

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Monnaies, banques et finance : vers une nouvelle ère crypto

Un enjeu de souveraineté et de compétitivité économique, financière et monétaire

Rapport personnel faisant suite au rapport relatif aux monnaies virtuelles

M. Pierre PERSON, député de Paris.

Remerciements liminaires :

À mon équipe parlementaire, sans qui ce mandat au service de nos concitoyens, n'aurait pu être aussi intense et complet.

*À **Nathan Brouet** qui, avec talent et agilité, a su découvrir la complexité du sujet afin de m'épauler dans la construction de ce rapport.*

*À **Claire Le Deuff** et **Mélodie Ambroise** qui ont tant œuvré lors du premier tome.*

*Et à **Victor Lailler, Simon Pecnard, Alexandre Le Bars, Hugo Barbazanges, Lucas Cherfils, Antoine Richard, Paul Hugo-Verdin et Ambroise Méjean** pour leur accompagnement sans faille dans cette aventure.*

AVANT-PROPOS

#DEFI is the Future of France (or NOT)

La nouvelle ère financière qui s'ouvre transformera irrémédiablement notre ordre monétaire et économique mondial. Plus que jamais, derrière la course technologique à l'innovation financière se jouent les rapports de force monétaires de demain. Par essence, l'Europe joue sa place dans le monde du XXI^{ème} siècle, ainsi que sa capacité à faire valoir sa future souveraineté étatique. À vouloir réguler des acteurs économiques qui n'existent pas ou qu'elle n'a pas su créer sur son territoire, l'Europe aura toutes les chances de rester à quai et de subir la domination des géants américains et chinois.

Le premier rapport fut celui du tâtonnement avec l'absolue volonté de ne pas définir la technologie exagérément, le souhait d'être humble face à l'innovation et à la création humaine, sans présumer de ce que pouvait être l'avenir technologique. Ce second volet sera empreint d'une plus grande gravité tant les enjeux présents et immédiatement à venir sont conséquents. Nos choix auront des impacts forts et durables. Ils sont à faire sans attendre. En 2025, il sera déjà trop tard.

L'approche initiale était une approche de modestie face au futur et au progrès. Combien de politiques, de chercheurs et d'intellectuels se sont entêtés et parfois même ridiculisés à vouloir dire ce que serait le futur technologique - en sélectionnant les projets et en décidant de leur droit de cité, au lieu de créer les conditions de leur développement. Nos échecs actuels en la matière, nous les devons à une absence de politiques visionnaires ainsi qu'à l'action de technocrates zélés qui ne vivent que dans le monde de la norme, censé contrer le risque.

Si politiquement, je suis un fervent pourfendeur de l'approche pragmatique, approche qui tend à résumer l'action politique comme uniforme et basée sur un empirisme de circonstance, je n'ai jamais souhaité projeter mes rêves et mon désir d'idéologie sur cette technologie balbutiante. Bien conscient des nouveaux usages qu'elle permet d'entrevoir, j'ai souhaité partir de la matière ainsi que de son objet et jamais y accoler une vision personnelle qui aurait pu constituer un biais de lecture. Tout débat sur la nature de l'objet, sur sa définition, aurait été stérile en 2018. La nature de l'objet s'imposera d'elle-même lors de sa pleine maturité, si cela devait intervenir.

La technologie n'a pas, intrinsèquement, d'appartenance politique. Seuls les usages et la façon dont elle est réglementée conduisent à colorer cette dernière. La blockchain n'y déroge pas. Ainsi, il est possible d'être étatiste, fervent défenseur de la souveraineté de l'État Nation, et défenseur des MNBC (monnaie numérique de banque centrale) ou, à l'inverse, d'être un libertarien, fervent Bitcoiner maximaliste, héraut de la décentralisation bancaire. Le moment venu, lorsque les usages seront matures, il sera temps de prendre position collectivement et de préciser comment les usages issus de cette technologie devront être régulés. Toutefois, ce ne pourra être qu'au terme de leurs développements et de leur démocratisation. Réguler TCP/IP n'aurait eu aucun sens, réguler la technologie blockchain en elle-même est à la fois une erreur et un objectif illusoire.

En 2018, personne n'aurait pu présager les évolutions d'un secteur qui ne laissait voir en surface que de simples promesses sur des projets bien souvent bancals, à travers notamment les ICO (*Initial Coin Offering*). Initialement qualifiés de crypto-monnaies puis de crypto-actifs pour mieux correspondre à leurs aspects polymorphes, les jetons, indissociables de la blockchain, sont aujourd'hui plus que jamais pluriels. D'ores et déjà, nous pouvons dire que les définitions d'hier sont obsolètes. En 2022, se créent, sous nos yeux, les futurs actifs qui permettront demain le financement de l'économie réelle, le développement des places de marchés décentralisées plus accessibles et plus transparentes, l'émergence des nouvelles monnaies centrales et des banques commerciales autonomes.

La finance sera directement 3.0. Pas simplement numérique, car elle l'est déjà, mais décentralisée avec tous les défis, les risques et les opportunités que cela pourra engendrer. Toutefois, si « l'imagination est un avant-goût de ce que la vie nous réserve », reste que la volonté politique est nécessaire. À l'heure d'écrire ces lignes, le constat est simple. Nous en manquons.

PLAN

AVANT-PROPOS	2
PARTIE I - La décentralisation financière, une nouvelle donne en matière de régulation	9
I. Au-delà du monopole bancaire, le triomphe du pair-à-pair	10
II. Le concept de crypto-actif, une définition déjà dépassée	11
III. Une régulation encore balbutiante	12
1. Le développement de la réglementation des crypto-actifs à travers le monde	12
2. L'avenir de la réglementation française	16
a. L'évolution du régime juridique relatif aux PSAN	17
b. La question persistante du droit au compte	19
c. Le nécessaire approfondissement de la fiscalité	24
IV. Le nécessaire changement de paradigme	30
1. Une autre conception de la réglementation	30
2. Les crypto-actifs, source de nouveaux enjeux géopolitiques	33
PARTIE II - Un nouveau rapport à la valeur	36
I. Bitcoin, l'ère de l'institutionnalisation et de la maturité	36
1. L'évolution financière du bitcoin	36
a. Les raisons exogènes et endogènes à la croissance du cours du bitcoin	37
b. L'émergence d'un phénomène d'institutionnalisation du bitcoin	41
i. Les différents aspects de l'institutionnalisation du bitcoin	42
ii. L'impact de l'institutionnalisation sur le bitcoin	48
2. Un crypto-actif aux sous-jacents protéiformes	52
a. Un crypto-actif associé à un réseau mondial	53
b. Un crypto-actif évolutif malgré lui	54
c. Un crypto-actif soumis à un coût de production	55
d. Un crypto-actif concurrencé	55
3. La valorisation extrinsèque de bitcoin, résultante de la parole d'Évangile selon Satoshi	56
a. Bitcoin, un actif financier	57
b. Bitcoin, une réserve de valeur	58
4. La place de Bitcoin dans la lutte contre le réchauffement climatique	65
a. Une consommation énergétique fortement critiquée	65
b. La consommation énergétique du réseau Bitcoin, un élément consubstantiel de sa valeur	67

i.	L'électricité : la ressource clé des mineurs	69
ii.	Une ressource aux origines diverses	70
c.	Bitcoin, un nouvel instrument au service de la transition écologique	72
i.	Un verdissement de l'activité de minage	73
ii.	Une consommation excessive, mais relativement à quoi ?	76
II.	Au-delà de Bitcoin, de nouvelles formes de <i>tokens</i>	80
1.	L'essor des NFT, entre euphorie et révolution	81
a.	Un nouveau standard technologique encore limité au monde de la culture	81
i.	Définition du jeton non fongible et caractéristiques	81
ii.	Au-delà de la mode, l'apparition des premiers cas d'usage	83
b.	Les enjeux liés au développement des NFT	85
i.	De nouveaux objets numériques au potentiel disruptif	86
ii.	De nouveaux objets source d'interrogations réglementaires	88
2.	L'émergence de nouveaux modes de financement tokenisés	93
a.	L'évolution des <i>security tokens</i> , de 2017 à aujourd'hui	94
i.	Notion et caractéristiques	94
ii.	Un développement encore limité et principalement tourné vers la finance	96
b.	Enjeux	100
i.	Une innovation technique aux potentiels multiples	100
ii.	La nécessité d'une réglementation adaptée	102
	PARTIE III - Souveraineté monétaire : entre rupture et continuité	105
I.	La qualification controversée de Bitcoin comme monnaie	108
II.	Les <i>stablecoins</i> , une représentation de la monnaie étatique dans le monde numérique	110
1.	Brève définition	111
2.	Les <i>stablecoins</i> dans le paysage des crypto-actifs	111
a.	Le <i>stablecoin</i> , un crypto-actif spécifique	112
b.	Diversification progressive du marché des <i>stablecoins</i>	114
3.	Typologie des <i>stablecoins</i>	115
a.	Caractéristiques générales des <i>stablecoins</i>	115
b.	<i>Stablecoins</i> adossés à des actifs <i>off-chain</i>	118
c.	<i>Stablecoins</i> adossés à des actifs <i>on-chain</i>	118
d.	<i>Stablecoins</i> algorithmiques	120
4.	Les <i>stablecoins</i> , un objet technologique aux nombreux enjeux	122
III.	La tokenisation de la monnaie : l'émergence des monnaies numériques de banque centrale	127
1.	Brève introduction	127

a.	Un outil monétaire entre la devise officielle et le crypto-actif	128
b.	Une grande diversité de MNBC	130
2.	Les différents projets de MNBC à travers le monde	132
a.	La première MNBC de détail : le Sand Dollar des Bahamas	132
b.	Le paiement transfrontalier tokenisé : la MNBC de gros de Hong Kong et de la Thaïlande	133
c.	L'émergence précipitée du yuan numérique	134
3.	Le positionnement de l'Europe : entre défiance et tâtonnements	138
a.	Les expérimentations de la Banque de France	138
b.	L'émission d'un euro numérique, entre sauvegarde de la souveraineté et nécessaire modernisation de l'outil monétaire	140
i.	Première fonction : offrir de nouvelles opportunités technologiques et économiques aux entreprises et citoyens européens	141
ii.	Deuxième fonction : renforcer la souveraineté monétaire de l'Union européenne et créer les ponts vers la finance crypto	147
iii.	Troisième fonction : moderniser les politiques publiques avec de nouveaux outils plus performants	149
	PARTIE IV - La finance numérique de demain	154
I.	La finance décentralisée, un nouveau modèle	154
1.	Notion et enjeux	154
2.	Un secteur encore émergent	156
3.	Un secteur particulièrement varié et innovant	159
a.	Les plateformes d'échanges décentralisées	159
i.	Notion de plateforme d'échanges décentralisée	159
ii.	Fonctionnement	161
b.	Les protocoles de prêt décentralisés	165
i.	Notion de protocole de prêt décentralisé	165
ii.	Fonctionnement	168
c.	L'optimisation automatisée des rendements	171
d.	Les actifs synthétiques	172
e.	L'assurance décentralisée	174
f.	Les protocoles d'infrastructure de données	177
i.	Les oracles, passerelle entre le monde physique et le monde virtuel	177
ii.	Le stockage décentralisé, outil de démocratisation des données	179
II.	La place de la finance décentralisée dans le système financier traditionnel	181
1.	Les apports de la blockchain à la finance	181
2.	La nécessaire rencontre de la finance traditionnelle et de la finance décentralisée	186

III. La DAO, une nouvelle forme de gouvernance	189
1. Principe et fonctionnement	189
2. Enjeux	192
Synthèse des propositions	195
Droit au compte	195
Fiscalité	195
Crypto-actifs et climat	196
Jetons non fongibles (NFT)	196
Souveraineté monétaire	196
Finance décentralisée	197
Remerciements	198
Abréviations	201
Glossaire relatifs aux crypto-actifs	202

PARTIE I - La décentralisation financière, une nouvelle donne en matière de régulation

La « crypto », comme désignée par ses pairs, s'est érigée sur une promesse politique. Celle d'une société totalement décentralisée permettant à l'individu de sortir des carcans, des titres et des statuts. Fondée sur une logique quasi-libertarienne, ses premiers inventeurs, génies parfois fantasques, ont très souvent critiqué l'organisation d'un pouvoir étatique centralisé, quitte parfois à le diaboliser. Depuis 2010, cet écosystème a considérablement évolué. Les possibilités offertes par cette nouvelle technologie ont dépassé sa vocation politique première et ont attiré des entrepreneurs à travers le monde, convaincu à leur tour de pouvoir changer le monde.

Face à l'émergence d'un nouveau secteur, les États tentent tant bien que mal de réglementer ces nouveaux usages et d'établir un cadre légal. Or, si la réglementation est nécessaire afin d'accélérer l'adoption des crypto-actifs, les approches des législateurs et régulateurs sont très hétérogènes selon les pays.

Quoiqu'il en soit, les technologies blockchain et « crypto » représentent un tournant majeur pour l'Humanité. Elles permettent à chacun de détenir son argent en compte propre, c'est-à-dire personnellement, sans avoir à recourir à un tiers et de manière sécurisée. Ces usages, aujourd'hui limités au domaine financier, se développeront et irrigueront toute la société. Il est donc primordial de développer une réglementation permettant d'encadrer les abus sans en restreindre la démocratisation. Or, le caractère décentralisé et totalement novateur de cet écosystème implique d'appréhender avec un regard neuf les approches réglementaires afin d'adapter les règles en vigueur. Cette nécessaire agilité ne peut se faire sans une réflexion de fond.

Il faut donc concevoir un nouveau paradigme réglementaire, adapté et compétitif. Cette nouvelle réglementation doit d'abord se construire sur la base de faits, sur la réalité de l'écosystème, de ses usages et de ses outils techniques, non sur des dogmes préétablis qui protègent davantage les acteurs en place et leurs rentes que les citoyens. Elle devra également se concentrer sur les cas d'usage davantage que sur la technologie en tant que telle. Depuis les années 1990, personne n'a souhaité réglementer les systèmes TCP/IP pour Internet ou SMTP pour les courriers informatiques. Dès lors, il faut comprendre ici que ce n'est pas le réseau Bitcoin ou le réseau Ethereum qu'il faut réglementer, mais bien les usages qui les accompagnent. De la même manière, il serait illogique de réglementer des standards

technologiques comme les NFT sans savoir comment ils seront utilisés à l'avenir. Il faut donc abandonner tout réflexe de transposition des réglementations existantes (notamment bancaires et financières) et appliquées à des acteurs centralisés. Il est utile de s'en inspirer évidemment, mais en les adaptant à des usages qui n'impliquent aucun tiers. L'exemple le plus marquant est celui du virement de personne à personne : alors qu'il implique une multitude d'acteurs dans le système actuel (banques et intermédiaires de paiements), il s'agit d'une simple opération immuable et authentifiée entre deux individus sur la blockchain.

À l'écriture de ces lignes, cette démarche de réflexion ne semble pas engagée en Europe. Pire, le législateur européen a cédé à la facilité en considérant, sans avoir approfondi ses connaissances de l'écosystème. Cette démarche mènera au déclin du secteur en Europe et à la domination des GAFAM de la finance, venus des États-Unis ou de Chine avec le risque pour le Vieux Continent d'être à nouveau relégué au rang de simple marché passif.

I. Au-delà du monopole bancaire, le triomphe du pair-à-pair

Les crypto-actifs sont indissociables de la technologie blockchain. Pour résumer simplement, la blockchain est un livre de compte partagé au niveau mondial, accessible par chacun et contrôlé - et sécurisé - de différentes manières par les individus présents sur le réseau. Les principaux rouages de ce réseau sont les crypto-actifs, qui assurent le transfert d'information - et de valeur - entre les différents utilisateurs. Les crypto-actifs sont en réalité des jetons purement numériques. Or, derrière la forme que revêt le jeton, les caractéristiques de ce dernier sont très différentes selon les réseaux et sont déterminées dès leur origine. Demain, ils constitueront la sous-couche économique et technologique du Web 3.0.

Si usuellement, cette technologie est considérée comme étant un profond changement de paradigme, c'est parce qu'elle induit une révolution qui permet de détenir, soi-même, ses propres actifs de manière sécurisée sans l'intervention d'un tiers dépositaire. Nul besoin de confier son argent à une banque afin de le sécuriser, sur laquelle le client ne détient plus qu'une créance - et non réellement ce qui est affiché sur le compte bancaire.

Ainsi, les crypto-actifs offrent la possibilité de créer de la rareté dans un monde digital où tout est copiable et centralisé. Appuyés sur ce qu'on appelle communément des contrats intelligents (*smart-contract*), les crypto-actifs permettent

de créer des mécanismes complexes décentralisés, ouvrant la voie à de nouvelles pratiques et à de nouveaux usages.

Demain, les citoyens posséderont directement leurs propres liquidités - mais aussi leurs actions, leurs comptes épargnes, etc. - dans leur poche (virtuelle) et tout cela sera mobilisable beaucoup plus facilement pour (i) consommer en ligne, (ii) investir à travers le monde, ou (iii) épargner sur des plateformes décentralisées. La suppression des tiers de confiance rendra les dispositifs les mécanismes d'investissement ou de prêt/emprunt plus profitables et plus transparents.

II. Le concept de crypto-actif, une définition déjà dépassée

À l'origine, les « crypto » étaient appelées « crypto-monnaies ». Cette formule est, encore aujourd'hui, parfois utilisée dans le langage courant. Toutefois, dès 2018, les économistes ont refusé de considérer ces nouveaux objets comme des monnaies. Ainsi, au terme de « crypto-monnaie » a été préféré le terme de « crypto-actif ». Ce terme a d'ailleurs été consacré par le législateur lorsque, au moment du vote de la loi Pacte, ces objets numériques ont été définis comme étant des « actifs numériques ».

Toutefois, si en 2018, le législateur avait souhaité écarter la question monétaire et créer une catégorie juridique *sui generis* intitulé afin de les différencier des actifs traditionnels, cette distinction a déjà atteint ses limites. Plus encore, elle paraît aujourd'hui obsolète. Avec l'incessante innovation qui accompagne cette technologie, la notion de crypto-actif est devenue hétérogène, regroupant des réalités très diverses. Ainsi, la définition légale qui en découle, précédemment évoquée, est devenue floue. Elle incorpore en son sein un nombre d'objets dont les propriétés rendent la qualification contestable au regard de la définition originelle.

Alors, le « crypto-actif » peut revêtir plusieurs caractéristiques et usages différents, parfois même de manière cumulative : (i) il peut avoir la qualité d'une monnaie, en étant un moyen d'échange volatile (comme le bitcoin) ou stable (comme un *stablecoin* qui est un crypto-actif ayant la valeur d'une monnaie traditionnelle) ; (ii) il peut avoir la qualité d'un actif financier, c'est-à-dire une représentation de la performance d'une entreprise ou un instrument financier traditionnel transposé dans le monde numérique ; (iii) il peut avoir la qualité d'un jeton utilitaire, c'est-à-dire un jeton représentant des droits sur un service futur, une créance sur une entreprise dans le développement de son futur produit ; enfin (iv) il peut être cet objet protéiforme qu'est le NFT, qui constitue une enveloppe technologique permettant de créer la

rareté en rendant numériquement une chose (qu'il s'agisse de biens matériels ou immatériels, de droits, etc.) totalement unique.

