à bas prix : pendant un temps la Chine ; aujourd'hui la Russie, l'Irlande, le Canada, les États-Unis, les Kazakhstan, etc²⁴.

Alors que la Chine était le pays numéro 1 du minage de bitcoins, les autorités chinoises ont interdit cette activité industrielle en 2021 (voire II. de la troisième partie). Cette interdiction a provoqué le déménagement des usines de minage ou de leurs matériels qui ont été revendus. Une partie importante de ces rigs de minage s'est retrouvée aux États-Unis où des États comme le Texas offrent des politiques favorables à l'installation de nouvelles usines de minage.

5/ Les entreprises informatiques nouvelles qui se financent par des ICO

L'un des usages des crypto-actifs est d'offrir un nouveau moyen pour mener des levées de fonds pour certaines entreprises. Celles-ci après avoir le plus souvent publié un « livre blanc » (« white paper ») dans lequel elles décrivent leurs projets, émettent un crypto-actif, c'est-à-dire un jeton numérique circulant d'un détenteur à l'autre par le biais d'un réseau *blockchain*, qui est souvent le réseau Ethereum.

Ces « Initial Coin Offering » (ICO) permettent aux entreprises concernées de disposer d'un capital pour développer leur activité. Les ICO émis sont rapidement cotés, et peuvent prendre ou perdre de la valeur selon le marché. Contrairement aux classiques IPO (*Initial Public Offering*) du monde boursier, les jetons ICO ne représentent pas des parts d'entreprise, mais simplement des certificats donnant à leurs détenteurs des droits particuliers, par exemple des réductions sur les produits de l'entreprise qui les émet, ou l'accès à des services qu'elle mettra en place. L'AMF met en garde contre les ICO qui ont donné lieu à une multitude d'escroqueries. Elle donne un visa à certaines ICO²⁵.

6/ L'émergence et les objectifs des NFT

Les *NFT* (*Non-Fungible Token*) sont des jetons issus par des *smart contracts* spécifiques qui, contrairement aux jetons entrant dans le fonctionnement économique de certaines

²⁴ Voir : https://ccaf.io/cbeci/mining_map

²⁵ Voir les [conseils aux épargnants](#) ; aux [professionnels](#) et la [liste des offres de jetons ayant obtenu un visa de l'AMF](#)

blockchains, a pour objectif d'être non-fongible. En d'autres termes, sa fonction première est de reconnaître une singularité à un objet numérique. Chaque NFT a son propre identifiant, assimilable à un numéro de série, un émetteur, un propriétaire et une description. L'objectif est donc d'apporter de la rareté à quelque chose qui ne l'est pas par nature : les données. Il n'est pas surprenant que les NFT aient connu un certain succès dans l'art numérique. Cette forme d'art est bien plus facilement sujette aux copies que les arts manuels comme la sculpture ou la peinture, et rien ne différencie une copie d'une autre. Le marché de la photographie a par exemple créé une rareté artificielle en ajoutant des propriétés supplémentaires *via* des impressions en série limitée, numérotées et signées par l'auteur. Les NFT reproduisent ce même procédé pour les œuvres numériques en permettant à un émetteur de signer la copie d'une donnée et de certifier qui en est le propriétaire. Mais en plus de ces propriétés, les *smart contracts* permettent de déterminer des conditions sous lesquelles un NFT peut être transféré.

Les artistes numériques ont utilisé ces propriétés afin de toucher une rémunération en crypto-actifs à chaque fois que le NFT change de propriétaire. Ce droit de mutation étant programmable, il est possible de déterminer un montant fixe, proportionnel, ou de choisir un tout autre mode de calcul de la part qui reviendra à chacun. Le traitement est automatisé ; une transaction ne respectant pas les critères définis au contrat sera rejetée par les hébergeurs-validateurs de la blockchain.

Si l'art numérique a été le cas d'usage le plus médiatisé, les NFT ne se limitent pas à ce domaine. Les données auxquelles font référence ces NFT peuvent être de natures très différentes. Certains ont par exemple expérimenté la création de tickets numériques donnant accès à des événements ou offrant des droits spécifiques dans un logiciel. Certains jeux en ligne utilisent également cette technologie afin d'établir un cadastre de leurs mondes virtuels respectifs (appelés *métavers*), bientôt imités par des grandes marques. Le NFT peut ainsi donner des droits sur une parcelle de terre dans un jeu vidéo ou dans un métavers. Les coordonnées peuvent être inscrites sur le jeton lui-même ou simplement être identifiées par l'éditeur du jeu. Nous verrons dans la seconde partie quels sont les défis plus spécifiques des NFT pour la réglementation.

7/ Les sociétés et associations regroupant certains types d'acteurs

Parmi les acteurs de l'écosystème des *blockchains* et des crypto-actifs, il faut encore mentionner diverses associations professionnelles jouant souvent le rôle de lobby auprès du monde politique et des médias. L'Association pour le Développement des Actifs Numérique (ADAN) en France et en Europe²⁶ se propose de soutenir le développement de l'industrie des

²⁶ <https://adan.eu/>

crypto-actifs : « L'ADAN fédère les acteurs du secteur des crypto-actifs et de la *blockchain* pour ériger la France et l'Europe en territoires majeurs d'innovation. ». Elle publie des rapports ²⁷ . On trouvera l'impressionnante liste de ses membres en <https://adan.eu/association/membres>.

À l'échelon mondial, il existe aussi Bitcoin Mining Council²⁸ qui promeut et défend l'industrie du minage du bitcoin dont nous avons déjà mentionné l'importance industrielle. Cette association annonce ses objectifs très clairement : « Le Bitcoin Mining Council est un forum ouvert de mineurs de bitcoins engagés vis-à-vis du réseau et sensibles à ses principes fondamentaux. Nous encourageons la transparence, défendons les meilleures pratiques et sensibilisons le public aux avantages de Bitcoin et du minage de Bitcoin. »²⁹ Nous verrons plus loin que parler des « avantages du minage du bitcoin » est aujourd'hui très largement contesté et l'on peut craindre que ce lobby ne soit au service d'une cause absurde engendrant un gâchis énergétique considérable. Ce lobby s'appuie en ce sens sur un discours rôdé, quasi-marketing, qui n'hésite pas à faire appel à des arguments divers et parfois contradictoires entre eux.

C/ Un discours rôdé entre séduction de l'argument de la modernité et nouveau terrain de spéculation pour des acteurs financiers traditionnels

« De la spéculation pour les pauvres », telle est la formule provocatrice employée par l'économiste Michel Santi pour qualifier le monde des crypto-actifs ³⁰ . Prétendument antisystème, n'hésitant pas à critiquer les banques centrales tout en profitant de leur largesse, cherchant à incarner une "alternative" aux marchés financiers en en reproduisant pourtant les pires pratiques, les promoteurs des crypto-actifs jouent sur un discours volontairement contestataire, alternatif, provocateur, tout en faisant appel à l'idéal de richesse rapide, à des influenceurs stars et à toutes les dernières techniques du marketing agressif appuyé sur la peur du FOMO ("fear of missing out" que l'on peut traduire par peur de manquer une belle opportunité financière). Cependant, ces arguments ne résistent pas à une analyse réelle du fonctionnement du marché des crypto-actifs.

1/ Un discours en trompe-l'oeil vantant une modernité politique et un recours contre l'inflation

²⁷ <https://adan.eu/publications?format=rapport>

²⁸ <https://bitcoinminingcouncil.com/>

²⁹ « The Bitcoin Mining Council is a voluntary and open forum of Bitcoin miners committed to the network and its core principles. We promote transparency, share best practices, and educate the public on the benefits of Bitcoin and Bitcoin mining. »

³⁰ « *Krach des cryptomonnaies : la spéculation pour les pauvres* », La Tribune, 19 mai 2022

Le bitcoin, et plus généralement les crypto-actifs, passent aujourd'hui aux yeux de beaucoup comme étant un élément constitutif de « la modernité ». D'où la réticence d'un certain nombre de politiques qui, en privé, font preuve de scepticisme sur l'utilité de bitcoin, à émettre publiquement des réserves pour ne pas passer pour des *"has been"*.

Aussi, plus la séduction vis-à-vis du bitcoin, grandit, plus les autorités politiques et financières, sous influence d'une partie de l'opinion publique et de lobbies, peuvent être réticentes à le réguler par peur d'être dénoncées comme étant rétrogrades en portant atteinte au droit de propriété et à la liberté d'échanger. Cela même à l'inverse d'une bonne administration des intérêts collectifs indispensables à l'exercice même des intérêts privés ; ce qui devrait inciter à des mesures tant anti spéculatives (pour éviter des risques financiers systémiques semblables à ceux de 2000 et de 2008) que protectrices de l'environnement et des ressources, en répondant ainsi à deux problèmes majeurs posés par le Bitcoin.

La modernité serait une inéluctable « dématérialisation de la monnaie » ; expression qui doit être critiquée compte tenu des éléments matériels (métaux rares et énergies) nécessaires à cette prétendue « dématérialisation ». Celle-ci constituerait une nécessité ou une fatalité contre laquelle il serait vain de s'opposer. Un argument sous-jacent à la défense du bitcoin comme « moderne » est généralement une conviction que la technique est un déterminant essentiel des évolutions des sociétés. Ce récit ne colle pas à la réalité historique et plusieurs modèles technologiques se sont finalement avérés être des échecs. Ce fut le cas en France pour les promoteurs du Minitel, terminal informatique largement exploité entre 1980 et 2000 dans lequel d'aucuns voyaient une nouveauté dont le succès ne pouvait pas être contesté du fait de sa supposée supériorité technique. On sait ce qu'il advint face à la concurrence d'internet. On peut aussi citer la télévision couleur SECAM made in France lancée en 1967, qui fut mise en échec par le système PAL qui avait su réduire ses coûts. On doit aussi se référer sur les marchés financiers à de nombreuses « valeurs technologiques » surestimées car leurs promesses se sont avérées illusoires.

La prétendue modernité du bitcoin, autrement dit le fait qu'il soit supposé bénéficier des progrès les plus récents des savoirs scientifiques et techniques, peut être contestée essentiellement dans trois champs qui sont d'ordre :

- écologique par sa surconsommation d'énergie (voir troisième partie du rapport),
- financier par ses dimensions fortement spéculatives,
- et politique à travers la négation de la dimension de commun et la mise en pratique du néolibéralisme qu'il réalise dans une période notamment d'épidémie et de conflits armés, où la reconnaissance du collectif devient de plus en plus prégnante (voir II. ci-dessous).

Du point de vue financier, le bitcoin est en effet annoncé comme étant en rupture avec l'organisation monétaire et financière dominante alors que, au contraire, il contribue au surdéveloppement des liquidités par la formation de survaleurs. Il renforce les aspects les plus stériles, les plus néfastes et les plus dangereux de l'hyper-financiarisation contemporaine. Jusqu'au printemps 2021, le marché du bitcoin était resté suffisamment marginal pour cantonner son éventuelle casse. Les grands acteurs du secteur de la finance et les gestionnaires de la trésorerie des grandes entreprises ont (jusqu'ici) pour l'immense majorité résisté à l'intégration de ce produit nouveau dans leurs portefeuilles, quand bien même les taux d'intérêt étaient « au plancher ». Mais le danger serait qu'une absence de régulation et une remontée de son cours lui donnent plus de poids encore, ainsi que les conséquences de sa rechute. En novembre 2022, la faillite de la plateforme FTX a conduit à s'interroger sur ses effets potentiels sur l'ensemble de la « sphère crypto » et même au-delà.

Dans certains pays (comme le Venezuela et le Liban, et dans une moindre mesure au Nigéria et en Argentine), le recours au bitcoin peut s'expliquer par une fuite devant la monnaie nationale due à l'effondrement quasi total de leur système financier et monétaire sous pression d'une hyperinflation ou de sa menace. La monnaie nationale ou fédérale y est fortement contestée et elle cesse alors d'être « souveraine » du fait d'une incapacité de l'État d'intervenir et de la soutenir. De nombreux « Bitcoin maximalistes » anticipent un effondrement du système monétaire et financier à des échelons non seulement nationaux mais aussi à un niveau mondial. Pour les tenants du Bitcoin, celui-ci libérerait les humains de la domination des banques et des États en matière monétaire et des risques de fortes inflations que de nombreux « Bitcoiners » prétendent inéluctables, à partir d'une lecture sommaire de la théorie quantitative de la monnaie (et sans voir qu'une inflation masquée se fait par l'augmentation du prix des actifs financiers et de l'immobilier). Mais, sauf à croire que l'ensemble des systèmes monétaires et financiers ne peut que, plus ou moins rapidement s'effondrer, il est possible de considérer les situations, où localement l'attrait pour le Bitcoin croît de façon considérable, comme étant conjoncturelles et spécifiques ; donc temporaires et non généralisables à l'évolution de l'ensemble de la planète monétaire et financière.

De façon récurrente, ici ou là, le bitcoin peut apparaître comme une roue de secours aux yeux de populations subissant la disparition ou une forte dépréciation de leur monnaie nationale alors que le cours du bitcoin s'envolait. Il constitue alors un moyen de protection de leurs avoirs (pouvant être très imparfait voire totalement illusoire en cas d'effondrement subi de son cours comme au printemps 2021 et en 2022). Mais il est fort probable que, lorsque ces pays retrouveront une stabilité monétaire, l'usage du bitcoin y reculera, en particulier si l'on se situe dans une phase de forte baisse du cours de celui-ci et qu'une devise comme le dollar apparaît une meilleure réserve de valeur.

Contrairement à ce qu'on lit souvent dans des textes vantant ce qui seraient les mérites du bitcoin en tant qu'instrument de lutte contre l'exclusion bancaire et financière, toutes les informations disponibles montrent que dans les situations de crise monétaire et financière ce ne sont ni les plus pauvres, ni les plus exclus (donc les fractions de la population les plus atteintes par la crise dans leur survie quotidienne), qui ont recours au bitcoin, ou plus exactement qui peuvent y avoir recours. Celui-ci ne constitue pas un moyen miraculeux de lutter contre l'exclusion financière car en bénéficiant principalement les familles qui possèdent le capital culturel et financier le plus élevé leur permettant de largement échapper à une détérioration du cours du change de la devise nationale. Loin de réduire l'exclusion financière, son adoption pourrait même l'accroître en raison des capacités différenciées d'accès à et d'usage d'un crypto-actif, tout comme d'ailleurs des devises étrangères.

L'argument d'une fuite devant la dépréciation de la monnaie nationale du fait de la hausse des prix ne peut donc pas expliquer l'intérêt porté par une fraction significative de la population en Europe ou aux États-Unis où l'intérêt de beaucoup pour le bitcoin est d'abord la quête de gains rapides et élevés y compris par des petits spéculateurs. Ceux-ci peuvent afficher une forte indifférence à toute idéologie. Aux États-Unis, plus de 17 % de la population adulte aurait possédé du bitcoin à la mi-2021. L'importance de la détention par ces ménages américains de ce qui apparaît comme actif spéculatif peut être mise en rapport avec le fait qu'alors que les taux d'intérêt ont fortement chuté, environ la moitié de la population américaine détiendrait des actions (pourcentage en recul après la crise de 2008...). Toutefois la chute de son cours en 2022 a ruiné de petits spéculateurs, dont certains avaient ainsi placé l'essentiel de leurs économies (y compris incluant leur plan de retraite...) et qui certains s'étaient même endettés pour spéculer à terme en prévision d'une augmentation du cours et se trouvent donc durablement ruinés

2/ Une nouvelle pensée libertarienne dangereuse

Rappelons ce qui serait les avantages du Bitcoin et des cryptoactifs qui s'inscrivent dans sa lignée, selon ceux qu'il séduit : anonymat supposé totalement étanche des transactions, affranchissement tant des devises des Banques centrales des États que des monnaies scripturales émises par les banques commerciales à travers le crédit, défense des droits de l'individu devant supplanter toute contrainte collective y compris fiscale, préservation de la valeur des biens privés face à une hausse des prix grâce une émission limitée. Beaucoup de pro-bitcoin affichent ainsi leur antiétatisme, leur refus de la création monétaire par endettement et comme modèle politique et économique alternatif une référence au néolibéralisme.

Ajoutons pour certains un anti-américanisme, car son adoption selon eux comme monnaie dite « officielle » permettrait d'évincer le dollar (mais sans doute pas la puissance américaine

quand on observe la répartition nationale des capitaux investis dans son minage...). De même l'opposition au franc CFA en Afrique est en train aussi de séduire un certain nombre d'Africains prétendant ainsi se libérer du « joug colonial » ou « néo-colonial » plaçant dans un monde sans intervention publique leurs espoirs de libération économique et selon eux aussi politique, et à travers celle-ci de leur développement.

3/ L'attrait des crypto-actifs pour les spéculateurs

Par l'augmentation du nombre de ses détenteurs et l'ascension de son cours, l'essor du bitcoin est incontestable. Tout comme sa notoriété, au vu de la quantité (pas nécessairement la qualité...) exponentielle d'articles, de formations en ligne, d'émissions et de conférences qui à travers la planète lui sont aujourd'hui quotidiennement consacrés.

En période de hausse de son cours, augmente aussi les sommes que certains sont disposés à payer pour acquérir ce qui paraît un objet n'ayant *a priori* aucune utilité propre mais qu'ils ont la quasi-certitude que d'autres souhaiteront rapidement acquérir à un prix supérieur. Comme dans beaucoup d'autres domaines relatifs au bitcoin, les statistiques précises sur son usage effectif notamment comme moyen de paiement sont défailtantes. Si son usage comme moyen de paiement en dehors de l'acquisition de biens spéculatifs (tels que des immeubles au Salvador), son utilité donc sa demande, sont essentiellement spéculatives. Ses acquéreurs ont la conviction que, lors d'une éventuelle cession, il permettra de réaliser des gains.

On peut par exemple noter que l'annonce faite par telle ou telle structure de sa décision d'utiliser le bitcoin est souvent fortement médiatisée. Mais, il est exceptionnel que soient ensuite publiées des informations sur l'usage qui en est fait. On peut par exemple relever ici que la possibilité offerte par plusieurs communes aux citoyens suisses de payer leurs impôts en bitcoins a eu un succès quasi nul.

Les variations de cours sont ainsi essentiellement les conséquences de spéculations liées aux anticipations sur la montée ou la baisse de son cours en relation avec telle ou telle information et dans certains cas de rumeurs. L'évolution du cours dépend de plus en plus de la demande d'autres actifs spéculatifs ou tout simplement de la variation des taux d'intérêt ou du cours de devises clefs. Les comportements grégaires peuvent là être importants. Quand un particulier reçoit des bitcoins, généralement il ne les conserve que s'il anticipe la montée de son cours et il les revend une fois cet objectif atteint. Il s'agit avant tout d'une diversification des risques dans la composition de son patrimoine. D'où, quand les placements à court terme offrent des taux quasi nuls voire négatifs, l'attention manifestée aussi par certaines entreprises disposant d'une abondante trésorerie.

Une erreur courante, quant à la croyance en la capacité des « cryptomonnaies » privées et plus spécifiquement du bitcoin à supplanter non seulement le cash mais l'ensemble des

paiements bancaires scripturaux, est de confondre les intentions, voire les désirs de leurs promoteurs, et la réalité ; c'est-à-dire leurs usages et leur fonctionnement effectifs aujourd'hui. Autrement dit de confondre un projet paré par certains de beaucoup d'espoirs et peut-être de vertus quand il serait pleinement accompli (c'est en cela que certains ont vu un discours messianique dans la croyance au bitcoin) et son état actuel et sa nature qui peuvent apparaître très distants du projet initial et déjà être considérés comme l'indice d'un possible effondrement.

Pour que le bitcoin soit reconnu et surtout largement utilisé comme moyen de paiement et/ou d'unité de compte, il faudrait que son cours soit stabilisé ; et pour que sa volatilité soit fortement réduite il faudrait que son usage soit très répandu. Mais est-ce suffisant ? Car l'extension de sa diffusion durant plus d'une décennie n'a pas amoindri les soubresauts de son cours (par exemple une baisse aussi forte que celle de la moitié de son cours entre novembre 2021 et janvier 2022, et encore en mai et septembre 2022). Et si l'on fait l'hypothèse d'une corrélation entre les variations de son cours et les raisons de le détenir, de l'acheter et de le vendre, son usage comme moyen de paiement demeure infime (relativement à ce qui est affiché comme étant sa « capitalisation ») ; et ce, comme on l'a vu, essentiellement dans très peu de pays qui sont en crise monétaire et financière ; ou quand la souveraineté monétaire a été abandonnée. Ainsi, seules des situations de forte crise monétaire et financière, avec ce qu'on appelle une « fuite devant la monnaie », expliquent l'avantage pratique de sa détention à des fins d'usages de paiement si le risque de détention de la monnaie nationale est supérieur à celui de bitcoins. Et encore, même dans ce contexte, les populations en crise se tournent généralement vers des monnaies plus fiables et plus facilement utilisables, comme le dollar ou l'euro.

L'appât du gain personnel agrémenté d'un effet de mode attire donc la majorité de ceux séduits par cet actif spéculatif privé. Domine la conviction que son cours ne peut, au-delà de ses fluctuations, que continuer à monter car ils sont persuadés qu'il y aura toujours de plus en plus d'adeptes du bitcoin (leur nombre s'accroîtra davantage que la quantité émise de nouveaux bitcoins, qui est décroissante jusqu'à cesser totalement). Une des raisons principales de cette croyance, que nous qualifions d'illusion, est que Bitcoin pourrait constituer demain une monnaie privée dont l'informatisation des paiements devrait lui permettre de se substituer au cash. Nous verrons dans la seconde partie que cela n'est pas près d'arriver.

Les défenseurs du bitcoin affirment en outre que si, actuellement, il ne sert pas principalement de moyen de paiement et d'unité de compte des transactions, il serait essentiellement un instrument de réserve. Selon eux, il n'en serait donc pas moins une monnaie. On doit tout d'abord objecter que le rôle de réserve, autrement dit la conservation de la valeur dans le temps, en tant que telle et à elle seule, ne fait pas d'un bien ou d'un instrument financier une monnaie. L'immobilier ou l'orfèvrerie et les bijoux, peuvent servir de réserve souvent mieux

qu'une monnaie, notamment en période de crise. Les deux usages essentiels de la monnaie sont le paiement et le compte ; et la réserve est subsidiaire de ceux-ci. En l'absence des deux premiers, ou de l'un ou de l'autre, on ne peut pas parler de monnaie.

Qui plus est, reconnaître au bitcoin le caractère d'instrument de réserve est contestable. Car, même si son trend reste ascendant sur une moyenne période, les fortes fluctuations à court terme de son cours le rendent inapte à être une « valeur refuge ». L'incertitude quant à sa valeur effective peut être forte car le délai peut être long pour réaliser un gain par rapport à son prix d'acquisition. L'amplitude des variations du cours d'un actif jouant le rôle de « réserve de valeur » doit être limitée. L'épargnant (sauf à posséder un très grand patrimoine liquide et que celui-ci soit diversifié), lorsqu'il éprouve un besoin urgent d'utiliser une partie de ses avoirs, en l'occurrence en la cédant sur un marché, doit raisonnablement pouvoir revendre sans préjudice ses bitcoins sans attendre plusieurs mois voire une année et plus, ou sans être obligé de subir des pertes s'il est contraint de s'en défaire subitement.

À ce jour, les crypto-actifs n'ont par ailleurs rien d'une finance alternative finançant une économie réelle qui serait elle-même alternative en matière écologique, économique, sociale ou financière. Le placement spéculatif apparaît ainsi comme étant l'objet principal du bitcoin et de nombreux crypto-actifs (on pense notamment au Dogecoin). Avec un risque d'addiction de certains de ces spéculateurs. D'où la création de services de traitements spécialisés, dont le plus connu est celui de Castle Craig Hospital en Écosse.

C'est d'ailleurs avec une définition comme actif financier qu'il est considéré dans de nombreux pays. Dans le système financier actuel, la nécessité d'étendre le champ des spéculations, afin d'y placer les masses croissantes de liquidités, fait du bitcoin un instrument de réalisation de survaleurs. Le poids croissant du bitcoin parmi les actifs financiers, loin d'être seulement une opportunité supplémentaire de spéculer, contribue à augmenter l'instabilité des systèmes financiers dans leur ensemble ; donc les risques pour les spéculateurs, compte tenu de comportements moutonniers en matière de spéculations et du rôle de certains influenceurs sur les réseaux sociaux.

Mais le problème est que cet usage spéculatif n'engage pas un effet multiplicateur de revenus, qui créerait une dynamique du système productif. C'est une différence importante avec les spéculations jadis par exemple dans l'exploitation des mines, lors de la construction de trains et de voies ferrées puis d'automobiles et d'autoroutes, d'immeubles, de canaux, dans l'industrie textile, chimique et électrique et plus tard de l'automobile puis des biotechniques et les technologies informatiques et de la communication.

On notera d'ailleurs que les mouvements ascendants de son parcours erratique apparaissent souvent provoqués par des rumeurs, comme à propos de Paypal en octobre 2020 ou d'Amazon en juillet 2021. Des rumeurs qui en tant que telles sont sans relations marquées avec des événements ou des évolutions touchant aux fondamentaux d'une économie dite «

réelle » ; si ce n'est ceux touchant directement aux conditions de son émission et de sa circulation (par exemple le déplacement forcé de ses « usines de minage »). Les soubresauts du cours du bitcoin peuvent très largement être mis en relation avec l'évolution de l'ensemble des titres financiers ou de certaines catégories d'entre eux (comme les valeurs dites « technologiques »). Et ils apparaissent très sensibles aux prises de position quant à son avenir (ainsi qu'à l'affichage des nouveaux placements en bitcoins ou sa cession) par tel ou tel responsable, des mondes non seulement économique ou financier mais aussi médiatique et politique voire sportif... dont on peut fortement douter pour la plupart d'entre eux de leurs compétences financières ou informatiques. Certaines déclarations peuvent correspondre à une manipulation du cours pour vendre à des moments opportuns. Il est frappant que ces déclarations aient eu plus d'effet sur le cours du bitcoin que, en février 2022, l'entrée des troupes russes en Ukraine. Le mélange d'informations et de rumeurs pouvant expliquer les soubresauts de son cours paraît invalider l'affirmation de son initiateur selon laquelle sa valeur serait d'ordre physique ; donc objective et impossible à manipuler car elle dépendrait de la « *preuve cryptographique* » et ne serait pas subjective à travers la réputation dont il jouirait. Ainsi, pour éviter d'alimenter la nature spéculative du marché des crypto-actifs, il pourrait être souhaitable de rendre obligatoire une couverture totale des investissements réalisés par les acteurs financiers classiques par des fonds propres. Ce faisant, les investisseurs traditionnels (banques, fonds de pension, compagnies d'assurance) ne participeraient pas au mouvement de spéculation et limiteraient le risque de contagion en cas de crise financière propre au marché des cryptoactifs.

PROPOSITION n°1 : imposer une couverture totale par des fonds propres des investissements réalisés par les acteurs financiers traditionnels dans les crypto-actifs.

4/ La « capitalisation » des crypto-actifs : un autre “mirage”.

Les débuts du bitcoin ont été confidentiels. Sa courbe reste assez plate de son apparition jusqu'à 2017 où son cours est encore à moins de 1000 dollars. Il a toutefois été multiplié par 60 000 entre 2012 et 2021. Dans une phase fortement ascendante de son cours de 42 000 dollars le 8 janvier 2021 à 64 000 dollars le 14 avril 2021, de nombreux médias ont alors titré que : « le bitcoin atteint une capitalisation supérieure à mille milliards de dollars ». Ce qui le situerait « dans le peloton de tête des grandes devises ». Certes derrière le dollar et l'euro, mais devant le yen.

Par ce qu'on désigne comme sa « capitalisation », le bitcoin représente de loin la principale « capitalisation » en crypto-actif. Mais si l'expression « capitalisation du bitcoin » est très

largement répandue dans les médias, elle interroge. En effet, l'on calcule généralement une « capitalisation » boursière en multipliant un nombre d'actions par leur cours en bourse. Par analogie, la capitalisation du bitcoin à un instant donné est obtenue en multipliant le nombre de bitcoins émis depuis sa création jusqu'à un jour donné, par son cours à la même date. Cela tendrait dès lors à classer le bitcoin parmi les actifs financiers.

Mais de trop nombreux médias ont cherché à comparer la « capitalisation du bitcoin » avec la masse monétaire en circulation des différentes devises. On parle communément de « masse monétaire » et chaque catégorie de masse monétaire est définie par le degré de liquidité des éléments la composant. M0 représente la « base monétaire » composée des pièces et de billets ainsi que la monnaie scripturale à la Banque centrale, M1 correspond à M0 à laquelle on ajoute les dépôts à vue, etc. Or, si on voulait comparer cette « capitalisation » du bitcoin à la masse monétaire de chaque monnaie nationale ou fédérale, il faudrait inclure dans celle-ci, non seulement le total des pièces et des billets émis mais y ajouter la masse beaucoup plus grande des dépôts scripturaux. Et, à l'inverse, du nombre de bitcoins minés depuis sa création il faudrait estimer et déduire une partie de ceux qui ne circulent plus (20 % peut-être) sans nul doute principalement parce que les codes d'accès informatique ont été perdus. Donc la « capitalisation du bitcoin » telle qu'elle est calculée pour la comparer au poids des principales devises a une signification limitée. Cette capitalisation est largement redondante avec la croissance de son cours (dont elle dépend directement alors que le nombre de bitcoins émis est informatiquement limité et programmé à l'avance et ne dépend pas de la demande). Une comparaison pertinente pour apprécier son poids relatif devrait être celle entre le nombre annuel et la valeur cumulée des transactions en bitcoin pour acquérir des biens et services avec le nombre annuel et la valeur cumulée de transactions faites avec chacune des principales devises dans le commerce international et intérieur sous toutes leurs formes. Les résultats seraient alors sans commune mesure et seraient très défavorables au Bitcoin qui ne circule pas ou peu au moyen de transactions dans l'économie réelle. Cette observation conduit dès lors plus largement à interroger le rôle des crypto-actifs en matière monétaire.

II. Une proposition monétaire aux allures de mirage

Une autre dimension essentielle des crypto-actifs porterait sur leur capacité à incarner une alternative monétaire. Or, sur ce volet monétaire encore plus que sur les autres dimensions évoquées jusqu'à présent, le discours de promotion des crypto-actifs relève d'un mélange entre le fantasme et une idéologie libérale de tendance libertarienne qui peut apparaître dangereuse pour la cohésion, l'efficacité, la souveraineté et la conduite de nos systèmes monétaires. En particulier, il est important de comprendre que la philosophie décentralisatrice et désintermédiée dont se réclament les tenants des crypto-actifs s'avère souvent trompeuse et, quand elle ne l'est pas, conduit en réalité à retirer davantage le pouvoir monétaire aux individus comme aux sociétés plutôt que de leur redonner. Dans leur conception et dans l'idéologie qui les inspire, les crypto-actifs s'opposent ainsi radicalement à l'idée d'une monnaie comme bien commun, ainsi que d'une monnaie attachée à une souveraineté politique nationale ou régionale.

A/ La philosophie décentralisatrice et désintermédiée qui sous-tend les crypto-actifs : entre mythe et réalité

Le premier de ces mythes concerne la capacité des crypto-actifs, et notamment du Bitcoin, à incarner en pratique un moyen de paiement accessible, sûr, transparent et pouvant prétendre s'appuyer sur la confiance des citoyens.

1/ Sécurité et gouvernance des systèmes de crypto-actifs

Comme vu précédemment, le bitcoin fonctionne en étant dépourvu d'autorité centrale, en théorie du moins. Ainsi, les partisans du bitcoin prétendent que son minage par "preuve de travail" sécurise mieux le fonctionnement du réseau ; alors que d'autres spécialistes pensent le contraire en relevant la confusion qui est notamment entretenue entre la sécurité de l'émission et celle des transferts des unités de bitcoin (surtout si l'on tient compte des ceux qui s'éloignent de la technique de la *blockchain*).

En outre, ce système conduit à ce que le pouvoir de changer les éléments du protocole Bitcoin se trouve entre les mains des mineurs, qui ont investi des sommes considérables dans leur ferme de minage. Ils ont donc grand intérêt à ce que soit conservée la validation par preuve de travail. On voit bien ici la différence existante entre des intérêts privés non coordonnés et des intérêts collectifs. On peut douter que soit adoptée pour le bitcoin une technique de validation de blocs qui dévaloriserait totalement les investissements qu'ils ont déjà été faits ; sauf si, pour des raisons écologiques et de sécurité des systèmes financiers, une interdiction

de ce type de protocole par les autorités publiques obligeait à une mutation du modèle Bitcoin (c'est ce que nous proposons notamment dans la troisième partie du rapport). Ainsi, il convient de remarquer que la philosophie décentralisatrice du bitcoin constitue un mythe au regard de la puissance des pools de mineurs sur l'évolution et l'avenir du réseau. Cette inégalité de pouvoir se double d'une forte concentration de la détention de ces actifs, au-delà même du Bitcoin, puisque tout émetteur centralisé de cryptoactifs en garde nécessairement une grande partie pour son propre compte.

2/ Coûts de transaction : contraire au discours libertaire d'égalité

Le système n'est pas mieux adapté pour être accessible et peu cher pour tous. Ainsi, pour des transactions de faibles montants le système Bitcoin sur la *blockchain* est totalement inadapté alors que, à l'inverse, il se révèle très avantageux pour ceux et celles qui pourront réaliser ainsi très rapidement des opérations aux montants considérables pour un faible coût ; rapidité indispensable pour spéculer avec profit en suivant les hausses et les baisses de son cours.

L'explication en est simple. À l'intérieur du réseau Bitcoin, le temps pour réaliser une transaction dépend du nombre de transactions qui sont engagées à ce moment-là. Or, si l'on compare le nombre d'unités de bitcoin qui peuvent circuler en un temps donné à la vitesse des transactions des devises par Visa, on constate que le Bitcoin est en moyenne beaucoup moins performant. Le Bitcoin ne peut traiter plus de dix transactions par seconde, certains disent sept. Par comparaison, selon la BRI dans son *Annual Report 2018* (Chap. V, *Cryptocurrencies : looking beyond the hype*), le réseau Visa permet 3500 transactions par seconde et Mastercard, 2000. Il s'ensuit que le traitement de la transaction peut être très rapide (10 ou 20 minutes) si le réseau Bitcoin est peu chargé. À l'inverse, il est très ralenti si le réseau est congestionné. Comment pourrait-on ordinairement s'en servir comme moyen de paiement alors que le coût de la transaction et la durée de réalisation de celle-ci s'avèrent ainsi beaucoup plus incertains que les tenants du bitcoin ne l'affirment ? Dans certains cas, la transaction peut même ne jamais passer si le réseau est congestionné.

En outre, comme l'ordre d'exécution de la transaction ne se fait pas selon le principe du premier arrivé, premier servi, mais qu'il dépend du montant de la commission proposée pour l'exécution de l'ordre (au bénéfice de ceux qui valident l'opération), dans les périodes de congestion du réseau ceux qui proposent de trop faibles commissions peuvent ne pas voir leur demande de transaction exécutée. L'observation de son accumulation entre juillet 2020 et juillet 2021, faite selon la taille des portefeuilles détenus, montre ainsi la différence des comportements en particulier l'accumulation par les « *whales* » (petit groupe des principaux détenteurs) à la fin du deuxième semestre 2020 et par les petits portefeuilles de février à juin

2021. Le petit nombre de détenteurs d'une portion significative des bitcoins leur donne la capacité de voir leurs ordres d'achat et de vente passer avant ceux des petits porteurs (qui proposent des commissions de transaction moindres) et donc de vendre ou d'acheter plus rapidement lors des moments d'intenses hausses et baisses des cours ; donc de bénéficier des premières et de se protéger contre les secondes si les anticipations se réalisent.

Là encore on peut établir un parallèle avec l'émission du bitcoin par minage. Ce sont les détenteurs des capacités de minage les plus grandes qui ont la probabilité la plus forte de gagner les nouveaux bitcoins émis tout comme ce sont ceux qui versent la commission la plus grande qui peuvent voir leur offre ou leur demande satisfaite. Le pouvoir sur le réseau ne suit donc pas le principe d'une décentralisation harmonieuse et égalitaire mais il recrée, bien au contraire, de fortes inégalités en fonction des capacités à payer et à disposer d'une puissance informatique élevée.

3/ Peut-on parler de confiance s'agissant des crypto-actifs ?

Enfin, peut-on penser que la sécurité technique qui entoure, bien que cela soit très relatif au regard du nombre de vols et d'attaques, les opérations autour de la blockchain peut suffire à susciter la confiance et l'adhésion des citoyens ? En s'appuyant sur *La Monnaie souveraine* sous la direction de Michel Aglietta, et André Orléan (Paris, Odile Jacob, 1998), qui rejettent une définition fonctionnelle de la monnaie, on peut reconnaître trois types de confiance sous-jacents à la monnaie et dont la combinaison la fonde :

- méthodique,
- éthique,
- et hiérarchique.

Les trois sont nécessaires au fonctionnement d'un système monétaire.

La confiance méthodique est celle qui se forge à travers les échanges quotidiens et qui fait qu'une monnaie est acceptée parce que l'on est certain que d'autres l'accepteront en paiement. Si le bitcoin circulait très largement entre prestataires de biens et services ainsi qu'entre ceux-ci et les consommateurs il bénéficierait de ce type de confiance à caractère horizontal. Ce n'est pas le cas... pas le cas *encore* diront les "bitcoin maximalistes".

La confiance éthique suppose une idéologie partagée. On pourrait donc la reconnaître aussi dans la croyance de la plupart des défenseurs du bitcoin aux vertus de la concurrence des intérêts et de la propriété privée. À cet individualisme est associé un antiétatisme très largement libertarien défiant l'État et les biens publics. L'affichage de ce type de confiance se concrétise par l'accent mis sur un anonymat des transactions. On peut se demander pourquoi le bitcoin et autres crypto-actifs auraient l'avantage de pouvoir payer anonymement sans limite

de montant quand cela demeurerait illégal avec du cash ? Sans doute les idéologues du bitcoin affirmeront que toutes les interdictions touchant à limiter l'usage de tel ou tel type de moyens de paiement devraient être levées. Le Bitcoin jouerait là le rôle d'un cheval de Troie. En revanche, est totalement absent un élément essentiel de la confiance dans la monnaie : la confiance hiérarchique qui suppose la reconnaissance d'institutions interdépendantes et d'une certaine façon solidaires faisant qu'il existe un système institutionnel garantissant la valeur d'une monnaie contre ses possibles défaillances. Cette absence de confiance pour le bitcoin est reconnue et même revendiquée dans le texte fondateur de *Satoshi Nakamoto* qui place la réputation du bitcoin non dans les institutions mais dans sa technique d'émission et de validation des transactions. C'est à partir de l'idée d'un « or numérique » que l'idée de confiance est récusée puisque sa valeur est supposée dépendre d'un protocole technique non manipulable : la *blockchain*. On peut parler à ce propos de logique sécuritaire. Or celle-ci doit être distinguée de ce qu'est la construction d'une logique de confiance.

Sur quoi la réputation (on peut parler aussi de crédibilité) du bitcoin est-elle assise si d'une part l'instrument est dépourvu de toute utilité propre et si d'autre part il est caractérisé par une absence de créance sur l'émetteur et par un déni de toute garantie institutionnelle ? Cette absence de garantie qui pour ses défenseurs en fait une qualité essentielle parce qu'il serait en quelque sorte « libre » fait aussi qu'il n'existe aucun frein institutionnel à une éventuelle perte de réputation et donc à un effondrement de son cours. La confiance éthique seule ne peut suffire.

La valeur du bitcoin doit donc être fondée sur sa réputation aux yeux de ceux qui l'acquièrent et le détiennent virtuellement ; et, plus encore, elle est fondée sur la croyance que pour les autres elle va perdurer et qu'ils croient aussi aux vertus techniques du réseau Bitcoin. Le *trend* ascendant à moyen et à long terme de son cours joue pour cette double croyance un rôle essentiel. On ne peut que constater ici encore qu'une sorte de foi dans une autre technique, la statistique, voire la lecture de “graphiques” de marché, dont les prédictions s'avèrent aussi fragiles que peu sérieuses. Mais tant les évolutions passées que les anticipations du cours ne sont pas reliées à des facteurs réels qui pourraient les expliquer. Toutefois, à l'automne 2022, la perception du lien avec l'évolution des autres actifs spéculatifs et des effets des décisions des banques centrales en matière de taux d'intérêt, largement oubliés jusque-là, ont été intégrés comme facteurs explicatifs ; y compris jusqu'à mettre en cause les décisions des banques centrales comme étant à l'origine des déboires du bitcoin, alors que les politiques expansionnistes de ces dernières ont largement participé à l'envolée des cours entre 2019 et 2021.

Le bitcoin diffère donc radicalement d'instruments monétaires et financiers alternatifs tels les systèmes d'échange locaux, les monnaies locales complémentaires ayant parité avec les monnaies nationales ou fédérales, les systèmes de crédit interentreprises ou les monnaies

fiscales, qui peuvent aussi s'appuyer sur la technique des chaînes de blocs mais en développant, eux, la solidarité et la gestion par leurs parties prenantes sous des formes et à des échelons divers. Comparés à ces instruments monétaires et financiers, le bitcoin présente les caractéristiques d'un anti-commun et, en tant que tel, il constitue une entrave à une transformation solidaire des pratiques financières et économiques.

Le bitcoin s'oppose aux caractéristiques essentielles des communs en se distinguant aussi des biens publics : à savoir le fait que non seulement la propriété de ceux-là est collective mais de plus que leur usage et leur gestion impliquent une répartition la plus équitable possible de la rareté. Cela afin de promouvoir l'inclusion de chacun et la reconnaissance et la participation de l'ensemble des parties prenantes que son fonctionnement implique. Dans la gestion d'un commun, il y a souci par chacun de reconnaître dans un collectif les besoins des autres et de permettre à chacun d'obtenir un maximum de satisfactions sans que ce soit au détriment d'autrui. Ainsi peuvent être reconnues les obligations de tous et les capacités de tirer des bénéfices et de les répartir le plus justement possible ; et ceci, point essentiel, non pas en proportion de droits inégaux de propriété privée mais au prorata de besoins tant collectifs qu'individuels. Rappelons aussi ici que si un commun monétaire ne circule pas parce qu'il est thésaurisé, sa particularité est, d'un point de vue collectif, sa destruction ; ou pour le moins son altération plus ou moins forte. Il s'agit d'une différence essentielle avec un commun environnemental que son usage épuise si l'on ne prévoit pas des mécanismes assurant son renouvellement. Or, le bitcoin, n'étant pas pour l'essentiel une monnaie de paiement et servant surtout à des placements spéculatifs, n'a pas non plus cette caractéristique de la monnaie dans sa dimension de commun.

Ni la dette, ni le partage ne fondent le bitcoin. Une de ses caractéristiques est que, par analogie avec la création monétaire, il est possible de désigner le profit tiré de son minage comme étant un « seigneurage ». Le droit et les revenus qui y sont afférents se trouvent ainsi privatisés par un groupe (les mineurs) occupant en quelque sorte une position hiérarchique dans son processus d'émission et de circulation. Son mode de production est un élément déterminant de la répartition très inégalitaire de sa possession.

La philosophie décentralisatrice et égalitaire revendiquée par les promoteurs des crypto-actifs apparaît ainsi souvent comme une illusion, qui ne permet pas à ces derniers de prétendre au statut d'alternative monétaire. C'est également le cas au niveau international.

B/ Le bitcoin et le mirage d'une monnaie universelle

Comme cela sera détaillé dans le point II. de la seconde partie du rapport, les insuffisances du système monétaire international, notamment du point de vue des paiements et des transferts de fonds internationaux, auraient pu permettre aux crypto-actifs de trouver

une place dans ces domaines-là. Le Bitcoin a notamment voulu prétendre au statut de monnaie universelle mais ses propres insuffisances ont rapidement exclu cette option du champ des possibles.

Pour que le bitcoin soit reconnu comme une monnaie universelle, il faudrait qu'il fonctionne déjà comme monnaie dans un certain nombre de sphères monétaires nationales ou fédérales. Sur cette base, sa reconnaissance pourrait devenir universelle à la suite de son adoption par de nombreux pays. Or ce n'est pas le cas. La liste des pays qui interdisent le bitcoin ou en limitent l'usage est bien plus longue que celle de ceux qui l'ont reconnu comme moyen de paiement, ainsi que le nombre d'habitants concernés.

Quand le bitcoin est passé au crible des caractéristiques d'une monnaie, l'analyse conduit à affirmer que le bitcoin au mieux ne les remplit pas encore, et plus encore qu'il demeurera incapable de le devenir. Même si un État se dote, comme le Salvador ou la République centrafricaine (RCA), d'une législation et d'une réglementation reconnaissant au bitcoin un pouvoir libératoire non seulement de fait mais légal, affirmer que le bitcoin y est monnaie suppose :

- qu'il soit déjà largement utilisé de plus en plus par une fraction elle-même croissante de la population comme moyen de paiement (et pas seulement comme instrument spéculatif dont le cours n'est en rien contre cyclique de celui des autres valeurs de placement) ;
- qu'il pourrait, dans une crise financière et monétaire, être une issue de secours monétaire et financière ; et donc qu'il convient de s'y préparer en en acquérant à toutes fins utiles.

Or, il n'y aurait sur toute la planète que 400 000 utilisateurs du bitcoin comme moyen de paiement (un nombre infime par rapport à celui de ceux pour qui c'est uniquement un placement spéculatif). Seulement 18 000 commerces l'accepteraient. Sans oublier que constater qu'un commerce affiche qu'il accepte le bitcoin ne signifie pas que le nombre de transactions y soit important.

De la même manière, le bitcoin ne sert pas d'unité de compte et n'a pas de vertu anti-inflationniste. Ses partisans lui donnent des qualités qui seraient celles d'une unité de compte s'il était communément accepté comme moyen de paiement. Selon eux, d'une part cela devrait réduire les fortes variations à court terme de son cours (à la hausse comme à la baisse) ; d'autre part la généralisation de son usage et la stabilité simultanée de son cours (qui se font attendre...) pourraient permettre son usage comme unité de compte dans les transactions et pour estimer les biens et services. Autrement dit, sont affirmées les conséquences d'une adoption du bitcoin sans expliquer les mécanismes à travers lesquels se feraient la transition

et l'adoption finale de ce qui serait une nouvelle unité de compte monétaire. Pour y croire, il faut être convaincu par les arguments d'une collapsologie financière affirmant comme inéluctable une disparition prochaine des monnaies nationales et fédérales.

Les conditions très particulières de pays connaissant une forte détérioration voire disparition de leur souveraineté monétaire sont alors considérées comme une anticipation permettant d'imaginer ce qui serait en tout lieu les suites d'un prochain effondrement des systèmes monétaires et financiers. Or tant que subsisteraient des devises apparaissant comme fiables et surtout plus fiables qu'une nouveauté encore largement mystérieuse et sans garantie institutionnelle tel que le bitcoin, il y a tout lieu de penser que, même étrangères, celles-ci seraient largement préférées au bitcoin dans les pays privés en fait ou en droit de leur devise nationale ; ce qu'ont manifesté des sondages menés auprès des Salvadoriens à la suite de l'annonce de l'adoption du bitcoin comme monnaie nationale en concurrence au dollar.

Les "bitcoins maximalistes" prétendent enfin qu'il serait un instrument de lutte contre la hausse des prix (celle-ci étant pensée par nature comme néfaste). Or, si le cours du bitcoin augmente, toutes choses égales par ailleurs en termes de quantité de biens et services disponibles, cela n'empêcherait nullement une variation des prix relatifs ; c'est-à-dire une variation à la hausse ou à la baisse de tel ou tel bien et service qui bénéficie à telle ou telle catégorie de la population ou pèse fortement dans son budget en tant que dépense contrainte. Car son fonctionnement incarne une inflation particulière : celle qui bénéficie essentiellement à une fraction limitée de la population détenant des actifs financiers et immobiliers. Quand on raisonne en unités de bitcoins, on peut avoir l'impression d'une baisse des prix quand bien même, en raison des variations de son taux de change, les prix, exprimés en dollar ou en euro, demeurent inchangés ou augmentent.

Mais surtout, si l'on pense que les variations de prix ne résultent pas simplement d'une augmentation ou d'une baisse de la quantité de monnaie émise (en particulier du fait des variations de la vitesse de circulation des différentes composantes de la masse monétaire et de l'accroissement et de la diminution des encaisses), la limitation du nombre de bitcoins n'endigue pas les hausses des prix. Elles sont provoquées par l'offre et la demande de biens et services. Mais il est erroné de prétendre que le bitcoin est anti-inflationniste, voire que ce serait sa principale vertu. En outre, la création d'une subdivision du bitcoin, le satoshi (qui représente un / 100 000 000 du bitcoin) permet d'exprimer les prix des devises, des biens et des services en bitcoin, alors que le cours du bitcoin a été multiplié par 60 000 entre 2012 et le printemps 2021. Le fractionnement du bitcoin en satoshi que l'on vient d'évoquer permet donc des variations nominales de prix très importantes.

Enfin, la très forte volatilité du cours du bitcoin, qui singularise cet objet numérique, fait beaucoup douter de sa capacité à être et à pouvoir devenir monnaie. Cette incompréhension des variations du cours du bitcoin a frappé les habitants du Salvador qui s'étaient vu créditer

à l'automne 2021 sur leur application pour payer en bitcoin d'un montant équivalent à 30 dollars et qui se sont aperçus que la somme s'était fortement dépréciée à la suite d'une chute de son cours. La très grande instabilité de son cours rend impossible en l'état d'en faire un instrument de réserve qui supposerait de pouvoir ainsi *a minima* garantir non seulement à long mais aussi à court terme son pouvoir d'achat. Seuls ceux et celles détenant un patrimoine suffisamment liquide important peuvent conserver une partie de leurs avoirs en bitcoin pour espérer bénéficier de hausses de son cours (en faisant l'hypothèse que celui-ci ne s'effondrera pas un jour...). Sinon le risque de devoir le céder à perte est élevé.

C/ L'illusion d'une souveraineté monétaire retrouvée

Un argument très souvent présenté en faveur du bitcoin est sa capacité à s'opposer tant à ce qui serait le monopole d'émission des banques centrales des monnaies nationales ou fédérales que des banques commerciales via le crédit (soumises à des normes et interventions publiques de contrôle). Il instaurerait donc une monnaie indépendante de ces institutions et supposée pour cela être « libre ». À la souveraineté publique de la monnaie, souveraineté jugée oppressive par les tenants du bitcoin, celui-ci substituerait une souveraineté privée constituée par la communauté de ses producteurs et détenteurs. Toutefois il est impossible de parler ici de « communauté » (puisque celle-ci supposerait des règles de gestion impliquant non seulement les principaux mineurs de bitcoin mais l'ensemble de ses parties prenantes (y compris les utilisateurs) et la reconnaissance de ces divers intérêts). Cette prétendue totalité n'a rien ici de « sociale » puisqu'elle ne résulte que de la sommation d'intérêts privés.

Faire du bitcoin la devise d'un pays constitue une régression considérable en matière de souveraineté monétaire publique puisque les autorités de ce pays n'ont aucune prise sur les dynamiques monétaires et financières. Elles sont alors déterminées essentiellement par un ensemble de forces extérieures et d'intérêts privés, les uns et les autres étant totalement aveugles aux besoins spécifiques du pays puisque le cours du bitcoin est soumis au marché international dans lequel le pays représente un poids infime. Comme au XIX^e et durant la première moitié du XX^e siècle avec les contraintes exercées par les régimes d'étalon or (ou argent) quand les crises de ceux-ci avaient nécessité de les dépasser par l'institution de banques centrales en charge de la régulation monétaire. Revenir à un système qui ressemble à la « banque libre » et à la concurrence sans régulation des monnaies a toute probabilité de reproduire les mêmes crises qui avaient fait abandonner ce système.

Plusieurs experts ont souligné que les acquisitions de bitcoins par la Banque centrale du Salvador alors que son cours a ensuite rapidement chuté risquait de mettre le pays en cessation de paiement (avec des réserves de change du pays en bitcoins qui avaient chuté dans les mêmes proportions). Face à ce risque, le recours à l'endettement extérieur a été de

plus en plus coûteux vu l'augmentation des taux d'intérêt que le pays doit acquitter en conséquence de la perte de crédibilité de ses titres financiers sur les marchés internationaux. Seulement deux pays (le Salvador et la République Centrafricaine) ont jusqu'ici reconnu le bitcoin alors que sont beaucoup plus nombreux les pays où il fait l'objet d'interdictions plus ou moins étendues ; au premier rang desquels la Chine.

La situation du Salvador reconnaissant jusque-là le dollar américain ou celle de la RCA membre d'une union monétaire africaine sous dépendance externe (le franc CFA) ont peu à voir :

- avec la conjoncture de populations fuyant leur monnaie nationale dans des pays en décomposition financière et subissant une forte inflation comme au Liban ou au Venezuela. Ce n'est pas le cas du Salvador où la hausse des prix en rythme annuel a été de 0,1 % en 2019. Elle a été de 3,9 % en 2021. La hausse des prix en RCA a été de 4,3 % en 2021 selon la Banque mondiale.
- ni avec la quête de gains rapides et élevés par des petits spéculateurs européens ou surtout nord-américains plaçant ainsi une partie de leur épargne accumulée en période de confinement.