Or, la question de la définition de l'objet est essentielle, en ce qu'elle permet ensuite d'en déduire la qualification juridique et, donc, la réglementation associée. Ainsi, on le comprend aisément, une épée virtuelle dans un jeu vidéo (sous forme de NFT) ne peut être régulée comme un instrument financier (actif numérique), tout comme un instrument financier ne doit pas être régulé comme de la monnaie numérique (*stablecoin*). Pourtant, aujourd'hui, la confusion entre ces différents objets complexes peut conduire à des situations incohérentes.

Cela est développé tout au long de ce rapport, l'enjeu auquel fait face le législateur et le régulateur découle principalement de l'aspect protéiforme des « crypto » et de leurs futurs usages qui restent difficiles à appréhender.

III. Une régulation encore balbutiante

La réglementation des crypto-actifs est disparate. Initialement nationale, elle tend à s'harmoniser à l'échelle internationale.

1. Le développement de la réglementation des crypto-actifs à travers le monde

La réglementation des crypto-actifs vit ses balbutiements. Pour autant, les prémices de cette future réglementation sont extrêmement disparates. Si certains pays ont affirmé dès 2018 vouloir interdire l'usage et le minage de crypto-actifs, d'autres ont au contraire pris le contrepied et ont accueilli les produits de cette nouvelle technologie à bras ouvert.

Si le crypto-actif est un nouvel objet numérique complexe et par essence d'envergure mondiale, ce sont pourtant les régulateurs nationaux qui s'en sont saisis les premiers. Par leurs implications, notamment financières, les crypto-actifs ont immédiatement attiré l'attention des autorités. Désireuses d'éviter tout risque de déstabilisation financière potentiellement systémique, les autorités nationales ont assujéti les crypto-actifs présentant des caractéristiques ou des usages semblables aux instruments financiers à la réglementation afférente.

Dès 2017, les États-Unis ont été les plus radicaux. La jurisprudence américaine a adopté une position extrêmement stricte reposant sur le test de Howey.

Ainsi, dans le cadre de jetons émis lors d'une *Initial Coin Offering* (ICO), la Securities and Exchanges Commission (SEC) a analysé la qualification juridique des jetons en application de la jurisprudence de la Cour suprême des États-Unis du 27 mai 1946, dite « *Securities and Exchanges Commission v. W.J. Howey Co* ». Ce test permet par analogie de catégoriser les crypto-actifs selon que ces derniers présentent, ou non, un caractère financier. Si tel est le cas, ils sont alors soumis à la réglementation afférente aux instruments financiers. Cette jurisprudence a conduit à une application extensive de la réglementation financière aux crypto-actifs qui, pour une part non négligeable, étaient alors assimilés à des instruments financiers, dits « *securities* ».

Avec le temps et la démocratisation de ces nouveaux objets, les régulateurs ont peu à peu appréhendé l'aspect protéiforme de ce nouvel écosystème afin de faire correspondre la réglementation à leurs vrais usages. Diverses réglementations se sont fait jour, portant sur des aspects aussi variés que la réglementation bancaire en lien avec la détention des jetons ou encore la publicité pour l'achat de crypto-actifs avec l'encadrement des influenceurs en Espagne¹. Toutefois, cette régulation progressive ne s'est pas développée de manière homogène sur l'ensemble du globe.

Chaque régulateur national a adopté des normes selon ses intérêts ou bien selon la conception politique que les dirigeants locaux se faisaient des crypto-actifs. L'exemple le plus éloquent est évidemment la réglementation adoptée par le Salvador, qui a reconnu légalement le bitcoin comme une monnaie. Au-delà d'un coup de communication, cette reconnaissance avait vocation à fournir à la diaspora salvadorienne une alternative aux institutions financières traditionnelles qui appliquent des frais prohibitifs aux transferts de fonds vers le pays.

Autre exemple, profitant du bannissement des mineurs de crypto-actifs de Chine, le Kazakhstan a adopté une réglementation favorable aux crypto-actifs afin d'attirer les mineurs vers ses centrales à charbon et ses centrales hydroélectriques. Plus récemment, afin de faire face aux sanctions occidentales, conséquence de l'invasion de l'Ukraine par la Russie, la banque centrale russe a autorisé la plus importante banque commerciale du pays à émettre et recevoir des crypto-actifs². À l'inverse, d'autres pays ont adopté une posture plutôt hostile à l'égard des crypto-actifs, comme l'Inde ou l'Iran - bien que ce dernier pays les utilise pour contourner partiellement les sanctions américaines.

¹ Cryptoast - [L'Espagne instaure des règles pour les influenceurs faisant la promotion des cryptomonnaies](#) - 17.01.2022

² Cryptoast - [Russie : la Banque centrale autorise la Sberbank à émettre des actifs numériques](#) - 18.03.2022

Conscient que les enjeux sont intrinsèquement de nature globale, la réglementation converge pour définir trois blocs de pays distincts.

Le premier bloc est celui des États-Unis. Tout comme lors de l'avènement d'internet, le gouvernement américain, toutes couleurs politiques confondues, a adopté une posture pragmatique et pro-innovation. Leur objectif est simple : laisser une relative souplesse aux acteurs privés afin qu'ils deviennent des leaders au niveau mondial. En somme, la stratégie américaine est de reproduire le modèle des GAFAM dans ce nouvel Eldorado technologique. L'innovation étant de loin le premier moteur de la croissance outre-Atlantique, ces nouveaux géants produiront de la valeur, notamment à l'étranger, tout en conservant l'entreprise nationale dans le giron du droit américain. Cette logique a été directement énoncée dans l'*executive order* signé récemment par le président Biden. Il s'agit là d'un virage crypto-compatible à l'adresse du régulateur national avec pour seule limite, le maintien de la stabilité financière.

Le deuxième modèle de réglementation est celui mis en œuvre par l'État chinois. Ce dernier a interdit sous toutes leurs formes les crypto-actifs. En effet, approfondissant davantage sa doctrine de maîtrise totale de la donnée et de la transmission de la valeur, la Chine a proscrit tout usage de ces objets dont le projet politique originel est la décentralisation des pouvoirs et la souveraineté de l'individu. La Chine a ainsi banni les plateformes d'échanges nationales de crypto-actifs qui, pourtant, étaient parmi les plus importantes au monde en matière de volume d'échange. Le pays a également exclu tous les mineurs de crypto-actifs de son territoire. En parallèle, il souhaite néanmoins tirer profit de ces nouvelles technologies en adoptant une vision nationaliste de ces dernières. Les blockchains publiques ayant été évincées, le gouvernement chinois a développé très rapidement des applicatifs centralisés autour du yuan numérique. Celui-ci a, vraisemblablement, une double vocation : (i) renforcer la maîtrise des données relatives au paiement afin de lutter contre les mouvements de capitaux considérés comme illégaux par le régime (ii) développer une monnaie alternative au dollar pour les échanges internationaux. Cette seconde fonction n'est pas celle privilégiée officiellement par les autorités mais il s'agit évidemment d'un enjeu majeur face au rival américain. Si à terme, le yuan numérique devait s'imposer dans l'économie mondiale comme monnaie d'échange à l'instar du dollar, l'ordre monétaire international en place depuis la fin de la seconde guerre mondiale serait complètement bouleversé.

Le troisième et dernier bloc est celui représenté par l'Union européenne. Contrairement aux deux précédents, l'Union européenne n'a pas adopté de stratégie claire s'agissant des crypto-actifs. Depuis 2017, seuls quelques États membres, dont

la France, ont légiféré sur la question des crypto-actifs sans pour autant que l'ensemble soit homogène. Entre 2017 et 2022, la concurrence réglementaire mais aussi fiscale a été un levier important d'attractivité de certains États membres au détriment d'autres. Ce n'est qu'à partir de 2019 et l'annonce de *Libra* que les institutions européennes ont développé un discours au sujet des crypto-actifs.

Toutefois, il est à regretter que les postures de l'Europe soient davantage défensives que proactives face aux nouveaux enjeux. Les prises de position répétées de Christine Lagarde, présidente de la Banque centrale européenne (BCE) contre les crypto-actifs sur le volet monétaire et l'approche quasi prohibitive du projet de règlement relatif aux marchés des crypto-actifs (en anglais, dénommé MiCa pour *markets in crypto-assets*) ont contribué à teinter négativement l'approche du politique et régulateur européen. Plus récemment encore, le discours de Fabio Panetta³, membre du conseil d'administration de la BCE devant l'université de Columbia n'a pas contribué à rééquilibrer le discours de l'institution provoquant une réelle divergence entre la politique de la Fed et celle de la BCE au sujet des crypto-actifs.

Dès 2020, la BCE a communiqué dans le sens d'une interdiction absolue d'un *stablecoin* adossé à l'euro. Cette position était censée protéger la nature publique de la monnaie commune en éliminant tout acteur privé qui aurait pu devenir émetteur d'un euro sous la forme de crypto-actifs. Pourtant, cette crainte de la BCE peut être doublement contredite. D'une part, parce que le système monétaire actuel repose largement sur la monnaie émise par les banques commerciales privées. D'autre part, parce que l'émission d'un *stablecoin* n'induit pas réellement une création monétaire. En effet il s'agit uniquement d'une transposition, sous forme numérique, d'une monnaie traditionnelle en *tokens*, c'est-à-dire des devises compatibles avec la blockchain. Ainsi, la monnaie traditionnelle est placée en compte de cantonnement, qui sert en principe de garantie « un pour un » pour les *stablecoins* qui sont émis. L'opération n'est donc que purement comptable.

Ces prises de positions sont de nature à renforcer le positionnement du dollar dans cet écosystème et fragilisent la place de l'euro sur la scène monétaire internationale future. Ceci n'est pas arrangé par la volonté de la BCE d'émettre un euro numérique, qui ne pourrait voir le jour qu'à l'horizon 2024. Ces questions seront abordées plus en détail ultérieurement.

³ Euractiv - [La cryptofinance, ce château de cartes qui pourrait s'écrouler](#) - 27.04.2022

Ces sujets sont d'autant plus importants que l'Europe est le premier marché du monde en la matière. Disposant d'un marché unique de près de 450 millions d'habitants, parmi les plus éduqués et les plus riches au monde, le Vieux Continent représente 25% de l'économie mondiale du secteur selon Chainalysis⁴. Pourtant, l'Europe n'a pas encore réussi à imposer cette troisième voie qu'elle essaie péniblement de construire au niveau politique, entre une Chine et des États-Unis de plus en plus hégémoniques au sein de l'écosystème.

2. L'avenir de la réglementation française

La France a été l'un des pays pionniers en matière de réglementation. En effet, la première ordonnance ayant évoqué la technologie a été publiée le 29 avril 2016. L'année suivante, la première pierre d'une véritable réglementation a été posée avec la publication de l'ordonnance du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.

À l'instar de l'écosystème, la réglementation restait encore embryonnaire. Le rôle du législateur était cantonné à un rôle d'observateur attentiste. En ce sens, le Sénat avait publié, le 23 juillet 2014, un rapport d'information intitulé « La régulation à l'épreuve de l'innovation : les pouvoirs publics face au développement des monnaies virtuelles », rédigé par les sénateurs Philippe Marini et François Marc⁵. Ultérieurement, deux missions d'informations ont été ouvertes au sein de l'Assemblée nationale pour travailler sur ces questions : (i) la première portant sur les blockchain et ayant abouti à la publication, le 18 décembre 2018, d'un rapport d'information n°1501 rédigé par les députés Laure de la Raudière et Jean-Michel Mis⁶ ; (ii) la seconde portant sur les monnaies virtuelles et ayant abouti à la publication, le 1er février 2019, d'un rapport d'information n°1624 rédigé par le député Pierre Person⁷.

Ces travaux, notamment les recommandations formulées dans le cadre du rapport d'information relatif aux monnaies virtuelles, ont constitué une base pour la construction d'un régime réglementaire *ad hoc*. Élaboré dans le cadre de la loi Pacte,

⁴ Chainalysis - The 2021 Geography of Cryptocurrency Report - 10.2021

⁵ Rapport d'information n°767 (2013-2014) de MM. Philippe MARINI et François MARC, fait au nom de la commission des finances du Sénat, déposé le 23 juillet 2014

⁶ Rapport d'information déposé en application de l'article 145 du règlement en conclusion des travaux de la mission d'information commune de l'Assemblée nationale sur les chaînes de blocs (blockchains), n° 1501

⁷ Rapport d'information déposé en application de l'article 145 du règlement, par la commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale, en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles, n° 1624

ce régime légal a été complété par l'ajout d'un volet relatif à la fiscalité lors de l'examen de la loi de finances pour 2019. Les dispositions de la loi portant sur les crypto-actifs avaient ainsi pour vocation de créer un cadre légal favorable, clair et stable au développement de l'innovation en France tout en protégeant les consommateurs. Ce régime a été imaginé avec la volonté de ne pas sur-réguler afin de ne pas brider de potentielles licornes qui placeraient la France à l'avant-garde de l'Internet de la valeur.

Outre la question de la réglementation des ICO, en plein essor à l'époque des travaux législatifs, la loi Pacte s'est attachée à apporter un cadre clair aux prestataires de services sur actifs numériques (PSAN) en créant un régime d'enregistrement et d'agrément. La question du droit au compte des entreprises exerçant une activité en lien avec la blockchain et, notamment, les crypto-actifs, a également fait l'objet d'un dispositif. Dernièrement, la fiscalité sur actifs numériques a été précisée et modifiée dans le cadre des discussions budgétaires pour l'année 2022.

a. L'évolution du régime juridique relatif aux PSAN

Le régime d'enregistrement et d'agrément des prestataires de services sur actifs numériques - dit régime PSAN - a été la première réglementation au monde à apporter un cadre juridique clair pour la fourniture de ces nouveaux services. Deux exigences ont commandé au développement de ce régime : d'une part, il s'agissait d'offrir des repères et des gages de sérieux aux consommateurs dans un écosystème encore chaotique ; d'autre part, il était nécessaire d'offrir un régime suffisamment souple afin de permettre à l'écosystème français de se professionnaliser et de se développer.

Le premier apport essentiel de ce régime réside dans la création d'une définition pour les activités des prestataires sur actifs numériques. En délimitant les activités les unes par rapport aux autres, la réglementation relative aux PSAN a apporté une clarté juridique sur le traitement à donner à ces activités. Dès l'entrée en vigueur du texte, chacun des prestataires pouvait demander un enregistrement auprès de l'AMF. Cet enregistrement optionnel était accordé à la suite d'une procédure vérifiant certains éléments comme l'honorabilité et la compétence des dirigeants, ainsi que le respect de la réglementation relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Depuis l'ordonnance n°2020-1544 en date du 9 décembre 2020, la procédure d'enregistrement est devenue obligatoire pour un certain nombre de services sur crypto-actifs. À l'écriture de ces lignes, trente-six entreprises ont été enregistrées comme PSAN auprès de l'AMF. Il s'agit d'un

premier pas. Toutefois, il est nécessaire d'aller plus loin et pour ce faire de lever certains obstacles.

Il est ainsi nécessaire de simplifier l'obtention de l'enregistrement du statut PSAN. Il ne s'agira pas ici de simplifier en étant moins disant ou en réduisant les exigences nécessaires à son obtention. D'une part, car les exigences actuelles en droit français ne paraissent pas disproportionnées. D'autre part, parce qu'elles permettent à l'écosystème de se confronter aux problématiques d'un monde bancaire et financier sujet à une réglementation importante.

Il convient tout d'abord de constater que les délais des procédures et de traitement des dossiers de candidature sont trop longs. Deux raisons président à cela. D'une part, les entreprises candidates sont insuffisamment préparées. Elles font face à des difficultés pour fournir les garanties nécessaires à la mise en conformité de leur activité avec les exigences légales. Sur ce point, il importe de noter le travail de pédagogie et d'accompagnement que réalise l'Association pour le développement des actifs numériques (ADAN) auprès de certaines entreprises candidates. En outre, depuis 2018, de nombreux spécialistes, avocats et conseils, se sont formés afin de mieux accompagner leurs clients. D'autre part, l'AMF est le réceptacle d'un nombre important de demandes d'enregistrement que l'autorité ne peut traiter dans des délais raisonnables du fait d'un manque de moyens affectés à l'examen de ces dossiers. Malgré ces difficultés, l'AMF fait preuve d'une implication majeure afin d'assurer le suivi et le traitement de ces dossiers. Dans le cadre du projet de loi de finances pour 2022, le Parlement a décidé l'augmentation des moyens de l'AMF pour faire face à ses nouvelles missions. Il paraît indispensable qu'une partie de ces moyens supplémentaires soit affectée aux équipes chargées des PSAN afin de ne pas rendre inopérante cette réglementation en raison de difficultés matérielles et humaines.

Après son enregistrement PSAN auprès de l'AMF, un acteur économique peut faire le choix de solliciter un agrément. Celui-ci est optionnel et permet de certifier auprès de la clientèle un niveau élevé de conformité.

Force est de constater qu'aucun acteur économique n'est agréé à ce jour. Ceci s'explique par des délais d'enregistrement longs et coûteux résultant d'une procédure trop complexe pour l'intérêt qu'elle représente. D'autre part, la réglementation européenne MiCa imposera à horizon 2025 l'obtention du statut de « *crypto-assets services provider* » (CASP). Inspiré du régime PSAN, ce statut permettra d'obtenir une seule et même autorisation d'exercice pour l'ensemble de l'Union européenne. Il convient de préciser que la réglementation MiCa n'a pas encore adopté sa forme

finale à de l'écriture de ces lignes. En l'état, le texte paraît être insatisfaisant. En effet, les dispositions actuelles se contentent de reproduire des réglementations existantes pour des activités traditionnelles, en les transposant à un écosystème fondamentalement différent et qui, structurellement, n'a pas les mêmes référentiels technologiques. Cela est évoqué ultérieurement, ce travail de transposition brute est insuffisant. Pire encore, il pourrait être inopérant pour les acteurs étrangers et mortifères pour les acteurs européens. En réalité, c'est un changement de paradigme réglementaire qui s'impose au législateur européen.

Enfin, la France doit aller plus loin et offrir un cadre réglementaire propice au développement de nouveaux champions afin de se démarquer des autres États membres. Cet écosystème étant mondialisé, la concurrence est globale. En outre, ce phénomène est accru par la décentralisation consubstantielle à cette technologie permettant à n'importe qui d'opérer depuis n'importe où. Par conséquent, la défense de la souveraineté européenne passe par une meilleure compétitivité réglementaire et économique. Le développement de nouveaux secteurs au sein même de l'écosystème des crypto-actifs appelle de nouveaux enjeux réglementaires.

Les prochains mois devront permettre d'éclaircir le volet relatif aux NFT et à la finance décentralisée. Ces derniers n'étant pas réglementés aujourd'hui, il en résulte de nombreuses zones grises qui, d'un point de vue juridique, devront être levées à l'avenir. Mais ces deux aspects des crypto-actifs ont émergé récemment et sont encore largement immatures. On ne connaît pas encore précisément les cas d'usage qu'ils offriront demain. Il est donc urgent d'attendre afin d'observer et de comprendre. Le législateur devra mettre en œuvre une démarche constructive à l'endroit de ces nouveaux objets, fruit d'une recherche d'équilibre entre protection de l'intérêt général et compétitivité économique.

b. La question persistante du droit au compte

La situation des acteurs de cet écosystème en France est marquée par des problématiques majeures relatives à l'accès aux services bancaires de base, concernant aussi bien les particuliers que les professionnels. L'attitude des banques commerciales françaises à l'égard de l'écosystème laisse craindre un développement plus faible de ce dernier au profit d'acteurs étrangers. Et pour cause, dès l'apparition de la technologie, les banques commerciales françaises ont adopté une opposition principielle à l'égard des sociétés exerçant une activité en lien avec la technologie blockchain. Ainsi, il est coutumier que ces dernières éprouvent des difficultés pour l'ouverture d'un compte bancaire doté des services bancaires essentiels à leurs

activités.