Dans le cas du Salvador comme de la RCA, il s'agit d'une décision politique de chefs d'États gérant leur pays de façon autocrate.

1/ Le cas du Salvador

Le Salvador a été le premier pays engagé dans la voie de l'adoption du bitcoin comme monnaie officielle, un pays de 6,4 millions d'habitants, dépourvu de devise nationale depuis plus de vingt ans. La résolution du Président a aussitôt été actée dans une loi entrée en application le 7 septembre 2021. On peut inscrire sa décision dans celle du 2020 Digital Agenda salvadorien visant à digitaliser le pays dans de nombreux domaines. Le président a aussi annoncé l'utilisation d'une électricité « propre » pour miner des bitcoins dans le pays grâce à la géothermie de ses volcans ; le Salvador espérant alors bénéficier du bannissement du minage du bitcoin par la Chine. Le Salvador aurait donc produit sa monnaie nationale pour autant qu'il ait eu rapidement les moyens de créer les infrastructures matérielles nécessaires à cette production informatisée.

On doit tout d'abord remarquer qu'il s'agit d'une décision autoritaire qui a fait l'objet ni d'une préparation technique à la diffusion et à l'adoption du bitcoin, cela impliquant les outils et les compétences informatiques nécessaires ni d'une concertation avec la population.

Pour ce qui est de la circulation interne du bitcoin, on peut douter que le gouvernement du Salvador, où l'exclusion bancaire frappe 70 % des habitants et où les inégalités sont très

fortes, ait été capable seul de créer les conditions techniques d'un usage généralisé du bitcoin parmi la population, notamment en raison d'un accès à internet très défectueux. Une enquête menée en 2017 avait aussi montré qu'uniquement 37,1% de la population du Salvador possédaient un smartphone.

La loi sur le bitcoin telle qu'elle avait été initialement et précipitamment présentée rendait non seulement possible mais obligatoire l'usage local du bitcoin dans les paiements. Ainsi celui-ci ne devait pas avoir seulement un pouvoir libératoire de fait mais de droit. Une fois la loi proclamée, nul n'aurait pu refuser de le recevoir en paiement. En fait, dès le 24 juin suivant, on a assisté à un rétropédalage des autorités publiques. Non seulement les bitcoins ont pu être refusés lors d'un paiement mais les salaires et les pensions n'ont pas été versés en bitcoins (sans doute en raison d'une chute du cours qui aurait entraîné une baisse des rémunérations). Donc, contrairement aux nombreuses affirmations dans la presse étrangère et dans les sites spécialisés favorables au bitcoin, ce crypto-actif ne peut pas être considéré comme ce que l'on désigne comme étant une monnaie « légale » ; ce qui supposerait tant l'obligation de le recevoir en paiement que de l'accepter comme unité de compte des paiements et des dettes.

On doit remarquer que le Salvador était dépourvu de monnaie nationale puisque, en 2001, il avait abandonné le colon, monnaie nationale depuis 1892 au profit du dollar des États-Unis. Le colon avait disparu de fait de la circulation en 2004. En Amérique latine l'importance de l'usage du dollar tient à celle des *remesas*, les fonds envoyés en dollars par les migrants. Ceux-ci représentent 20,9% du PIB au Salvador. Chaque famille reçoit ainsi en moyenne 195 dollars par mois. On peut remarquer qu'un des principaux arguments du gouvernement salvadorien pour justifier l'adoption du bitcoin a été de réduire ainsi le coût de ces envois de fonds. Or, ce coût pourrait au contraire doubler voire tripler avec le bitcoin par rapport aux méthodes traditionnelles d'envoi. Cela tient à ce que pour le dollar, à la commission d'envoi (en moyenne 2,85%, une des plus basses du monde et la plus basse d'Amérique latine et des Caraïbes) ne s'ajoute pas une commission de change en monnaie nationale, vu l'usage interne courant du dollar. Or la commission de change en bitcoin du dollar (qui demeure le moyen de paiement le plus usité) est a minima de 5 %.

La majorité des Salvadoriens, qui utilisent massivement le cash du fait même d'une exclusion bancaire de plus de 70 % d'entre eux, ont manifesté leur opposition à la décision du président. L'hostilité massive de la population et de nombreuses organisations explique que six mois après une légalisation qui aurait dû faire du bitcoin la monnaie du Salvador, un rapport de la Chambre de commerce et d'industrie du pays, constate que 86 % des entrepreneurs interrogés affirment qu'ils n'ont jamais fait une seule transaction en bitcoin. Par ailleurs, moins

de 2 % des transferts internationaux de monnaie vers le Salvador se font *via* bitcoin³¹. À ce jour, le Salvador, qui a accusé des pertes et a vu sa note financière dégradée par les agences de notation en raison de ses mauvais investissements, représente donc un contre-exemple pour ce qui est de l'efficacité de l'adoption du Bitcoin par un pays en développement. Cela n'a pourtant pas empêché le "lobby" international du Bitcoin de convaincre un autre autocrate de son adoption en République Centrafricaine.

2/ Le cas de la Centrafrique

La reconnaissance du bitcoin comme monnaie nationale par la Centrafrique le 3 juillet 2022 sous le nom de Sango est trop récente et est encore trop peu documentée pour que l'on puisse en tirer des conséquences solidement étayées. Toutefois, on peut déjà retenir un certain nombre d'éléments en particulier certaines similarités (et quelques différences) avec le Salvador. Selon la loi, tout agent économique est désormais en RCA tenu d'accepter le bitcoin comme moyen de paiement lorsqu'il est proposé pour un achat, mais l'on doit aussitôt ajouter que cela n'est valable que pour autant qu'il dispose de l'équipement nécessaire pour le recevoir. Ce qui ne peut que limiter la diffusion effective du crypto-actif dans le pays. En effet, plus encore qu'au Salvador, le pays ne dispose pas d'infrastructures techniques permettant ce développement du numérique (problème non seulement d'accès à un réseau informatique ; moins de 11 % de la population a accès à internet mais également d'accès à l'électricité). Le taux d'exclusion financière de la population y est encore plus élevé qu'au Salvador et son niveau d'éducation permettant de comprendre le fonctionnement d'un réseau numérique y est encore plus faible.

Comme au Salvador, il s'agit d'un pays qui ne jouit pas d'une autonomie monétaire du fait de son appartenance à la zone franc (arrimée à la zone euro). Donc la décision est politique et est justifiée par la volonté « anti-impérialiste » affichée du président Faustin-Archange Touadéra d'une reconquête de sa souveraineté monétaire ; avec ce qui peut apparaître comme un paradoxe car l'adoption du bitcoin revient de fait à nier la dimension publique de la monnaie et donc en partie la souveraineté monétaire nationale. Comme au Salvador, la décision est "top down" car elle n'a été précédée d'aucun débat public qui pourrait lui donner quelques appuis dans une partie significative de l'opinion.

En RCA, deux groupes ont plus particulièrement fortement intérêt à l'usage du bitcoin dans leurs relations monétaires extérieures :

³¹ Étude du NBER (Working Paper NBER n°29968) par Fernando E. Alvarez, David Argente et Diana Van Patten, "Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador" d'avril 2022
[\[https://www.nber.org/system/files/working_papers/w29968/w29968.pdf\]](https://www.nber.org/system/files/working_papers/w29968/w29968.pdf)

- Une partie de la classe politique locale corrompue et tous ceux pratiquant l'évasion des capitaux vers l'Europe et l'Amérique du Nord.
- Les troupes de mercenaires russes fortement présents dans le pays et qui ont tout avantage à fonctionner en bitcoin (en particulier compte tenu du contrôle des revenus des expatriés russes depuis le déclenchement de la guerre en Ukraine).

Aussi, plus encore que dans le cas du Salvador, l'adoption du Bitcoin en Centrafrique risque de ne se révéler être qu'une opération de communication bien orchestrée, sans conséquences réelles pour la population.

D/ Le risque du retour des monnaies privées et du libertarisme financier

Si les crypto-actifs privés ou décentralisés ne permettent en aucun cas, bien au contraire, de retrouver une souveraineté monétaire pour les États, ils peuvent au contraire considérablement l'affaiblir. Une analyse téléologique est ainsi nécessaire pour montrer que les crypto-actifs s'inscrivent généralement dans une volonté démontrée de s'opposer au système monétaire officiel, voire de le remplacer.

1/ Les crypto-actifs représentent l'outil parfait pour les promoteurs de l'idéologie de la privatisation de la monnaie

Cette idée selon laquelle un régime de concurrence de monnaies privées serait préférable à un système monétaire unifié n'est pas nouvelle dans l'histoire. En réalité, pendant la majeure partie de l'histoire humaine, plusieurs types de monnaies coexistaient au sein de mêmes espaces d'échanges et de transactions. Cette diversité était tempérée par l'exigence pour les monnaies de reposer, directement ou indirectement, sur un poids évalué en métaux précieux. Avec le développement massif du crédit et de la monnaie bancaire au XIXe siècle, il est rapidement apparu nécessaire d'organiser l'unification des systèmes monétaires autour de banques centrales qui jouaient le rôle de prêteur en dernier ressort et qui devenaient progressivement les « gardiennes » de la liquidité ultime.

Cela ne s'est pas fait sans heurts ni sans débats et retours en arrière. On a ainsi pu observer plusieurs périodes de concurrence monétaire, dont la plus célèbre est le régime de *free banking* qui a marqué les États-Unis entre 1837 et 1864. Mais ce type de régime monétaire a également été celui de l'Écosse entre 1716 et 1845. Dans cette configuration, les banques étaient libres d'émettre de la monnaie sans limites, bien que la compensation de leurs échanges reposât sur l'or qui servait donc d'étalon et de « base monétaire ». Devant les multiples problèmes posés par ce type de régime (double comptabilité, instabilité du système monétaire, problème de conversion, difficultés à lever l'impôt, complexification des échanges), ces systèmes ont été abandonnés partout dans le monde. La quasi-totalité des États au

monde reconnaissent ainsi implicitement le fait qu'il n'y a pas de monnaie sans autorité publique qui la garantisse et en soit responsable.

Cette évolution n'est pourtant pas acceptée par un certain nombre de penseurs néolibéraux, ou libertariens, qui continuent de penser que la monnaie est une affaire privée et doit être considérée comme une marchandise laissée à la libre définition par le marché. Dans son livre publié en 1976 et intitulé *The Denationalization of Money* (publié en français sous le titre *Pour une vraie concurrence des monnaies*), Friedrich von Hayek écrivait ainsi que produire de la monnaie « *est un service utile comme la production de n'importe quel autre bien* », ce qu'il complétait en indiquant que : « *dès qu'on arrive à se libérer de la croyance acceptée de façon universelle mais tacite qu'un pays doit être alimenté par son gouvernement avec sa propre monnaie distincte et exclusive, toutes sortes de questions intéressantes apparaissent qui n'ont jamais été examinées* ».

Aujourd'hui, de nombreux promoteurs des crypto-actifs se réclament des thèses de Hayek et, plus largement, de l'école autrichienne de la monnaie. Pour les tenants de cette idéologie, l'État ne doit disposer d'aucune prérogative particulière en matière monétaire, car il serait tenté d'abuser de ce pouvoir pour des raisons électoralistes, ce qui fausserait les mécanismes de marché par l'inflation et favoriserait la perte de confiance de la population dans la monnaie. Ainsi le développement de monnaies privées sur lesquelles l'État n'a aucun contrôle permettrait de prévenir ce risque. Si l'on regarde l'usage des crypto-actifs dans les années récentes, il va sans dire que cette vision paraît complètement erronée puisque les crypto-actifs se révèlent bien plus instables et spéculatifs que les monnaies officielles.

2/ Une abolition de la monnaie comme bien commun et souverain : quels risques pour les États ?

Très concrètement, si les États reconnaissaient aujourd'hui aux crypto-actifs, ou même à une petite fraction d'entre eux (comme le bitcoin), une valeur monétaire équivalente à celle des monnaies nationales, un nouveau régime de concurrence des monnaies pourrait s'installer, qui serait porteur de toutes les difficultés citées précédemment. Le cas du Salvador, évoqué ci-dessus, est particulièrement éclairant à cet égard.

Un système monétaire anarchique pourrait alors émerger. Plusieurs problèmes émergeraient alors.

En premier lieu, il serait impossible de disposer d'un prêteur en dernier ressort et d'une garantie des dépôts car les acteurs impliqués seraient très divers et les crypto-actifs également.

En second lieu, il serait très difficile de définir les règles permettant de savoir quels crypto-actifs ont vocation à pouvoir servir de moyens de paiement et de compte et quels autres ne

devraient pas accéder à ce statut. Des décisions dans ce domaine comporteraient nécessairement une part d'arbitraire.

En troisième lieu, il serait difficile pour les États de lever l'impôt car le droit de lever l'impôt est étroitement associé à l'existence d'une monnaie officielle souveraine. Dès lors que de multiples monnaies privées coexisteraient, les services fiscaux auraient de grandes difficultés pour savoir qui devrait être taxé, dans quelle « monnaie » et à quelle proportion. Si ce type de questions apparaît pour l'instant assez théorique dans les pays développés, les manœuvres opérées par le lobby des crypto-actifs pour faire reconnaître le bitcoin comme monnaie officielle au Salvador et en République centrafricaine doivent servir de signaux d'alarme.

En quatrième lieu, un régime de concurrence des monnaies rendrait toute politique monétaire nationale impossible. En effet, comment serait-il possible de transmettre des impulsions monétaires coordonnées et volontaires à des systèmes monétaires différents, utilisés sur des aires de transaction ne recoupant pas nécessairement les espaces politiques de décision ? Idem s'il s'agit de financer une relance monétaire pour faire face à une crise économique.

En cinquième lieu, le développement économique pourrait être entravé par l'incertitude entourant les échanges ayant lieu dans des monnaies différentes, de la même manière que le risque de change freine parfois le développement du commerce international et suppose de faire appel à des instruments de couverture du risque de change. En effet, l'utilisation de monnaies volatiles, instables, émises par des acteurs pas toujours fiables ou par des communautés n'ayant pas d'unité politique, pourrait gravement handicaper le commerce et les échanges au sein d'une Nation, obligeant les acteurs économiques à s'adapter à des systèmes de comptabilité avec des prix et des valeurs exprimés en plusieurs devises, complexifiant la tenue des registres et des échanges, etc.

En sixième lieu, si une monnaie privée venait à acquérir une large communauté d'utilisation parce qu'elle est liée à une grande multinationale privée, le pouvoir politique de cette dernière serait tellement important qu'elle pourrait faire pression sur les États pour modifier la réglementation à son avantage. Ainsi, si Libra avait été adopté par les deux milliards d'utilisateurs de Facebook, le consortium à l'origine du projet aura certainement pu avoir une influence majeure sur des pays en développement fragiles dont la population aurait pu se tourner vers ce type d'actifs.

Il y a ainsi un grand nombre de paramètres à considérer dès lors que des innovations prétendent bouleverser l'ordre monétaire. Ces enjeux dépassent de loin la question de l'innovation technologique ou même de la simple réglementation financière. Dans le cas présent, il s'agit de savoir si le mouvement d'unification des systèmes monétaires qui a accompagné l'essor des États modernes pourrait être remis en cause par ce type d'évolutions. Face au retour des monnaies privées et aux difficultés majeures qu'il pourrait entraîner, il nous paraît bien plus prometteur d'encourager une réflexion globale et ambitieuse autour des

monnaies numériques de banque centrale, comme nous le verrons ultérieurement. En effet, l'opposition entre crypto-actifs et monnaies numériques de banque centrale réside fondamentalement dans une confrontation de visions politiques et idéologiques, et non dans une considération technologique.



Deuxième partie : Contenir l'impact des crypto-actifs sur la souveraineté monétaire et sur la stabilité financière

Le constat des risques que fait peser le secteur des crypto-actifs sur les investisseurs ainsi que sur la stabilité financière en général (sans compter les enjeux en termes de lutte contre le blanchiment d'argent, l'évasion fiscale ou le financement du terrorisme ou encore les enjeux environnementaux...) est partagé par de multiples acteurs au niveau international. Les différents régulateurs et législateurs s'en sont emparés et en particulier les institutions européennes qui font figure de *leader* en la matière avec l'arrivée prochaine du règlement MiCA. Toutefois, précurseur ne veut pas dire modèle indiscutable et les textes européens, s'ils sont novateurs, sont encore insuffisants au regard des risques nouveaux et du développement continu de nouvelles pratiques (ex. DeFi) et de nouveaux objets (ex. NFT). La difficulté a d'abord été d'appliquer le droit existant aux nouvelles technologies. Ensuite, les législateurs ont proposé de premières réglementations spécifiques au secteur, encore largement divergentes au niveau international.

I. Une législation encore en construction qui doit s'adapter à des objets mouvants

Les nouvelles technologies et en particulier l'environnement de la *blockchain* ne s'embarrassent pas des catégories juridiques préexistantes et semblent même tout mettre en œuvre pour apporter de la confusion juridique. Le législateur est donc confronté à une véritable difficulté lorsqu'il cherche à encadrer les activités de ce secteur. Les différents régulateurs internationaux divergent quant à l'encadrement approprié à ces activités : réglementation financière (information de l'investisseurs, règles d'abus de marché...) ou réglementation bancaire (protection des fonds propres, protection du consommateur...) ?

L'UE est la juridiction la plus avancée en la matière, créant un cadre juridique nouveau et tentant de la porter au niveau international pour assurer la convergence réglementaire. L'encadrement présente toutefois des failles et des vides qu'il convient de combler sans attendre le développement des pratiques non régulées.

A/ Les évolutions du droit européen relatif aux crypto-actifs

Alors que l'initiative réglementaire dans le domaine des crypto-actifs a longtemps été portée par les États membres de l'Union européenne (UE)³², les institutions européennes ont

³² Voir notamment la réglementation française en la matière qui date de la [loi PACTE n° 2019-486 du 22 mai 2019](#) et qui a instauré un régime spécifique pour les ICO et les prestataires de services sur actifs numériques (PSAN).

présenté en septembre 2020 un « *Digital Finance Package* », c'est-à-dire un ensemble de mesures, en vue de définir et encadrer le secteur des crypto-actifs. Ce paquet est composé de plusieurs textes dont l'objectif central est de garantir que les nouvelles activités, par-delà l'innovation que représente la *blockchain*, se voient imposer des règles équivalentes aux activités traditionnelles qui leur sont similaires. Le principe est en effet : « même activité, mêmes risques, mêmes règles »³³.

Le texte pivot est le règlement européen sur les marchés de crypto-actifs (*Markets in Crypto-Assets* - MiCA), qui vise à établir un cadre réglementaire européen harmonisé encadrant les émetteurs de crypto-actifs, ainsi que les activités sur ce nouveau marché. Ce règlement doit encore faire l'objet d'une traduction, d'un accord formel du Conseil et du Parlement européen (PE), puis d'une publication au Journal officiel de l'UE (JOUE) qui n'est pas attendue avant le 1^{er} trimestre 2023. Son entrée en application est prévue pour l'automne 2024, date à laquelle il se substituera, le cas échéant, aux régimes nationaux déjà mis en place³⁴.

Le règlement MiCA s'articule avec le règlement européen visant à instaurer un « régime pilote » pour les infrastructures de marché reposant sur *blockchain* (« règlement PILOTE »)³⁵. L'objet de ce texte est de créer un cadre dérogatoire et temporaire permettant à des infrastructures de marché³⁶ d'expérimenter l'usage de *blockchains* pour exécuter certaines de leurs opérations. Ce texte vise donc un développement des expérimentations dans le secteur financier pour déterminer dans quelle mesure l'utilisation de la *blockchain* pourrait permettre d'améliorer la rapidité et la sécurité des transactions financières. Les acteurs privés agiront ici en lien étroit avec les différents régulateurs européens puisqu'ils devront être agréés et surveillés. À l'issue de ces trois années d'expérimentation (qui peuvent être étendues à six ans), il s'agit de déterminer si, et dans quelle mesure, il conviendra d'adapter la législation de l'UE en vigueur pour soutenir l'usage de *blockchains* dans le secteur financier³⁷.

Ensuite, le règlement européen sur la résilience opérationnelle du numérique (DORA) vise à harmoniser les exigences concernant les règles de sécurité des systèmes d'information pour l'ensemble des acteurs du secteur financier. Il s'agit de faire en sorte que toutes les entreprises veillent à pouvoir résister à tous les types de perturbations et de cyber-menaces,

³³ Commission européenne, [communiqué de presse du 24 septembre 2020](#)

³⁴ Le règlement est d'application directe dans l'ensemble de l'UE. Il n'y aura donc pas de besoin de transposition pour qu'il s'impose sur tout le territoire de l'UE. Pour autant, certaines juridictions devront modifier leur législation existante pour l'aligner sur le nouveau cadre qui s'impose 18 mois après l'entrée en vigueur de MiCA (on parle de "transposition négative").

³⁵ [Règlement \(UE\) 2022/858 du Parlement européen et du Conseil du 30 mai 2022 sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, et modifiant les règlements \(UE\) n° 600/2014 et \(UE\) no 909/2014 et la directive 2014/65/UE](#)

³⁶ Les infrastructures de marchés financiers, comme les systèmes de paiement, les chambres de compensation ou les dépositaires centraux de titres (DCT) et les systèmes de règlement-livraison, constituent la « tuyauterie » des marchés financiers. Elles permettent l'échange des instruments financiers en traitant non seulement les flux de paiement, mais aussi les flux de titres.

³⁷ Ce règlement temporaire limite les risques financiers des expérimentations en imposant des plafonds d'émission de d'instruments financiers numériques définis en fonction des valeurs mobilières émises (ex. pour les actions, un seuil de capitalisation boursière de l'émetteur à 500 millions d'euros ; pour les obligations et autres formes de dette sécurisée, un seuil de volume d'émission à 1 milliard d'euros ; un plafonnement de la valeur de marché totale des actifs échangés à 6 milliards d'euros par DCT ; etc...).

y répondre et s'en remettre. Ce cadre s'appliquera aux différents types d'institutions financières, ainsi qu'aux entreprises fournissant des services au secteur financier.

Enfin, la Commission européenne a publié en 2021 un ensemble de propositions législatives sur la thématique de la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT), dont une des avancées principales est la création d'une autorité européenne (*Anti-Money Laundering Authority*, AMLA), qui a vocation à devenir le centre d'un système intégré d'autorités nationales de surveillance en matière de LCB-FT. Cet ensemble réglementaire, désigné sous l'acronyme « AMLD5 », va notamment permettre d'étendre le champ d'application des règles LCB-FT de l'UE à l'ensemble du secteur des crypto-actifs, obligeant tous les acteurs à appliquer des mesures de vigilance à l'égard de leurs clients. L'objectif de l'AMLD5 est de garantir une traçabilité complète des transferts de crypto-actifs pour empêcher leur utilisation frauduleuse. L'AMLD5 inclut une révision du règlement transferts de fonds³⁸ qui fait notamment appliquer aux crypto-actifs une recommandation du Groupe d'action financière (GAFI)³⁹ dite « *travel rule* » imposant que les prestataires de service sur crypto-actifs (CASP⁴⁰) obtiennent et conservent les informations sur les initiateurs ainsi que sur les bénéficiaires des transferts de crypto-actifs et les mettent à disposition des autorités pertinentes.

Ces différents textes permettent d'aboutir à une catégorisation fine des crypto-actifs et des activités qui leur sont associées. Le cadre européen qui se dessine encadre chaque actif et activité en fonction des risques qu'ils posent pour les utilisateurs et des intérêts de l'UE.

1/ Les différentes catégories juridiques du secteur des crypto-actifs

Le secteur des crypto-actifs est longtemps resté *terra incognita* pour le législateur européen. Aujourd'hui encore, les différents crypto-actifs restent des “*animals with whom it is difficult to engage*”⁴¹. Pour cette raison, un des enjeux centraux du règlement MiCA était de créer les catégories juridiques permettant l'imposition de la réglementation appropriée. En fonction de leurs caractéristiques, en effet, les crypto-actifs peuvent correspondre à des instruments de paiement, d'investissement, ou encore à des objets d'art. La réglementation doit donc

³⁸ Règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) 1781/2006

³⁹ Le GAFI est un organisme intergouvernemental qui élabore des normes et promeut l'application de mesures législatives, réglementaires et opérationnelles en matière LCB-FT vis-à-vis du système financier international. Il a notamment élaboré une série de recommandations (1990) constituant un cadre international de LCB-FT qui a vocation à être transposé dans les réglementations de tous les pays du monde. À cette fin, le GAFI surveille les progrès réalisés par ses membres dans la mise en œuvre des mesures et identifie également au niveau des pays les vulnérabilités afin de protéger le secteur financier international contre son utilisation à des fins illicites.

⁴⁰ La terminologie choisie est CASP pour *crypto-asset service provider*, ce qui est la qualification retenue par le règlement MiCA. Toutefois, le terme employé dans la législation française est « prestataire de service sur actif numériques » (PSAN, voir glossaire). Il appartiendra au législateur français de faire coïncider le régime français « PSAN » avec le régime européen « CASP » qui s'imposera désormais.

⁴¹ A. Enria, président du Conseil de surveillance prudentielle (BCE) au [Financial Times](#), 13 nov. 2022

s'adapter à ces objets mouvants et aux risques spécifiques qu'ils présentent en termes de protection du consommateur ou de stabilité financière.

La typologie européenne issue de l'ensemble réglementaire est la suivante (voir aussi glossaire) :

- **Crypto-actifs** (art. 1(2) de MiCA⁴²) : Il s'agit de la catégorie la plus large pour définir les actifs circulant sur une *blockchain*. Est un crypto-actif toute représentation numérique « *of a value or a right which may be transferred and stored electronically, using distributed ledger technology or similar technology* »⁴³. C'est à cette catégorie que seront rattachés les crypto-actifs volatils de type bitcoin ou ether.

Toutefois, le règlement MiCA s'applique seulement à des personnes physiques et morales, ainsi qu'aux activités et services qu'elles exercent, fournissent ou contrôlent, directement ou indirectement. Dès lors, lorsque l'émission de crypto-actifs est effectuée de manière totalement décentralisée, sans aucun intermédiaire, elle sort du champ d'application de du règlement (cons. 12a de MiCA). À ce stade donc, l'émission de crypto-actifs complètement décentralisés, comme le bitcoin, n'est pas encadrée par le règlement, alors même que le bitcoin est qualifié par le texte. Ce vide juridique est en réalité un choix par défaut du législateur : dans la mesure où il est impossible pour les régulateurs de déterminer qui émet un bitcoin, il n'est pas utile d'envisager d'encadrer cette activité.

Pour autant, à défaut d'encadrer les émetteurs de crypto-actifs décentralisés, le texte s'imposera aux CASP qui fournissent des services sur de tels crypto-actifs. Enfin, la Commission devra, dans un délai de 24 mois puis de 48 mois après la date d'entrée en vigueur du texte, présenter au PE et au Conseil un rapport sur l'application de MiCA accompagné, le cas échéant, d'une proposition législative. Ce rapport devra notamment porter sur « *an assessment of the development of decentralised-finance in the crypto-assets markets and of the adequate regulatory treatment of decentralised crypto-asset systems* » (art. 122(jc) de MiCA).

- **Stablecoins** : La notion technique et économique de *stablecoin* n'est pas définie par la réglementation européenne qui préfère employer les deux sous-catégories suivantes :

⁴² La numérotation des articles du règlement MiCA renvoie au texte issu du trilogue dont la numérotation est provisoire, en attendant l'adoption en session plénière du Parlement européen et la publication du Règlement MiCA au Journal officiel de l'UE (JOUE).

⁴³ Les terme « technologie des registres distribués » (*distributed ledger technology*, DLT) est employé pour désigner une technologie qui permet l'exploitation et l'utilisation de registres distribués, c'est-à-dire de répertoire d'informations qui conserve un enregistrement des transactions et qui est partagé et synchronisé au sein d'un ensemble de nœuds de réseau DLT, au moyen d'un mécanisme de consensus (art. 2.1 et 2.2 de PILOTE). Cette définition correspond à la définition de *blockchain* dans le cadre de la présente analyse (cf. glossaire).

- **Asset-referenced tokens (ART)** (art. 1(3) de MiCA) : Ils désignent des crypto-actifs adossés à plusieurs monnaies ayant cours légal ou à d'autres types d'actifs et qui ont vocation à maintenir « *a stable value by referencing to any other value or right or a combination thereof, including one or more official currencies* »⁴⁴. Ils sont supposés être principalement utilisés à des fins d'investissement, et non de paiement.

Le projet Libra/Diem porté par Facebook dès 2019 fut l'initiative mondiale de *stablecoin* la plus ambitieuse à ce jour. Il s'agissait de simplifier les paiements en émettant un jeton « multidevises » dont la valeur était stable vis-à-vis d'un panier de monnaies officielles (euro, dollar, sterling, yen et dollar de Singapour). La stabilité du jeton devait être garantie par une réserve d'actifs liquides (par exemple, des titres d'État). Le crypto-actif proposé par ce projet serait vraisemblablement entré dans la catégorie d'ART, mais le projet a été abandonné entre-temps.

Le régime des ART impose notamment à l'émetteur de ce crypto-actif d'offrir un remboursement, gratuit, à tout moment, et à la valeur de marché, au détenteur d'ART qui le demande (art. 35 de MiCA)⁴⁵. Les émetteurs d'ART et les CASP qui fournissent des services sur des ART ne peuvent pas proposer d'intérêts en lien ceux-ci (art. 36 de MiCA).

- **Jetons de monnaie électronique** (*electronic money tokens* - EMT) : Il s'agit d'une autre sous-catégorie de crypto-actifs qui correspondent à des crypto-actifs ayant vocation à maintenir « *a stable value by referencing to the value of one official currency* » (art. 1(4) de MiCA). La différence principale avec les ART est que les EMT ne sont pas stables vis-à-vis de plusieurs autres actifs mais d'un seul, une monnaie officielle, dont ils sont supposés reproduire les caractéristiques économiques. Dès lors ils sont, contrairement aux ART, supposés être utilisés à des fins de paiement. Leur régime juridique renvoie vers le régime de la monnaie électronique⁴⁶, ce qui suppose notamment un

⁴⁴ Les *stablecoins* « algorithmiques », c'est-à-dire, les *stablecoins* qui visent à maintenir une valeur stable *via* des protocoles, qui prévoient l'augmentation ou la diminution de l'offre de ces crypto-actifs en réponse aux variations de la demande, doivent être considérés comme inclus dans le champ de MiCA en tant qu'ART ou EMT (voir ci-dessous). Ils devront donc constituer une réserve (cons. 26 de MiCA).

⁴⁵ Les actifs de la réserve devront être liquides pour que les risques de liquidités liés aux demandes de remboursement des utilisateurs soient traités.

⁴⁶ [Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE](#)

remboursement à la valeur faciale, et non pas à la valeur de marché, des EMT par l'émetteur (art. 44 de MiCA).

Le *tether*, ou du moins un équivalent à ce *stablecoin* qui aurait pour objet de reproduire les caractéristiques économiques de l'euro sur une *blockchain* devrait pouvoir être rangé dans cette catégorie. Le livre blanc publié par Tether⁴⁷ indique en effet que : « *Each tether unit issued into circulation is backed in a one to one ratio (i.e. one tetherUSD is one US dollar) by the corresponding fiat currency unit held in deposit by Hong Kong based Tether Ltd. Tethers are fully redeemable/exchangeable at any time for the underlying fiat currency or, if the holder prefers, the equivalent spot value in Bitcoin. [...] The fiat currency on reserve has gained the properties of a cryptocurrency and its price is permanently tethered to the price of the fiat currency* ».

- **Utility tokens** (art. 1(5) MiCA) : Il s'agit d'une sous-catégorie de crypto-actifs émis lors des opérations de financement de projet de type ICO, et dont la principale fonction est de permettre l'accès futur à un service ou à un produit proposé par l'émetteur de cet actif.
- **Non-fungible tokens** (art. 2.2a de MiCA) : Le règlement MiCA ne doit pas s'appliquer à cette sous-catégorie de crypto-actifs qui sont uniques et non fongibles^{48,49}. Ils concernent notamment l'art numérique et les objets de collection, dont la valeur est attribuable aux caractéristiques uniques de chaque crypto-actif et à l'utilité qu'il procure au détenteur du jeton (leur fonctionnement et les risques associés sont décrits à la partie I.A.2). La Commission, à l'occasion de son rapport sur les derniers développements en matière de crypto-actifs qu'elle doit rendre 18 mois après la date d'entrée en vigueur du règlement MiCA, devra procéder à une évaluation du développement des marchés des NFT et de l'adéquation de leur traitement réglementaire (art. 122b de MiCA).

⁴⁷ « [Tether: Fiat currencies on the Bitcoin blockchain](#) », 2016

⁴⁸ La fongibilité implique qu'un objet ou un actif (ici un crypto-actif) n'est pas individualisé et n'est désigné dans un contrat que par son espèce et sa quantité. Cette spécificité a pour conséquence que celui qui détient un actif fongible pour le compte d'un tiers n'est obligé qu'à la restitution de la même quantité de la même espèce sans devoir rendre l'actif qui lui a été remis. Le [tribunal de commerce de Nanterre, 26 févr. 2020, BitSpread c/ Paymium](#) a considéré que les bitcoins étaient des biens fongibles « car de « même espèce et de même qualité » en ce sens que les BTC sont tous issus du même protocole informatique et qu'ils font l'objet d'un rapport d'équivalence avec les autres BTC ». Au contraire, par hypothèse, un NFT n'est pas fongible. Le règlement MiCA précise dans le même sens que « *the sole attribution of a unique identifier to a crypto-asset is not sufficient to classify it as a unique or not fungible* » (cons. 6c de MiCA).

⁴⁹ [B. Sousi, Banque-Notes Express du 30 octobre 2022, « Le Règlement européen MiCAR vient d'être adopté : les NFTs sont-ils réglementés ? Non, mais... »](#)

- **Instruments financiers numériques** (*security tokens*) (art. 2(11) de PILOTE) : Les actifs qui, de par leur nature, correspondent à la qualification d'instruments financiers telle que définie dans la directive sur les marchés financiers (*Markets in financial instruments directive* - MiFID II)⁵⁰ avec la seule différence qu'ils circulent sur une *blockchain* et non pas sur les comptes d'un DCT⁵¹. Le règlement PILOTE prévoit la possibilité d'effectuer des transactions avec ces actifs sur des infrastructures de marché fonctionnant sur *blockchain* (voir ci-dessous). Ces security tokens n'entrent pas dans le champ d'application du règlement MiCA mais doivent s'insérer dans le cadre des règles traditionnelles applicables aux marchés financiers. Il s'agit en effet d'éviter que des instruments financiers soient "déguisés" en crypto-actifs, au mépris de leur fonction économique véritable.

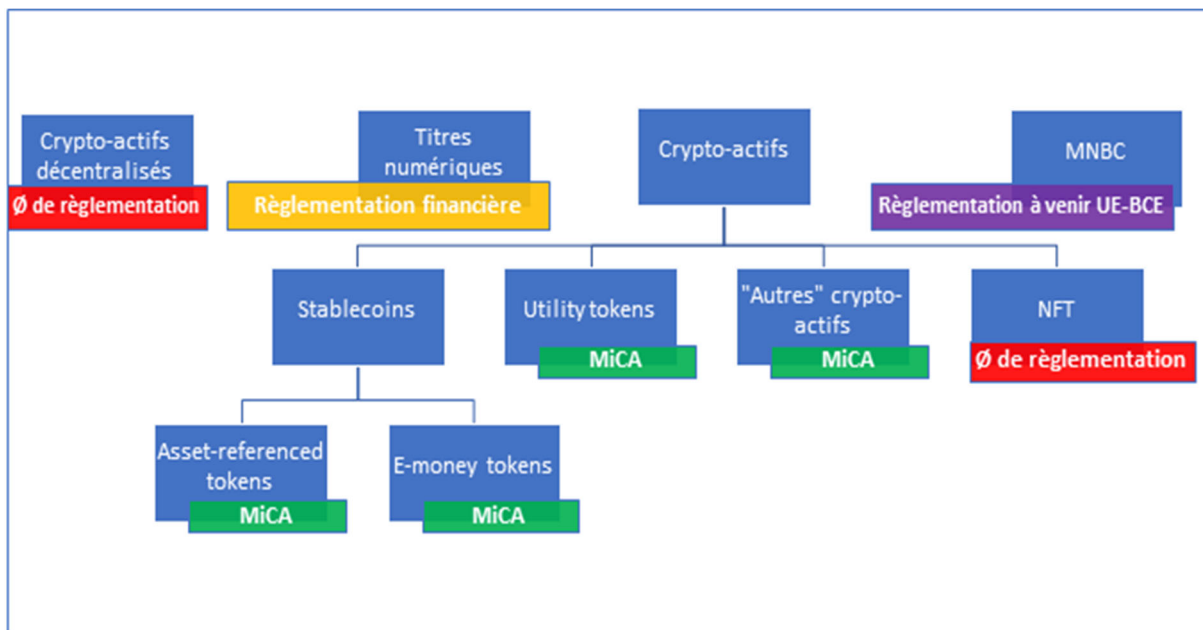
Pour la même raison, le règlement MiCA ne s'applique pas aux les crypto-actifs qui seraient qualifiables de dépôts, dépôts structurés, fonds, produits de titrisations, produits d'assurance, d'assurance-vie et de réassurance, ou certains produits liés aux fonds de pension, entrant dans le champ d'application des réglementations européennes existantes (art. 2.3 de MiCA).

- **Monnaies numériques de banque centrale** (MNBC, *central bank digital currencies*, CBDC). Cette catégorie n'est pas à proprement parler définie dans les textes actuels, mais elle est explicitement exclue de MiCA (cons. 7 de MiCA). Il s'agit d'une catégorie d'actif circulant, ou non, sur *blockchain* qui n'entre dans aucune des catégories définies précédemment. Le règlement PILOTE les désigne comme « monnaie de banque centrale sous forme tokenisée » (art. 5.8 de PILOTE) et indique que le règlement des paiements dans les infrastructures de marché sur *blockchain* doit se faire *via* ces MNBC lorsque c'est possible en pratique (et seulement à défaut par des actifs de règlement « privés »). La spécificité des MNBC, et leur potentiel révolutionnaire en matière monétaire, sera explicitée plus loin.

⁵⁰ [Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE](#)

⁵¹ Voir notamment le [rapport sur les titres financiers digitaux du Haut Comité Juridique de la Place Financière de Paris, 27 novembre 2020](#)

Catégories de crypto-actifs



La réglementation définit et encadre aussi les activités qui peuvent être réalisées à partir de ces différents crypto-actifs.

2/ Les différents acteurs du secteur des crypto-actifs

Le règlement MiCA s'applique aux « *natural and legal persons and other undertakings that are engaged in the issuance, offer to the public and admission to trading of crypto-assets or that provide services related to crypto-assets in the Union* » (art. 2.1 de MiCA). Ce règlement ne s'applique donc pas dans le cas où une personne établie dans l'UE recherche, de sa propre initiative, de services de crypto-actifs fournis par une entreprise d'un pays tiers. Toutefois, lorsqu'une entreprise d'un pays tiers sollicite des clients ou des clients potentiels dans l'UE ou fait la promotion ou la publicité de services ou d'activités de crypto-actifs dans l'UE, elle doit être agréée en tant que CASP (cons. 51 de MiCA).

Les réglementations imposées aux acteurs du secteur des crypto-actifs sont plus ou moins contraignantes en fonction des risques que font peser ces actifs. Elles permettent un encadrement harmonisé des activités du secteur des crypto-actifs, les acteurs pouvant désormais "passeporter" leurs activités dans l'UE, dès lors qu'ils sont agréés dans un des États membres.

- **Émetteurs de crypto-actifs** (art. 3(6) de MiCA) : Ces nouveaux acteurs doivent obtenir une autorisation d'offrir au public des crypto-actifs et de demander leur admission à la négociation sur une plateforme de négociation de crypto-actifs (art. 15 de MiCA). À cette occasion, ils doivent publier un document d'information (*white paper*,

art. 17 de MiCA) pour les utilisateurs de leur crypto-actif. Cela permet d'assurer que les détenteurs potentiels de crypto-actifs sont informés des caractéristiques, des fonctions et des risques des crypto-actifs qu'ils ont l'intention d'acheter⁵². Ils seront alors listés sur un registre de l'Autorité européenne des marchés financiers (AEMF).

En cas de manquement de l'émetteur de crypto-actif au regard des règles posées par le règlement MiCA, l'autorité de régulation nationale pourra imposer des amendes et d'autres sanctions administratives (ex. *name & shame*). Ces amendes peuvent monter jusqu'au double du montant des profits réalisés ou des pertes évitées du fait de l'infraction.

Pour les émetteurs d'ART et EMT⁵³, le règlement MiCA prévoit, en fonction de certains seuils, un statut d'émetteur d'EMT et d'ART significatifs qui serait soumis à des exigences renforcées et supervisés par l'Autorité bancaire européenne (ABE) et l'AEMF.

- **CASP** (art. 3(8) de MiCA) : Ce sont les entités qui s'occupent de la « *provision of one or more crypto-asset services to third parties on a professional basis, and are allowed to provide crypto-asset services in accordance with Article 53* ». Les plateformes d'échange de crypto-actifs entrent dans cette catégorie et les acteurs français ont déjà obtenu un agrément en tant que PSAN auprès de l'AMF, dans le cadre du droit français⁵⁴. L'article 53 de MiCA leur imposera un agrément de CASP pour les acteurs qui ne sont pas déjà des acteurs financiers⁵⁵. Les CASP ne sont soumis qu'à un enregistrement avec des exigences prudentielles minimales à respecter (ex. : droit de rétractation, obligation d'agir de manière honnête, loyale et professionnelle, règles de conflit d'intérêts, responsabilité de la diffusion d'une information complète, loyale et claire). Certains CASP, considérés comme significatifs et se voient imposer des contraintes supplémentaires⁵⁶.

Les activités que pourront proposer les CASP sont la conservation et l'administration de crypto-actifs pour le compte de tiers (art. 67 de MiCA) ; la gestion de plateformes de négociation pour crypto-actifs (art. 68 de MiCA) ; l'échange de crypto-actifs, soit

⁵² Les informations à fournir sont notamment l'identité de l'émetteur ; l'identité de la plateforme qui admettra ces actifs ; les droits et obligations liés aux crypto-actifs offerts ; les informations relatives à la technologie sous-jacente ; et l'information sur les risques liés aux crypto-actifs, incluant notamment ceux liés à la perte partielle ou totale de valeur, au risque de liquidité.

⁵³ Les émetteurs d'EMT doivent être agréés en tant qu'établissement de monnaie électronique ou en tant qu'établissement de crédit.

⁵⁴ La liste des PSAN agréés par l'AMF est disponible sur [son site](#).

⁵⁵ Les établissements de crédit, DCT, entreprises d'investissement, opérateurs de marchés, établissements de monnaie électronique, sociétés de gestion d'OPCVM ou fonds d'investissement alternatif se soumettent, eux, à des exigences particulières du fait de leur agrément « principal ».

⁵⁶ Le caractère significatif s'évalue au nombre d'utilisateurs actifs sur une année dans l'UE.

contre des fonds en monnaie légale, soit contre d'autres crypto-actifs ou encore les services de conseil et de gestion de portefeuille en crypto-actifs.

- **Infrastructure de marché sur *blockchain*** (art. 2 de PILOTE). Le règlement PILOTE permet l'apparition d'un ensemble de nouveaux acteurs, cette fois pour ce qui concerne les infrastructures de marché (voir définition ci-dessus). Chacune de ces nouvelles entités devra reproduire le fonctionnement de ses homologues « traditionnels » sur une *blockchain*. Toutefois, leurs opérateurs pourront s'exempter de certaines des règles applicables aux infrastructures ne fonctionnant pas sur *blockchain*. Notamment, l'obligation de règlement en monnaie de banque centrale (prévue par l'article 40 de CSDR⁵⁷) est adaptée à l'absence actuelle de MNBC et les infrastructures de marché sur *blockchain* pourront utiliser des EMT ou de la monnaie commerciale « tokenisée » (art. 5.8 de PILOTE).

3/ Le cadre de surveillance

Le cadre européen de surveillance du secteur s'articulera entre un niveau national et un niveau européen :

- Au niveau national, les États membres auront l'obligation de désigner les autorités nationales compétentes pour exercer les fonctions d'agrément et de surveillance au titre du règlement. La liste des autorités nationales compétentes sera publiée sur le site de l'AEMF. Ces autorités disposeront de larges pouvoirs d'intervention et d'investigation. Elles auront également le pouvoir d'interdire ou de restreindre certaines activités liées aux crypto-actifs en cas de risque relatif à la protection des utilisateurs ou de risque de stabilité financière.
- Au niveau européen, l'AEMF et l'ABE assureront la coordination et joueront un rôle de facilitation pour que les mesures prises dans toute l'UE soient justifiées et proportionnées et que les autorités compétentes adoptent une approche cohérente. A ce titre, il leur appartiendra de publier un ensemble de textes techniques pour préciser le règlement MiCA.

L'analyse de la réglementation dans les autres juridictions au niveau international permet de réaliser que le cadre proposé par l'UE est relativement exhaustif et pionnier dans le contrôle du secteur des crypto-actifs.

⁵⁷ [Règlement \(UE\) 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres, et modifiant les directives 98/26/CE et 2014/65/UE ainsi que le règlement \(UE\) 236/2012](#)

B/ Recension de quelques exemples étrangers

Dans la plupart des pays, le secteur des crypto-actifs a mobilisé régulateurs et législateurs. Une large partie des économies mondiales appliquent ou sont en train d'élaborer une régulation vis-à-vis des crypto-actifs et des *stablecoins*. Cependant, les approches diffèrent entre pays.

Une partie des juridictions a décidé d'élargir les textes existants (sur la LCB-FT, les activités de paiement, les titres financiers...) aux activités portant sur les crypto-actifs. Ce type de réglementation présente l'avantage de pouvoir être mise en œuvre rapidement et d'imposer des cadres juridiques déjà éprouvés dans d'autres contextes. Toutefois, elle tient compte difficilement des spécificités et risques nouveaux qu'apporte le secteur des crypto-actifs.

D'autres pays, à l'image de ce qui est proposé en UE, envisagent la création de régimes d'autorisation *ad hoc*. C'est par exemple le cas de Singapour qui soumet les CASP à un agrément obligatoire auprès de la *Monetary Authority of Singapore* (MAS), et leur impose les principes LCB-FT du GAFI⁵⁸. Par ailleurs, la réglementation nationale sur les titres financiers s'applique désormais aux *security tokens*. Récemment, la MAS a proposé des mesures visant à réduire les risques pour les consommateurs liés aux crypto-actifs et à renforcer les normes *stablecoins*⁵⁹. L'approche de Singapour est considérée comme plutôt favorable à un développement encadré des crypto-actifs, alors que la MAS est très active dans le domaine des MNBC⁶⁰.

D'autres pays ont une approche plus restrictive. Par exemple, la Chine a interdit en 2017 toute émission et tout service d'échange de crypto-actifs. L'interdiction s'est étendue en 2021 aux activités de minage du bitcoin⁶¹. Il s'agit pour ce pays de proposer à la place des crypto-actifs privés une MNBC fermement contrôlée par la *People's Bank of China* (PBoC).

Aux États-Unis, la réglementation des crypto-actifs est encore confuse puisque les compétences sont divisées entre de nombreuses autorités fédérales (*Securities and Exchange Commission* - SEC, *Commodity Futures Trading Commission*...) et qu'en plus les régulations varient d'un État fédéral à l'autre. La SEC considère toutefois qu'une bonne partie des crypto-actifs échangés sur les plateformes américaines sont des valeurs mobilières. Les régulateurs se sont coordonnés au sein d'un *President's Working Group on Financial Markets*,

⁵⁸ [Payment Service Act, 2019](#)

⁵⁹ « *MAS proposes measures to reduce risks to consumers from cryptocurrency trading and enhance standards of stablecoin-related activities* », MAS, communiqué de presse, oct. 2022

⁶⁰ Voir par exemple : [Project Dunbar - International settlements using multi-CBDCs](#), Banque de règlements internationaux, mars 2022

⁶¹ « *China expands crackdown by declaring all crypto activities 'illegal'* », *Financial Times*, 24 sept. 2021

qui a publié en novembre 2021, ses recommandations sur la régulation des *stablecoins*⁶², la principale étant que les émetteurs doivent bénéficier de la garantie des dépôts (soit comme des établissements de crédit, soit comme des associations d'épargne). Par ailleurs, le sujet de la MNBC est abordé, certes de manière prudente et quelque peu tardive par rapport aux initiatives européennes. Un *executive order* de mars 2022⁶³, sur le développement responsable des actifs numériques et la MNBC a acté le début des travaux communs aux régulateurs américains. En septembre 2022, les différents rapports ont permis au gouvernement des États-Unis de définir un *Comprehensive Framework for Responsible Development of Digital Assets*, qui ouvre la voie à de nouvelles actions au niveau fédéral⁶⁴.

C/ Les travaux dans les différents forums internationaux

Les enceintes internationales sont très actives sur le sujet des crypto-actifs, sous l'impulsion du G20 et conformément à leurs différents mandats. Le *Financial Stability Board* (FSB)⁶⁵ a par exemple émis des recommandations sur l'encadrement réglementaire des *global stablecoins*⁶⁶, puis sur les autres formes de crypto-actifs⁶⁷. L'organisation de coopération et de développement économiques (OCDE)⁶⁸ s'est penché sur les aspect fiscaux internationaux via un cadre fiscal sur la déclaration des crypto-actifs et les échanges d'informations⁶⁹. Le *Committee on Payments and Market Infrastructures* et l'*International Organization of Securities Commissions* (CPMI-IOSCO)⁷⁰ ont abordé la question de l'applicabilité des *Principles for Financial Market Infrastructures* (PFMI)⁷¹ aux *stablecoins* systémiques.

⁶² [Interagency report on stablecoins, nov. 2021](#) : « To address risks to stablecoin users and guard against stablecoin runs, legislation should require stablecoin issuers to be insured depository institutions, which are subject to appropriate supervision and regulation, at the depository institution and the holding company level. »

⁶³ [Executive Order on Ensuring Responsible Development of Digital Assets, mars 2022](#)

⁶⁴ « [White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets](#) », communiqué de presse, sept. 2022

⁶⁵ Le FSB, créé lors de la réunion du G20 à Londres en 2009, regroupe 26 autorités financières nationales (banques centrales, ministères des finances, etc.) ainsi que plusieurs organisations internationales et élabore des normes dans le domaine de la stabilité financière.

⁶⁶ « [Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements](#) », rapport et recommandations, FSB, oct. 2020. Les *global stablecoins* (GSC) sont les *stablecoins* largement adoptés, dont la portée et l'utilisation pourraient s'étendre à de multiples juridictions, qui pourraient acquérir une importance systémique dans et entre une ou plusieurs juridictions, y compris comme moyen d'effectuer des paiements. Le FSB propose donc 10 recommandations pour favoriser une réglementation, une supervision et une surveillance coordonnées et efficaces des GSC afin de faire face aux risques pour la stabilité financière posés.

⁶⁷ « [Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets](#) », rapport consultatif, FSB, oct. 2022

⁶⁸ L'OCDE est une organisation internationale d'études économiques qui joue un rôle d'assemblée consultative.

⁶⁹ « [Cadre de déclaration des Crypto-actifs et modifications de la Norme commune de déclaration](#) », OCDE, oct. 2022 : Ce cadre propose une déclaration d'informations fiscales sur les transactions via crypto-actifs de manière standardisée, en vue d'échanger automatiquement ces informations avec les juridictions de résidence des contribuables.

⁷⁰ L'organisation internationale des commissions de valeurs (IOSCO) est l'organisme international qui rassemble les régulateurs de valeurs mobilières du monde entier et qui est reconnu comme l'organisme de normalisation mondial du secteur des valeurs mobilières. Le comité sur les infrastructures de paiement et de marché (CPMI) est son équivalent dans le domaine des infrastructures de marché. Il sert également de forum pour la coopération des banques centrales dans les domaines de la surveillance.

⁷¹ Les principes pour les infrastructures des marchés financiers (PFMI) sont les normes internationales applicables aux infrastructures des marchés financiers. Ils font partie d'un ensemble de 12 normes clés que la communauté internationale considère comme essentielles pour renforcer et préserver la stabilité financière.

En particulier, dès octobre 2018, le GAFI avait mis à jour ses recommandations concernant l'application des exigences LCB-FT aux actifs numériques. Ces recommandations ont été révisées en octobre 2021, englobant désormais les NFT et la DeFi. De plus, le GAFI vient de publier un rapport sur l'état de la mise en œuvre par les juridictions nationales de ses recommandations sur les crypto-actifs⁷². Il rappelle aux États l'importance de transposer la recommandation 15 du GAFI, visant à appliquer les obligations de LCB-FT aux CASP, ainsi que la recommandation 16, visant à leur appliquer la *travel rule*.

La déclaration du G20 de Bali de novembre 2022⁷³ a pris acte de ces évolutions internationales récentes en accueillant favorablement les travaux en cours du FSB et des organismes internationaux de normalisation pour faire en sorte que l'écosystème des crypto-actifs, y compris les *stablecoins*, soit étroitement surveillé et soumis à une réglementation, une supervision et un contrôle solides afin d'atténuer les risques potentiels pour la stabilité financière.