La question du droit au compte pour les acteurs liés aux crypto-actifs est une problématique majeure et récurrente. En 2018 déjà, la difficulté et parfois même l'impossibilité d'avoir accès à un compte bancaire afin d'y assurer le simple paiement des salaires avait été soulignée par les acteurs du secteur à l'occasion de la mission d'information relative aux monnaies virtuelles. Le législateur avait alors émis une série de recommandations afin de renforcer l'inclusion bancaire des acteurs de la blockchain. Or, le rapport de suivi de la mise en oeuvre des recommandations du précédent rapport d'information⁸, daté du 1^{er} décembre 2021, présenté par le député Éric Woerth, président de la commission des finances de l'Assemblée nationale, a confirmé que ces propositions n'avaient été que partiellement reprises dans les faits.

Malgré les évolutions induites par la loi Pacte, la situation n'a pas évolué en cinq ans. Un récent rapport de l'ADAN, avance que près de trois entreprises « crypto » sur quatre ont connu de « grandes difficultés à recourir à un service bancaire, et plus précisément à une ouverture de compte »⁹. Pire encore, alors que le statut de PSAN aurait dû permettre de rassurer les acteurs bancaires sur la pratique de leurs clients et notamment sur le contrôle interne, certaines banques sont allées jusqu'à fermer discrétionnairement les comptes de sociétés qui venaient pourtant d'obtenir un enregistrement PSAN auprès de l'AMF.

Pourtant dès 2019, l'AMF et l'ACPR ont adopté le rôle de médiateur afin de trouver un compromis rassurant les banques sur les standards de contrôle et permettant aux acteurs de nouer des partenariats bancaires. Après plusieurs mois de discussions et la mise au point de plusieurs propositions¹⁰, la Fédération bancaire française (FBF) a refusé de s'associer au compte rendu de ces travaux et a souhaité conserver le *statu quo*, sans défendre d'autres propositions. Cette position de principe de la FBF pèse lourd sur un écosystème qui fait pourtant le nécessaire pour se conformer aux mêmes exigences LCB-FT que la finance traditionnelle. Plusieurs pistes, envisagées par le groupe de travail, permettaient pourtant d'assainir les relations entre ces deux secteurs.

Il convient toutefois de noter les cas spécifiques de la banque Delubac et de

⁸ Rapport d'information déposé en application de l'article 145 du règlement, par la commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale sur la mise en oeuvre des conclusions de la mission d'information relative aux crypto-actifs, n° 4753, déposé(e) le mercredi 1er décembre 2021

⁹ ADAN - [La crypto en France : structuration du secteur et adoption par le grand public](#) - 14.02.2022

¹⁰ Forum Fintech ACPR-AMF - [Compte-rendu des travaux](#) du groupe de travail sur l'accès des prestataires de services sur actifs numériques (PSAN) aux comptes bancaires et sur le fonctionnement des comptes de clients bancaires lors d'achat ou de vente d'actifs numériques - 25.03.2021

la Société Générale. Cette dernière a adopté une position d'ouverture à l'égard de la technologie et des acteurs de son écosystème notamment en créant la société Forge. Forge est spécialisée dans la fourniture de services relatifs aux *security tokens*. En parallèle, la banque accompagne également le projet *Lugh*, en partenariat avec le groupe Casino, qui distribue un *stablecoin* adossé à l'euro en partenariat avec la société Coinhouse.

Dans l'attente de cette prise de conscience, le législateur doit agir pour préserver le développement de ces nouveaux acteurs au profit de l'intérêt général. Il doit pour cela renforcer le droit au compte auquel peuvent prétendre les entreprises de ce secteur, au même titre que toute personne physique ou morale en vertu de l'article L312-1 du Code monétaire et financier. La loi Pacte avait déjà souhaité renforcer ce droit en permettant, notamment, aux acteurs enregistrés comme PSAN de faire valoir leur droit au compte auprès de l'ACPR. Or, comme le démontre le rapport d'information du président Woerth, cette faculté de saisine de l'ACPR n'a jamais été utilisée par les acteurs de l'écosystème. Pour cause, cette procédure s'est révélée être beaucoup trop longue et coûteuse pour être réellement utile.

En vertu des articles L312-23, D312-23 et D312-24 du Code monétaire et financier, l'ACPR peut être saisie par un PSAN s'étant vu refuser l'ouverture d'un compte bancaire par un établissement de crédit.

Ce refus peut être explicite, émanant d'une attestation de refus émise par l'établissement de crédit, ou implicite, faisant suite au silence de l'acteur bancaire, deux mois après la notification d'une demande d'ouverture de compte. Or, dans une majorité de situations, les banques ne justifient pas leur décision permettant le déclenchement de la procédure de droit au compte. Par conséquent, cette situation de fait impose à l'acteur économique d'attendre l'expiration du délai de deux mois. À l'expiration de ce délai, l'entreprise peut saisir l'ACPR, l'autorité ayant à son tour deux mois afin de donner suite. À l'issue de ce délai, l'ACPR peut (i) user de ses pouvoirs de contrôle et de sanction à l'encontre de l'établissement de crédit concerné et (ii) proposer à l'entreprise de se tourner vers la Banque de France afin d'entamer une procédure de droit au compte « classique ».

Intervient alors la procédure de droit commun, qui peut être utilisée par défaut, sans avoir recours à la procédure spécifique aux PSAN. Dans le délai d'un jour ouvré à partir de la réception des pièces justificatives - dont l'attestation de refus délivrée obligatoirement par la banque, la Banque de France désigne d'office une banque, qui est dans l'obligation d'ouvrir un compte de dépôt dans les trois jours suivant la réception du dossier requis.

Or, contrairement à la procédure de droit commun qui impose la fourniture d'une attestation de refus émanant de la banque, la procédure dédiée aux acteurs du secteur des crypto-actifs permet de se passer de cet acte après un silence prolongé de deux mois. Si ce délai est conséquent pour une entreprise en plein développement, *a fortiori* dans un écosystème aussi mouvant que celui de la blockchain, la possibilité de passer outre la fourniture d'une attestation est primordiale. Les acteurs bancaires dont l'obligation de nature légale est de fournir cette attestation sans délai, mettent parfois plusieurs semaines voire plusieurs mois à la remettre aux acteurs concernés. Cette problématique ne concerne pas seulement les acteurs exerçant dans les crypto-actifs mais l'ensemble des bénéficiaires potentiels du droit au compte¹¹. Il paraît donc pertinent de prévoir une nouvelle disposition permettant de réputer acquis un refus en cas de silence prolongé de la part de l'établissement bancaire. En ce sens, le Gouvernement a récemment publié un décret permettant de réputer acquis ce refus après l'expiration d'un délai de quinze jours suivant la notification de la demande d'ouverture de compte¹².

De la pratique, il est constaté l'inefficacité du dispositif prévue par la loi Pacte en 2019. En effet, les entreprises de l'écosystème des crypto-actifs sont, par nature, admissibles à recourir à la procédure de droit commun, plus rapide que la procédure qui leur est dédiée. Par conséquent, aucune d'entre elles n'a souhaité y recourir. Il serait ainsi pertinent de la supprimer au profit d'une procédure de droit commun adaptée.

Proposition 1 : Supprimer la procédure de droit au compte dédiée aux acteurs crypto au profit de la procédure de droit commun.

En parallèle, il est nécessaire de prévoir un outil efficace afin de lutter contre l'inaction volontaire des banques commerciales. En ce sens, les dispositions spécifiques aux acteurs du secteur permettent à l'ACPR de prendre des sanctions contre les établissements bancaires concernés, notamment de leur imposer une astreinte tant que le compte n'est pas ouvert. Il semble donc pertinent de prévoir, légalement, que l'ACPR contrôle et sanctionne le non-respect d'une ouverture de compte en vertu d'une procédure de droit au compte.

¹¹ Les Echos - [Compte bancaire : ce décret qui doit simplifier la vie des clients retoqués](#) - 16.02.2022

¹² Décret n° 2022-347 du 11 mars 2022 relatif à la procédure de droit au compte

Proposition 2 : Rendre systématique l'imposition d'une sanction pécuniaire, sous forme d'astreinte, lorsqu'un établissement de crédit attribué par la Banque de France en vertu du droit au compte ne se conforme pas à ses obligations.

Afin de refuser l'ouverture de comptes bancaires aux acteurs de l'écosystème, les établissements de crédit avancent que ceux-ci ne seraient pas en mesure de respecter les normes de LCB-FT. Or, dans le cadre de la procédure d'enregistrement PSAN, un travail de fond important est mené par les acteurs afin d'assurer le strict respect de ces règles et procédures. Ainsi, l'ACPR veille à l'application desdites règles avant l'octroi de l'enregistrement PSAN. Par conséquent, l'argument du secteur bancaire apparaît comme déraisonnable et le refus d'accès aux services bancaires à des acteurs qui ont pourtant reçu une validation de leur processus par les régulateurs est disproportionné. En ce sens, il semble pertinent que l'ACPR puisse user de son pouvoir de contrôle afin de s'assurer que les acteurs enregistrés comme PSAN aient accès aux services nécessaires à l'exercice et au développement de leurs activités. Ces derniers, ayant fait le choix de l'exigence face aux difficultés de nature réglementaire, ne doivent pas en outre subir une double peine. En cas de non-respect, l'ACPR devra alors user de son pouvoir de sanction et imposer une astreinte à la banque concernée.

Proposition 3 : Permettre aux acteurs enregistrés comme PSAN d'obtenir les services bancaires nécessaires à l'exercice et au développement de leurs activités. En parallèle, confier à l'ACPR la mission de contrôler la mise en œuvre régulière de ces services et, à défaut, d'imposer une mesure d'astreinte.

Au-delà de ces mesures, il est nécessaire de continuer le travail de pédagogie afin de rapprocher ces deux secteurs économiques. Aussi, sous l'égide de l'AMF et de l'ACPR, des pistes de solutions avaient été envisagées dans le cadre du groupe de travail entre le secteur bancaire et les acteurs de l'écosystème des crypto-actifs. Ces pistes ciblaient notamment la problématique relative au respect de la réglementation de LCB-FT. Ce travail doit être approfondi et doit se traduire par des lignes directrices concrètes émises par les autorités de régulation. Cette proposition apparaissait déjà dans le rapport d'information relatif aux monnaies virtuelles.

Proposition 4 : Approfondir les travaux engagés par le groupe de travail sur l'accès des PSAN aux comptes bancaires et, sur cette base, confier à l'ACPR le développement de lignes directrices à destination des établissements de crédit et des acteurs de l'écosystème des crypto-actifs.

Si la frilosité des banques françaises était compréhensible face à l'extraterritorialité des sanctions américaines en 2017, elle ne l'est plus à l'heure où les régulateurs américains envisagent les premières banques commerciales autonomes et où les premiers ETF crypto-actifs sont validés par les régulateurs. La nature de la technologie blockchain et ses applications imposent de nouveaux référentiels de LCB-FT et les lignes directrices nécessitent d'être modifiées et précisées en fonction de la technologie et de son potentiel. Toutefois la situation actuelle et l'absence de dialogue asphyxient le développement des entreprises françaises. Pire encore, elle induit la fuite des talents vers l'étranger. La bataille pour la défense de la souveraineté européenne se gagnera seulement si tous les acteurs, politiques, médiatiques, économiques, et régulateurs prennent conscience de l'enjeu. Aussi, les banques commerciales doivent-elles intégrer qu'elles ne pourront pas dresser éternellement des herses contre l'innovation alors qu'elles pourraient bénéficier elles-mêmes des apports et atouts de cette révolution.

c. Le nécessaire approfondissement de la fiscalité

La fiscalité est l'un des leviers essentiels au développement d'une industrie. Elle doit trouver un juste équilibre entre deux volontés antinomiques : la première découlant d'une volonté de justice sociale visant à imposer les gains provenant du capital, et la seconde visant à inciter fiscalement les personnes et les entreprises à se développer et à innover en France. Dès l'élection d'Emmanuel Macron en 2017, la France a adopté une posture visant à réduire la fiscalité des revenus issus du capital mobilier afin d'inciter davantage à réinvestir dans l'économie réelle. Ce postulat a ainsi profité indirectement à l'écosystème des crypto-actifs qui bénéficie, au même titre que les valeurs mobilières, de la suppression de l'impôt de solidarité sur la fortune et l'instauration de la *flat tax* - le prélèvement forfaitaire unique à 30%.

En 2019, le législateur a fait le choix d'opter pour un régime fiscal attractif et clair autour des crypto-actifs, conformément à son souhait d'accompagner cette révolution numérique de la valeur. En 2021, il s'est à nouveau intéressé à cette question. Trois axes structurent l'action nécessaire afin d'améliorer et de compléter

le régime fiscal actuel : (i) lever les incertitudes et les contraintes existantes, (ii) approfondir la logique de 2019 en assimilant davantage - et en adaptant - le régime fiscal des actifs numériques au régime des actifs traditionnels et (iii) appréhender les nouveaux usages de cet Internet de la valeur.

Ainsi le régime fiscal des actifs numériques, s'il est clair par son taux unique de 30%, ne l'a pas toujours été dans sa mise en œuvre. En effet, nombre de contribuables - ayant profité de la forte volatilité des crypto-actifs - ont craint de voir leur situation requalifiée en activité professionnelle, avec les conséquences fiscales et comptables que cela implique.

Cette requalification interviendrait en raison de l'absence de lisibilité de la notion d'activité professionnelle. En principe, l'imposition d'une cession d'actifs numériques par un particulier relève des dispositions de l'article 150 VH bis du Code général des impôts. Par exception, si la cession est considérée relever d'une activité professionnelle d'achat-revente d'actifs numériques, alors elle est imposée selon le régime applicable aux bénéfices industriels ou commerciaux (BIC). Par conséquent, les incertitudes juridiques et fiscales découlaient de l'absence de clarté des critères permettant de qualifier la nature de l'activité d'achat-revente d'actifs numériques, habituelle ou occasionnelle. En effet, pour caractériser le caractère professionnel de l'activité, la doctrine fiscale utilise (i) la fréquence des opérations caractérisant l'habitude, (ii) le montant des opérations, et (iii) les conditions d'exercice de l'activité.

Or, les deux premiers critères - les plus essentiels car les plus facilement quantifiables - ne sont pas adaptés aux crypto-actifs. D'une part, il est aisé de réaliser un grand nombre d'opérations : les coûts d'achat et de vente de crypto-actifs sont drastiquement réduits par rapport à la finance traditionnelle. Par ailleurs, il suffit d'une simple connexion internet afin d'avoir accès à toutes les places de marché. D'autre part, le marché des crypto-actifs est particulièrement volatil, ainsi est-il possible de réaliser des gains importants sans forcément être un trader professionnel. Face à la volatilité, il est fréquent de réaliser de nombreuses transactions afin de gérer de manière active ses investissements. En outre, le caractère divisible des crypto-actifs implique que chacune des transactions est constituée d'un ensemble de sous-transactions afin d'atteindre la quantité exacte de crypto-actif échangé. Ainsi, le nombre de transaction n'est pas toujours représentatif de l'activité réelle d'un trader.

La requalification représentait alors un risque réel pour des contribuables qui ont investi sur ce marché depuis plusieurs années, avant les différentes phases

haussières qui sont intervenues en 2017 et en 2020. Or, selon les spécialistes, cette épée de Damoclès qui pèse sur ces contribuables n'incite pas ces derniers à convertir leurs gains en euros, par crainte de se voir imposer au titre des BIC. Pire encore, cette incertitude fiscale a conduit, en 2020 et 2021, certains contribuables à s'exiler fiscalement dans des pays proches de la France comme le Portugal ou la Suisse. Cet exil fiscal représente une perte d'attractivité pour la France, qui se voulait pourtant être une terre d'accueil pour cet écosystème des crypto-actifs.

À l'occasion du projet de loi de finances pour 2022, le rédacteur du présent rapport a déposé un amendement visant à clarifier cette incertitude. Il a été fait le choix de transposer le régime fiscal similaire aux opérations de bourse exercées à titre professionnel, prévu à l'article 92 du CGI, à l'activité d'achat-revente d'actifs numériques exercée à titre professionnel. Ainsi, cette dernière activité serait qualifiée selon des critères davantage qualitatifs que quantitatifs et reposerait non plus sur le régime des BIC mais sur celui des bénéfices non commerciaux (BNC). L'amendement a été adopté à la suite d'un sous-amendement du Gouvernement visant à décaler l'entrée en vigueur de la disposition en 2023. L'insécurité juridique devrait donc prendre fin d'ici quelques mois.

Une autre problématique de compétitivité fiscale est prégnante pour les entrepreneurs. Elle concerne les entreprises directement impliquées dans l'écosystème des crypto-actifs. Les échanges de crypto-actifs entre professionnels sont devenus fréquents pour, notamment, (i) utiliser des applications de finance décentralisée (prêt, emprunt en crypto-actifs), (ii) utiliser un droit attaché à un jeton (gouvernance décentralisée, *staking*, etc ...), ou (iii) apporter de la liquidité sur le marché. Or, ces échanges constituent un fait générateur de l'impôt alors que, dans le même temps, les entreprises ne bénéficient d'aucune recette et que la valeur du jeton reçu peut être soumise à une forte volatilité. En parallèle, si les opérations d'échange de crypto-actifs s'avèrent souvent nécessaires pour assurer le bon développement de l'entreprise, celles-ci représentent une charge administrative et fiscale conséquente. Elles limitent ainsi les marges de manœuvre des entrepreneurs.

Ainsi, l'examen du projet de loi de finances pour 2022 a été l'occasion de présenter un amendement, déposé par le rédacteur du présent rapport, afin de faciliter les opérations des entreprises et en réduire les frictions fiscales. L'amendement avait vocation à introduire un sursis d'imposition permettant aux entreprises de reporter le paiement de l'impôt sur les revenus tirés de l'échange de crypto-actifs jusqu'à trois ans après cette opération. Cette proposition évitait ainsi à une entreprise de devoir payer un impôt pour une transaction non lucrative. Ce sursis d'imposition aurait été limité dans le temps afin de ne pas grever les finances publiques.

L'amendement n'a toutefois pas été adopté dans le projet de loi de finances pour 2022.

Proposition 5 : Instaurer un sursis d'imposition, limité à trois ans après l'opération faisant l'objet d'une imposition, pour les échanges d'actifs numériques réalisés par des entreprises et professionnels.

Outre ces corrections du régime fiscal actuel, la volonté du législateur en 2019 était de calquer le régime fiscal des crypto-actifs sur celle des actifs traditionnels. Or, il existe à ce jour des disparités majeures qui ne sauraient plus s'expliquer d'un point de vue politique et juridique. Par conséquent, il est nécessaire d'aller plus loin dans la convergence des régimes fiscaux des crypto-actifs et des actifs traditionnels.