II. Aller plus loin dans la réglementation des crypto-actifs et adapter les institutions

L'UE propose le régime le plus étendu d'encadrement des crypto-actifs. Pour autant, dire "étendu" ne veut pas dire "strict". La mise en œuvre opérationnelle de ce cadre devra être efficace et adaptée aux caractéristiques des acteurs du secteur : souvent de plus petites entreprises que la moyenne du secteur, dont le fonctionnement interne est parfois moins encadré (comme l'a malheureusement illustré l'exemple FTX). Il s'agira aussi d'éviter que le règlement MiCA soit interprété comme une approbation par les institutions de l'UE des activités de ce secteur, encourageant les consommateurs à se tourner vers des crypto-actifs risqués ou développant l'usage de *stablecoins* à de fins de paiement⁷⁴.

Il est donc nécessaire d'aller plus loin dans le champ des activités régulées par les lois européennes et en même temps d'imposer des contraintes et des garde-fous plus stricts à des acteurs dont tout semble indiquer que la gouvernance et les contrôles internes sont très faibles. En complément, des initiatives doivent être entreprises au niveau européen et international pour que les autorités publiques fournissent elles-mêmes les services prétendument offerts par le secteur des crypto-actifs.

⁷² « [Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers](#) », GAFI, juin 2022

⁷³ [G20 Bali Leaders' Declaration, 16 nov. 2022](#)

⁷⁴ Voir une réflexion similaire pour les États-Unis : ["Beware the proposed US crypto regulation - it may be a Trojan horse"](#), H. Allen, *Financial Times*, 17 nov. 2022

A/ Aller plus loin dans la réglementation européenne

Il est délicat de déterminer dans quelle mesure le règlement MiCA est insuffisant puisqu'il n'est même pas encore entré en vigueur. Les régulateurs européen et nationaux pourront émettre des recommandations au fur et à mesure de l'application de ces textes. Certains éléments apparaissent toutefois dès aujourd'hui, qu'il s'agisse des vides juridiques ou des insuffisances réglementaires.

Une première faille dans la réglementation actuelle, assumée par le législateur européen, est l'absence d'encadrement de la finance décentralisée

(*decentralised finance* ou DeFi) qui désigne un pan de l'innovation financière développé sur *blockchain*. La DeFi propose un ensemble de services financiers spécifiques aux crypto-actifs et répliquant en grande partie des services existants dans la finance régulée (épargne, prêts, échanges, produits dérivés et assurances). S'appuyant sur une multiplicité d'acteurs, la DeFi est plus complexe à réguler que la finance traditionnelle structurée autour d'un écosystème bancaire. De fait, les éléments de régulation traditionnels (ratios de fonds propres, règles de gouvernance, obligations de contrôle) sont adaptés pour des acteurs bien identifiés, qui traitent des catégories limitées d'opérations, de façon centralisée, et qui ont atteint une certaine masse critique, tout l'inverse de ce qui caractérise la DeFi où une multiplicité d'acteurs parfois de petite taille proposent des services extrêmement variés sur une base décentralisée. Cette activité est donc un angle mort de la réglementation actuelle. MiCA ne s'appliquera qu'aux activités centralisées et n'intègre pas de règles sur les activités d'emprunt ou de prêt de crypto-actifs. Dans les 18 mois suivant l'entrée en vigueur du texte, la Commission sera chargée de la publication d'un rapport sur la nécessité et la faisabilité d'encadrer ces activités. Cette temporalité est largement insuffisante et repousse toute proposition législative européenne à des années, laissant la main au législateurs nationaux et faisant peser le risque d'arbitrage réglementaire en Europe.

Le risque est d'autant plus prégnant qu'une large partie de l'attrait de la DeFi est tirée de son caractère non régulé. Certains acteurs proposent des activités de prêt en crypto-actifs. Outre leur nature fondamentalement instable, cela reviendrait à conférer à ces acteurs un certain pouvoir de "création monétaire" si les crypto-actifs venaient à être plus largement acceptés comme moyen de paiement. La vigilance du régulateur est indispensable, et l'on peut se féliciter que le projet Libra ait été mis en échec par l'action conjointe des pouvoirs publics. Cependant, le rythme de l'innovation et d'adoption de ces instruments, amplifiés par les effets de réseau, implique une réglementation stricte et surtout réactive (voir supra).

PROPOSITION n°2 : Accélérer l'analyse des spécificités et risques de la finance décentralisée en vue d'un encadrement approfondi des pratiques au niveau international.

Ce manque de cadre réglementaire est aussi constaté du côté des NFT. Ces objets virtuels qui ont été popularisés pour la commercialisation d'images exposent les utilisateurs à des risques de multiples fraudes. Il faut savoir que les images associées aux NFT ne sont pratiquement jamais directement stockées sur la *blockchain*. Le *smart contract* constituant le NFT renferme en fait une référence, une adresse à laquelle trouver l'œuvre. En effet, la plupart des *blockchains* publiques proposant un coût en fonction de la taille d'une transaction, héberger un fichier de type image, musique ou vidéo représente souvent un coût prohibitif. La plupart des *blockchains* ont également des limites techniques imposant une taille maximale aux données déposées, rendant ainsi très compliqué le dépôt de fichiers volumineux. Cela a provoqué la stupeur chez certains utilisateurs lorsque l'image qu'ils pensaient avoir achetée a soudainement disparu⁷⁵. Ils disposent toujours bien du NFT, mais l'image a été supprimée de l'adresse à laquelle était stockée.

Dans leur pratique actuelle, c'est-à-dire utilisés comme des certificats, les NFT comportent les mêmes risques que leurs homologues hors *blockchain*. On a beau être en possession d'un certificat, si l'émetteur n'a aucune autorité pour le créer, celui-ci n'a aucune valeur. Il n'est pas rare de voir plusieurs NFT associés à un même objet, parfois émis par un même acteur. Cela est parfois souhaité, tel que dans le cas d'un ticket pour un concert, ou d'une licence d'utilisation donnant accès à un logiciel. Dans le cas des œuvres numériques, lorsqu'aucune licence n'est attribuée, un NFT est assimilable à un papier signé par son émetteur, indiquant une adresse où se trouve une image, et spécifiant qui est le propriétaire de ce papier. Or les plateformes commercialisant ces objets numériques se trouvent être très laxistes sur ce sujet, ne procédant à aucune vérification des droits dont dispose le vendeur.

Dans la plupart des cas, très peu de choses garantissent que l'émetteur d'un NFT ne détienne le moindre droit sur un actif numérique. En 2021, le site web DeviantArt, hébergeant une communauté d'artistes et leur permettant d'y exposer leur portfolio, a connu une vague de NFT utilisant les œuvres qui y sont publiées. Un cas emblématique illustre la frustration de certains artistes : l'artiste Liam Sharp, connu pour avoir collaboré avec le géant DC Comics, a annoncé en décembre 2021 qu'il fermait son compte DeviantArt à cause de la réutilisation répétée de ses œuvres sans son autorisation pour vendre des NFT sur le site OpenSea. DeviantArt est allé jusqu'à publier un scanner avertissant les artistes lorsqu'une copie potentiellement illicite a été détectée mais la faible coopération de la place de marché dédiée

⁷⁵ ["People's Expensive NFTs Keep Vanishing. This Is Why", Vice, 29 mars 2021](#)

aux NFT a tout de même eu raison de la patience de l'artiste. Si cet épisode est loin d'avoir été la première infraction aux droits d'auteur, il était spectaculaire par l'ampleur de la fraude. Sur ces aspects de protection du droit d'auteur, aucune disposition particulière aux NFT n'est prévue dans le droit européen. Le règlement MiCA, qui a pour objet d'encadrer les activités portant sur les crypto-actifs, exclut de son champ d'application les NFT et renvoie toute réglementation à un rapport d'analyse que devra présenter la Commission européenne dans plusieurs mois (voir partie II.A). Le droit applicable aux NFT est donc le droit correspondant à leurs différents usages (ex. droit de la propriété intellectuelle et artistique pour les œuvres d'art), sans tenir compte de leur spécificité.

Ce qui pose un problème majeur dans les cas cités en exemple, et plus généralement avec les NFT, c'est l'absence d'autorité fiable. Les NFT étant des certificats, il est nécessaire de recourir à une autorité émettrice. L'intérêt d'un NFT par rapport à un certificat numérique traditionnel n'est donc pas évident du tout. Les conditions auxquelles celui-ci s'échange étant déterminées par l'émetteur, un registre centralisé permet d'en faire tout autant. Ce que permettent les NFT est principalement de déléguer à des tiers la gestion de la base de données des certificats émis. La principale utilité réside dans le fait d'être valide et échangeable même après la disparition de son émetteur.

Un autre risque intrinsèque aux solutions informatiques est lié aux bugs et aux piratages. Certains utilisateurs ont pu faire l'amère expérience de voir leur portefeuille dépouillé de leurs actifs. Si « le code est la loi », comme le dit l'adage des premiers adeptes des crypto-actifs, il faudrait alors reconnaître les pirates comme des propriétaires légitimes des actifs volés. Imaginons maintenant que ces actifs fassent référence à un actif bien réel, tel qu'une maison ; un propriétaire pourrait par un simple acte de piratage perdre son habitation. En l'état, appliquer les DLT aux actifs réels semble prématuré tant que de tels cas ne seront pas adressés.

Enfin, il existe un autre risque technique présent sur la majorité des *blockchains*, celui du *fork*. Il s'agit du cas où deux versions parallèles de la *blockchain* coexistent de façon persistante. Comme indiqué en introduction, le consensus décide de la version qui fait foi selon un principe simple : on reconnaît la chaîne la plus longue qui respecte les règles. La quasi-totalité des *blockchains* ne contiennent aucun mécanisme permettant de s'accorder sur les règles à appliquer. Dans le cas d'un changement de règle validé par certains et non par d'autres, il peut alors y avoir une séparation de la chaîne de transactions : une maintenue par le consensus suivant les règles historiques, une autre maintenue par celui suivant les nouvelles règles. On se retrouve donc avec deux versions parallèles. Ceci s'est déjà produit à de multiples reprises sur Bitcoin, mais également sur Ethereum. Le dernier événement de ce type connu est survenu le 15 septembre 2022 lors du passage de Ethereum au protocole de consensus *Proof of Stake*. Une partie des mineurs, voyant leur modèle économique bousculé,

persistent à maintenir la version *Proof of Work* de la *blockchain*. Cela duplique de fait tous les actifs qui se trouvaient sur le protocole. Qui décide alors laquelle fait foi ? Si l'émetteur d'un NFT reconnaît une version mais pas l'autre, a-t-il malgré tout le droit de profiter des revenus perçus de la version répudiée ?

Par ailleurs, se pose, comme dans tout texte européen, la question de l'application du cadre UE à des entités extra-européennes. En effet, les créanciers européens d'entreprises non-européennes sont souvent en grande difficulté pour faire valoir leurs droits. Il n'existe pas de droit de la faillite internationale. Dans le cas, par exemple, des sociétés Voyager et Celsius qui ont demandé l'ouverture d'une procédure de redressement aux Etats-Unis en 2022⁷⁶, la question s'est posée des droits des clients qui sont soumis à la loi américaine (moins précise que la réglementation européenne). La société Voyager, tout en ayant une filiale agréée comme PSAN en France, était destinée uniquement aux citoyens américains. Pendant la procédure, les clients européens n'ont plus eu accès à leurs crypto-actifs déposés sur chaque plateforme et ils risquent de perdre une partie, sinon tous leurs actifs⁷⁷. Ces aspects internationaux trouvent, comme souvent, un pendant particulièrement important dans leurs aspects fiscaux.

Le récent cas de la plateforme FTX ajoute une complexité supplémentaire puisque la société possède un réseau multi-juridictionnel de filiales avec des prêts internes à des entités aux Bahamas, aux îles Caïmans, à Antigua et Barbuda, ainsi qu'aux États-Unis, au Japon, en Allemagne et en Suisse. En Europe, FTX a obtenu une licence pour opérer en tant qu'entreprise d'investissement chypriote en septembre après avoir acquis un rival chypriote, K-DNA Financial Services, qui lui permettait d'opérer dans toute l'UE, mais le régulateur local a suspendu cette autorisation.

S'ajoute à cela le fait que, les crypto-actifs n'étant pas des instruments financiers, la défaillance d'un intermédiaire ne permet pas de bénéficier d'un mécanisme de garantie, comme pour les dépôts bancaires et les titres financiers. Par exemple, en UE, la garantie des titres indemnise les investisseurs en cas de défaillance de leur prestataire de services d'investissement jusqu'à 70 000 euros par client et par établissement⁷⁸. D'ailleurs, parmi les obligations qui incombent à l'émetteur d'un crypto-actif dans le cadre de MiCA, il y a l'obligation pour celui-ci d'avertir les utilisateurs que le crypto-actif émis n'est pas couvert par les mesures de compensation destinées aux investisseurs en application de la réglementation européenne existante en matière de garantie des dépôts.

Il est nécessaire que le législateur se saisisse de cette question de la garantie des dépôts. S'il est évident qu'imposer une telle protection serait dans l'intérêt des investisseurs, cela

⁷⁶ Ces procédures dites "Chapter 11" permettent une reprise d'activité après un accord avec les créanciers des entreprises.

⁷⁷ ["Les détenteurs de crypto-monnaies sont-ils des créanciers chirographaires des plateformes d'échange ?", C. Boismain, Dalloz, 2022](#)

⁷⁸ ["Faillite de FTX : comment récupérer vos cryptos ?", Les Echos, 18 nov. 2022](#)

permettrait aussi un développement du marché des crypto-actifs dont l'opportunité n'est pas positivement démontrée (comme l'explique le présent document). Dans tous les cas, il faudra s'assurer que, si mécanisme de garantie il y a, ce mécanisme devra s'appuyer sur des fonds provenant du secteur lui-même et en aucun cas sur des fonds publics, à l'instar de ce qui a été mis en place - bien qu'avec un succès relatif - avec le Fonds de Résolution Unique (FRU) pour le système bancaire traditionnel.

Dans la mesure où les établissements proposant des crypto-actifs ne sont pas agréés en tant qu'établissements de crédit (au sens de la réglementation bancaire européenne), cela signifie que les avoirs détenus en crypto-actifs ne font l'objet d'aucune garantie légale (voir ci-dessus), contrairement aux déposants dans un établissement de crédit⁷⁹. D'autres garanties, telles que celles de fournir un remboursement en cas d'usage frauduleux ou d'usurpation d'identité, ne s'appliquent pas non plus.

PROPOSITION n°3 : Analyser la pertinence d'un système de garantie interne au secteur qui permettrait d'assurer une plus grande stabilité financière et une responsabilisation des acteurs par leurs pairs.

PROPOSITION n°4 : Accroître la coordination internationale et l'échange d'informations entre Etats pour éviter toute pratique de *forum shopping*. Mettre en place au niveau international une typologie unique ou *a minima* des orientations de régulation commune.

Le cadre réglementaire n'est pas particulièrement contraignant pour les émetteurs de crypto-actifs "classiques" et pour les CASP. Un exemple, le *white paper* qui doit être publié par les émetteurs de crypto-actifs pour assurer l'information des investisseurs n'aura pas à être validé au préalable par le régulateur. Certes, les règles sont renforcées pour les émetteurs d'EMT ou d'ART, *a fortiori* pour les EMT et ART significatifs. Il en va de même pour les CASP considérés comme significatifs.

Néanmoins l'esprit de la réglementation européenne sur les crypto-actifs est de les analyser sous un angle "marchés financiers", c'est-à-dire en veillant à apporter une information claire et précise à l'investisseur, tout en le laissant prendre les risques qu'il souhaite. Cette réglementation est déjà discutée dans les marchés financiers traditionnels. Dans le cadre du

⁷⁹ En effet, selon les articles L. 312-4 et suivant du code monétaire et financier, les établissements de crédit français sont dans l'obligation d'adhérer au fonds de garantie des dépôts et de résolution (FGDR). Ce fonds a notamment pour mission de gérer et de mettre en œuvre le mécanisme de garantie des dépôts. Ce sont les adhérents au FGDR qui lui procurent les ressources financières nécessaires à l'accomplissement de ses missions. Le mécanisme de garantie des dépôts est mis en œuvre sur demande de l'ACPR dès que celle-ci constate qu'un établissement de crédit n'est plus en mesure de restituer, immédiatement ou à terme rapproché, des fonds à un déposant. Le plafond d'indemnisation par déposant est de 100 000 euros.

marché des crypto-actifs, où les investisseurs sont généralement plus jeunes et plus sensibles aux fluctuations des marchés que les investisseurs traditionnels⁸⁰, cette position est d'autant plus discutable.

PROPOSITION n°5 : Soumettre les acteurs de l'écosystème des crypto-actifs à des règles de capitalisation et de garantie adaptées aux risques, et pas seulement les acteurs fournissant des services en lien avec des *stablecoins*.

Une réglementation conservatrice est d'autant moins adaptée que l'interconnexion entre DeFi et finance traditionnelle est croissante, bien que limitée à l'heure actuelle. Or, associé à des lacunes dans la réglementation, cette interconnexion fait craindre la propagation de faillites d'acteurs de la DeFi aux acteurs traditionnels. Cet effet de contagion pose ainsi la question du futur risque systémique que pourraient représenter les crypto-actifs si des acteurs parviennent à contourner la législation.

B/ Les risques pour le système financier traditionnel provoqués par les crypto-actifs

L'interpénétration croissante entre l'éco-système des crypto-actifs et les marchés financiers traditionnels, qui y voient un nouveau terrain de spéculation, peut laisser craindre un risque de contagion d'une crise affectant le premier secteur vers le second. Pour mieux appréhender ce risque, il convient de revenir sur les « promesses » de la finance décentralisée avant de montrer leurs limites et surtout les risques croissants qu'elle peut faire peser sur la stabilité financière.

1/ Les promesses de la finance décentralisée

Avec l'arrivée d'Ethereum et de ses *smart contracts*, il est devenu possible et aisé de créer de nombreux petits programmes informatiques appelés « dApps » (pour *decentralized applications*) dont l'exécution est assurée par les validateurs de son réseau. Les algorithmes des bourses de crypto-actifs peuvent ainsi à leur tour bénéficier d'une décentralisation et ainsi échapper à la censure. La finance a été d'ailleurs parmi les premières applications de cette nouvelle *blockchain* et est toujours actuellement cité comme principal cas d'usage sur le site

⁸⁰ ["Crypto trading and Bitcoin prices: evidence from a new database of retail adoption", BIS Working Papers, 14 nov. 2022](#) : "40% of users are men under 35, commonly identified as the most "risk-seeking" segment of the population. These users are more sensitive to changes in the price of Bitcoin than female users and older men."

ethereum.org. Au début, des services simples tels que des prêts sur gage ont été développés. Le principe est simple, il est possible de déposer un crypto-actif en garantie pour pouvoir emprunter une somme d'un autre crypto-actif. Si le remboursement n'est pas effectué, le dépôt de garantie est liquidé. C'est-à-dire qu'il est automatiquement vendu *via* un système d'enchères pour couvrir les pertes liées au non-remboursement du prêt. Ce système de prêt sur gage est par exemple au cœur d'un crypto-actif appelé Dai, opéré par une DAO (*Decentralized Autonomous Organization*) sur la *blockchain* Ethereum.

Les *smart contracts* étant des programmes informatiques, il est possible de programmer à peu près n'importe quel type de produit financier avec pour seule limite le fait d'être cantonné aux crypto-actifs. En effet, dès lors qu'on entre dans la sphère du réel, il faudra forcément passer par une autorité de confiance comme le démontrent les exemples des trois émetteurs de *stablecoins centralisés* cités dans ce paragraphe. Il y a donc tout un écosystème de produits financiers qui s'est développé. Pour rester sur l'exemple du Dai, le protocole Maker qui spécifie les règles de son émission émet lui aussi son propre jeton, le MKR. Le pouvoir de vote pour déterminer les évolutions des règles est proportionnel à la quantité de MKR détenue. Il s'agit là d'un autre type d'actif financier, ayant lui-même besoin d'un écosystème financier plus vaste encore dans lequel s'inscrire.

En effet, les validateurs des *blockchains* anonymes, qu'elles fonctionnent avec un consensus de type *Proof of Work* ou *Proof of Stake*, sont rémunérés en jetons internes au protocole. Les frais de fonctionnement (matériel, hébergement, maintenance, etc.) étant libellés en des devises locales, les validateurs doivent pouvoir vendre ces crypto-actifs contre de la monnaie. Des marchés financiers dédiés aux crypto-actifs ont donc émergé dès le début de Bitcoin. Ces bourses étaient en revanche opérées de façon centralisée, chacune d'entre elles étant contrôlée par une entreprise. Il s'agissait d'un véritable talon d'Achille pour un système censé être résistant à la censure grâce à sa décentralisation.

L'une des promesses de la finance décentralisée est donc de permettre aux *blockchains* anonymes d'exister telles qu'elles ont été pensées, c'est-à-dire en dehors de tout cadre juridique et ne se soumettant qu'aux règles qu'elles se fixent elles-mêmes. Cela peut sembler récursif, mais sans la garantie de pouvoir vendre ses crypto-actifs, les incitations économiques protégeant l'intégrité de ces *blockchains* ne tiennent plus. Le caractère le plus important de cette promesse est sa volonté de se soustraire à toutes règles autres que celles programmées informatiquement. Une fois un *smart contract* déployé sur une *blockchain*, rien n'est censé pouvoir l'arrêter.

Il s'agit là de la deuxième promesse de la DeFi, qui est héritée de celle des *blockchains* publiques, pseudonymes et anonymes : la résistance à la censure. Quand bien même les législateurs chercheraient à interdire les transactions impliquant certains produits financiers, les opérateurs de *blockchains* étant dispersés à travers plusieurs juridictions et cachés

derrière un pseudonyme, il devrait toujours être possible de trouver un acteur pour valider cette transaction.

L'autre promesse découlant du pseudonymat ou anonymat de ces *blockchains* est de rendre la finance accessible à tout le monde, sans filtre, contrairement aux bourses traditionnelles qui nécessitent un contrôle d'identité ou le passage par un intermédiaire (une banque, opérateur de marché ou autre organisme financier) pour émettre des ordres et effectuer ses transactions. L'ensemble de ces intermédiaires serait ainsi remplacé par des programmes informatiques qui mettraient en relation les différentes parties (prêteurs et emprunteurs, acheteurs et vendeurs, etc.) directement entre elles, de pair à pair.

2/ Des promesses à la réalité

Si Ethereum a été le premier protocole à proposer des applications de finance décentralisée, d'autres protocoles ont tenté d'émerger. Ceux-ci restent néanmoins assez anecdotiques. Ethereum supporte près de 60 % de la DeFi en termes de capitalisation. La BNB Smart Chain, deuxième plus grosse *blockchain* de la DeFi, contrôlée par Binance, arrive loin derrière avec une capitalisation des actifs qui s'y échangent autour environ cinq fois moindre. La nature même des marchés financiers pousse à une certaine centralisation. En effet, la liquidité est un paramètre primordial dans la finance. Trop faible, elle expose un actif à une forte volatilité et expose donc à des manipulations de marché par un ou plusieurs gros acteurs.

Ethereum n'est cependant pas un protocole de DeFi à proprement parler. Il est un socle sur lequel se construisent des dApps. L'une de ces dApps est UniSwap, la principale place de marché de la DeFi. Les volumes échangés (convertis en USD) sur cette bourse décentralisée sont près de huit fois supérieurs à ceux de ses plus proches concurrents (fin octobre 2022). C'est pour cette liquidité que UniSwap trône la première place du podium. Comme on peut le deviner, ce paramètre fait qu'il y a un fort effet de réseau sur les plateformes de finance. On le constate dans la finance traditionnelle, et la DeFi ne fait pas exception. Il faut cependant relativiser cet avantage compétitif avec le volume total des échanges sur les marchés de crypto-actifs. Alors que Binance, le leader des bourses de crypto-actifs, cumulait des volumes d'échanges supérieurs à 1470 milliards de dollars américains sur le mois d'octobre 2022, UniSwap dépassait péniblement les 25 milliards de dollars. Il faut dire que les bourses centralisées ont un avantage compétitif de taille : la rapidité. Un ordre peut y être exécuté en quelques millisecondes alors que la structure de la *blockchain* décentralisée impose d'attendre un certain temps entre deux enregistrements. Trop cher pour les petites transactions comparé à ses homologues centralisés, trop lente et avec une liquidité trop faible pour les plus grosses, la DeFi semble être restreinte à un usage de niche. Son principal avantage étant probablement le flou juridique qui l'entoure et qui devrait perdurer dans l'Union

européenne encore plusieurs mois puisque le cadre réglementaire actuel n'aborde pas cette question.

En termes de protocoles, il y a donc déjà une forte centralisation, mais ces protocoles sont également très peu décentralisés eux-mêmes. Ethereum est par exemple contrôlé par un très faible nombre d'acteurs. Le droit de validation et donc le pouvoir de vote étant proportionnel à la somme d'ethers (le jeton émis par le protocole) mis en gage, 5 entités en cumulent plus de la moitié. Pour la BNB Smart Chain, la centralisation est bien pire ; seuls les 21 validateurs avec le plus de jetons engagés sont autorisés à participer au consensus. A noter qu'il est question de 21 validateurs, mais rien n'empêche une même société à contrôler plusieurs d'entre eux. Il y a de forts soupçons sur le fait que Binance agisse de la sorte et en contrôle une majorité. L'objectif est probablement plutôt pour Binance de pouvoir naviguer entre plusieurs juridictions. L'entreprise est d'ailleurs connue pour cela, elle n'a pas clairement de siège social établi pour son activité d'opérateur de marché. Il existe bien des entités dans plusieurs pays, dont à Malte et en France⁸¹, mais celle qui opère sa place de marché centralisée n'est pas communiquée⁸².

Autre exemple avec MakerDAO, construit sur la *blockchain* Ethereum qui est déjà très centralisée ; la gouvernance du protocole de prêt sur gage émettant le *pseudo-stablecoin* Dai est également concentrée entre une poignée d'acteurs. La structure conditionne la soumission de propositions d'évolution à un minimum de jetons MKR. Une fois soumis, leurs détenteurs peuvent voter en proportion de leurs jetons engagés. Sur l'ensemble des adresses ayant participé à au moins un vote, une seule concentre plus de 20% des voix. Les 20 adresses ayant voté au moins une fois concentrent la plus grande part de votes concentrent plus de 94% des voix (début novembre 2022) sur l'ensemble des participants.

L'observation des différents scrutins laisse constater un très faible nombre de votants, la participation médiane étant autour de 23 votants et la moyenne autour de 24,6. Lorsqu'on étudie le détail de chaque scrutin, la concentration du pouvoir est encore plus marquée. Etant donné que tous les votants ne participent pas à l'ensemble des scrutins, le votant possédant le plus grand pouvoir concentre en moyenne plus de 52% des voix, la médiane se situant à plus de 48%. Le scrutin ayant connu la plus faible concentration des voix a tout de même vu plus de 20% des voix détenues par une seule adresse et celui ayant la plus forte en a vu près de 98,5% des voix détenues par le votant le plus puissant⁸³.

⁸¹ En France, BINANCE France SAS dispose du [statut de PSAN](#) depuis le 4 mai 2022 et peut offrir des services relatifs à la conservation d'actifs numériques, à l'achat / vente d'actifs numériques contre monnaie ayant cours légal, à l'échange d'actifs numériques contre d'autres actifs numériques. L'entreprise peut enfin exploiter sa plateforme de négociation d'actifs numériques.

⁸² ["Where Is Bitcoin Giant Binance Headquartered? Answer Coming 'In Due Time'", Decrypt, 19 juin 2022](#)

⁸³ [Sun, Xiaotong and Stasinakis, Charalampos, "Decentralization illusion in DeFi: Evidence from MakerDAO", 25 Novembre 2021](#)

L'exercice pourrait être refait sur de nombreux protocoles, il est probable de retrouver des résultats similaires. Certaines plateformes de DeFi ont même connu des épisodes de centralisation éclair. C'était notamment le cas pour le protocole Curve dont cet épisode a été baptisé « Curve Wars », en référence à la bataille pour prendre le contrôle du protocole. Actuellement, la majorité absolue du protocole est détenue par Convex Finance. L'intérêt principal de la DeFi étant le rendement des placements, beaucoup de détenteurs de jetons abandonnent facilement leur droit de vote pour maximiser leurs revenus. La DeFi institutionnalise la corruption comme mode de fonctionnement. Le cynisme du protocole Curve est allé jusqu'à créer des incitations économiques appelées « bribes », se traduisant littéralement « pot-de-vin » en Français.

Fort de ce constat, il apparaît donc que l'idée de désintermédiation des échanges annoncée par les promoteurs des technologies *blockchain* demeure un mythe. Il est plus cohérent avec la réalité de considérer les opérateurs de ces protocoles comme des intermédiaires. Cela permet de résoudre une question faussement complexe : « à qui appliquer la loi dans un contexte de protocole réputé décentralisé ? »

3/ Les risques de la DeFi

Forte latence et faible liquidité, ces deux limites de la DeFi l'exposent déjà à des manipulations de marché, mais d'autres limites peuvent être pointées. Avant exécution d'un ordre, ce dernier est diffusé aux réseaux. Sous couvert d'anonymat, il est ainsi facile pour un membre du réseau de DeFi de doubler un *trader* en émettant un ordre qui serait exécuté en priorité. Dans la finance traditionnelle, des règles interdisent ce type de comportement qualifié de délit d'initié, mais la finance décentralisée baignant dans un flou juridique ne s'applique que les règles qu'elle-même se définit. Aux États-Unis, la SEC (voir supra) a beau avoir essayé de proclamer qu'Ethereum dépend de sa juridiction pour la raison que la majorité des opérations se déroulent sur son sol, les implications de telles déclarations restent très obscures. Dans les faits, il n'existe aucun cadre juridique entourant la DeFi et MiCA n'y répond pas pour l'instant. La complexité technique du fonctionnement de ces protocoles rend difficile l'appréhension par les régulateurs des responsabilités de chaque acteur du système. L'UE s'est donc pour l'instant concentrée sur un volet plus aisé à mettre en œuvre : la réglementation des activités délivrées par des personnes morales ou physiques, ayant donc une existence légale. Cette décision est avant tout pragmatique ; il est difficile de condamner une technologie, un concept ou une idée. Ce sont donc aux personnes qui en font l'usage que l'on peut faire appliquer la loi.

Cela est d'autant plus pertinent que les risques que les crypto-actifs peuvent représenter pour l'économie réelle passent nécessairement par des acteurs centralisés. Si la place de marché

de Binance n'opère officiellement que des crypto-actifs et que les opérations en dollars y sont faites en *stablecoins*, il y a bien un intermédiaire qui encaisse de vrais dollars. De la même façon que l'OFAC (office du Trésor étasunien) interdit toute transaction utilisant des actifs américains avec certaines entités, il est possible d'en faire de même avec des entités manipulant ces crypto-actifs. C'est d'ailleurs ce que fait le département du Trésor en maintenant une liste noire d'adresses de divers crypto-actifs avec lesquelles il est interdit d'échanger.

Les consignes de l'OFAC s'avèrent malgré tout insuffisantes puisqu'on constate tous les jours de nouvelles transactions interdites sur la *blockchain* Ethereum. Ces dernières peuvent par exemple être procédées par des acteurs étrangers. Une solution pourrait être pour l'OFAC d'automatiser la maintenance de sa liste noire en ajoutant automatiquement toute adresse d'opérateur ayant validé une transaction interdite. Ceci entraverait davantage l'accès au dollar aux acteurs ne se conformant pas au droit étasunien et serait d'autant plus dissuasif. Enfin, il serait également possible d'imposer aux validateurs de rejeter toute transaction illicite sur la *blockchain*. Tel qu'expliqué en introduction, tout nouveau bloc de transactions ajouté à la *blockchain* valide implicitement l'ensemble des transactions précédentes. Il serait ainsi possible de considérer légalement complice tout validateur ne rejetant pas un bloc contrevenant à la juridiction dont il dépend.

PROPOSITION n°6 : Imposer aux opérateurs de transaction, qu'ils soient opérateurs de nœud d'une *blockchain* ou CASP, de refuser les transactions manifestement illicites sur le territoire de l'UE sous peine de sanctions.

Ceci pourrait pousser à une bifurcation des protocoles (appelée « *fork* ») avec une version conforme et une autre non-conforme. Potentiellement, il pourrait y avoir de multiples bifurcations pour que chacune puisse se conformer à la réglementation locale s'imposant aux validateurs. Ce risque nécessiterait à tout acteur centralisé émettant des actifs réels « *tokenisés* », c'est-à-dire représentés sous forme d'un crypto-actif, à annoncer quelle version de *blockchain* il reconnaît. Cela s'est déjà produit en 2022, peu avant le passage d'Ethereum d'un consensus de type *Proof of Work* à un nouveau de type *Proof of Stake*. Les émetteurs de *stablecoins* tels que Tether, Circle ou Binance ont annoncé que seuls les actifs sur la nouvelle version seraient reconnus, malgré le fait qu'une version parallèle d'Ethereum avec des USDT, USDC et BUSD continue d'être maintenue par des mineurs dissidents. Ces crypto-actifs ainsi répudiés par leurs émetteurs perdent toute valeur.

4/ Le risque de contagion entre crypto-actifs et sphère financière traditionnelle, notamment par les « stablecoins »

Si la finance décentralisée permet en théorie de créer un marché dans lequel un crypto-actif pourrait s'échanger contre n'importe quel autre, et donc en somme créer un marché de troc mondial de crypto-actifs, les faits dépeignent une toute autre réalité. Comme nous l'avons vu, les jetons émis par un protocole ont peu d'utilité en dehors de ce dernier et les personnes qui maintiennent ces *blockchains* ont besoin d'interagir avec le monde réel. Pour cela, le moyen le plus facile reste encore de vendre une partie de ses crypto-actifs contre une monnaie largement acceptée. Ainsi, c'est le dollar qui est privilégié de par son statut de monnaie de référence pour les échanges internationaux.

Certains acteurs privés ont donc entamé la « *tokenisation* » d'actifs réels avec la monnaie du commerce mondial : le dollar américain. La société pionnière en la matière est Tether qui a lancé son jeton USDT en 2014. D'autres l'ont rejoint par la suite, dont Circle avec son USDC, Paxos avec son USDP ou encore Binance et son BUSD pour en nommer quelques-unes. Ces sociétés proposent d'échanger des USD contre une reconnaissance de dette *tokenisée*, c'est-à-dire inscrite sous forme de crypto-actif sur une *blockchain* et ainsi échangeable sur le réseau.

Ces sociétés sont donc des sociétés financières qui vont ensuite acheter des actifs afin de faire fructifier cet argent pour se rémunérer. 100 % des gains leur reviennent, mais c'est l'argent de leurs clients qui est engagé. Certaines d'entre elles se sont d'ailleurs adonnées à des activités bancaires au-delà de la légalité. L'État de New York a condamné la société Tether à l'interdiction de proposer ses services à ses citoyens. La société avait en effet menti sur la nature de ses réserves. Elle affirmait que chaque USDT était assuré par un USD alors que le montant de leur réserve d'USD était inférieur à la quantité d'USDT en circulation. En effet, non seulement rien ne garantit que la société dispose de fonds suffisants pour rembourser les USDT en circulation, mais la nature des actifs en réserve pose également question. En mai 2021, seuls 2,9 % étaient constitués de cash, et 49,6 % de titres créances privées sans collatéral. Il a notamment été question d'émettre un crédit au Salvador en USDT, remboursable en USD.

Cette *tokenisation* ne touche pas que les monnaies, mais également d'autres types d'actifs réels. La société Paxos propose, en plus de son USDP ou du BUSD (qu'il émet pour Binance), le PAXG dont chaque unité correspond à une once d'or. En Europe, on pourra citer également la Société Générale qui, via sa filiale Forge, émet un jeton OFH, un produit structuré d'obligations immobilières garanties par Crédit Logement. Ce jeton fait partie des actifs pouvant servir de collatéral pour soutenir le cours du DAI. En effet, la Société Générale n'est pas la seule à proposer des obligations *tokenisées*. L'OFH n'est d'ailleurs en pratique pas

utilisé par MakerDAO, ils font cependant appel à d'autres sociétés similaires comme Centrifuge, Huntington Valley Bank ou encore 6s Capital qui fournissent une valeur totale d'un peu plus de 400 millions de dollars américains en garanties.

C'est par ce biais de la finance traditionnelle que les crypto-actifs peuvent avoir des impacts sur l'économie réelle. En effet, lorsque les sociétés émettrices de jetons adossés à des actifs réels se voient réclamer un remboursement par leurs clients de l'argent déposé chez eux, cela peut amener à une vente rapide d'actifs tels que des créances. Cela peut entraîner une pression baissière sur les cours de ces obligations et être interprété par les investisseurs comme une augmentation du risque de défaut sur la dette des entreprises concernées. Les taux d'emprunt de ces dernières peuvent augmenter en conséquence, rendant plus difficiles leurs conditions de financement.

Les lacunes de la régulation actuelle et l'ensemble des risques évoqués ont motivé de nombreuses banques centrales à se lancer dans des projets de monnaie numériques de banques centrales (MNBC - voir *glossaire*), actifs monétaires sûrs dont elles assurent l'émission et qui offrent, à l'inverse des crypto-actifs, de fortes garanties.

C/ Encourager la réflexion autour de monnaies numériques de banque centrale (MNBC) réellement accessibles aux citoyens et aux entreprises

Si les crypto-actifs ont bien été un électrochoc à l'origine du développement de plusieurs dizaines de projets de MNBC, une grande partie de ceux-ci restent paradoxalement tournés vers les transactions domestiques et visent seulement à adapter à la marge le système financier actuel. Par peur de risques accrus pour les acteurs financiers, les pouvoirs publics restent timorés dans leur approche alors que des perspectives révolutionnaires pourraient être ouvertes en changeant de regard et d'approche sur l'intermédiation bancaire.

1/ Les MNBC à l'heure actuelle : des systèmes peu ambitieux servant uniquement aux transactions internes au marché monétaire

Plus de cent banques centrales à travers le monde sont déjà engagées sur des projets de MNBC. Les motivations sont variées et dépendent des contextes nationaux. Les pays en voie de développement peuvent y voir un moyen de remédier à la faible bancarisation de leur population, à l'instar du projet d'e-Naira au Nigéria, où l'essentiel des paiements s'effectuent à partir de portefeuilles numériques (*e-wallets*). Cette faible bancarisation structurelle est par ailleurs accentuée par un refus des banques traditionnelles d'investir dans des couloirs de paiements qu'elles ne considèrent pas rentables et dont la conformité aux règles LCB-FT est parfois difficile à assurer (stratégies dites de *derisking*). C'est pourquoi les fintechs prennent une place croissante dans certains pays en développement. Or, les modalités de paiement

qu'elles proposent sont parfois peu sécurisées. Si elles sont soumises, comme les acteurs traditionnels, à la législation de leur pays qui les oblige le plus souvent à garantir les dépôts et s'assurer que les transferts d'argent ne se perdent pas dans la nature, ces fintechs n'encourent de fait qu'un risque de réputation limité et ne disposent parfois même pas des moyens humains ou techniques pour se conformer à ces obligations légales. L'émission d'une MNBC vise alors à profiter de l'effet de levier suscité par la numérisation pour, à la fois, sécuriser les transactions et capturer une part de l'économie informelle ainsi que les recettes publiques qui vont avec. C'est aussi et surtout un moyen de promouvoir l'inclusion financière. Pour les pays développés, il s'agit simultanément d'accompagner le déclin dans l'usage du cash et de faire face à la concurrence des crypto-actifs. À cet égard, le projet Libra/Diem présenté puis abandonné par Méta (ex-Facebook) a fait l'effet d'un électrochoc en menaçant de constituer une forme de circuit alternatif où les États perdraient de fait la main sur le pilotage de la politique monétaire. La pandémie de Covid-19 a pour sa part significativement accéléré la numérisation des moyens de paiements, faisant diminuer la place relative des pièces et billets qui sont l'un des éléments essentiels de l'offre de monnaie de banque centrale. L'ensemble de ces raisons, ainsi qu'un contexte plus global d'accélération des paiements et de numérisation des transactions et des identités, explique l'engouement actuel pour la création de MNBC. Par ailleurs, certaines opérations conduites aujourd'hui par le biais de crypto-actifs, à l'instar des ICO, pourraient demain être conduites avec plus d'efficacité et de sûreté à travers des MNBC.

Cependant les projets de MNBC restent à l'heure actuelle peu ambitieux, car ils se contentent d'adapter l'architecture financière aux évolutions numériques et se concentrent quasi-exclusivement sur chaque territoire national. Ce faisant, ils tendent à minimiser la portée théorique et pratique potentielle des MNBC. En outre, le fait que ces projets demeurent pour l'heure largement nationaux relève de deux raisons principales : d'une part, la conception technique d'une MNBC est d'une complexité élevée, même au sein d'une seule juridiction nationale. Intégrer une dimension internationale nécessitant d'adapter les infrastructures non seulement aux évolutions numériques mais aussi aux usages et techniques d'un ou plusieurs autres pays apparaît pour l'heure utopique. D'autre part, nombre de juridictions, en particulier des juridictions occidentales pour lesquelles le phénomène des *remittances* évoqué plus haut reste marginal, semblent considérer, à tort, que les échanges internationaux demeurent secondaires et concernent un faible public. En effet, les paiements transfrontières se multiplient à mesure que s'approfondit la mondialisation, et sont amenés à augmenter encore davantage, puisque l'on estime que leur volume total devrait avoisiner les 250 000 milliards de dollars d'ici 2027. Il y a donc un enjeu économique majeur à développer rapidement des MNBC capables de servir d'instrument de règlement au niveau international. La Chine semble

l'avoir compris à travers le projet de yuan numérique qui sert à appuyer les projets des nouvelles routes de la soie.

2/ Des perspectives révolutionnaires pourraient être ouvertes par la réflexion autour de MNBC ouvertes aux acteurs privés

A l'heure actuelle, de nombreux projets de MNBC visent simplement à adapter le système financier actuel aux mutations technologiques, à l'instar du projet d'euro numérique. Il s'agirait concrètement de garder le modèle d'intermédiation bancaire tel qu'il est, y compris sous l'angle de la création monétaire endogène – c'est-à-dire que la quantité totale de monnaie en circulation est déterminée en première instance par les prêts accordés par les banques commerciales, ces prêts étant plus ou moins nombreux selon le pilotage des taux d'intérêt directeur. Pour rappel, ce modèle emporte deux conséquences principales :

- Le pouvoir de création monétaire, autrefois plus encadré par le pouvoir politique (notamment grâce à des mécanismes de contrôle et d'encadrement du crédit bancaire pendant la période de l'après-guerre), est désormais essentiellement dans la main des institutions financières et monétaires (c'est à dire des banques commerciales), qui peuvent ne pas répercuter immédiatement et parfaitement un changement au niveau des taux d'intérêt directeurs ;
- Seuls ces mêmes intermédiaires financiers ont un accès direct à la « monnaie centrale », et les autres acteurs privés (entreprises et citoyens) sont dépendants des banques pour accéder à des moyens de paiement et à la monnaie.

On comprend dès lors qu'une MNBC qui viserait simplement à adapter ce modèle, en introduisant un compte dit « en monnaie centrale » pour chaque citoyen mais dont la distribution et la gestion est toujours assurée par les intermédiaires financiers, ne changerait fondamentalement pas l'architecture du système monétaire actuel. On peut cependant imaginer que les comptes en monnaie centrale bénéficieront d'une garantie complète de la part de la banque centrale, ce qui représente déjà un progrès par rapport aux comptes bancaires actuels, toujours soumis au risque de faillite bancaire, ainsi qu'une différence majeure par rapport aux crypto-actifs qui ne bénéficient d'aucune garantie.

Pourtant, si les banques centrales décidaient de ne pas fixer de limite aux dépôts sur le compte en monnaie centrale, et déléguaient uniquement la gestion des comptes aux intermédiaires financiers, elles pourraient de fait piloter bien plus étroitement l'offre de liquidités dans l'économie. L'émission de monnaie numérique publique, garantie par une

banque centrale et largement accessible, pourrait ainsi permettre de réaliser cette idée récurrente d'un lien direct entre la monnaie banque centrale et le citoyen, dont le prix Nobel d'économie James Tobin rêvait déjà en 1987 en préconisant de : "mettre à disposition du public un dispositif alliant la commodité des dépôts et la sécurité des espèces – essentiellement des dépôts d'espèces, transférables par chèque ou autre type d'ordre et ce, quel que soit le montant »⁸⁴. Cela permettrait d'introduire une unité monétaire sûre, sous forme numérique, qui pourrait permettre à la banque centrale de mener des opérations de politique monétaire de manière plus directe. Il ne serait ainsi plus nécessaire de passer par l'intermédiaire des banques pour conduire des opérations d'assouplissement quantitatif et injecter de la monnaie dans le système économique. Les changements de taux auraient un effet direct et transparent sur les déposants.

Cette hypothèse soulève toutefois deux types de problèmes :

- D'abord, le modèle actuel de rentabilité des banques, du moins des banques de dépôts, se fonde sur leur capacité à gérer l'épargne des agents privés et à prélever une commission (qui se matérialise par le paiement du taux d'intérêt) sur les prêts qu'elles octroient. Si les citoyens décidaient de transférer massivement leur épargne vers les comptes en monnaie centrale, les banques pourraient être confrontées à une forme de bank run qui déséquilibrerait leur modèle économique. Or, le modèle présenté ci-dessus implique de déléguer la gestion et la distribution de l'euro numérique aux intermédiaires financiers en leur supprimant de fait leur principale source de revenus. Des sources de financement alternatives devraient alors être trouvées, dans la mesure où il n'est pas envisageable que la banque centrale détienne et gère en temps réel les comptes bancaires de 450 millions d'habitants dans l'Union européenne.
- Par ailleurs, les banques remplissent aujourd'hui, certes imparfaitement, un rôle de réduction des asymétries d'information : elles évaluent les projets viables et non viables et allouent des prêts en fonction de ces évaluations. Cette fonction essentielle devrait quoiqu'il arrive être remplie quelle que soit la forme prise par la distribution de liquidités à l'avenir.

Une monnaie numérique publique, associée à l'ouverture de comptes de particuliers directement auprès de la banque centrale (ou mise en circulation via des intermédiaires financiers agréés), conduirait également à réduire drastiquement le risque de crise de

⁸⁴ James Tobin (1987), « The case for preserving regulatory distinctions », Proceedings of the Economic Policy Symposium, Jackson Hole, Federal Reserve Bank of Kansas City, p. 167-83.

liquidités bancaires. En effet, si la monnaie est émise et garantie directement par la banque centrale, celle-ci sort du champ de dépendance aux institutions financières. Le recours même aux banques devient, pour ainsi dire, superflu. En définitive, des MNBC bien pensées pourraient constituer un véritable moyen de désintermédiation du système financier et d'évolution de la monnaie vers une forme de bien commun. Elle conduirait dès lors à devoir repenser non seulement la place des banques centrales mais également celle des banques commerciales.

PROPOSITION n°7 : Développer des monnaies numériques de banque centrale accessibles aux citoyens et aux entreprises et permettre une transmission directe de la politique monétaire via des comptes en monnaie centrale hébergés par des acteurs bancaires publics ou privés sous contrat.

3/ Gérer les risques pour le système financier traditionnel

Le système financier traditionnel doit dès lors faire face à trois types de risques. Premièrement, la montée en puissance des crypto-actifs qui pourrait introduire une forme de concurrence si des entreprises répliquent le modèle des banques commerciales dans la sphère des crypto-actifs (par exemple, en accordant des prêts en crypto-actifs contre nantissement, ou bien en proposant des produits d'épargne). Deuxièmement, une réorganisation du système financier permis par les mutations technologiques et qui permettrait un lien plus direct entre banques centrales et acteurs privés, remettant en cause de fait le rôle et l'utilité des acteurs financiers traditionnels. Enfin, à la jonction de ces deux problématiques, se pose le cas d'acteurs de la finance traditionnelle (TraFi) qui développent des projets liés aux crypto-actifs, à l'instar de la Société Générale et de sa filiale Forge. De tels développements sont de nature à mettre en danger la santé financière de ces banques si d'aventure un phénomène de type Terra/Luna devait se reproduire dans un monde où les banques détiendraient une quantité non négligeable de crypto-actifs à leur bilan.

Le premier de ces risques peut être pris en considération à l'aide de la régulation (cf. ci-dessous), mais les banques ne feront pas l'économie d'une remise en question de leur modèle et de la structure oligopolistique du marché. La concurrence des « Fintechs » (entreprises spécialisées dans les technologies numériques, notamment dans le financement) est un enjeu structurel qui impose aux banques de trouver d'autres sources de revenus, éventuellement en finançant des projets particuliers qui nécessitent une masse critique ou en se positionnant sur certains segments de marché.

Le second de ces risques impose un accompagnement des acteurs financiers afin de définir leur nouveau rôle dans un système technologiquement décentralisé, mais dont la viabilité est garantie en dernière instance par une autorité publique (en l'espèce, une banque centrale). Enfin, le dernier de ces risques impose à court terme de définir des ratios de détention de crypto-actifs et d'esquisser des règles strictes sur le développement de projets liés aux crypto-actifs, comme tente de le faire le règlement MiCA (cf. *supra*).

D/ Le cas particulier des transferts internationaux d'argents (ou paiements transfrontières)

Les paiements transfrontières qui transitent par le système financier mondial souffrent de nombreuses lacunes qui expliquent en partie le développement des crypto-actifs comme moyen de substitution. Cela constitue une justification supplémentaire pour adopter une focale plus internationale dans les projets de développement de MNBC.

1/ Les difficultés posées par les paiements transfrontières

Les transferts internationaux d'argent (ou paiements transfrontières) sont l'un des seuls cas d'usage où les crypto-actifs apporteraient une potentielle plus-value, bien que de nombreuses entreprises privées (Western Union, MoneyGram, ou encore Wise) soient déjà positionnées sur ce créneau. Il convient de noter tout d'abord que les paiements transfrontières connaissent une forte croissance depuis le milieu des années 1980, sous l'effet d'une double logique d'approfondissement de la mondialisation et de croissance du commerce international, mais aussi d'augmentation massive de la spéculation qui se traduit par une multiplication des échanges en devise. Cette double logique est en partie⁸⁵ capturée selon la segmentation de marché suivante :

- Les transactions dites “de gros” (*wholesale*), qui correspondent essentiellement aux échanges monétaires réalisés entre institutions financières, ainsi que par les plus grandes entreprises privées ;
- Les transactions dites “de détail” (*retail*), qui ont en commun d'être des transactions de petit montant, mais qui recouvrent une grande variété de situations, de l'achat de bien à une firme étrangère sur une plateforme de e-commerce à l'envoi d'argent par

⁸⁵ En partie seulement car les transactions “de gros” ne correspondent heureusement pas toutes à des transactions spéculatives, et que certaines transactions de détail sont regroupées (compensées) pour être traitées sur le segment des transactions de gros. Le seuil à partir duquel une transaction est considérée comme appartenant à l'un ou l'autre des segments ne fait d'ailleurs pas l'objet d'un consensus et varie selon les régions du monde.

un migrant de son pays d'accueil vers son pays d'origine (cas spécifique des remises ou *remittances*).

Quel que soit le segment concerné, les paiements transfrontières font face à plusieurs types de “frictions” dont quatre ont été identifiées par la BRI⁸⁶ : coûts élevés, délais importants, transparence insuffisante et manque d'inclusion. Les crypto-actifs se proposent de répondre à certaines de ces problématiques, et en particulier celle du manque d'inclusion, qui résulte dans les pays en voie de développement du manque d'infrastructures bancaires. Par ailleurs, alors que le système bancaire traditionnel fait toujours face à la problématique du change - que celui-ci soit particulièrement défavorable pour certaines devises, ou que certaines devises s'apprécient ou se déprécient brutalement (risque de change) -, les crypto-actifs seraient à même de constituer une “monnaie” universelle, non soumise à ces problématiques. La réalité est bien sûr fréquemment tout autre : les prestataires sur actifs numériques n'offrent pas le même niveau de garantie que le système bancaire traditionnel dont la solidité est assurée en dernier ressort par la puissance publique. Dès lors, rien n'oblige légalement les CASP à garantir les dépôts ou l'acheminement des transactions (cf. *supra*) et rien ne garantit les déposants contre la faillite.

Contre les risques inhérents aux crypto-actifs, les États tentent donc de conserver leur souveraineté par le truchement de monnaies numériques de banques centrales (cf. partie précédente) qui, si elles sont connectées, pourraient permettre d'échanger des devises en garantissant la sécurité des transactions.