Ainsi, une mesure de compétitivité indispensable afin de permettre le réinvestissement consisterait en l'instauration d'un régime fiscal de faveur similaire au régime de l'apport-cession prévu à l'article 150-0-B ter du Code général des impôts. Aujourd'hui, toute personne souhaitant investir dans l'économie réelle en apportant ses crypto-actifs à une entreprise est contrainte de s'acquitter de l'imposition sur la plus-value alors même qu'elle reçoit des titres en contrepartie de son apport, et non un paiement monétaire. Cette difficulté freine tout fléchage des plus-values latentes détenues par les Français en crypto-actifs vers l'économie réelle. La transposition du régime de l'apport-cession permettrait de lever ces freins en prévoyant un report d'imposition au moment de la cession des titres reçus en contrepartie de l'apport de crypto-actifs. Cette proposition, défendue lors du projet de loi de finances pour 2022, n'a pas été adoptée.

Proposition 6 : Instaurer un régime de faveur similaire au régime de l'apport-cession pour les apports d'actifs numériques à des sociétés traditionnelles.

Dans la lignée de l'extension aux crypto-actifs du régime relatif aux actifs mobiliers, plusieurs dispositifs de report des moins-values de cession sont prévus pour chaque catégorie de valeurs mobilières. Toutefois, ce régime n'existe pas pour les moins-values sur actifs numériques. Ainsi, l'extension du régime paraît être une mesure de cohérence vis-à-vis du régime global applicable à ces nouveaux actifs, largement inspiré du régime des valeurs mobilières. Il s'agirait également d'une mesure d'équité. En l'état, les investisseurs en crypto-actifs disposent de moins de

droits que les investisseurs dans des actifs traditionnels. Or, il ne s'agit pas de transposer purement et simplement le régime applicable à d'autres actifs, il faut l'adapter. Prévoir une capacité de report des moins-values sur cession jusqu'à trois ans après sa constatation permettrait de prendre en compte la réalité économique de cet écosystème et des cycles qui le caractérisent. Cette décision notable renforcerait l'attractivité de la France sur le terrain fiscal. Cette proposition, défendue au moment du projet de loi de finances pour 2022 n'a pas été adoptée.

Proposition 7 : Instaurer la possibilité, pour le contribuable, de reporter les moins-values sur cession d'actifs numériques sur les plus-values de même nature, jusqu'à trois ans après leur constatation.

Dans cet écosystème, détenir des crypto-actifs est l'expression concrète d'une conviction : le monde est en train de changer avec l'apparition d'un nouvel Internet de la valeur. Dès lors, il est fréquent que, dans les projets et entreprises du secteur, les associés et les salariés souhaitent percevoir une partie de leur rémunération en crypto-actifs. Ces attributions sont également un moyen supplémentaire de motiver les équipes avec une récompense pécuniaire supplémentaire - au format numérique. Or, contrairement aux attributions gratuites de droits sociaux (AGA notamment), les attributions gratuites d'actifs numériques (AGAN) sont soumises à différents régimes fiscaux, qui dépendent donc de la relation entre l'émetteur et le bénéficiaire. Les AGAN donnent lieu, pour le bénéficiaire, à une imposition immédiate au moment de la réception, alors que ce dernier n'a reçu aucune contrepartie permettant le paiement de cet impôt. Le bénéficiaire est donc contraint de vendre ses actifs reçus gratuitement pour se conformer à ses obligations fiscales. La création d'un cadre clair et unifié est nécessaire afin de permettre aux salariés d'entreprises spécialisées de bénéficier de cet avantage sans friction fiscale. Cela permettra également de donner un avantage certain au salariat par rapport à la collaboration libérale, favorisant la protection des personnes participant au développement de ces projets et ces entreprises. Cette proposition, défendue au moment du projet de loi de finances pour 2022 n'a pas été adoptée.

Proposition 8 : Instaurer un régime fiscal similaire au régime des attributions gratuites d'actions (AGA) aux attributions gratuites d'actifs numériques (AGAN) réalisées par une entreprise émettrice de jetons à ses salariés.

Enfin, l'attractivité de la France dépend évidemment de sa fiscalité. Cette dernière ne peut anticiper les nouveaux usages, mais elle doit s'y adapter en laissant autant de souplesse que nécessaire pour ne pas entraver les contribuables et les pousser à l'exil fiscal.

Aussi, deux questions d'avenir doivent-elles être abordées : le cas du traitement fiscal des paiements en crypto-actifs et le cas du traitement fiscal des NFT. S'agissant de cette dernière question, elle est évoquée ultérieurement, à l'occasion de l'étude relative aux NFT. S'agissant du traitement fiscal des paiements en crypto-actifs, il existe un problème majeur relatif à la contrainte déclarative. En effet, chaque paiement en crypto-actifs constitue un fait générateur de l'impôt. Ainsi, chaque contribuable qui souhaite, par exemple, acheter une baguette de pain en crypto-actifs se doit de déclarer cette transaction dans le cerfa n°2086. Cette lourdeur empêche les contribuables d'utiliser leurs crypto-actifs dans l'économie réelle. Cette situation n'est pas tenable et impose de repenser la fiscalité des paiements en crypto-actifs. Les paiements en crypto-actifs, *stablecoins* ou autres seront monnaie courante à l'avenir. Par conséquent, il convient d'ores et déjà d'imaginer les futurs régimes permettant de payer sans contrainte dans l'économie réelle.

Proposition 9 : Repenser le système fiscal et déclaratif lié aux paiements en crypto-actifs afin de lever les frictions fiscales afférentes.

Par ailleurs, une autre difficulté a émergé avec le déclenchement des premiers contrôles fiscaux. L'écosystème des crypto-actifs étant particulièrement technique, le coût d'entrée pour en comprendre toutes les subtilités est assez élevé. Par conséquent, cette technologie crée des disparités dans l'appréhension et le traitement qui leur est réservé. Ces disparités territoriales de traitement sont le plus souvent défavorables au contribuable et crée une hétérogénéité de doctrine vectrice d'insécurité juridique. Par conséquent, il pourrait être nécessaire de centraliser la gestion des dossiers relatifs aux crypto-actifs auprès d'équipes spécialisées sur la question au sein de la Direction générale des finances publiques.

Proposition 10 : Centraliser le traitement des dossiers relatifs aux crypto-actifs auprès d'équipes spécialisées au sein de la Direction générale des finances publiques.

IV. Le nécessaire changement de paradigme

Les crypto-actifs induisent un bouleversement structurel dans l'ordre monétaire et financier à l'échelle mondiale. Comparable à une nouvelle révolution industrielle des mondes financiers et bancaires, il paraît important de comprendre la dualité qu'elle impose, une profonde transformation de paradigme réglementaire et géopolitique, afin de mieux percevoir la puissance du changement à venir.

1. Une autre conception de la réglementation

La blockchain et les crypto-actifs évoluent selon des principes qui sont propres à l'économie numérique du XXI^{ème} siècle. Ils sont les fruits d'une évolution qui a commencé avec l'apparition de l'informatique et qui s'est accélérée depuis le développement d'Internet et l'interconnexion mondiale. Les sociétés contemporaines se sont adaptées à ces évolutions technologiques majeures et les réglementations ont intégré ces nouveaux systèmes et leurs enjeux afin d'apporter un cadre protecteur, garant de l'intérêt général. Ainsi, il s'agit de continuer à effectuer ce travail de compréhension et d'adaptation à l'endroit des crypto-actifs. La question ne sera pas de savoir si ces nouvelles technologies vont prospérer ou non. L'histoire récente prouve que leur démocratisation s'accroît très rapidement et qu'ils impacteront durablement les sociétés dans lesquelles ils évoluent. La réglementation doit pouvoir prendre toute la mesure de cet essor afin de permettre le développement de ces progrès technologiques tout en protégeant les citoyens de potentielles dérives.

Or, face aux modèles réglementaires traditionnels, la technologie blockchain, vectrice de décentralisation, empêche de faire peser des obligations sur des personnes nommément identifiées. Au-delà de la seule question du pseudonymat, plus la décentralisation des protocoles sera effective, plus les responsabilités seront difficiles à cerner. En l'état de la technologie, il est d'ores et déjà envisageable que l'identification de responsables soit rendue impossible, les relations étant régies par des lignes de code qui agissent de manière automatisée, sans tiers de confiance - sans intervention humaine.

La blockchain a ainsi permis l'émergence d'entités sans visage, sans dirigeant, totalement autonomes. Cet apport constitue en lui-même une révolution des rapports humains, devenant totalement horizontaux. Se pose alors une question : comment ces nouvelles entités peuvent s'intégrer dans le paysage juridique des

sociétés modernes, en parallèle ou en remplacement des structures centralisées et pyramidales ? Cette profonde révolution impose d'engager une réflexion en profondeur sur l'adaptation de la réglementation de ces nouveaux acteurs.

Cette réflexion est d'autant plus fondamentale que cette technologie est totalement programmable. Ainsi, un acteur décentralisé n'est pas nécessairement similaire à un autre. Le niveau de décentralisation peut varier en fonction des projets et des aspirations de leurs créateurs. Par conséquent, il serait simpliste de considérer qu'il existe d'une part des entités totalement décentralisées et, d'autre part, des entités entièrement centralisées. Des nuances existent. Elles dépendent des structures d'organisation de ces entités ou de ces applications. Ainsi, plusieurs éléments doivent être analysés afin de déterminer le réel niveau de décentralisation d'une entité.

L'élément prédominant est la nature de la blockchain sur laquelle l'entité ou l'application fonctionne. Il peut s'agir d'une blockchain publique, à l'image de la blockchain Bitcoin ou Ethereum. Les blockchains publiques favorisent un niveau élevé de décentralisation dans la mesure où les opérations sont validées par un nombre important de nœuds qui, à travers le monde, sont indépendants les uns des autres. À l'inverse, l'entité ou l'application peut fonctionner aussi sur une blockchain privée, dite « permissionnée ». Ce type de blockchain est généralement centralisé, dans la mesure où les nœuds chargés de valider les opérations ont été choisis et autorisés par les initiateurs de la blockchain. Contrairement à une blockchain publique dans laquelle le pouvoir de validation est diffusé entre un nombre important d'acteurs différents et dont les intérêts ne sont pas alignés, la blockchain privée concentre usuellement le pouvoir de validation entre les mains d'un nombre limité d'acteurs. Par conséquent, il n'est pas envisageable de qualifier de la même manière une structure fonctionnant sur un réseau distribué à l'échelle mondiale et une structure dirigée par quelques individus en contact les uns avec les autres.

Le second élément à analyser, plus complexe, est la nature de la gouvernance de l'entité ou de l'application. En effet, la gouvernance des entités traditionnelles - associations, sociétés, administrations - répond à une logique pyramidale depuis longtemps établie. Ce n'est toutefois pas nécessairement le cas des entités et applications fonctionnant sur blockchain. La gouvernance peut ainsi fonctionner à partir d'une organisation autonome décentralisée (« *decentralized autonomous organization* » ou *DAO*). Cette dernière prend la forme d'une organisation horizontale dans laquelle les détenteurs de jetons de gouvernance décident de

l'évolution du protocole¹³. Le niveau de décentralisation de la gouvernance dépend donc du nombre de jetons de gouvernance émis, mais surtout de la répartition de ces jetons entre les différentes personnes participant au protocole. S'ils sont trop concentrés au bénéfice d'un nombre restreint de personnes, ces dernières exercent une influence exorbitante sur l'évolution du protocole, ce qui proscrit toute décentralisation. La gouvernance peut également résulter d'une intervention directe des initiateurs du projet ou des développeurs du protocole dans l'évolution de celui-ci. Cette situation peut intervenir lorsque le protocole a adopté un mode de gouvernance centralisé (constitution d'une société traditionnelle). En outre, ce cas peut également intervenir lorsque les personnes à l'origine du protocole ont conservé la capacité de modifier unilatéralement les *smart-contracts* malgré une apparente décentralisation.

Le niveau de décentralisation apparaît donc comme une construction complexe dont l'exhaustivité ne saurait être simplement résumé en quelques lignes. Le lecteur doit simplement retenir qu'à l'opposé des organisations traditionnelles, de nouveaux types d'organisations décentralisées verront le jour d'ici peu avec leurs propres règles de fonctionnement. Par conséquent, il semble impossible, et par ailleurs illogique, d'appliquer un ensemble de règles imaginées pour des modèles centralisés à des entités qui n'auront pas les mêmes fonctionnements. Un travail de réflexion doit être engagé afin de concevoir la réglementation pertinente afférente à ces différents types d'entités décentralisées, en fonctionnant notamment par logique de blocs et par niveau de décentralisation.

Outre la question de la personnalité juridique des entités décentralisées et des règles qui en découlent, le développement de la technologie implique d'immenses enjeux de régulation. La tentation des régulateurs et des législateurs est de transposer par assimilation la réglementation des services centralisés aux crypto-actifs ayant le même objet. Ainsi, selon ce raisonnement, un actif ayant les mêmes usages devrait être soumis strictement aux mêmes règles, sans prise en compte des modalités de son fonctionnement. Ce raisonnement est un raccourci intellectuel qui ne prend pas en compte le sous-jacent technologique, la nature et le fonctionnement de ces nouveaux objets.

Aussi, l'un des exemples les plus flagrants est celui de l'échange monétaire traditionnel entre deux agents économiques *via* leur interface bancaire (virement traditionnel). Dans ce cas de figure, le premier agent va ordonner à sa banque d'effectuer un transfert de fonds au profit de la banque du second. Or, dans le cadre

¹³ Une analyse plus approfondie des DAO est présentée ultérieurement dans le présent rapport.

d'un échange *via* crypto-actifs, la transmission monétaire peut s'effectuer sans intermédiaire. Les deux agents peuvent échanger librement de pair-à-pair. Par conséquent, l'ensemble des règles et des contraintes qui reposent sur l'acteur centralisé régissant la relation entre deux agents intermédiés ne peut fondamentalement être reproduit sans distinction des nouvelles modalités permises par la technologie.

Ainsi, la question n'est pas de savoir s'il faut réglementer ou non les activités liées aux crypto-actifs. Si la technologie blockchain est, en elle-même, totalement neutre, certains n'hésitent pas à s'en servir à des fins malveillantes. La réglementation est donc une nécessité afin de garantir la protection et l'équité des investisseurs, de garantir leurs intérêts et de faire respecter l'ordre public. Toutefois, un compromis doit être trouvé entre innovation et régulation, afin de faire éclore un écosystème compétitif en France et en Europe. En somme, il est nécessaire de réglementer intelligemment et de ne pas simplement reproduire une réglementation qui serait inopérante car inadaptée.

2. Les crypto-actifs, source de nouveaux enjeux géopolitiques

Outre-Atlantique, le dernier *executive order* de Joe Biden a récemment donné le ton. Les crypto-actifs ne sont plus une mode, réservés à quelques *geeks* ou spéculateurs inconscients. Ils représentent désormais une véritable tendance de fond. Ils sont à la transmission de la valeur ce qu'Internet a été à la transmission de l'information.

À l'origine, le débat s'est focalisé sur leur définition en tant qu'objet : les crypto-actifs peuvent-ils être qualifiés de monnaie ? Si cette interrogation a été le sujet de nombreux débats entre économistes, ce point a néanmoins été tranché en droit par le Salvador qui a reconnu le bitcoin comme monnaie officielle. En outre, la Russie a récemment légiféré afin d'attribuer au bitcoin le statut de devise étrangère. Certains crypto-actifs peuvent donc être considérés comme des monnaies. Au-delà de cette question, la propagation des crypto-actifs à la sphère monétaire a pris une ampleur inédite avec les premiers développements de monnaies numériques de banque centrale (MNBC).

L'émergence de ces nouvelles technologies a conduit les grandes puissances économiques mondiales à une course à l'armement monétaire. Sur cet aspect, la Chine est le pays le plus avancé. Avec le projet pilote du yuan numérique, déjà émis à grande échelle dans les principales villes du pays, l'État-parti chinois pourra

compléter son dispositif de contrôle de la population, adossé au mécanisme de crédit social déjà existant. Plus encore, Pékin pourra utiliser cette nouvelle technologie monétaire afin de créer un système parallèle au système financier mondial reposant sur le dollar au sein d'une nouvelle zone monétaire.

En parallèle, l'invasion de l'Ukraine par la Russie a récemment mis en exergue la faculté des crypto-actifs à remettre en cause le système financier actuel. En effet, outre l'intervention armée, les pays occidentaux - notamment les États-Unis - ont principalement recours à l'arme économique. Ces sanctions visent à accentuer la pression afin d'obtenir une issue favorable au rapport de force qui les oppose. Or, certains responsables politiques, comme la présidente de la BCE Christine Lagarde, ont appelé à davantage de régulation des crypto-actifs afin d'éviter que ces derniers soient utilisés afin de contourner les sanctions imposées à la Russie.

En l'état, il semble toutefois peu probable que les crypto-actifs permettent de contourner ou d'atténuer les sanctions imposées à la Russie. D'une part, parce que cet écosystème est encore essentiellement imperméable ; il est difficile d'échanger et de communiquer intégralement sans passer par les acteurs bancaires et plus généralement la finance traditionnelle. D'autre part, parce qu'il est fondé sur un principe d'absolu décentralisation et de transparence des échanges. Cela implique qu'aucune entité, qu'il s'agisse d'un État ou d'une entreprise, ne peut contrôler le fonctionnement ou la gouvernance d'une blockchain publique. Sans doute, certains oligarques russes se sont-ils servis des crypto-actifs pour passer outre le gel de leurs avoirs ou bien encore pour se protéger de la dévaluation du rouble mais les conséquences ne peuvent pas, pour l'instant, aller au-delà. En outre, il est également probable que la Corée du Nord, isolée, utilise les crypto-actifs pour rançonner les victimes de leurs cyberattaques. À l'instar de toute nouvelle technologie, certaines personnes aux intentions malveillantes s'en saisissent afin d'accomplir leurs desseins.

Quoiqu'il en soit, l'arme économique repose principalement sur la force des monnaies et notamment la puissance du dollar américain. Couplé à des organismes indispensables au routage des flux entre les institutions financières, les États-Unis ont pu imposer l'extraterritorialité des sanctions. Aussi, qu'advierait-il si les monnaies traditionnelles perdaient en attractivité dans le reste du monde, concurrencées par de nouvelles monnaies numériques plus efficaces ?

La Chine l'a bien compris. En tant qu'acteur majeur du commerce mondial, elle souhaite à terme imposer le recours au yuan numérique pour l'importation de

biens produits sur son propre sol. Ce changement de paradigme lui permettrait d'imposer un autre rapport de force monétaire, à la manière des sanctions extraterritoriales américaines. Ainsi, il est urgent que l'Europe prenne acte de cette nouvelle réalité monétaire. Elle ne doit pas seulement intervenir à la marge, de manière à contenir un écosystème qui, de par sa nature décentralisée, ne peut l'être. Elle doit conduire une politique de souveraineté monétaire ambitieuse. Cela passera notamment par la création d'un euro numérique qui représentera à la fois une avancée majeure pour les acteurs européens mais également un outil à la défense de ses intérêts et de ses valeurs dans le reste du monde. Cet euro digital de banque centrale devra être couplé à des monnaies électroniques émises par des acteurs privés. L'Europe ne peut bâcler ce chantier et les débats politiques à venir sur cette question. Depuis la crise de la Covid et la guerre en Ukraine, face au retour du tragique, il convient que les décideurs aient le courage et la lucidité d'asseoir une vision à long terme. Le concept d'Europe puissance est devenu un thème majeur de la pensée géostratégique. Toutefois, il ne peut y avoir de puissance géopolitique sans une puissance monétaire.