2/ Des monnaies numériques de banques centrales interconnectées plutôt que des crypto-actifs

Les projets d'interconnexion des MNBC actuellement à l'étude (mCBDC pour multi-CBDC) visent à combiner les avantages de la numérisation des moyens de paiement avec la sécurité garantie par des États souverains. Si plusieurs modèles sont à l'étude, ils ont tous en commun de vouloir tisser des liens tant opérationnels - sur les normes des messages financiers par exemple - que juridiques et pratiques afin que les banques centrales de pays différents puissent “parler le même langage”. L'objectif ultime (et pour l'instant utopique) serait de pouvoir envoyer un paiement sans frais supplémentaires à l'autre bout du monde et en toute sécurité de la même façon que l'on envoie un paiement de compte à compte en France. C'est d'ailleurs l'une des promesses initiales des crypto-actifs : surmonter les différentes monnaies et les liens d'éloignement géographiques en permettant d'échanger avec le monde entier. Or, cette volonté d'universel se heurte au dilemme inhérent des crypto-actifs (et des communs de

⁸⁶ “Enhancing Cross-border Payments - Stage 1 report to the G20”, *Financial Stability Board*, 2020 (<https://www.fsb.org/2020/04/enhancing-cross-border-payments-stage-1-report-to-the-g20/>)

manière générale, la stabilité financière ne faisant pas exception), que l'on peut résumer ainsi : une monnaie universelle implique un accord mondial pour accepter cette monnaie dans tous les pays. En matière monétaire, cet accord implique d'avoir confiance dans le moyen d'échange. Dès lors, soit cette confiance est gagnée progressivement directement auprès des citoyens (c'était l'idée du projet Libra, voir *supra*), ce qui nécessite une stabilité que les crypto-actifs n'ont pas à l'heure actuelle ; soit elle est assurée par un *proxy*, à savoir les États, en l'espèce au travers des banques centrales.

Les projets de MNBC interconnectées cherchent ainsi précisément à concilier souveraineté monétaire, de laquelle découle la confiance dans la monnaie, et aspiration à réduire les frictions qui affectent les échanges internationaux. L'interconnexion doit également être pensée dans sa dimension nationale, c'est-à-dire avec les systèmes de paiement déjà existants.

On distingue conceptuellement plusieurs degrés d'interconnexion des MNBC, de l'établissement de liens techniques à la mise en place d'une plateforme accueillant des MNBC intégrées. Les deux enjeux essentiels de ces plateformes sont (i) que, comme tout projet international, plus les MNBC sont intégrées, plus les bénéfices à en attendre sont élevés, mais plus les difficultés relatives à la gouvernance sont accrues et (ii) que ces projets doivent être compatibles avec la préservation de la souveraineté monétaire des États participants. De nombreux projets, aux degrés de maturité et aux ambitions d'intégration variables, voient ainsi progressivement le jour.

3/ Une expérience de MNBC interconnecté : la mCDBC Bridge initiative en Asie⁸⁷

La *mCDBC Bridge initiative*, développé entre l'Autorité Monétaire d'Hong Kong (HKMA), la Banque centrale de Thaïlande, la PBoC et la Banque centrale des Emirats Arabes Unis vise dans ce contexte à « *prendre en charge les opérations de change transfrontières PvP en temps réel dans plusieurs juridictions fonctionnant 24 heures sur 24, 7 jours sur 7* »⁸⁸. Il s'agit de créer une plateforme dite « multidevise » commune de MNBC, permettant de combiner plusieurs MNBC nationales avec un règlement d'opérations instantané et en temps réel. Ce projet ambitieux permettrait ainsi potentiellement de présenter des avantages similaires aux crypto-actifs (« universalité », facilité d'usage, accessibilité) tout en étant respectueux de la souveraineté monétaire des États. Les défis techniques, juridiques et de gouvernance sont évidemment à la hauteur des enjeux, c'est-à-dire très élevés.

⁸⁷ [Auer, R., Haene, P., Holden, H. "Multi-CBDC arrangements and the future of cross-border payments", BIS Papers, N° 115, Mars 2021.](#)

⁸⁸ Ibid, p. 8.

Les crypto-actifs sont ainsi nés en partie pour répondre à des demandes, des segments de marchés qui n'étaient ou mal couverts par le secteur financier classique, en particulier dans le monde des paiements transfrontières. Pour autant, leur instabilité inhérente et leur difficulté à s'imposer comme « monnaie universelle » soulignent l'intérêt d'explorer d'autres pistes qui permettent de lutter contre les frictions nées des transactions internationales tout en conservant la souveraineté monétaire des États.



Troisième partie : Intégrer les crypto-actifs dans la vie commune sans risque pour la société

Être actif et non passif face aux mutations technologiques suppose de ne pas subir les orientations de société imposées par une poignée d'acteurs. Cette partie concerne l'ensemble des impacts des crypto-actifs sur la vie des individus au-delà de la remise en question du système monétaire.

A l'échelle nationale, les intérêts de la société sont représentés par la défense de l'ordre public, c'est la définition des limites de la légalité qui peut permettre de matérialiser la position et la pensée de la société sur le sujet des crypto-actifs. A l'échelle de l'individu, il s'agit de questionner les usages que peuvent avoir les simples particuliers.

I. Un environnement soumis à de nombreux risques techniques et technologiques, loin de la sûreté promise

Les réseaux de *blockchains* sont un moyen de sécuriser le transfert d'objets numériques auquel est attribuée une valeur (les crypto-actifs). En effet, si tout fonctionne bien dans un réseau de *blockchain*, il ne peut pas y avoir duplication des objets numériques porteurs de la valeur. Cependant une multitude de problèmes sont susceptibles de perturber la confiance qu'on pourrait avoir dans la circulation des crypto-actifs. Nous en énumérons ici une liste sans entrer dans les détails.

A/ L'illusion de la décentralisation

Alors que tout est assez bien décentralisé (pas de tiers de confiance) pour les crypto-actifs de type bitcoin, ether et quelques autres et que c'est cette décentralisation qui constitue l'obstacle aux principales fraudes (pourvu que le nombre de validateurs soit assez important et qu'ils soient indépendants), ce n'est pas le cas de tous les crypto-actifs dont de nombreux sont liés à l'existence des tiers de confiance plus ou moins cachés et souvent ignorés.

Pour les *stablecoin* centralisés, comme tether, il se peut que l'émetteur (la société Tether Limited) soit défaillant et par exemple qu'il ne garde pas la contrepartie (le collatéral) qu'il devrait avoir. Pour les NFT, il y a aussi une société ou un acteur (parfois anonyme) qui émet le NFT ; c'est un tiers de confiance qui peut être défaillant. Pour les NFT associés à des œuvres d'art, l'artiste créateur doit donner son accord, et ne doit le donner qu'une seule fois. Il peut ne pas avoir été consulté, et il pourrait donner son accord à plusieurs plateformes

d'émission, auquel cas le détenteur du NFT n'aurait pas en main ce qu'il croit avoir acheté. Bien évidemment, les plateformes d'échanges sont aussi des tiers de confiance, ainsi que les émetteurs de produits dérivés basés sur des crypto-actifs.

Une multitude d'acteurs autour des crypto-actifs sont en fait des tiers de confiance et nombreux utilisateurs croient à tort que ce qu'ils font avec ces tiers de confiance est garanti parce que à un moment du processus mis en œuvre (achat, vente, emprunt, etc.) il y a un réseau de *blockchain*. Ils pensent bénéficier de la sécurité que donne une *blockchain* proprement et complètement décentralisée ce qui est une illusion parfois gravement payée. Les faillites et escroqueries diverses du monde des plateformes et des *Hedge funds*, montrent clairement que l'introduction de ces tiers de confiance annule totalement la confiance qu'on aurait pu avoir dans de véritables protocoles de *blockchain* décentralisées comme Bitcoin ou Ethereum qui ne sont bien souvent que des prétextes pour construire autour un monde finalement fragile et risqué. La finance décentralisée (DeFi) ne l'est pas toujours vraiment ! Comme de plus elle utilise des protocoles souvent complexes elle a souvent été le théâtre d'accidents (voir les pages de ce rapport consacrées à la DeFi).

Il faut noter aussi que les acteurs centraux peuvent être l'objet eux-mêmes de vols (c'est arrivé un très grand nombre de fois aux plateformes d'échange), peuvent commettre des erreurs techniques et par exemple développer des logiciels comportant des bugs, peuvent être tout simplement malhonnêtes. Comme le monde des crypto-actifs est moins surveillé et soumis à des contrôles que le monde bancaire courant, les erreurs et escroqueries y sont plus fréquentes. Cela conduit ceux qui — à tort encore — pensent que la réglementation y est aussi rigoureuse que dans le monde financier et bancaire courant à prendre de graves risques, et à être victimes de pertes conséquentes.

B/ Les opérations sur des *blockchains* bien décentralisées

Même utilisée sans passer par des tiers de confiance (par exemple quand on opère des transactions directement en bitcoins en utilisant un compte dont on gère soi-même les clés) la manipulation des crypto-actifs est sujette à différents risques :

- Les « attaques 51 % » sont celles que peut mener un validateur qui détient la capacité de valider plus de la moitié des pages de la *blockchain*, soit, dans le cas de la *Preuve de travail*, parce qu'il détient plus de la moitié de la puissance de calcul du réseau des mineurs, soit, dans le cas de la *Preuve d'enjeu*, parce qu'il contrôle plus de la moitié des sommes mises sous séquestre. Ces attaques envisagées dès 2008 dans le livre blanc de Satoshi Nakamoto concernent surtout les petites *blockchains* avec des validateurs peu engagés. Dans le cas des réseaux de *blockchains* plus importants

(Bitcoin, Ethereum, etc.) ces attaques sont peu probables et d'ailleurs ne se sont jamais produites car elles ne sont pas en mesure de produire un profit intéressant comparé à l'investissement qu'elles exigent. Un État très puissant pourrait tenter de mener une attaque 51% mais son but ne serait pas d'en tirer profit, mais seulement de détruire la confiance envers la *blockchain* attaquée ; on parle alors « d'attaque Goldfinger », en référence au fameux film de James Bond⁸⁹.

- D'autres attaques basées sur les primitives cryptographiques (mathématiques) utilisées dans les protocoles doivent être envisagées. Le développement des ordinateurs quantiques est par exemple un souci car, si on progresse rapidement dans leur mise au point, il deviendra possible pour ceux qui en disposent de casser la fonction de hachage SHA256, ce qui serait la porte ouverte à toute sorte d'opérations frauduleuses comme le vidage à son profit de n'importe quel compte. Des modèles de *blockchain* résistance aux attaques quantiques sont étudiés, mais aujourd'hui les principales *blockchains* n'en sont pas protégées.
- Enfin, on constate de nombre erreurs de programmation. Un réseau de *blockchain* fonctionne nécessairement avec des programmes informatiques qui peuvent comporter des erreurs (bugs). De telles erreurs se sont produites y compris pour Bitcoin. Le 15 août 2010 l'une d'elle a failli faire tomber le Bitcoin⁹⁰. Des erreurs potentiellement graves ont parfois été détectées et corrigées juste à temps, par exemple en septembre 2018 ⁹¹, ou récupérées sans qu'il en résulte de dysfonctionnement graves, par exemple en mars 2013 pour le réseau Bitcoin. Ces risques sont limités pour les parties les plus importantes des programmes par l'expertise des programmeurs et éventuellement l'utilisation de méthodes de développement robustes. Cependant personne ne peut prétendre que ces risques sont inexistants.

Notons pour conclure que, dans les faits jusqu'à présent, ce sont les risques liés aux tiers de confiance qui ont été à l'origine des pertes les plus significatives pour ceux qui détiennent des crypto-actifs. D'autres attaques théoriques que l'attaque 51 % ont été décrites par les cryptologues, par exemple les attaques Eclipse, mais elles sont difficiles à mettre en œuvre et ne constituent pas un souci grave comparé au problème des erreurs de programmation possibles, et aux fragilités possibles des primitives cryptographiques. Les risques de type (b) ne doivent pas être oubliés, mais ce sont surtout ceux de type (a) qui

⁸⁹ [The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, Princeton University, 2013](#)

⁹⁰ ["Des bitcoins à l'infini – Le jour où quelqu'un a créé 92 milliards de bitcoins", Le journal du Coin, 15 août 2020](#)

⁹¹ <https://bitcoincore.org/en/2018/09/20/notice/>

doivent être adressés en priorité, en particulier en imposant des mesures réglementaires fermes à tous les tiers de confiance de l'écosystème des crypto-actifs.

Outre les failles intrinsèques aux *blockchains*, les crypto-actifs renouvellent et accentuent par ailleurs un certain nombre de problèmes de sociétés déjà connus. Il s'agit dès lors de continuer à lutter contre certains phénomènes en y intégrant désormais cette nouvelle mutation technologique.

C/ Les risques criminels et sociaux majeurs liés à l'absence de réglementation adéquate des crypto-actifs

Outre les enjeux liés à la conception même des *blockchains*, les crypto-actifs suscitent un certain nombre de risques sociaux et légaux qui impliquent une régulation ferme du secteur.

1/ Les risques liés à la lutte contre le blanchiment et le financement du terrorisme (LCB-FT)

i. Les crypto-actifs accentuent les difficultés de la LCB-FT

À l'instar du blanchiment "classique" d'argent, les crypto-actifs offrent la possibilité d'anonymiser les transactions, ce qui en fait des candidats idéaux pour le financement du crime et du terrorisme internationaux. La LCB-FT passe notamment, dans le cadre financier classique, par des obligations imposées aux banques (nommée "entités assujetties") d'effectuer des contrôles réguliers de leur clientèle et des transactions que celle-ci effectue (obligations dites de KYC ou *Know-your-customer*). À l'heure actuelle, si M. Dupont décide d'ouvrir un compte dans la banque A pour y blanchir de l'argent illégalement gagné, la banque s'assurera, en rentrant son nom dans une base de données, que celui-ci ne fait par exemple l'objet d'aucune sanction (nationale ou internationale) ni d'un mandat d'arrêt, à l'image des sanctions adoptées récemment contre des oligarques russes. De plus, toutes les transactions font l'objet d'un criblage (*screening*) automatisé pour s'assurer qu'émetteur et bénéficiaire ne sont pas engagés dans des activités illégales. Cette sécurité « à double détente », si elle ralentit parfois la vitesse des transactions, permet de minimiser le risque que l'argent déposé dans les banques finance des activités illégales.

ii. Une volonté d'adaptation du cadre aux crypto-actifs

On comprend donc que les intermédiaires financiers, en appliquant les réglementations nationale, européenne et internationale, constituent ici la clé de voûte de la légalité des transactions. Or, jusqu'en 2020, certaines lacunes juridiques subsistaient dans la mesure où les acteurs crypto-actifs, tant ceux fournissant des services de conversion de monnaie

officielle en crypto-actifs que les « prestataire de services de portefeuille de conservation », n'étaient pas soumis aux mêmes obligations de conformité que les banques. La 5^e directive relative à la lutte contre le blanchiment d'argent et le financement du terrorisme (dite « AMLD5 »), adoptée en 2018 et entrée en vigueur dans les Etats membres en 2020, faisait ainsi le constat que “Les prestataires de services d'échange entre monnaies virtuelles et monnaies légales [...] ainsi que les prestataires de services de portefeuilles de conservation ne sont soumis à aucune obligation de la part de l'Union consistant à identifier les activités suspectes. Les groupes terroristes peuvent ainsi avoir la possibilité de transférer de l'argent dans le système financier de l'Union ou à l'intérieur des réseaux de monnaies virtuelles en dissimulant les transferts ou en bénéficiant d'un certain degré d'anonymat sur ces plates-formes.”⁹²

Le législateur européen a donc entrepris d'adapter la réglementation financière existante en matière de LCB-FT et de conformité aux spécificités des crypto-actifs. L'AMLD5 étend le champ de la réglementation applicable aux banques aux “prestataires de services d'échange entre monnaies virtuelles et monnaies légales ainsi qu'[aux] prestataires de services de portefeuilles de conservation. [...]”⁹³ et oblige ces acteurs à s'enregistrer auprès des instances nationales. Pour autant, à l'instar de toute réglementation régionale s'appliquant à un phénomène international, l'absence d'extraterritorialité implique que les autorités des Etats membres sont impuissantes pour imposer des obligations à des acteurs non enregistrés sur le sol européen (le problème s'étend aussi aux questions de fiscalité, cf. *infra*).

PROPOSITION n°8 : Renforcer et rendre effectives les obligations liées à la lutte contre le blanchiment et le financement du terrorisme (LCB-FT) et à la conformité par tous les émetteurs et plateformes d'échange de cryptoactifs

PROPOSITION n°9 : Contrôler l'utilité sociale des crypto-actifs par l'introduction d'un visa obligatoire auprès des autorités d'enregistrement nationales ou européennes.

iii. Le cas particulier de l'anonymat

En théorie, une jurisprudence constante au sein de l'UE implique que “les États membres interdisent à leurs établissements de crédit et établissements financiers de tenir des comptes anonymes ou des livrets d'épargne anonymes”. L'AMLD5 vise ainsi à déjà à lutter contre les risques liés à l'anonymat en disposant que “les cellules de renseignement financier (CRF)

⁹² <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018L0843&from=FR>

⁹³ Sa transposition a été assurée en France par la loi PACTE (2019).

nationales devraient être en mesure d'obtenir des informations leur permettant d'associer les adresses correspondant à la monnaie virtuelle à l'identité du propriétaire de la monnaie virtuelle.”⁹⁴ La directive relative à la coopération administrative dans le domaine fiscal (dite DAC) est également censée faire l'objet d'une mise à jour prochainement (DAC8) pour s'adapter au secteur des crypto-actifs, favoriser les échanges d'information entre les autorités nationales et donc renforcer la transparence du secteur.

Cet objectif reste un vœu pieux lorsqu'il s'agit de prestataires non localisés sur le territoire de l'Union européenne. Il conviendrait dès lors d'aller plus loin en interdisant purement et simplement les crypto-actifs dont l'objet est précisément de fournir un anonymat complet des transactions et des détenteurs de compte.

PROPOSITION n°10 : Interdire les crypto-actifs ayant pour but avéré de protéger l'anonymat des transactions en toutes circonstances (par exemple : Monero, Dash, etc.)

iv. Le problème du “smurfing”

Le “smurfing” est une pratique bien connue dans le domaine de la LCB-FT dont le nom semble dérivé des actions originellement entreprises par les trafiquants de drogue. L'idée est la suivante : les banques doivent toujours signaler les transferts dits “suspicieux” aux autorités. Afin de faciliter l'application de ces règles, un seuil (défini nationalement) existe au-delà duquel le signalement est automatique. Dès lors, ceux qui pratiquent le “smurfing” divisent la transaction originelle qui aurait déclenché le signalement automatique en plusieurs transactions de plus faibles montants pour rester sous le seuil de signalement. Cette pratique n'est pas spécifique aux crypto-actifs : les criminels peuvent par exemple simplement demander à plusieurs complices d'ouvrir des comptes en banque pour réaliser chacun un transfert de faible montant. Pour autant, les crypto-actifs permettent d'une part de diversifier les supports (c'est-à-dire le type de compte sur lequel l'argent illégal est déposé), les méthodes de conversion (l'argent peut être converti en une multiplicité de crypto-actifs différents), mais aussi d'investissement (une fois l'argent converti, il peut être réinvesti dans d'autres transactions en crypto-actifs ou utilisé comme collatéral). Dès lors, les crypto-actifs posent un risque supplémentaire en accroissant les difficultés des autorités et des banques pour détecter les transactions illégales.

Outre les risques liés à l'illégalité, les crypto-actifs favorisent également des comportements à la limite de la légalité et contribuent à brouiller les frontières, et plus particulièrement en matière de fiscalité.

⁹⁴ <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015L0849&from=EN>

2/ Les enjeux liés à la fiscalité

i. Les risques de fraude et d'évasion fiscale

En raison de la faible harmonisation des législations nationales concernant la fiscalité directe, les règles fiscales au niveau des crypto-actifs demeurent largement à la main des pays et se déclinent soit au niveau légal et réglementaire, soit, lorsque des zones grises subsistent, au niveau de la doctrine de l'administration fiscale. Ces risques sont avérés dans la mesure où les crypto-actifs sont actuellement traités comme des actifs mobiliers standards. Or, l'imposition de règles fiscales, au niveau européen autant qu'au niveau national, implique de pouvoir retracer l'origine d'une transaction ou d'un comportement. Dès lors, si ces transactions s'effectuent entre prestataires non régulés (donc non surveillés) et que les sommes échangées ne sont pas converties en monnaie commerciale, il est impossible de leur appliquer une quelconque règle fiscale. Deux types de risques émergent dès lors :

- Des risques d'évasion et de fraude fiscale, dans la mesure où ces actifs, tant qu'ils demeurent dans "l'espace numérique", ne sont pas taxés (cas des échanges de crypto-actif à crypto-actif) ;
- Des risques de rupture d'égalité devant l'impôt : les plus-values réalisées lors d'échanges de crypto-actifs ou même de simple minage font l'objet de régimes fiscaux complexes et différenciés, et les plus-values dites "latentes" ne sont pas comptabilisées tant que le crypto-actif n'est pas converti en monnaie commerciale.

La faillite de FTX (cf. *supra*) est un ainsi un exemple canonique de ces zones grises légalo-fiscales : FTX a opéré de manière numérique et transfrontalière, avec une base de clients mondiale, avec son siège aux Bahamas, paradis fiscal notoire. Selon ses dépôts de bilan (renseignés consécutivement à sa faillit), FTX possède ou est affiliée à un réseau complexe de plus d'une centaine d'entités réparties sur cinq continents, dont l'une, FTX (EU) Ltd, est domiciliée à Chypre, supervisée par la Commission chypriote des valeurs mobilières et des changes et a été suspendue par cette dernière le 11 novembre 2022. La société employait des centaines de personnes et a récemment affirmé avoir plus d'un million d'utilisateurs enregistrés, dont moins de 10 % sont compris comme étant basés dans l'UE. D'autres sociétés de crypto-actifs sont enregistrés dans d'autres paradis fiscaux tels que le Delaware, les îles Vierges ou encore les îles Britanniques. Le projet *Anti Tax Avoidance Directive* (ATAD III), actuellement à l'étude et censé entrer en vigueur en janvier 2024, prévoit d'étendre les règles de la lutte contre la fraude et l'évasion fiscale au secteur des crypto-actifs. Une société (*holding*) détenant des crypto-actifs sera alors susceptible de rentrer dans le champ de la

directive, même si les prestataires de service financiers liés aux crypto-actifs sont eux exclus du champ et renvoyés au règlement MiCA (cf. *supra*). Des réflexions sont par ailleurs menées au niveau de l'OCDE sur le régime fiscal des crypto-actifs et notamment des NFT. Enfin, la

dire
Il peut alors être tentant d'accorder un régime fiscal préférentiel pour ce type d'actifs afin d'inciter leurs détenteurs à les déclarer et encaisser ainsi les recettes publiques afférentes. Pour autant, cela reviendrait à favoriser fréquemment les détenteurs les plus riches, le monde des crypto-actifs étant par essence un monde oligopolistique fondé sur le principe selon lequel les premiers entrants sur un marché font les plus gros bénéfices.

PROPOSITION n°12 : Généraliser l'obligation de déclarer tous comptes en crypto-actif à l'ensemble de l'UE.

PROPOSITION n°11 : Interdire les transactions en cryptos avec des plateformes enregistrées dans des paradis fiscaux.

ii. Les risques associés à une rupture d'égalité entre les citoyens due à une fiscalité préférentielle

Au niveau français, l'article 79 de la loi de finances pour 2022 modifie le régime fiscal des plus-values de cessions de "cryptomonnaies" [*sic*]⁹⁵ à compter de 2023 :

- Les cessions réalisées à titre non-professionnel relèveront systématiquement du régime du prélèvement forfaitaire unique (taux de 30%) ;
- Les contribuables pourront choisir d'être imposés soit au taux forfaitaire de 12,8 %, soit au barème progressif de l'impôt sur le revenu.

Cet alignement sur le régime des actifs financiers traditionnels implique les mêmes inégalités qui sont déjà à l'œuvre pour ces actifs, la détention de ce type d'actifs étant souvent réservées aux déciles supérieurs de la population. Surtout, les mouvements entre crypto-actifs (par exemple, échanger un bitcoin contre un ether avec une potentielle plus-value selon les cours de chacun des actifs) ne sont à l'heure actuelle pas imposés.

Cette zone grise de la fiscalité est une véritable lacune, alors que les transactions en devises font, elles, l'objet d'une imposition spécifique. Dès lors, la fiscalité liée aux crypto-actifs devrait à la fois combler les lacunes réglementaires actuelles et s'aligner au moins sur

⁹⁵ <https://www.economie.gouv.fr/cedef/regime-fiscal-cryptomonnaies>

la fiscalité des actifs financiers classiques, voire être intégrée au barème de l'IR pour en désinciter l'acquisition.

PROPOSITION n°13 : Comblent les lacunes en matière fiscale et imposer les mouvements de crypto-actif à crypto-actif.

3/ Les enjeux institutionnels

i. Un nouveau champ du népotisme et du conflit d'intérêt à réguler d'urgence

Tout comme les sujets de LCB-FT et de fiscalité, les crypto-actifs n'ont pas l'apanage du lobbying, mais leur force de frappe est particulièrement importante étant donné les moyens à disposition. A titre d'exemple, le *Transparency register* de la Commission européenne propose 75 résultats lorsque l'on rentre le terme "crypto" dans le moteur de recherche.

Les cas de pantouflage et de "rétro-pantouflage" sont également nombreux, les derniers en date étant le passage d'une partie du personnel de l'AMF, dont la directrice juridique, chez le mastodonte des crypto-actifs Binance.

Ces cas sont particulièrement inquiétants pour au moins deux raisons :

- La puissance financière de ces lobbies implique un fort pouvoir d'attraction, parfois même plus fort que les acteurs de la finance traditionnelle (à l'image de la Fédération Bancaire de France), et sont pour le moment moins bien connus des autorités que les lobbyistes plus "classiques" ;
- L'infléchissement des règles en faveur des crypto-actifs peut être particulièrement dommageable pour les citoyens dans la mesure où l'expansion du secteur est relativement récent. Comparativement à la régulation bancaire, qui demeure encore imparfaite en dépit des nombreuses crises qui ont affecté le système financier depuis les grandes vagues de dérégulation des années 1980, la régulation des crypto-actifs en est encore à ses balbutiements alors même que les services proposés sont largement similaires aux services financiers traditionnels, et que les acteurs des crypto-actifs posent de nouveaux types de risques (modèles d'affaires innovant donc difficile à évaluer/assimiler par le régulateur, publicité ciblée sur des publics peu avertis au risque mais sans expertise réelle d'investisseur...).

Dès lors, outre l'application de règles identiques à celles appliquées à des lobbys classiques, les autorités devraient porter une attention particulière sur les cas de conflit d'intérêt et de lobbying dans le secteur des crypto-actifs.

ii. Donner les moyens aux services de l'Etat d'accéder à toute information à tout moment sur les *blockchains*

À l'heure actuelle, les *blockchains* publiques permettent à tout un chacun d'observer les transactions qui sont validées, mais seul le détenteur de la clé privée a connaissance du montant de crypto-actifs dont il dispose. Le procédé est similaire pour un compte en banque : l'État n'a pas accès directement au solde de chaque citoyen, mais impose des régulations aux banques qui, elles, y ont accès en tant que tiers de confiance. Or, l'absence de tiers de confiance au fondement même du fonctionnement des *blockchains* décentralisées implique qu'en cas de bug, d'attaque ou d'illégalités (cf. *supra*), la puissance publique n'a pas accès aux informations pour, le cas échéant, intervenir et réguler. La faillite de FTX a démontré que ceux qui décident d'investir n'ont aucune garantie de retrouver leur argent.

Le cas des *blockchains* privées est un peu différent dans la mesure où elles sont souvent opérées par un acteur centralisé, telle que la *blockchain* développée par JPMorgan. Dès lors, le tiers de confiance est bien présent, mais la puissance publique n'a pas un accès direct à la *blockchain* : elle se contente de vérifier que ce tiers suit les règles imposées, règles qui sont imparfaites et pas encore totalement adaptées à ce type d'innovations. En toute logique, une adaptation du cadre légal aux crypto-actifs doit donc aller de pair avec la possibilité pour la puissance publique de pouvoir accéder directement aux informations contenues sur tous les types de *blockchain*. Encore faut-il pour cela qu'elle en ait les moyens.

iii. Renforcer les moyens juridiques, humains et financiers des services adaptés à la traque des criminels et des fraudeurs dans le milieu des crypto-actifs

Les services visant à lutter contre les crypto-actifs sont fréquemment sous-dotés, et les crypto-actifs ne font souvent l'objet que d'un axe marginal de lutte contre le problème plus large des cybermenaces. Or, au vu des risques spécifiques posés par ces actifs et du niveau de compétence technique et technologique nécessaire, un investissement conséquent est nécessaire tant dans les moyens destinés à analyser les évolutions du marché que dans ceux visant à lutter contre la prolifération des transactions illégales.

Au niveau européen, une "plate-forme des cellules de renseignement financier de l'Union européenne" permet des échanges de données entre cellules de renseignement financiers (CRF) nationales depuis 2006 et favorise la coopération transfrontalière dans la LCB-FT. La CRF française, Tracfin, s'est dotée depuis 2021 d'une cellule Cyber qui "retrace les

transactions financières effectuées sur la *blockchain* et identifie les flux financiers résultant d'opérations délictueuses commises sur le deep ou le dark web. La cellule assure également un rôle transverse en apportant son expertise à l'ensemble du Service sur tous les aspects de la cybercriminalité et des crypto-actifs.⁹⁶ TRACFIN disposait de 191 agents fin 2020⁹⁷, et, bien que nous ne disposions pas du détail des affectations, la cellule Cyber apparaît clairement sous-dimensionnée. Il conviendrait également de renforcer les moyens des et les liens avec les autres organisations telles que la Direction Générale de la Consommation, de la Concurrence et de la Répression des Fraudes (DGCCRF), ainsi que les échanges d'informations au niveau européen entre juridictions nationales.

Enfin, la multiplication des *ransomwares* implique d'alerter, éduquer et sensibiliser les citoyens aux méthodes utilisées par les cyber-criminels. Les demandes de rançons en crypto-actifs sont plus difficiles à déceler et, dans le cas où la rançon est payée, les fonds envoyés plus difficile à tracer, ce qui nécessite donc une vigilance accrue.

PROPOSITION n°15 : Renforcer les moyens juridiques, humains, financiers et la coordination des autorités nationales et européennes chargées de lutter contre les activités illégales liées au secteur des crypto-actifs.

PROPOSITION n°16 : Sensibiliser davantage les citoyens à l'augmentation des risques liés à la multiplication des *ransomwares*.

II. Réduire l'impact écologique et la consommation énergétique des crypto-actifs par l'interdiction progressive des protocoles dits « *proof of work* »

Un dernier élément apparaît comme nécessitant une action forte du législateur : l'impact écologique désastreux de certains crypto-actifs. En effet, si la nouvelle génération de crypto-actifs utilise essentiellement des protocoles dits de "preuves d'enjeux", beaucoup moins énergivores que les protocoles de "preuve de travail" (voir encadré du I.A de la première partie), le poids toujours considérable d'un certain nombre de crypto-actifs utilisant encore la preuve de travail apparaît foncièrement incompatible avec l'exigence de sobriété énergétique et, plus largement, d'atteinte de la neutralité carbone puisque le minage de ces crypto-actifs consomme une énergie considérable, qui plus est souvent générée grâce à l'utilisation de ressources fossiles.

⁹⁶ <https://www.economie.gouv.fr/files/2021-05/tracfin-2021-2023.pdf>

⁹⁷ https://www.economie.gouv.fr/files/2021-07/RA_TRACFIN_2020_VDEF_0.pdf?v=1626430833

A/ La consommation électrique du minage

La consommation électrique du minage des réseaux fonctionnant en utilisant le protocole de *Preuve de travail* basé sur un concours de calcul est énorme, et personne aujourd'hui ne le conteste. La consommation totale d'électricité des mineurs du réseau Bitcoin est estimée à au moins 50 TWh/an par le site spécialisé de l'université de Cambridge en novembre 2022⁹⁸. Cette évaluation est en accord pour l'ordre de grandeur avec celle du site spécialisé Digiconomist qui indique lui un minimum de 75 TWh/an⁹⁹, et avec d'autres calculs publiés et explicités en détail¹⁰⁰.

Du fait de la méthode de calcul le chiffre de 50 TWh/an est un minimum absolu qu'il faut doubler pour avoir une estimation plus vraisemblable de la réalité. Sachant qu'un réacteur nucléaire moyen produit 8 TWh/an, ce que consomme le réseau Bitcoin est donc l'équivalent (en novembre 2022) de la production d'au moins 6 réacteurs nucléaires et vraisemblablement du double. Notons aussi que le chiffre minimum de 50 TWh/an est celui de la production électrique d'un pays comme la Grèce (52 TWh/an en 2020). Le chiffre plus vraisemblable de 100 TWh/an est lui supérieur à la production électrique de la Belgique (80 TWh/an en 2020)¹⁰¹ et correspond à 20% de la production électrique en France. Il est impossible aujourd'hui de nier que cela pose un grave problème.

B/ L'impact écologique des crypto-actifs et l'interdiction progressive de la "preuve de travail"

L'idée est parfois évoquée qu'environ la moitié de l'électricité dépensée par le minage du bitcoin est de l'énergie renouvelable. De tels chiffres sont difficiles à établir et on ne peut par ailleurs guère faire confiance au chiffre de 59,5 % donnés par le Bitcoin Mining Concil¹⁰² car c'est une organisation de promotion du minage et qui ne publie que des chiffres partiels. Il est parfois aussi affirmé que la proportion d'énergie renouvelable utilisée pour le minage pourrait aller en s'accroissant. Il est important de noter que cela ne conduit pas à la conclusion que la dépense du minage est sans gravité. En effet, toute production électrique produit de la pollution : construction et démantèlement des usines nucléaires, même chose pour les éoliennes, les parcs de panneaux photovoltaïques, les barrages hydro-électriques, etc. Toute électricité produite engendre une pollution directe ou indirecte et devrait donc avoir une utilité

⁹⁸ <https://ccaf.io/cbeci/index>

⁹⁹ <https://digiconomist.net/bitcoin-energy-consumption>

¹⁰⁰ Voir "Au-delà du Bitcoin, Dans l'univers de la blockchain et des cryptomonnaies", Jean-Paul Delahaye, 2022

¹⁰¹ Voir : <https://www.indexmundi.com/map/?v=79&l=fr>

¹⁰² Ex. : "Q2 Bitcoin Mining Council Survey Confirms Year on Year Improvements in Sustainable Power Mix and Technological Efficiency" Bitcoin Mining Council, juillet 2022

incontestable. L'argument que l'électricité utilisée pour le minage est parfois de l'électricité sur produite, qui sans le minage serait perdue, n'est pas recevable non plus. En effet dans de telles situations cette énergie pourrait par exemple être utilisée pour produire par électrolyse de l'eau de l'hydrogène liquide ou comprimé ensuite utilisable pour faire fonctionner toutes sortes de machines¹⁰³.

Notons encore que le site Digiconomist évalue en novembre 2022 l'empreinte carbone du minage du bitcoin à 61 Mt Co2 par an¹⁰⁴. L'utilisation de la « Preuve de travail » est une sorte de piège, car une fois adoptée pour le fonctionnement d'une *blockchain* de crypto-actif, il est très difficile de la faire y renoncer puisque les mineurs s'y opposent et détiennent l'essentiel du pouvoir. Comme cela s'est produit en Chine, au Kosovo et dans l'État de New York aux États-Unis, il semblerait souhaitable d'interdire le minage, ou au moins de pénaliser fortement les crypto-actifs qui y ont recours¹⁰⁵.

PROPOSITION n°17 : Aller vers une interdiction de la production de crypto-actifs utilisant le procédé de la preuve de travail dans l'Union européenne ou pour les sociétés de droit européen. Interdire en particulier aux plateformes d'échange et aux émetteurs de crypto-actifs de distribuer de tels crypto-actifs sous peine de perdre leur agrément et leur autorisation d'exercer dans l'Union européenne.

Il convient par ailleurs de souligner que, dans son rapport d'analyse, la Commission devra évaluer des options politiques et, le cas échéant, des mesures réglementaires justifiées pour atténuer les incidences négatives sur le climat et l'environnement des technologies utilisées et, en particulier, des mécanismes de consensus. Ces mesures pourraient avoir pour effet d'inclure dans la taxonomie européenne de la finance durable les mécanismes des consensus permettant de réduire le coût environnemental de fonctionnement des *blockchains*. De plus, les CASP devront communiquer, dans leur document d'information (*whitepaper*), sur la consommation énergétique de leurs crypto-actifs, cette information devra être « publicly available, in a prominent place on their website ». Les plateformes qui admettront les crypto-actifs offerts devront rendre publique, de façon visible sur leur site internet, l'information relative à cette analyse environnementale.

C/ Sécurisation du fonctionnement du réseau

¹⁰³ <https://www.blog-ecolo.fr/production-d-hydrogene-par-electrolyse-de-l-eau.html>

¹⁰⁴ <https://digiconomist.net/bitcoin-energy-consumption>

¹⁰⁵ "Crypto : le gouvernement du Kosovo interdit le minage", Cointribune, 6 août 2022

L'argument utilisé pour défendre la consommation électrique considérable du protocole de *Preuve de travail* (utilisée par Bitcoin) est qu'il s'agit d'un moyen indispensable pour sécuriser la *blockchain* et donc les transactions qui s'y déroulent. Cet argument est maintenant contesté par une partie importante des spécialistes des *blockchains*. La MIT Technology Review a par exemple considéré que l'alternative non consommatrice d'électricité qu'est la *Preuve d'enjeu* (présentée un peu plus bas) était l'une des dix percées technologiques (« Breakthrough Technology ») de l'année 2022¹⁰⁶. Notons aussi qu'une campagne menée par Greenpeace et d'autres associations écologistes demande à propos du bitcoin et des crypto-actifs utilisant la *Preuve de travail* de « changer le programme pas le climat »¹⁰⁷.

Le protocole de *Preuve d'enjeu* existe sous des formes variées, mais aucune ne provoque une consommation électrique équivalente à celle du concours de calcul de la *Preuve de travail*. D'ailleurs lorsque le réseau Ethereum est passé de l'une à l'autre, il a été estimé que la dépense électrique du réseau a été divisée par un facteur de mille au moins, faisant alors de cette consommation électrique du réseau Ethereum quelque chose d'insensible à l'échelon mondiale¹⁰⁸.

Expliquons pourquoi le passage de la *Preuve de travail* à la *Preuve d'enjeu* provoque une économie électrique aussi importante. L'idée déjà évoquée plus haut est que le travail de calcul d'un validateur dans le cas de la *Preuve de travail* comporte deux composantes :

- (a) la validation au sens stricte : conservation du registre *blockchain*, vérification des transactions et des pages, mise en circulation des transactions et des pages, et
- (b) participation au concours de calcul qui sert à désigner lequel des validateurs va recevoir la récompense et sera chargé de proposer la prochaine page.

Or le choix du validateur peut se faire sans concours de calcul. L'idée de la *Preuve d'enjeu* est d'opérer un choix probabiliste en fonction de la somme en jetons du crypto-actif mise sous séquestre par chaque validateur souhaitant avoir sa chance d'être désigné par le protocole. Cette seconde méthode de choix ne provoque aucune dépense énergétique et donc permet l'économie des millions des rigs de minage et de leur fonctionnement qui en réalité sont la source de très loin la plus importante de consommation électrique d'un protocole fonctionnant avec la *Preuve de travail*. On peut dire que le choix par Nakamoto dans son protocole de *blockchain* d'utiliser la *Preuve de travail* procède d'une erreur, ou pour le moins d'un manque d'anticipation de ce que pouvait devenir le concours de calcul quand la valeur du bitcoin

¹⁰⁶ «Proof of stake», MIT Technology Review, 23 fév. 2022

¹⁰⁷ « Change the code not the climate », voir : <https://cleanupbitcoin.com/> ; «Climate campaign pushes Bitcoin network to drop energy-hungry code», The Verge, 29 mars 2022

¹⁰⁸ «Ethereum plonge de 99,9 % – Une excellente nouvelle apportée par le PoS», Journal du Coin, 31 octobre 2022

s'accroîtrait, engendrant une compétition féroce entre mineurs, et donc une consommation électrique déraisonnable.

L'argument principal aujourd'hui utilisé pour défendre l'utilisation de la *Preuve de travail* est qu'il sécuriserait mieux que la *Preuve d'enjeu*. Il est vrai que concevoir un bon modèle technique de fonctionnement de la *Preuve d'enjeu* est un peu plus compliqué que pour la *Preuve de travail*. Cependant, on sait aujourd'hui le faire et l'existence des plusieurs crypto-actifs très importants en capitalisation fonctionnant sans problème majeur depuis plusieurs années avec la *Preuve d'enjeu* prouve définitivement que cette méthode de sécurisation d'un réseau *blockchain* est tout à fait satisfaisante. Le passage sans le moindre problème du réseau Ethereum à la *Preuve d'enjeu* devrait clore le débat. L'obstacle à ce passage (par exemple pour Bitcoin) est que les mineurs qui détiennent une part très importante du pouvoir n'y ont pas intérêt et donc s'y opposent violemment. Ce fut l'une des difficultés pour le réseau Ethereum et elle a sans doute retardé la mise en œuvre de son basculement (appelé "*The Merge*") de la *Preuve de Travail* à la *Preuve d'enjeu* effectué le 15 septembre 2022. Le plus gênant dans ce débat est l'utilisation par le lobby du minage d'arguments absurdes allant jusqu'à prétendre que la *Preuve de travail* favorise le développement des énergies renouvelables (dont il est sous-entendu qu'elles seraient non polluantes, ce qui est faux comme nous l'avons déjà noté) alors que sans doute la moitié du minage est fait avec de l'électricité produite par du charbon et du gaz. Le comble de l'absurde est sans doute la remise en marche d'usines de production électrique fonctionnant au charbon et qui sont destinées uniquement au minage comme cela a été fait dans l'État de New York aux États Unis, État qui d'ailleurs a fini par décider d'interdire la minage utilisant des énergies fossiles¹⁰⁹.

D/ Les comparaisons avec le système bancaire traditionnel n'ont pas de sens

Pour défendre la dépense électrique de la preuve de travail, il est parfois évoqué la dépense électrique du système bancaire traditionnel¹¹⁰ qui serait bien supérieure. L'argument est absurde car ceux qui le présentent ne comptent que le minage du côté du bitcoin en oubliant les firmes comme Binance et bien d'autres qui emploient des centaines de personnes et dépensent dans leurs bureaux et avec leurs systèmes informatiques de l'électricité qu'il faudrait prendre en compte, sans parler du coût de fabrication des millions de rigs de minage, etc.

Du côté du système bancaire traditionnel, cet argument mobilise en revanche l'électricité dépensée par chaque agence bancaire, distributeur de billets, etc. Il est alors aisé de

¹⁰⁹ "New York Becomes First State to Temporarily Ban Some Crypto Mining", Gizmodo, 23 novembre 2022 (<https://gizmodo.com/new-york-crypto-crypto-mining-1849816697>)

¹¹⁰ "Bitcoin: Cryptopayments Energy Efficiency", M. Khazzaka, 20 av. 2022

démontrer que le bitcoin dépense moins que le système bancaire. Surtout, une telle comparaison n'a aucun sens du simple fait que le système bancaire est aujourd'hui utilisé quotidiennement par plusieurs milliards d'individus sur terre pour mener de véritables opérations commerciales de toutes sortes, alors que les crypto-actifs ne sont utilisés principalement que pour la spéculation et ne servent pas, loin de là, à des milliards de personnes. Ainsi, la dépense énergétique et l'impact écologique du Bitcoin ne peuvent en aucun cas être comparé, au regard des services rendus, à la dépense énergétique du système monétaire traditionnel.

Conclusion

L'écosystème des crypto-actifs, loin de se résumer à un enjeu technique, s'intègre dans un ensemble complexe de questions politiques, idéologiques, économiques et écologiques. Laisser ce domaine aux "experts" impliquerait d'abandonner la réflexion sur des enjeux qui concernent tous les citoyens, la monnaie étant l'un des fondements du lien social.

L'évolution constante des pratiques, des habitudes de consommation et d'investissement, des techniques ou encore des législations implique de surveiller et légiférer sans céder aux technophiles béats, mais également sans préjugés sur des outils qui, à la condition d'un encadrement strict, pourraient dans certains cas bien précis être utiles à la collectivité.

Pour l'heure on peine toutefois à trouver les arguments réellement décisifs qui démontreraient la plus-value sociale apportée par les cryptoactifs. Au contraire, force est de constater que l'écosystème des cryptoactifs n'apporte au mieux qu'un fac-similé du système financier et bancaire traditionnel, sans pour autant disposer des mêmes atouts, à commencer par la capacité légale de créer de la monnaie, et surtout sans aucun des garde-fous qui ont progressivement (et encore incomplètement) conduit à encadrer l'action des acteurs bancaires et financiers.

Il reviendra aux citoyens et à leurs élus de se saisir de ces enjeux pour lutter contre les dérives libertaires qui visent à détricoter le vivre-ensemble et déshabiller la puissance publique au profit d'une société atomisée où la technologie règne, seule, en maître.

Récapitulatif des propositions

Proposition n°1	Imposer une couverture totale par des fonds propres des investissements réalisés par les acteurs financiers traditionnels dans les crypto-actifs.
Proposition n°2	Accélérer l'analyse des spécificités et risques de la finance décentralisée en vue d'un encadrement approfondi des pratiques au niveau international.
Proposition n°3	Analyser la pertinence d'un système de garantie interne au secteur qui permettrait d'assurer une plus grande stabilité financière et une responsabilisation des acteurs par leurs pairs.
Proposition n°4	Accroître la coordination internationale et l'échange d'informations entre Etats pour éviter toute pratique de <i>forum shopping</i> . Mettre en place au niveau international une typologie unique ou <i>a minima</i> des orientations de régulation commune.
Proposition n°5	Soumettre les acteurs de l'écosystème des crypto-actifs à des règles de capitalisation et de garantie adaptées aux risques, et pas seulement les acteurs fournissant des services en lien avec des <i>stablecoins</i> .
Proposition n°6	Imposer aux opérateurs de nœuds d'une <i>blockchain</i> de refuser les transactions manifestement illicites sur le territoire de l'UE.
Proposition n°7	Développer des monnaies numériques de banque centrale accessibles aux citoyens et aux entreprises et permettre une transmission directe de la politique monétaire via des comptes en monnaie centrale hébergés par des acteurs bancaires publics ou privés sous contrat.
Proposition n°8	Renforcer et rendre effectives les obligations liées à la lutte contre le blanchiment et le financement du terrorisme (LCB-FT) et à la conformité.
Proposition n°9	Contrôler l'utilité sociale des crypto-actifs par l'introduction d'un visa obligatoire auprès des autorités d'enregistrement nationales ou européennes
Proposition n°10	Interdire les crypto-actifs ayant pour but avéré de protéger l'anonymat des transactions en toutes circonstances (p. ex. Monero, Dash)
Proposition n°11	Interdire transactions en crypto-actifs avec des plateformes enregistrées dans des paradis fiscaux
Proposition n°12	Généraliser l'obligation de déclarer tous comptes en crypto-actif à l'ensemble de l'UE.
Proposition n°13	Comblar les lacunes en matière fiscale et imposer les mouvements de crypto-actif à crypto-actif.
Proposition n°14	Mieux encadrer le lobbying des acteurs des crypto-actifs en Europe.
Proposition n°15	Renforcer les moyens juridiques, humains, financiers et la coordination des autorités nationales et européennes chargées de lutter contre les activités illégales liées au secteur des crypto-actifs.

Proposition n°16	Sensibiliser davantage les citoyens à l'augmentation des risques liés à la multiplication des <i>ransomwares</i> .
Proposition n°17	Aller vers une interdiction de la production de crypto-actifs utilisant le procédé de la preuve de travail dans l'Union européenne ou pour les sociétés de droit européen. Interdire en particulier aux plateformes d'échange et aux émetteurs de crypto-actifs de distribuer de tels crypto-actifs sous peine de perdre leur agrément et leur autorisation d'exercer dans l'Union européenne.

Glossaire

Terme	Définition
<i>Asset-referenced token (ART)</i>	Catégorie de <i>stablecoin</i> adossé à plusieurs monnaies ayant cours légal ou à d'autres types d'actifs et qui a vocation à maintenir une valeur stable vis-à-vis de ceux-ci.
“Bac à sable” réglementaire (regulatory sandbox)	Cadres concrets qui, en fournissant un contexte structuré pour l'expérimentation, permettent, le cas échéant, dans un environnement réel, de tester des technologies, des produits, des services ou des approches innovants pendant une durée limitée et dans une partie restreinte d'un secteur ou d'un domaine soumis à une supervision réglementaire garantissant la mise en place de garanties appropriées.
<i>Blockchain</i> ou <i>distributed ledger technology (DLT)</i> ; dispositif d'enregistrement électronique partagé (DEEP)	Technologie de registre distribué sécurisé par un système cryptographique d'horodatage et disposant d'un mécanisme de consensus permettant l'enregistrement et la validation d'informations par lots séparés mais reliés entre eux, appelés blocs.
Cours légal	Concept juridique qui définit un moyen de paiement qui ne peut généralement être refusé comme paiement, à sa valeur nominale, avec effet libératoire. Le cours légal s'applique en UE aux pièces et billets en euro.
Cryptographie	Techniques et algorithmes qui peuvent être appliqués aux données pour garantir des objectifs tels que la confidentialité, l'intégrité des données ou l'authentification sécurisée.
Crypto-actif (<i>crypto-asset</i>) ou actif numérique	Actif enregistré sous forme numérique qui représente une valeur ou un droit et qui peut être transféré et stocké en utilisant une <i>blockchain</i> .
Crypto-actif stable (<i>stablecoin</i>)	Catégorie de crypto-actif qui a vocation à maintenir une valeur stable vis-à-vis d'un actif réel grâce à un ensemble d'outils de stabilisation (financier ou algorithmique).
Effet de levier	L'effet de levier est une technique qui consiste à s'endetter pour augmenter sa capacité d'investissement.
Instruments financiers numériques (<i>security tokens</i>)	Instruments financiers qui circulent sur une <i>blockchain</i> .

Jeton d'usage (<i>utility token</i>)	Catégorie de crypto-actif émis lors des opérations de financement de projet (ICO), et dont la principale fonction est de permettre l'accès futur à un service ou à un produit proposé par l'émetteur de cet actif.
Jeton de monnaie électronique (e-money token – EMT)	Catégorie de <i>stablecoin</i> adossé à une seule monnaie ayant cours légal et qui a vocation à maintenir une valeur stable vis-à-vis de celle-ci.
Jetons non fongibles (non-fungible tokens – NFT)	Catégorie de crypto-actif uniques et non fongibles.
Mineur	Ordinateur cherchant à être le premier à trouver un nombre aléatoire lui offrant le droit d'ajouter un bloc de transactions dans une <i>blockchain</i> fonctionnant avec un consensus par preuve de preuve de travail.
Monnaie centrale	Engagements d'une banque centrale, sous forme de billets ou de dépôts bancaires détenus auprès d'une banque centrale, qui peuvent être utilisés à des fins de règlement.
Monnaie commerciale (secondaire)	Engagements des banques commerciales qui prennent la forme de dépôts de particuliers détenus auprès d'une banque commerciale et qui peuvent être utilisés à des fins de règlement.
MNBC de détail (<i>retail CBDC</i>)	Actif émis par une banque centrale sous forme numérique et destiné à être utilisé par le grand public (ex., les citoyens, les entreprises et les entités gouvernementales) pour leurs paiements de détail.
MNBC interbancaire ou de gros (<i>wholesale CBDC</i>)	Actif émis par une banque centrale sous forme numérique et destiné à être utilisé par des entités spécifiques pour leurs paiements de gros montant dans les infrastructures financières.

Offre au public de jetons (<i>Initial Coin Offering - ICO</i>)	Opération de levée de fonds par laquelle une émet des jetons auxquels les investisseurs souscrivent principalement avec d'autres crypto-actifs.
Portefeuille numérique (<i>digital wallet</i>)	Service auquel on accède numériquement et qui permet à l'utilisateur d'accéder et de gérer des actifs numériques en toute sécurité.
Prestataire de service sur crypto-actifs (PSAN, <i>crypto-asset service provider – CASP</i>)	Entités fournissant un ou plusieurs services en relation avec des crypto-actifs à des tiers sur une base professionnelle et agréés en tant que tels. Les services sont la conservation et l'administration de crypto-actifs pour le compte de tiers ; la gestion de plateformes de négociation pour crypto-actifs ; l'échange de crypto-actifs, soit contre des fonds en monnaie officielle, soit contre d'autres crypto-actifs ou encore les services de conseil et de gestion de portefeuille en crypto-actifs.
Preuve d'Autorité (Proof of Authority)	Mécanisme de validation d'une <i>blockchain</i> dans lequel chaque participant est identifié, permettant ainsi d'accorder une voix équivalente par participant.
Preuve d'enjeu (Proof of Stake)	Mécanisme de validation d'une <i>blockchain</i> dans lequel s'opère un choix probabiliste en fonction de la somme en jetons du crypto-actif mise sous séquestre par chaque validateur souhaitant avoir sa chance d'être désigné par le protocole.
Preuve de travail (Proof of Work)	Mécanisme de validation d'une <i>blockchain</i> dans lequel l'ordinateur qui validera les prochaines transactions est celui qui est le premier à découvrir un nombre aléatoire.