PARTIE II - Un nouveau rapport à la valeur

L'écosystème des crypto-actifs est marqué par la grande diversité des *tokens* qui le composent. Le premier d'entre eux est le bitcoin. Il a été conçu afin d'être une monnaie et un réseau d'échanges autonomes des banques centrales et acceptés dans le monde entier. À la différence des systèmes monétaires traditionnels, dans lesquels la devise ayant cours légal est indépendante du réseau (bancaire et de paiements) sur lequel elle circule, le Bitcoin est un tout fonctionnant sans intervention humaine. Mal compris et parfois méprisé par les économistes, ses caractéristiques en font pourtant un outil monétaire inédit et unique, voire une véritable révolution.

I. Bitcoin, l'ère de l'institutionnalisation et de la maturité

Après plus de dix années d'existence, le Bitcoin a fait la démonstration de sa résilience. Étant donné ses qualités intrinsèques, cet actif est en passe de devenir un incontournable de la finance du XXI^{ème} siècle. Étalon monétaire, valeur refuge ou actif ultra-spéculatif, le bitcoin n'a pas fini d'interroger sa véritable nature.

1. L'évolution financière du bitcoin

Depuis ses débuts en 2009, le cours du bitcoin n'a cessé de s'apprécier, passant ainsi de quelques centimes de dollars à plus de 69.000 dollars en novembre 2021. Toutefois, cette progression n'a jamais été linéaire. Bien que cela soit le lot commun d'une majorité d'actifs financiers, l'évolution financière du bitcoin a été particulièrement mouvementée. Il a connu une progression fulgurante, rarement observée par ailleurs, lors du *bull run*¹⁴ de 2020 et 2021. Cette progression haussière qui a vu le cours passer de 4.000 dollars environ à plus de 69.000 dollars, se démarque par certaines de ses causes sous-jacentes et notamment par rapport au précédent mouvement haussier de 2017, mouvement qui avait alors donné naissance à la bulle des ICO.

En 2017, sous la plume de la presse généraliste ou spécialisée, le bitcoin apparaissait comme un actif immature à destination des seuls particuliers en quête de profits rapides. Il était alors moqué par les experts financiers. À l'instar de Jamie

¹⁴ La métaphore du *bull run* désigne une période prolongée de hausse sur le marché des crypto-actifs. En français, on parle de marché haussier.

Dimon, alors PDG de JPMorgan Chase & Co, qui déclarait que le bitcoin était une fraude¹⁵ - et relevait davantage d'une blague ou d'un placement risqué pour des investisseurs aventureux que d'un véritable investissement. En 2021, les esprits ont radicalement changé. S'agissant des particuliers, durement touchés par l'explosion de la bulle ICO, ils ont été nombreux à perdre une partie substantielle de leur investissement initial. S'agissant des investisseurs institutionnels, en revanche, ils ont pris le temps d'observer le bitcoin ainsi que la technologie sous-jacente. Depuis 2019, ils ont été nombreux principalement outre-Atlantique à sauter le pas. En conséquence, le bitcoin a clôturé l'année 2020 à 29.022 dollars, soit 48 % de plus que son plus haut niveau de 2017. Sur l'ensemble de l'année 2021, le cours aura plus que doublé.

Cette forte progression résulte de plusieurs facteurs. D'une part, les circonstances exogènes et endogènes ont favorisé cette tendance haussière. D'autre part, le bitcoin bénéficie d'un mouvement d'institutionnalisation d'ampleur qui affecte aussi bien son cours que sa structure financière.

a. Les raisons exogènes et endogènes à la croissance du cours du bitcoin

Le contexte sanitaire et ses conséquences économiques n'ont pas été sans effet sur le cours du bitcoin et plus généralement la valorisation des crypto-actifs. Avec l'apparition de la pandémie de la Covid-19, la planète tout entière s'est mise à l'arrêt. Ce choc inédit a créé un sentiment de panique sur les marchés. Premier impacté du fait de sa liquidité, le marché des crypto-actifs a subi un véritable « krach » au mois de mars 2020. Face aux confinements généralisés, à la propagation du virus et à l'incertitude économique qui en a résulté, les investisseurs ont souhaité vendre les actifs les plus risqués.

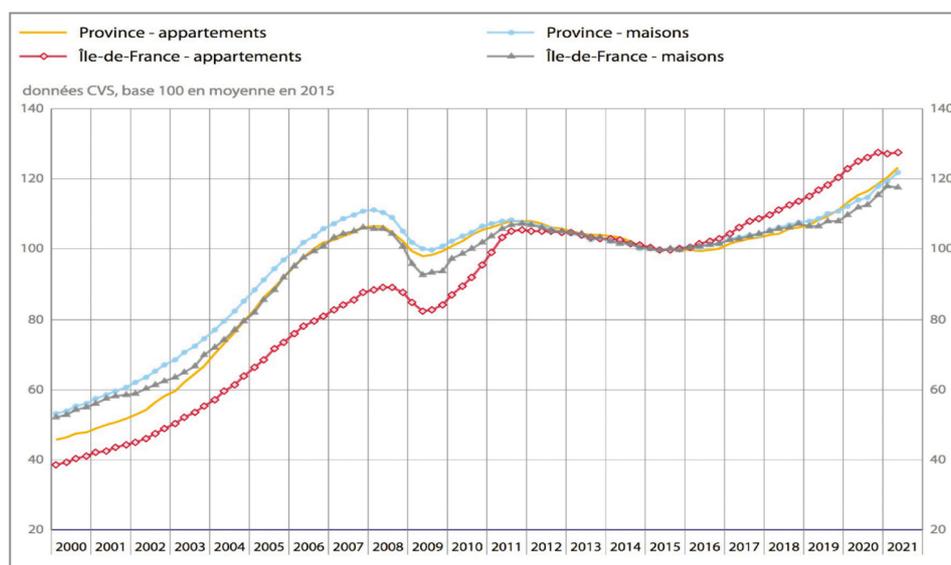
Si les conséquences ont été immédiates sur les marchés financiers, la crise sanitaire a frappé l'ensemble des couches de l'économie sans distinction. Face à la nécessité impérieuse d'épauler des pans entiers de l'économie, les États occidentaux ont mis en œuvre des plans d'aide d'urgence puis des plans d'investissement sans commune mesure depuis plus d'un demi-siècle. L'ampleur de la réponse n'aurait pu être possible sans le concours des banques centrales. Afin d'éviter l'effondrement des États et de leurs économies, les deux principales banques centrales au monde, la Fed et la BCE, ont amplifié massivement leurs programmes de rachat d'actifs

¹⁵ Reuters - [JPMorgan's Dimon says Bitcoin 'is a fraud'](#) - 21.09.2017

(*quantitative easing*) afin de faciliter l'endettement des États et la mise en place des aides à destination des secteurs touchés.

Le rachat par les banques centrales sur le marché secondaire des actifs obligataires émis par les États sur le marché primaire a contribué à injecter massivement des liquidités dans le système financier. Le *quantitative easing* a notamment eu pour conséquence un renchérissement généralisé du prix des actifs. Ainsi malgré le « krach Covid » de mars 2020 et malgré des indicateurs économiques en net recul, les principaux indices boursiers ont battu en 2020 et 2021 une succession de records. Ces derniers ont affiché une croissance insolente, rarement observée sur une période aussi courte. Le S&P 500 a ainsi augmenté de plus de 40% par rapport à son niveau pré-pandémie, alors que le CAC 40 a progressé de plus de 1.300 points dans une période économiquement incertaine.

La politique de *quantitative easing* des banques centrales a induit des effets discutables sur le long terme. Outre les actifs financiers, le marché de l'immobilier a directement été impacté par les injections massives des banques centrales. En Europe notamment, dès 2015 et l'assouplissement monétaire engagé par la BCE afin de faire face à la crise des dettes souveraines, les prix de l'immobilier ont entamé une longue croissance. Cette recrudescence d'investissements, notamment dans les zones en tension, a conduit à une explosion des prix au détriment des ménages plus modestes.



Champ : France métropolitaine. Sources : Insee, ADSN-BIEN-Notaires du Grand Paris, Notaires de France - Perval.

Notaires de France - Variation des prix des logements anciens sur un an en France entre 2000 et 2021¹⁶

¹⁶ Notaires de France - [Marché immobilier : tendance et évolution des prix de l'immobilier](#) - 28.10.2021

Ainsi, dans cet environnement économique instable marqué par (i) une croissance relativement faible, (ii) des taux d'intérêt proches de zéro voire parfois négatifs, (iii) une politique monétaire expansionniste provoquant une inflation sur les marchés immobiliers et boursiers, les ménages ont cherché d'autres sources de rendement pour leur épargne. Dans ces circonstances, et alors que le bitcoin commençait à atteindre une certaine maturité après la traversée du désert qui a suivi l'explosion de la bulle ICO de 2018, les investisseurs ont commencé à s'intéresser aux crypto-actifs comme nouvelle source de rendement. C'est ainsi que la politique monétaire des banques centrales, honnie par les libertariens adeptes du Bitcoin, a eu une incidence directe sur le cours de ce dernier.

Outre les questions relatives à la politique monétaire, le cours du bitcoin a également progressé sur la base de fondamentaux ayant alimenté cette hausse rapide et continue. De manière endogène, la structure même de la « politique monétaire » de Bitcoin induit une raréfaction de ses jetons et donc une augmentation de leur valeur. Cette augmentation ne peut exister sans une démocratisation croissante de l'écosystème auprès de nouveaux publics, alimentée par les entreprises du secteur mais aussi par de nouveaux entrants institutionnels.

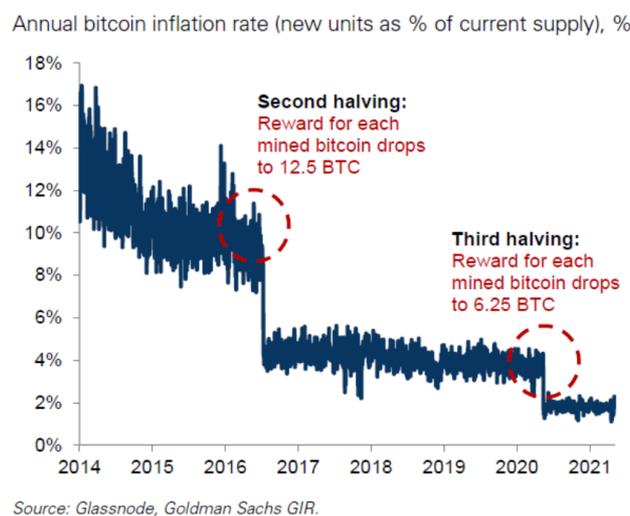
L'évolution du cours du bitcoin dépend, pour une majeure partie, de sa structure monétaire. L'un des principaux arguments de Bitcoin face à la politique monétaire des banques centrales réside dans la limite, quasi-intangible, du nombre de *tokens* émis sur le réseau et limité à 21 millions d'unités. Par conséquent, la valeur de l'actif est le reflet de ses caractéristiques intrinsèques et non le fruit d'une variation du nombre d'actifs en circulation qui tendrait à ce que ce dernier s'apprécie ou se déprécie.

Toutefois, si les 21 millions de bitcoins n'ont pas encore tous été émis, ceux restant le seront en guise de récompense pour la validation des blocs de la blockchain par les « mineurs ». L'activité de minage consiste à sécuriser la blockchain en résolvant un algorithme complexe. Le fruit du minage est une récompense délivrée en bitcoins. Le système est conçu de manière à diviser par deux (phénomène de *halving*¹⁷) la récompense attribuée à chaque validation de bloc, afin de lisser les émissions de *tokens* sur un temps long. Cette réduction de la récompense intervient tous les 210.000 blocs, soit tous les 4 ans environ. À ce titre, si les premiers mineurs

¹⁷ Un *halving* est une réduction par deux de la récompense attribuée à un mineur en contrepartie de la validation d'un bloc, réalisée en mobilisant de la puissance de calcul (dans le cas de la blockchain Bitcoin).

percevaient environ 50 bitcoins pour chaque validation, ils ne perçoivent désormais que 6,25 bitcoins par bloc.

Ces cycles ont une incidence directe sur le coût de production, les revenus et donc le rendement des mineurs. Contrairement à ce qu'opposent ses détracteurs, le bitcoin n'est pas un actif décorrélé de tout sous-jacent dans le monde réel. En effet, il n'est pas uniquement la somme de la confiance dans le réseau. Son prix est aussi dirigé par son coût de production qui, s'agissant du réseau Bitcoin, est un savant équilibre entre la quantité de récompense émise pour la résolution de l'algorithme, le taux de difficulté afin de résoudre l'équation et le prix de l'électricité nécessaire à faire fonctionner les machines. Le *halving* a donc des conséquences importantes sur le prix du bitcoin, prix naturellement poussé à la hausse. La combinaison de ces phénomènes induit une tendance haussière de l'actif à long terme.



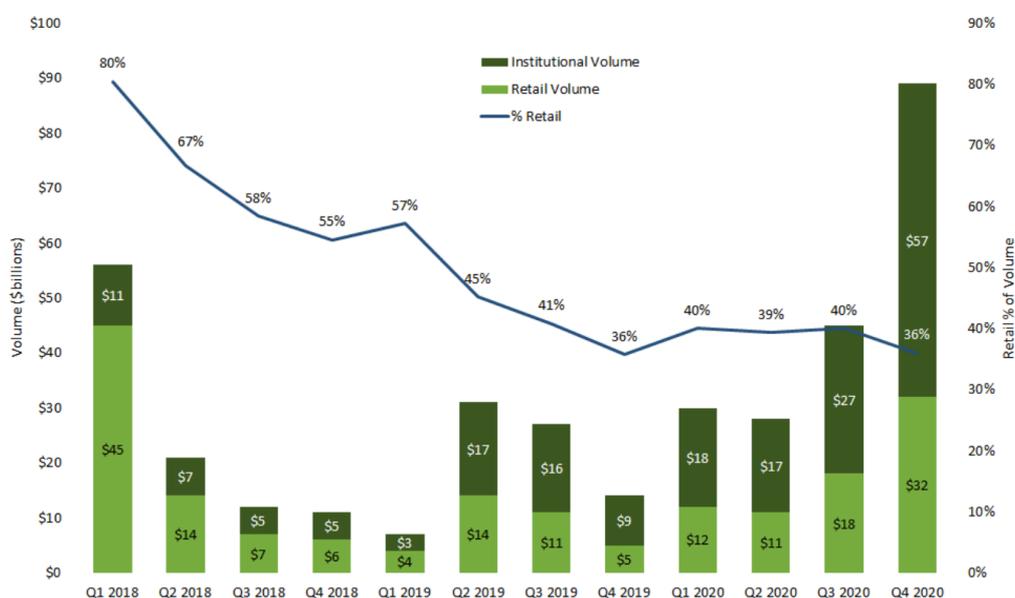
Goldman Sachs - Évolution de la quantité de bitcoins attribuée par le réseau en récompense de la validation d'un bloc entre 2014 et 2021

Depuis 2018, l'écosystème des crypto-actifs a beaucoup évolué. D'une part, les nombreux projets issus de la vague ICO, qui manquaient de sérieux ou présentaient des motivations fictives, ont été balayés par l'éclatement de la bulle. D'autre part, les entreprises survivantes ont su capitaliser sur un savoir-faire et des produits innovants. En quelques mois seulement, des acteurs systémiques et mondiaux de la taille de banques commerciales se sont développés. *Via* ces nouveaux géants, comme Coinbase ou Binance, et grâce au soutien d'acteurs déjà établis comme Paypal, l'écosystème s'est doté de relais puissants auprès d'un public toujours plus large. Cette démocratisation a permis un afflux constant de nouvelles liquidités.

b. L'émergence d'un phénomène d'institutionnalisation du bitcoin

Pendant longtemps, les crypto-actifs ont été considérés par les investisseurs institutionnels comme une classe d'actifs honnie, voire prohibée en raison de son impact réputationnel ou des risques réglementaires afférents. Depuis trois ans, les crypto-actifs se sont progressivement démocratisés. Ils font désormais partie du paysage numérique des sociétés contemporaines. De surcroît, l'année 2020 a profondément été marquée par l'entrée des investisseurs institutionnels dans ce nouveau monde et, par voie de conséquence, l'entrée des crypto-actifs dans le paysage financier traditionnel.

Si les investisseurs institutionnels sont restés attentifs aux crypto-actifs depuis leurs créations, bitcoin en tête, ce n'est que dans la seconde partie de l'année 2020 que certains acteurs américains ont décidé d'intervenir sur ce nouveau marché. À titre d'exemple, alors que les investisseurs institutionnels ne représentaient qu'un cinquième des transactions réalisées sur Coinbase début 2018, ils en représentaient près de deux tiers au dernier trimestre 2020¹⁸. Au premier trimestre 2021, Coinbase annonçait que sur les 335 milliards de dollars de transactions réalisées sur sa plateforme, 215 relevaient de transactions d'investisseurs institutionnels¹⁹.



Source: Coinbase, CoinDesk Research

coindesk

Coindesk - Volumes d'échanges par segment de clientèle sur Coinbase entre 2018 et 2020

¹⁸ Coindesk - [Coinbase Institutional, Retail Trading Volume Grew at Equal Rates in 2020](#) - 25.02.2021

¹⁹ Institutional Investor - [Why Institutional Investors Are Buying Bitcoin – Again](#) - 26.08.2021

Avec l'arrivée de ces nouveaux investisseurs, les crypto-actifs sont à un tournant important. Il ne s'agit plus seulement de « rêves libertariens » ou de « folies spéculatives ». Désormais certains investisseurs connus et expérimentés s'impliquent dans ce nouvel écosystème. Qu'il s'agisse de grandes multinationales, d'institutions financières traditionnelles ou de géants du paiement, tous lorgnent sur le nouveau marché des cryptos.

i. Les différents aspects de l'institutionnalisation du bitcoin

L'institutionnalisation du bitcoin a pris plusieurs formes. D'une part, certaines entreprises ont décidé d'allouer une partie significative de leur trésorerie aux crypto-actifs, bitcoin en tête. D'autre part, le secteur financier a commencé à innover, à s'exposer pour finalement créer les ponts entre la finance traditionnelle et le monde crypto afin d'en capter une partie de la valeur.

Les placements des grandes entreprises américaines - Un chiffre démontre l'engouement des acteurs institutionnels pour le bitcoin : la détention de ce *token* par les entreprises cotées américaines a augmenté de 400% entre janvier 2019 et janvier 2020, passant de 20.000 bitcoins intégrés aux bilans à plus de 100.000²⁰. À l'écriture de ces lignes, 27 sociétés cotées américaines détiendraient plus de 225.000 bitcoins dans leurs comptes, pour un montant total cumulé de plus de 8,6 milliards de dollars²¹.

En août 2020, MicroStrategy a ouvert la marche en achetant plus de 21.000 bitcoins pour 250 millions de dollars. Michael J. Saylor avait alors déclaré que le bitcoin était « une réserve de valeur fiable et un actif d'investissement attrayant avec un potentiel d'appréciation à long terme plus important que la détention de liquidités »²². MicroStrategy « a donc fait de bitcoin le principal avoir de sa stratégie de réserve de trésorerie », a déclaré Saylor. Si cette opération fut marquante, c'est parce qu'elle a constitué le premier achat massif et public de bitcoins par un investisseur institutionnel renommé et coté sur les marchés financiers. En mai 2022,

²⁰ Cointelegraph - [Bitcoin held by public companies has surged 400% in 12 months to \\$3.6 billion](#) - 27.01.2021

²¹ CoinGecko - [Bitcoin Holdings by Public Companies](#) - 03.05.2022

²² Coindesk - [MicroStrategy Buys \\$250M in Bitcoin, Calling the Crypto 'Superior to Cash'](#) - 11.08.2020

MicroStrategy est l'entreprise cotée américaine qui détient le plus de bitcoins, avec près de 130.000 *tokens* à son bilan, contre 70.784 en janvier 2021.

Il est difficile d'évoquer l'appropriation de bitcoin par les sociétés cotées sans évoquer le cas de Tesla. Dans le même temps, le sujet reste complexe à aborder tant cette relation est marquée par les soubresauts d'Elon Musk.

Le 8 février 2021, Tesla a acquis pour un milliard et de demi de dollars de bitcoins et annoncé que ce dernier sera désormais disponible comme moyen de paiement pour l'achat de ses voitures²³. L'entreprise a ainsi modifié sa politique d'investissement pour la rendre plus flexible et pouvoir investir dans des actifs d'un nouveau genre comme le bitcoin. L'objectif était alors d'assurer une meilleure diversification des liquidités inutilisées et, ainsi, une maximisation de leurs rendements. Dans le cadre de ce plan, la société a annoncé qu'elle allait investir dans certains « actifs de réserve alternatifs, notamment des actifs numériques, des lingots d'or et des fonds négociés en or »²⁴. Toutefois, dès le 13 mai 2021, Tesla a annoncé faire machine arrière et ne plus accepter le bitcoin comme moyen de paiement, justifiant ce choix sur Twitter par « l'énorme coût environnemental du minage et du traitement des transactions ».

Si l'arrivée, plus ou moins massive, d'acteurs institutionnels sur le marché des crypto-actifs est une bonne chose en ce qu'elle permet à ce dernier de mûrir et de croître, elle pose également d'autres questions. Les décisions de Tesla et les tweets d'Elon Musk ont en effet conduit à des variations très brutales - dans des proportions parfois importantes - des cours des crypto-actifs, avec des effets qui peuvent être tout à fait néfastes pour les petits porteurs notamment. Or, là où les marchés traditionnels sont protégés par des régulations strictes, corrélées à des sanctions pénales lourdes, le monde des crypto-actifs ne bénéficie d'aucune de ces protections. Il est par conséquent totalement soumis aux effets de communication des géants du secteur et autres manipulations à court terme des gros portefeuilles. En découle un manque de protection des petits porteurs qui peuvent donc être exposés aux manipulations médiatiques, voire financières, de ces personnalités mondialement influentes. Il convient toutefois de préciser que l'institutionnalisation du marché depuis 2018 a contribué à sa plus grande liquidité, permettant *de facto* de réduire les marges de manœuvre et les effets néfastes d'acteurs isolés qui souhaiteraient manipuler le marché.

²³ Le Monde - [Tesla investit 1,5 milliard de dollars dans le Bitcoin et l'accepte comme moyen de paiement](#) - 08.02.2021

²⁴ Cointelegraph - [The convergence between Tesla, SpaceX, renewable energy and Bitcoin mining](#) - 25.04.2021

L'irruption de Bitcoin au sein des marchés financiers - Outre les acquisitions de bitcoins par de grandes multinationales, l'afflux de fonds à destination du « roi des crypto-actifs » a été facilité par le développement de produits financiers traditionnels avec comme sous-jacent le bitcoin lui-même.

Grayscale fut fondé en 2013. Cette société est dorénavant le plus grand gestionnaire en crypto-actifs au monde et permet à des investisseurs institutionnels ainsi qu'à des particuliers initiés et fortunés de s'exposer au cours du bitcoin *via* un véhicule financier traditionnel. Début 2021, le Grayscale Bitcoin Trust (GBTC) gérait plus de 28 milliards de dollars²⁵ avec plus de 600.000 bitcoins sous gestion, soit environ 3% de l'ensemble des bitcoins en circulation. À cet égard, le GBTC constitue la porte d'entrée privilégiée par les investisseurs institutionnels afin d'investir sur le bitcoin, et notamment pour les acteurs réglementés tels que les banques et les fonds spéculatifs. Pour ce faire, GBTC est constitué d'un véhicule financier traditionnel. Les investisseurs institutionnels peuvent par conséquent être exposés à l'investissement en crypto-actifs sans avoir à en acheter, en stocker et en conserver directement. Le tout est organisé dans les cadres réglementaires existants²⁶.

Après le succès du GBTC auprès des investisseurs institutionnels, Grayscale a lancé, depuis 2017, plusieurs autres fonds du même genre mais portant sur les *tokens* d'autres blockchains (Ethereum, Chainlink, Litecoin, etc ...) démontrant l'intérêt croissant des acteurs institutionnels pour les crypto-actifs, bien que le bitcoin reste le produit privilégié.

Autre acteur financier de taille, la banque d'affaires Goldman Sachs s'est récemment convertie au bitcoin, après une phase d'hostilité affirmée. En effet, en mai 2020, la banque d'affaires indiquait dans un rapport que ce nouvel objet numérique ne correspondait pas à une « nouvelle classe d'actifs » et déconseillait à ses clients de le considérer dans leurs opérations d'investissement. Pour arriver à cette conclusion, Goldman Sachs se basait sur trois éléments : un risque élevé de piratage, les activités illicites liées au bitcoin et la volatilité très élevée des cours.

Un an plus tard, un nouveau rapport de la banque d'affaires a pris le contrepied et indiqué que le bitcoin constituait une nouvelle classe d'actifs²⁷. Ce changement de position est le résultat d'un long processus d'acceptation du bitcoin

²⁵ Chiffres officiels fournis par [Grayscale](#)

²⁶ [Site officiel](#) de Grayscale

²⁷ Goldman Sachs - [Global Macro Research – Crypto: A New Asset Class?](#) - 21.05.2021

comme nouvel actif financier mais aussi la preuve d'un réalisme commercial. En effet, selon une enquête menée auprès des clients de Goldman Sachs au premier trimestre 2021, 40% d'entre eux étaient déjà exposés aux crypto-actifs et 61% estimaient que leurs cours seraient amenés à augmenter dans les prochaines années²⁸.

En parallèle, Goldman Sachs souhaite pouvoir offrir à ses clients une gamme élargie de services sur crypto-actifs, allant de produits dérivés²⁹ sur bitcoin à un ETF corrélé à la performance des crypto-actifs³⁰. En outre, elle a organisé et participé à une levée de fonds d'un montant de 15 millions de dollars, au profit de Coin Metrics, une start-up américaine spécialisée dans l'analyse des blockchains et du marché des crypto-actifs³¹. L'engouement récent de Goldman Sachs pour les crypto-actifs s'inscrit dans une démarche plus globale d'appropriation par la finance traditionnelle de ce nouvel écosystème.

En février 2021, la Bank of New York Mellon, plus ancienne banque des États-Unis, a ainsi indiqué vouloir intégrer les crypto-actifs à son réseau financier - au même titre que les bons du Trésor américain ou les actions - et de permettre à ses clients de se positionner³². En mars 2021, la banque d'affaires Morgan Stanley souhaitait également offrir une exposition à des fonds liés au bitcoin, au profit de ses clients les plus fortunés seulement - c'est-à-dire les clients disposant d'une « tolérance au risque excessive »³³.

Ces exemples illustrent l'institutionnalisation croissante de l'écosystème des crypto-actifs. Ils laissent présager que les flux de capitaux en provenance de la finance traditionnelle à destination de la finance des crypto-actifs vont continuer à croître dans les prochains mois et les prochaines années. Outre le développement des fonds sur crypto-actifs, Grayscale en tête, la financiarisation des crypto-actifs se développe également au travers des produits financiers émis sur les bourses, notamment américaines. À ce titre, le Chicago Mercantile Exchange, ou encore le Nasdaq, ont commencé à proposer, dès 2017, des contrats dits *futures* (contrats à terme³⁴) avec pour actif sous-jacent le bitcoin.

²⁸ Cointelegraph - [40% of Goldman Sachs' clients already have exposure to crypto, survey shows](#) - 08.03.2021

²⁹ Reuters - [Goldman Sachs offers Bitcoin derivatives to investors- Bloomberg News](#) - 06.05.2021

³⁰ Cryptoast - [Goldman Sachs envisage de créer un ETF avec une exposition au Bitcoin](#) - 24.03.2021

³¹ Bloomberg - [Goldman Sachs leads investment in crypto firm Coin Metrics](#) - 05.05.2021

³² CNBC - [BNY Mellon to offer Bitcoin services, a validation of crypto from a key bank in the financial system](#) - 11.02.2021

³³ CNBC - [Morgan Stanley becomes the first big U.S. bank to offer its wealthy clients access to Bitcoin funds](#) - 17.03.2021

³⁴ Un contrat à terme (ou *future*) est un contrat qui permet à l'investisseur de miser sur l'évolution positive ou négative du prix d'un actif sous-jacent (en l'espèce : le bitcoin).

Ce développement des actifs financiers dérivés sur le bitcoin trouve son public parmi les investisseurs institutionnels, puisqu'en janvier 2021 - alors que son cours atteignait des sommets - environ 17.549 contrats dérivés sur bitcoin étaient conclus auprès des services de CME. En hausse de 57% par rapport au mois de décembre 2020, les contrats dérivés de CME représentaient environ 87.700 bitcoins, contre 55.900 un mois plus tôt. S'il est évident que cette hausse significative suit le cours du bitcoin, lui-même hautement volatile, elle dénote toutefois la volonté des institutionnels de s'exposer plus encore aux crypto-actifs, au même titre que d'autres classes d'actifs. Cela s'est traduit notamment dans les comptes ouverts par les acteurs institutionnels : 7.400 comptes ouverts depuis sa création en 2017, plus de 700 nouveaux comptes lors des deux premiers mois de 2021.

L'appropriation de bitcoin par les leaders des systèmes de paiements -

Cette appropriation de bitcoin par des acteurs institutionnels s'étend également à la sphère des moyens de paiement. À cet égard, la société Visa est la plus investie. Ainsi, à l'occasion de la présentation des résultats du premier trimestre 2021, cette dernière a affiché sa volonté d'accroître son activité autour des crypto-actifs, en traçant deux axes majeurs : (i) permettre l'acquisition, puis, la transaction en crypto-actifs ; et (ii) développer la présence des crypto-actifs dans le monde financier traditionnel, au travers des fintechs et des institutions financières. Cette démarche « pro-crypto » s'inscrit dans une politique d'ouverture à plus long terme, qui a trouvé son point d'orgue avec le partenariat conclu avec Circle, autour de l'USDC³⁵ (un *stablecoin* adossé au dollar américain). Visa devient ainsi le premier grand réseau de paiement à permettre le règlement de transactions en *stablecoins*.

En parallèle, MasterCard, autre leader des réseaux dédiés aux paiements, s'est prononcé en faveur du développement d'une nouvelle offre autour des crypto-actifs. Début 2021, la société a déclaré introduire les crypto-actifs sur son réseau³⁶. Cette nouvelle étape est, selon la société, une réponse à l'engouement grandissant du grand public envers ces crypto-actifs et constitue « l'avenir des moyens de paiement ».

Cet attrait appuyé des acteurs institutionnels des paiements pour les crypto-actifs fait échos aux nouveaux services développés par PayPal. La société a lancé, en mars 2021, un nouveau service intitulé « *Checkout with Crypto* », permettant à ses utilisateurs de régler leurs transactions avec l'un des trois crypto-actifs acceptés (bitcoin - ether - litecoin). Ce nouveau service fait suite à la possibilité, offerte par

³⁵ Forbes - [Visa Partners With Ethereum Digital-Dollar Startup That Raised \\$271 Million](#) - 02.12.2020

³⁶ Mastercard - [Why Mastercard is bringing crypto onto its network](#) - 10.02.2021

PayPal en octobre 2020, d'acheter et de vendre des crypto-actifs directement depuis le compte utilisateur.

L'objectif de Dan Schulman, son PDG, est clair : démocratiser les crypto-actifs et en favoriser l'adoption dans tous les pans de l'économie. Cette vocation s'inscrit dans une démarche plus globale d'évolution des moyens de paiement telle qu'anticipée par la société. Dans une interview au Time³⁷, Dan Schulman déclarait que les espèces et cartes bancaires sont amenées à disparaître au profit de « super applications » disponibles directement sur mobile. C'est dans cette optique que les crypto-actifs et autres monnaies numériques constituent une alternative intéressante pour faire évoluer les moyens de paiement actuels.

À terme, l'intégralité de l'industrie des moyens de paiement sera révolutionnée par la technologie blockchain. Associée à des protocoles plus rapides et plus efficaces (layer 1 améliorés ou layer 2), la technologie blockchain permettra dans un futur proche de supprimer les intermédiaires qui constituent la chaîne de paiement et par là même réduire les coûts d'infrastructures qui pèsent sur le consommateur et le commerçant.

Une dynamique institutionnelle limitée en Europe - Si l'appropriation du bitcoin par les acteurs institutionnels de la finance est une étape cruciale dans le développement des crypto-actifs, elle reste cependant limitée aux acteurs américains. L'Europe, dont les entreprises sont généralement plus averses aux risques que leurs homologues américaines, n'a pas encore franchi le pas de la diversification. Il est toutefois à noter que certaines entreprises européennes se sont engagées sur ce chemin. À ce titre, XBT Provider, société du groupe suédois Coinshares, permet aujourd'hui à des banques et des fonds d'investissement d'investir dans le bitcoin, comme s'ils procédaient à l'acquisition de produits financiers traditionnels. En août 2021, la société détenait plus de 48.000 bitcoins, ce qui la plaçait parmi les dix acteurs institutionnels en détenant le plus au monde.

En France, trois sociétés de gestion ont reçu l'accord de l'AMF pour vendre des produits basés sur le bitcoin ou d'autres crypto-actifs : Napoleon AM (racheté fin 2021 par Coinshares), Tobam et Melanion Capital³⁸. S'agissant des moyens de paiement, la société Worldline, a d'ores et déjà permis à plus de 85.000 commerçants suisses d'accepter des crypto-actifs comme moyen de règlement des transactions du

³⁷ Time - [PayPal CEO Dan Schulman: Cryptocurrency Is the Real Deal. And the Superapps Are Coming](#) - 25.04.2021

³⁸ Les Echos - [Les fonds de cryptomonnaies prennent leur envol](#) - 11.01.2022

quotidien³⁹. Parmi les institutions publiques, la Caisse des Dépôts ainsi que Bpifrance ont largement investi le champ de la finance des crypto-actifs. Ces derniers, *via* leurs départements spécialisés, font partie des acteurs les plus avancés en France. Ils explorent les solutions permettant de tirer le meilleur parti de cette révolution financière.

ii. *L'impact de l'institutionnalisation sur le bitcoin*

L'afflux constant d'acteurs institutionnels n'a pas uniquement induit un accroissement des liquidités. Ce phénomène à l'échelle internationale a conduit à un véritable changement de nature de l'actif bitcoin. L'affluence de la demande a poussé les prix à la hausse en 2020/2021. En parallèle, les offres de produits dérivés sur crypto-actifs proposées sur les marchés financiers traditionnels, à l'image des *futures* précédemment évoqués, ont permis à la finance traditionnelle de s'exposer aisément à la performance de cette nouvelle classe d'actifs. Désormais, les prises de position des investisseurs traditionnels à l'égard des crypto-actifs sont scrutées par l'ensemble de l'écosystème qui espère y déceler des indices sur les évolutions futures du cours des crypto-actifs.

Outre la consolidation des cours à des niveaux élevés et une capitalisation haussière, ce phénomène d'institutionnalisation a également pour effet de concentrer un peu plus la détention de bitcoins. Ce sujet a fait l'objet de vives inquiétudes de la part des utilisateurs historiques qui perçoivent le bitcoin comme un outil indépendant de tout gouvernement ou de toute organisation privée. Au contraire, pour d'autres, cette concentration apporterait plus de maturité à l'écosystème et permettrait d'assurer une meilleure stabilité de celui-ci.

Sur ce point, Bloomberg, reprenant une étude de Flipside⁴⁰, considère qu'environ 2% des adresses enregistrées sur la blockchain Bitcoin détiendraient environ 95% des bitcoins aujourd'hui en circulation. À l'inverse, l'étude estime à plus de 70% les adresses détenant moins de 0,01 bitcoin. Cependant, ces données ne reflètent pas précisément ce qu'est la réalité de la concentration du bitcoin entre les différents acteurs de l'écosystème.

En préambule, il convient toutefois de préciser qu'il est d'usage de catégoriser les détenteurs de crypto-actifs selon le volume de *tokens* qu'ils possèdent selon une

³⁹ Worldline - [Worldline et Bitcoin Suisse lancent WL Crypto Payments en Suisse](#) - 01.09.2021

⁴⁰ Bloomberg - [Bitcoin Whales' Ownership Concentration Is Rising During Rally](#) - 18.11.2020

métaphore halieutique. En effet, les entités détenant entre 1.000 et 10.000 bitcoins sont décrites comme des « baleines »⁴¹. Il convient de préciser que les « baleines » sont des entités qui sont catégorisées comme telles seulement en raison du nombre de bitcoins qu'elles détiennent. Rien ne permet immédiatement d'identifier leur vraie nature. Par conséquent, elles peuvent être une multinationale récemment convertie aux crypto-actifs qui a décidé de placer une partie de sa trésorerie en crypto-actifs, une plateforme d'échange qui conserve les crypto-actifs pour le compte de ses clients, et parfois des personnes physiques qui ont fait le pari du bitcoin au début des années 2010.

Le premier constat est que l'arrivée des acteurs institutionnels sur le marché a induit une augmentation substantielle du nombre de « baleines » présent sur le marché. En effet, selon une étude menée par Glassnode⁴², leur nombre a progressé de 27% sur l'ensemble de l'année 2020. L'offre de bitcoins détenue par ces baleines a progressé de 13,4% sur la même période.



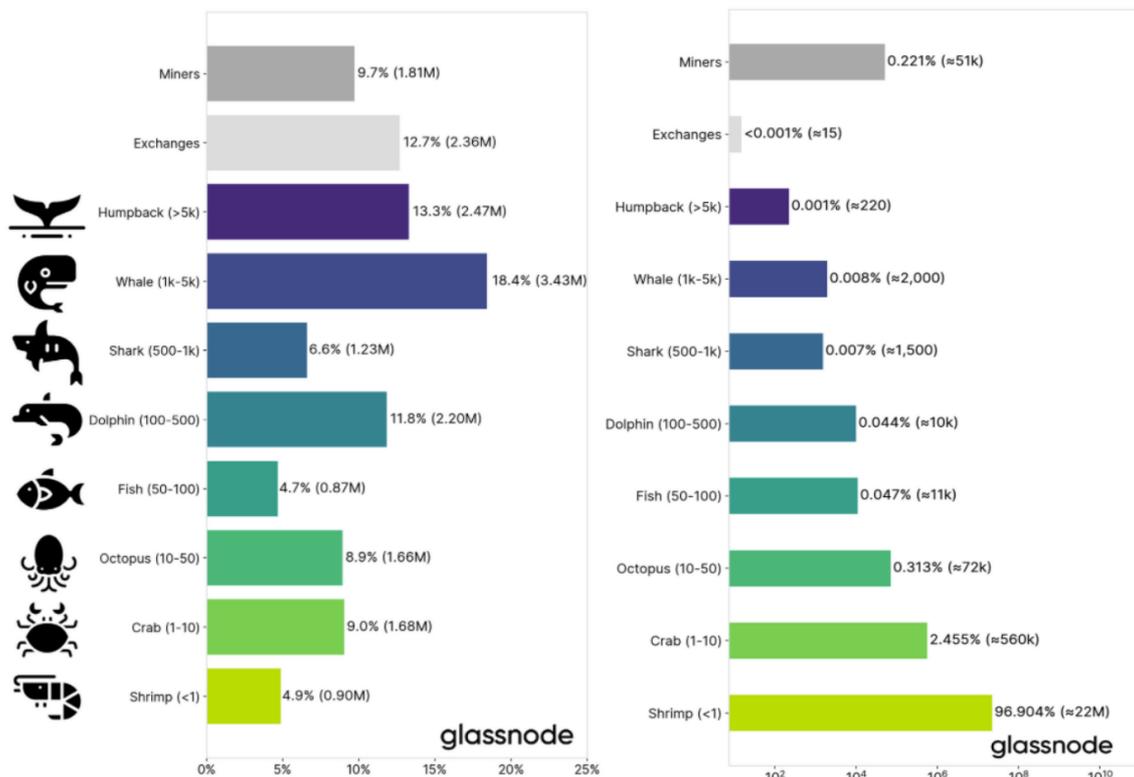
Glassnode - Évolution cumulée du nombre de baleines et de leur offre de bitcoins sur l'année 2020

Toutefois, contrairement à ce que semble arguer l'étude précitée, l'offre de bitcoins n'est pas aussi concentrée qu'on pourrait le penser. En effet, si 2% des adresses détiennent 95% des bitcoins en circulation, il est important de noter qu'une adresse ne correspond pas toujours à un utilisateur unique. La détention par une entité physique ou morale de plusieurs adresses est monnaie courante, tout comme la détention par plusieurs personnes d'une seule adresse partagée. Dès lors, un utilisateur peut contrôler plusieurs adresses et une adresse peut contenir les fonds de plusieurs utilisateurs.

⁴¹ Cette métaphore se déploie dans la même logique aux autres détenteurs selon leur patrimoine en crypto-actifs.

⁴² Glassnode - [No. Bitcoin Ownership is not Highly Concentrated – But Whales are Accumulating](#) - 02.02.2021

Fort de ce constat, afin de pouvoir présenter au lecteur une estimation réaliste de la concentration du bitcoin, il faut s'intéresser aux entités qui détiennent ces adresses. Sur ce point, l'étude de Glassnode conclut sur le fait qu'environ 2% des entités du réseau Bitcoin détiennent environ 70% de l'ensemble des bitcoins en circulation. L'étude met en exergue une analyse de la répartition des adresses en fonction de leur détention de bitcoins et, en parallèle, une distribution de l'offre de bitcoins selon ces mêmes catégories.

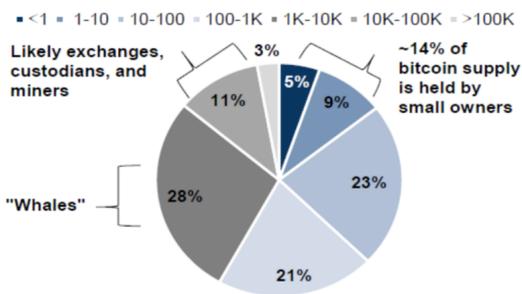


Glassnode - Distribution estimée de l'offre de bitcoins entre les entités du réseau selon leur patrimoine (gauche) et distribution estimée des entités du réseau selon leur patrimoine (droite) en janvier 2021⁴³

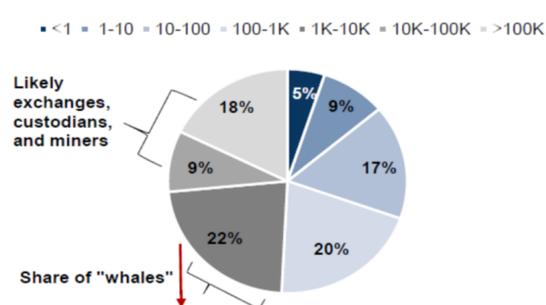
À l'appui de l'étude de Glassnode, on constate que les baleines détiennent environ 31% de l'offre totale de bitcoins (correspondant à environ 5,9 millions de *tokens*). À l'opposé, les plus petits détenteurs de bitcoins (les catégories inférieures à 50 *tokens*, correspondant probablement aux investisseurs particuliers) possèdent près de 23% de l'offre totale de bitcoins (correspondant environ à 4,24 millions de *tokens*). À mi-chemin entre ces deux catégories, les détenteurs de taille intermédiaire (entre 50 et 1.000 *tokens*) possèdent également environ 23% de l'offre totale de bitcoins.

⁴³ Glassnode - [No. Bitcoin Ownership is not Highly Concentrated – But Whales are Accumulating](#) - 02.02.2021

Total supply held by size of addresses' coin holdings, % total

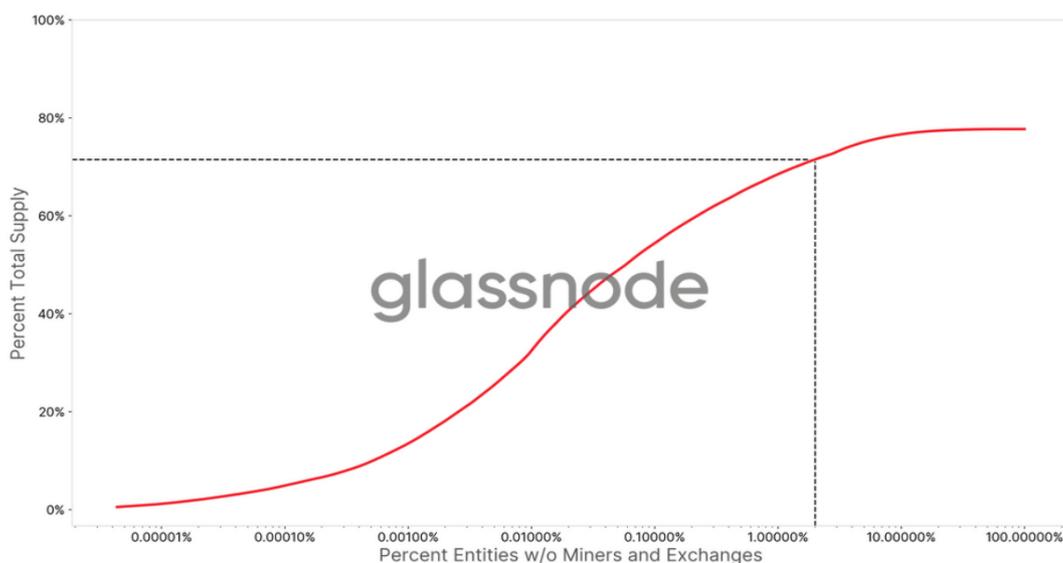


Total supply held by size of entities' coin holdings, % total



Goldman Sachs - Distribution estimée de l'offre de bitcoins entre les adresses du réseau selon leur patrimoine (gauche) et distribution estimée de l'offre de bitcoins entre les entités du réseau selon leur patrimoine (droite) en mai 2021⁴⁴

Ainsi, si les bitcoins sont détenus à 70% par seulement 2% des adresses du réseau, c'est parce que plus de 96% de ces entités sont des micro-détenteurs qui possèdent moins d'un bitcoin. *In fine*, si la répartition de l'offre totale de bitcoins semble relativement équilibrée entre les différentes catégories de détenteurs, elle témoigne d'un phénomène d'institutionnalisation encore balbutiant. En effet, si les acteurs institutionnels et, plus globalement, la finance traditionnelle se forment aux enjeux liés au bitcoin, seule une minorité a sauté le pas.



Glassnode - Pourcentage estimé de l'offre totale de bitcoins détenue par les entités du réseau (soustraction faite des mineurs et des échanges) en janvier 2021

⁴⁴ Goldman Sachs - [Global Macro Research – Crypto: A New Asset Class?](#) - 21.05.2021

Il est à noter que ce phénomène de concentration se poursuit et s'accroît. Ainsi, au plus fort de la chute des cours intervenue au mois de mai 2021, les « baleines » ont acquis pour plus de 122.000 bitcoins⁴⁵ - parmi lesquels on retrouve notamment les fonds d'investissement MVPQ Capital, ByteTree Asset Management et Three Arrows Capital⁴⁶. Cette progression est caractéristique de la volonté des acteurs institutionnels de s'exposer durablement au bitcoin.

Toutefois, la forte concentration de bitcoin n'est pas sans conséquence sur la tenue du marché. À cet égard, le cumul de cette concentration couplée à l'absence de régulation du marché et une liquidité parfois faible induit une relative facilité quant à la manipulation des cours à court terme. Certains acteurs disposant de positions dominantes sur le marché sont la cause volontaire de mouvements brusques et erratiques destinés à chercher la liquidation de positions de particuliers utilisant des effets de levier proposés par les plateformes d'échange. Cette chasse à la liquidité ainsi que l'excès de levier sur les marchés est délétère. Elle témoigne de l'immaturation d'une partie des intervenants ainsi que de la nécessité de réguler les plateformes proposant à leurs utilisateurs des effets de levier démesurés afin d'éviter les abus et la transformation en casino géant.

Avec l'avènement d'une réglementation à l'échelle des nations ainsi qu'à l'international, l'institutionnalisation devrait se renforcer. Elle permettra au bitcoin d'atteindre sa maturité, et avec pour conséquence une réduction de sa volatilité et une imperméabilité plus forte aux événements extérieurs.

2. Un crypto-actif aux sous-jacents protéiformes

Certes, le bitcoin n'est pas un actif considéré comme « productif », dans le sens où il ne produit pas de rendement par lui-même. Cela ne signifie pas qu'il est dénué de valeur. Cette dernière repose en effet sur sa structure intrinsèque, basée sur une technologie mondiale, évolutive et transparente. Par ailleurs, sa structure technique attache ce réseau au monde physique en lui associant un coût de production effectif. Enfin, l'ensemble de ces caractéristiques justifient la place prépondérante du réseau Bitcoin dans l'écosystème des crypto-actifs.

⁴⁵ Cointelegraph - [Bitcoin whales accumulate 122.5K BTC amid latest market mayhem](#) - 23.05.2021

⁴⁶ Bloomberg - [Crypto hedge funds buy the dip in Bitcoin's week of reckoning](#) - 21.05.2021

a. Un crypto-actif associé à un réseau mondial

Qu'il s'agisse du *bull run*, qui a débuté au second trimestre 2020, ou des dernières chutes brutales des cours, intervenues en mai 2021 et au début de l'année 2022, plusieurs événements ont attiré l'attention du grand public vers le bitcoin au cours des 24 derniers mois. Ce coup de projecteur a incité les spécialistes et profanes à envisager la nature et les caractéristiques intrinsèques du bitcoin.

L'histoire a donné raison à ceux qui, dès 2015, défendaient un actif aux caractéristiques multiples et complexes. *A contrario*, elle a infirmé la position de nombreux spécialistes ou économistes dubitatifs qui ne voyaient que dans bitcoin la bulle des tulipes (en référence à la première bulle spéculative de l'économie moderne ayant touché le marché des bulbes de cette fleur aux Pays-Bas, dans les années 1630). Avec plus d'une décennie de recul, il n'est plus question aujourd'hui d'évoquer le bitcoin comme une simple folie spéculative. En outre, le présupposé d'un bitcoin *eldorado* des criminels et des terroristes a été largement infirmé par les spécialistes et économistes du secteur. Selon le dernier rapport de Chainalysis, les transactions en crypto-actifs réalisées dans le cadre d'activités illicites représenteraient environ 0,62% de l'ensemble des transactions en crypto-actifs en 2020 et 0,15% en 2021. À noter que ce chiffre était d'environ 3,37% en 2019. De plus, contrairement aux idées reçues, l'essentiel de ces transactions reposerait davantage sur des mécanismes d'escroquerie ou le fruit de piratages informatiques que sur des financements d'activités criminelles ou du blanchiment d'argent⁴⁷.

Par ailleurs, la valeur intrinsèque de bitcoin est fréquemment remise en question. En effet, contrairement à des actifs traditionnels, il n'est pas productif au sens où il ne génère pas de rendement. Toutefois, considérer que bitcoin n'a aucune valeur au motif qu'il ne génère aucun revenu est une erreur de jugement majeure. Sa valeur intrinsèque repose en réalité sur sa structure technologique. Au fur et à mesure de sa démocratisation, le réseau Bitcoin rassemble de plus en plus d'utilisateurs. En outre, les échanges de valeur sont inscrits de manière irrémédiable dans la blockchain. Afin que les transactions puissent être valides, les blocs qui les agrègent doivent être validés, « miné » dans le cas du réseau Bitcoin, et ainsi être superposés à l'ensemble des transactions précédentes, lui-même constitués sous forme de blocs. Ce processus décentralisé et immuable, dont les règles sont préétablies et transparentes, est la principale garantie de la sécurisation des transactions et de l'inviolabilité du système.

⁴⁷ Chainalysis - 2022 Crypto Crime Report - 02.2022

Ainsi, la force de Bitcoin réside dans le fait que son réseau est mondial et décentralisé. Par ailleurs, il a démontré au fil des années toute sa fiabilité - le réseau affiche une disponibilité de 99.98% - ainsi que sa sécurité - le système de blockchain publique n'a jamais été hacké. Là où certaines matières premières, à l'instar du pétrole ou du charbon, ont une valeur déterminée par leur demande dérivée⁴⁸, le bitcoin n'en dispose pas. Il est valorisé à hauteur de l'importance de son réseau et de la confiance que les membres de ce réseau accordent dans ce dernier représenté par le jeton. Cette absence de demande dérivée se retrouve également dans des actifs physiques de réserve de valeur comme l'or par exemple⁴⁹.

b. Un crypto-actif évolutif malgré lui

Si la valeur de bitcoin est intimement liée à son réseau, l'attention doit être portée sur l'évolution de ce dernier. Après plus de dix années d'existence, le réseau Bitcoin aurait pu voir son leadership contesté par l'émergence de nouveaux réseaux plus performants entraînant son déclin. Pourtant, le bitcoin reste l'actif le plus capitalisé et de loin.

Chaque protocole blockchain est tenu par une règle intangible dictée par le trilemme de la blockchain. Ce trilemme implique un équilibre entre la scalabilité du système, sa sécurité et la décentralisation de l'ensemble. L'optimisation de chacune de ces caractéristiques se fait au détriment des autres. Ainsi en minorant la décentralisation d'un protocole ou sa sécurité, on accroît la scalabilité. Tout est question d'équilibre et de l'usage recherché.

Bitcoin est un protocole *open source*. Par conséquent, son code peut être copié afin d'en modifier la structure originelle. Ainsi, depuis sa naissance, il a été possible de proposer une version optimisée de ce dernier notamment en modifiant les règles de consensus permettant de sécuriser le réseau. C'est ainsi qu'est né le « Bitcoin Cash ». Toutefois malgré le *fork*⁵⁰ du réseau Bitcoin original, cet avènement n'a pas suffi à réduire la dominance du bitcoin dans la capitalisation globale des crypto-actifs. Début 2022, il reste le leader incontesté des crypto-actifs.

⁴⁸ Le pétrole est consommé pour produire du carburant ou des matériaux transformés ; le charbon pour produire de l'énergie.

⁴⁹ Est éludée la question de la transformation de l'or en bijoux - qui est marginale au regard de la détention de l'or pour stocker de la valeur.

⁵⁰ Un *fork* (en français on parle d'un « embranchement ») désigne une évolution d'une blockchain soit par une modification compatible avec le protocole de base (on parle alors de *soft fork*), soit par une modification incompatible avec le protocole de base, nécessitant la création d'un nouveau réseau (on parle alors de *hard fork*).
Source : Assemblée nationale - [Rapport n°1624 de la mission d'information relative aux monnaies virtuelles](#) - 30.01.2019

Et pour cause, le développement de solutions technologiques intitulé Layer-2 a permis d'optimiser indirectement le fonctionnement des protocoles sans pour autant nécessiter la modification dudit protocole initial. Ainsi les Layers-2 reposant sur différents mécanismes (*sidechain*, *plasma* ou *ZKrollup*) ont permis d'optimiser la chaîne principale en exécutant des opérations en parallèle. Avec le projet Lightning Network, Bitcoin a su dépasser les limites liées à sa construction initiale. En concentrant les transactions *off-chain*, il aura permis d'accroître massivement le nombre de transactions par seconde. Cette adaptabilité permet à Bitcoin d'être davantage résilient vis-à-vis de protocoles tiers plus efficaces.

c. Un crypto-actif soumis à un coût de production

Au-delà de la valeur conférée par son réseau, le bitcoin est valorisé par son coût de production. En effet, il est erroné de considérer qu'il n'a pas de valeur intrinsèque dans la mesure où il n'est pas « produit », comme peut l'être l'or pris comme réserve de valeur. En réalité, le bitcoin a un coût de production et ce dernier est la résultante de plusieurs composantes : le prix d'acquisition des machines de minage, le prix de l'électricité, le montant de la récompense de validation du bloc et la difficulté de résolution de l'énigme de validation. Le coût de production du bitcoin est par conséquent très variable en fonction de la structure des charges de chaque mineur. Un mineur individuel qui déciderait de miner sur sa propre carte graphique et avec de l'énergie au prix du marché français aura un coût plus élevé qu'un mineur industriel alimenté par de l'énergie renouvelable ayant négocié ses machines sur le marché du gros. Ce point est davantage détaillé ultérieurement.

d. Un crypto-actif concurrencé

En dépit de l'importance de Bitcoin pour l'écosystème, d'autres réseaux ont émergé en 2020, présentant des caractéristiques novatrices. Ainsi, le réseau Ethereum a progressivement pris une place centrale avec l'émergence de la finance décentralisée⁵¹ à partir de 2019. Ce dernier occupe dorénavant une position incontournable dans l'univers des crypto-actifs, puisqu'il constitue le socle d'une majorité d'applications de finance décentralisée. En raison de sa structure et de la grande programmabilité des *smart-contracts*, ce réseau est un « bac à sable » permettant de faire émerger de nombreux cas d'usage. Le potentiel d'adaptabilité d'Ethereum dont les évolutions et mises à jour sont pilotées par la fondation du

⁵¹ Les sujets relatifs à la finance décentralisée sont abordés en partie IV du présent rapport.

même nom est quasiment illimité. Ceci lui permet de faire évoluer sa structure et son protocole. L'emballement est tel que les innovations s'y développent à un rythme effréné, de sorte que l'écosystème de 2020 ne ressemble plus à celui de 2021. Entre-temps, de nombreux Layer-1 sont apparus afin de concurrencer Ethereum et permettant d'accroître encore plus le nombre d'applications de finance décentralisée (Elrond, Polkadot, BinanceSmartChain, Atom, Solana).

Ce fonctionnement sous forme de réseau est l'axe principal de développement des protocoles blockchain. En effet, la valorisation d'un protocole résulte essentiellement de son réseau. Chaque protocole doit attirer les développeurs et les capitaux afin de faire croître l'ensemble du dispositif et notamment la valeur de son jeton.

Si le nombre d'applications attachées au réseau Bitcoin lui est limité, le nombre d'utilisateurs du réseau est en croissance permanente. C'est donc moins dans ses applicatifs - bitcoin étant une monnaie plus qu'un jeton utilitaire - qu'il attire toujours de plus en plus d'utilisateurs. *De facto*, le réseau Bitcoin possède une position dominante qui ne semble pas pouvoir être remise en cause à court terme. Toutefois, ce constat n'est durable qu'à la seule condition que ses utilisateurs croient éternellement en ses qualités extrinsèques, l'accomplissement de la prophétie monétaire originelle.

3. La valorisation extrinsèque de bitcoin, résultante de la parole d'Évangile selon Satoshi

Le bitcoin revêt donc une valeur intrinsèque. Toutefois, il ne peut être uniquement valorisé par sa seule structure technologique et économique. Une telle démonstration reviendrait à faire fi des qualités que ses détenteurs voient en lui. Valeur refuge ou futur étalon monétaire mondial, ce sont autant de qualités transcendées en destinée. bitcoin ne peut plus être regardé comme une simple monnaie ou un simple actif spéculatif.

Afin de mieux comprendre la réalité de l'objet vis-à-vis de ses qualités supposées, il convient de replacer son comportement au regard du contexte macro-économique dans lequel il évolue depuis une décennie, marqué par un double mouvement de balancier.

Dans un premier temps, la politique de taux bas induite par la nécessité de faire baisser la pression sur les États européens endettés a prévalu depuis 2015. Cette politique a été permise par le « *quantitative easing* ». Cette politique consiste pour

une banque centrale, à intervenir de façon massive, généralisée et prolongée sur les marchés financiers en achetant des actifs - notamment des titres de dette publique - aux banques commerciales et aux acteurs institutionnels. Ces achats massifs ont pour incidence d'opérer une pression baissière sur les taux d'intérêts. Toutefois, cette politique n'est pas sans conséquence. En sus des effets néfastes et inégalitaires d'une telle politique expansionniste sur la répartition des richesses, l'absence de rentabilité du marché obligataire a conduit à ce que les investisseurs se précipitent sur les marchés des actifs dits risqués, bitcoin en tête (ces dernières années ont démontré qu'il était l'actif risqué par excellence).

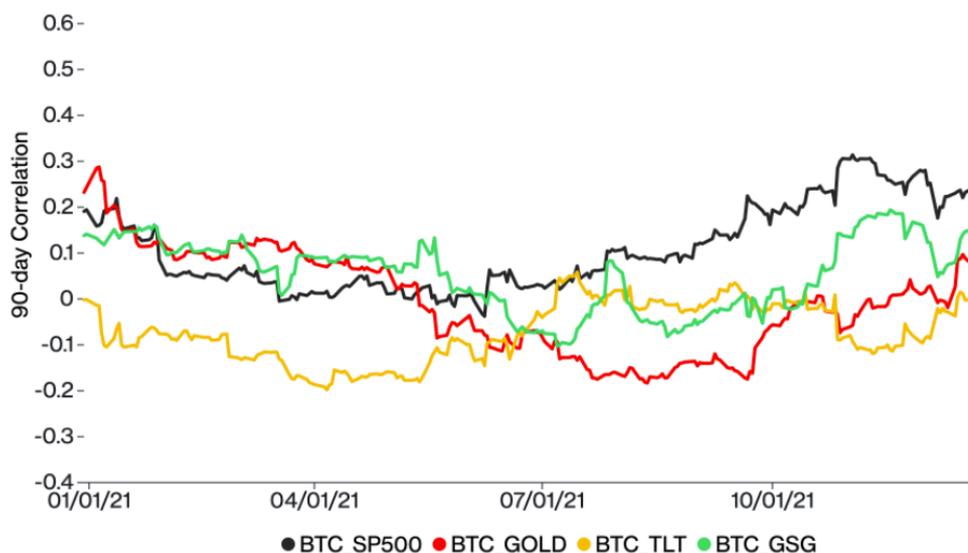
Autre facteur, l'approvisionnement en matière première a été profondément déstabilisé par l'épidémie de la Covid-19. Les chaînes de production et la logistique du transport maritime ont subi de fortes perturbations. L'inflation, que de nombreux économistes n'avaient pas voulu voir, s'est déclarée de manière massive et mondiale dès le second semestre 2021. La question est dorénavant posée ; bitcoin peut-il être un équivalent numérique de l'or ? Ou reste-t-il un actif performant dans une configuration macro-économique où les actifs risqués sont prisés et actif refuge lorsque les indicateurs macro-économiques sont en berne ? Peut-il être tout à la fois ?

a. Bitcoin, un actif financier

En tant qu'actif financier, la croissance du cours du bitcoin lui a permis d'enregistrer de solides performances par comparaison aux actifs traditionnels. Conséquence de sa démocratisation et de son institutionnalisation, la demande de bitcoins ne cesse de croître alors que les *tokens* disponibles, limités au maximum à 21 millions, se raréfient. Ces deux tendances antagoniques contribuent à provoquer des tensions sur les cours et explique la performance spectaculaire de l'actif.

Néanmoins, si le bitcoin revêt toutes les caractéristiques d'un actif financier, il s'agit de déterminer s'il est corrélé ou non à la sphère financière traditionnelle. Le bitcoin et les crypto-actifs en général sont sensibles aux aléas du marché traditionnel. En effet, conséquence de sa forte liquidité - l'actif est aisé à vendre - il est le premier à être liquidé des portefeuilles quand l'inquiétude et parfois la panique gagnent les investisseurs. Ainsi, la déferlante mondiale de la Covid au printemps 2020 a infligé au bitcoin l'une des chutes les plus importantes parmi tous les autres actifs. Il est également particulièrement sensible aux positions réglementaires des principales puissances telles que les États-Unis et la Chine.

Récemment la forte correction du NASDAQ ou du SP500, couplée à la remontée du dollar dans un contexte d'inquiétude suite à l'invasion de l'Ukraine et au retour de l'inflation, a démontré une forte corrélation entre les actifs considérés comme risqués et les crypto-actifs, bitcoin au premier chef. Lorsque les marchés sont haussiers à la défaveur du dollar, le bitcoin apparaîtrait comme un actif performant. Dans les phases rémunérant moins la prise de risque, le cours du bitcoin a tendance à corriger. Or, si le bitcoin peut être une aubaine pour les investisseurs en quête de risque, peut-il également être considéré comme une réserve de valeur par ceux cherchant à se préserver du retour de l'inflation ?



CoinDesk - Corrélation sur 90 jours du bitcoin avec différents actifs traditionnels en 2021⁵²

b. Bitcoin, une réserve de valeur

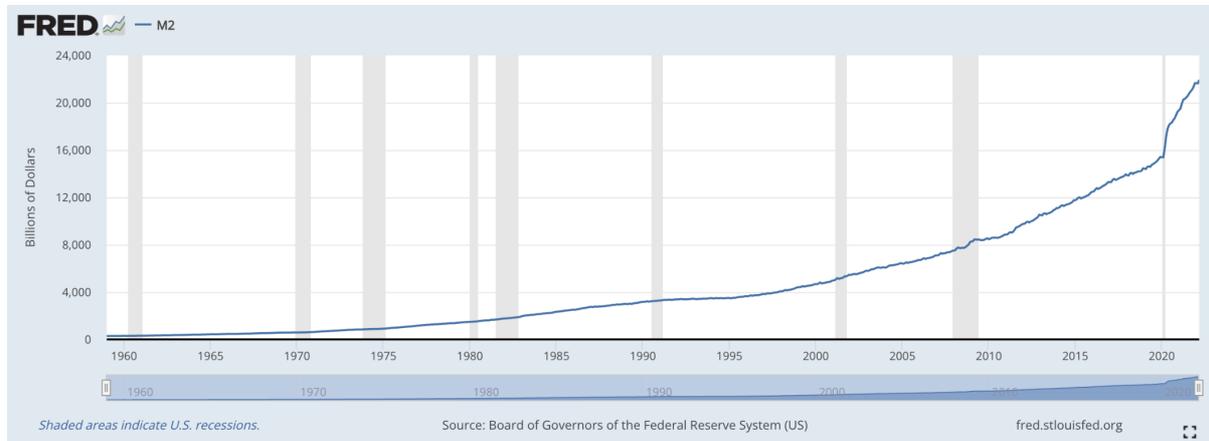
Le bitcoin est fréquemment assimilé à de l'or numérique. De nombreux détenteurs le considèrent comme un actif refuge. Les plus convaincus ont fait le choix de ne jamais vendre leurs bitcoins et ce, quelle que soit l'évolution des cours : c'est le phénomène dit de « *hodling* »⁵³. Toutefois, si cette stratégie s'est révélée être substantiellement profitable, il ne s'agit pas uniquement d'une logique d'investissement. Le *hodling* est avant tout la résultante d'une croyance dans le rôle de l'actif et sa place dans un nouvel ordre monétaire. En effet, les détenteurs de

⁵² Explication de graphique : La courbe noire représente la corrélation du bitcoin avec l'indice du marché actions américains, le S&P 500. La courbe rouge représente la corrélation du bitcoin avec l'or. La courbe jaune représente la corrélation du bitcoin avec l'ETF i Shares 20+ Year Treasury Bond, représentant le marché obligataire. La courbe verte représente la corrélation du bitcoin avec l'indice iShares S&P GSCI Commodity-Indexed Trust.

Source : CoinDesk - [Why Portfolio Managers Will Need to Look at Altcoins in 2022](#) - 26.12.2021

⁵³ Terme, répandu dans la culture bitcoin, pour définir la pratique qui consiste à conserver ses crypto-actifs - quels que soient l'évolution des cours - sans les vendre.

bitcoin sont nombreux à critiquer l'actuel système monétaire, sa gouvernance et les politiques qui en émanent. Ils font le pari que, face à la perte de valeur des monnaies traditionnelles en perpétuelle augmentation, le bitcoin sera un moyen de protéger leur pouvoir d'achat.

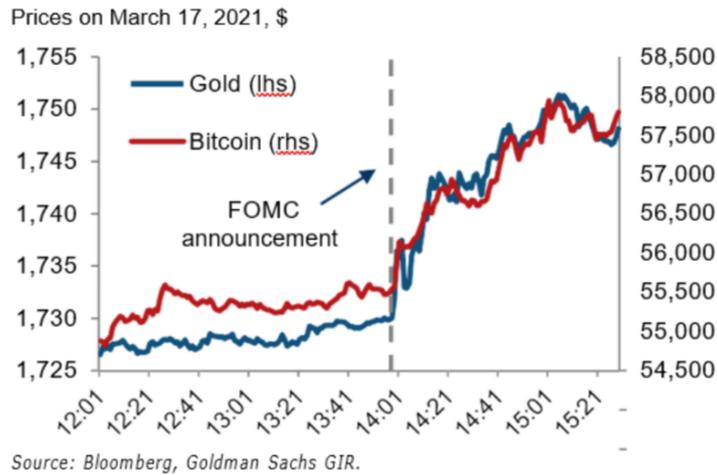


Federal Reserve Economic Data - Agrégat monétaire M2 des dollars en circulation entre 1960 et 2022⁵⁴

En outre, conséquence des politiques monétaires expansionnistes ainsi que de la reprise économique post-Covid, l'inflation a fait son grand retour. Dans ce contexte, les acteurs économiques ont cherché à se protéger de la perte de pouvoir d'achat occasionnée. Le bitcoin a alors été considéré par certains comme un actif de réserve - comparé à l'or, sous format numérique. A cet égard, des analystes ont mis en évidence que le bitcoin réagissait à certains événements macro-économiques de la même manière que ce métal précieux. Lors de la décision de la FOMC⁵⁵ datée du 17 mars 2021, Jerome Powell, président de la Fed, avait alors annoncé maintenir la politique de rachat d'actifs afin de soutenir la politique budgétaire américaine. Cette annonce en faveur du soutien à une politique monétaire expansionniste a eu pour effet immédiat d'accroître la demande des investisseurs sur les actifs de réserve, comme l'or mais également le bitcoin. En outre, les récentes annonces relatives à l'inflation ont parfois eu un léger effet haussier sur le cours du bitcoin.

⁵⁴ FRED - [M2 and components](#)

⁵⁵ La *Federal Open Market Committee*, ou FOMC, est un organe de la Réserve Fédérale américaine, ou Fed, chargée de diriger la politique monétaire des États-Unis.



Goldman Sachs - Évolution du cours de l'or et du cours du bitcoin le 17 mars 2021⁵⁶

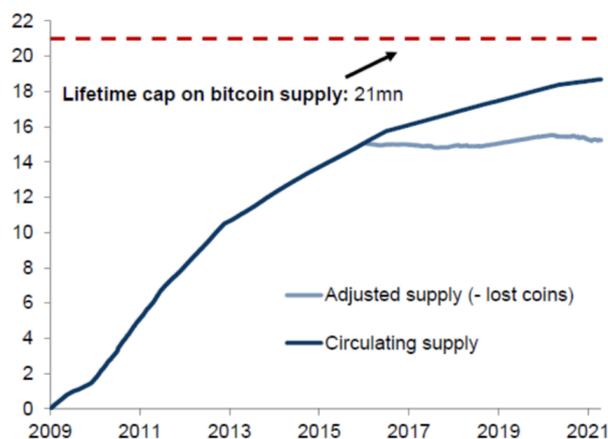
Pour autant, si bitcoin est assimilé à une valeur refuge sur le long terme, il n'a pas démontré qu'il réagissait différemment des actifs dits risqués sur le court terme. En effet, force est de constater que cet actif suit depuis quelques mois la même tendance baissière et correctrice des autres actifs risqués dans un contexte inflationniste et d'incertitude liée à la guerre en Ukraine. Il est par conséquent difficile de considérer qu'il soit assimilé sur le court terme par les investisseurs, notamment traditionnels, comme une valeur refuge à l'instar des obligations et métaux précieux.

Toutefois, depuis l'éclatement de la bulle ICO, le phénomène de *hodling* s'est renforcé pendant le marché baissier de 2018 à 2020. Nombreux des petits porteurs pour lesquels l'horizon d'investissement était court-termiste, sont venus rejoindre les rangs des « holders ». Durant cette période, le phénomène d'accumulation s'est accru. Les portefeuilles de long terme ont par conséquent continué à acheter une partie de l'offre présente sur les marchés sans jamais la vendre. Cette croyance dans le long terme, qu'il s'agisse de particuliers plus confiants ou d'acteurs institutionnels plus robustes, est un nouvel indicateur de la maturité du bitcoin vers un actif de réserve de valeur.

En outre, cette logique de réserve de valeur modifie la nature même du bitcoin en lui attribuant un caractère illiquide. Afin d'expliquer ce phénomène, il convient de préciser ce qu'est l'état de la détention du bitcoin à l'écriture de ces lignes.

⁵⁶ Goldman Sachs - [Global Macro Research – Crypto: A New Asset Class?](#) - 21.05.2021

Le 12 décembre 2021, le 18.899.000^{ème} bloc fut miné. Par conséquent, le réseau Bitcoin a émis environ 90% du montant total de bitcoins, soit 19 millions de *tokens* sur un total de 21 millions. Si l'offre est limitée dans le temps, il est important de préciser que l'ensemble des jetons émis ne sont pas disponibles sur les *exchanges*. En effet, une part substantielle des bitcoins en circulation est considérée comme « perdue ». Cette quantité est aisée à quantifier dans la mesure où ces bitcoins n'ont fait l'objet d'aucun mouvement depuis plus de sept ans. Depuis l'émission du premier bitcoin, de nombreux *tokens* sont aujourd'hui bloqués sur des adresses inaccessibles (pour différentes raisons : hack ; perte de mot de passe ; etc ...). On estime à environ trois millions le nombre de bitcoins devenus inaccessibles et inutilisables de manière irrévocable.



Goldman Sachs - Volume total et ajusté de bitcoins en circulation entre 2009 et 2021

Ainsi, environ 16 millions de bitcoins sont effectivement détenus par des entités du réseau et peuvent être échangés sur les *exchanges*. Néanmoins, s'ils peuvent être vendus et achetés, une tendance à la conservation de longue durée s'est dessinée chez les investisseurs, ce qui nuit à la liquidité des échanges et favorise une hausse de son cours. En effet, selon une étude publiée par Glassnode⁵⁷, environ 14,5 millions de bitcoins seraient illiquides - ce qui représente plus de 75% de l'ensemble des *tokens* en circulation. Cela signifie que seulement 4 millions sont liquides et actuellement disponibles à l'achat et à la vente sur les *exchanges*.

⁵⁷ Glassnode - [78% of the Bitcoin Supply is Not Liquid](#) - 29.12.2020

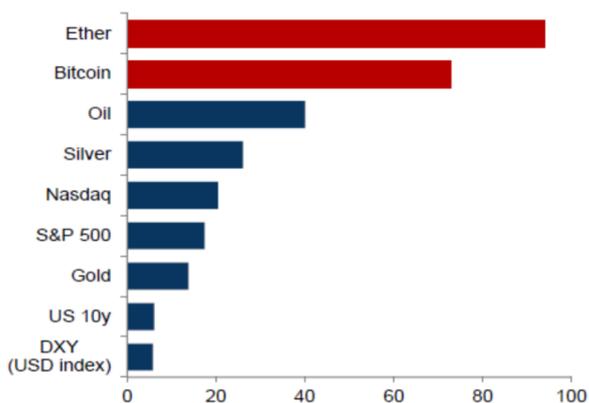
Bitcoin: Liquid and Illiquid Supply



Glassnode - Évolution du prix et de la liquidité du bitcoin entre 2009 et 2020

Cette illiquidité s’explique par deux causes : (i) elle est la résultante d’une stratégie de conservation de la valeur par les différents détenteurs, que leurs motivations soient politiques ou financières ; (ii) les investisseurs font le pari que le prix du bitcoin aura tendance à s’apprécier avec le temps et en fonction de sa démocratisation. Or, cette dernière stratégie semble être une forme de prophétie auto-réalisatrice dans la mesure où cela réduit l’offre de bitcoins en circulation sur les marchés et provoque des tensions à la hausse sur son cours.

Average daily volatility in ann. terms, %



Note: Based on returns since 2014 and since 2015 for ether.
Source: Bloomberg, Goldman Sachs GIR.

Goldman Sachs - Indice de volatilité de certains actifs, entre 2014 (bitcoin et autres) ou 2015 (ether) à 2021⁵⁸

Néanmoins, cette stratégie de conservation et de valorisation à long terme doit prendre en considération la forte volatilité de cet actif. En effet, en seulement une année, le prix du bitcoin aura oscillé entre 27.000\$ et 69.000\$. Cette instabilité peut s’avérer problématique pour un actif dont la fonction serait de stocker la valeur à court terme.

⁵⁸ Goldman Sachs - [Global Macro Research – Crypto: A New Asset Class?](#) - 21.05.2021

Il doit être noté toutefois que l'institutionnalisation du bitcoin a tendance à réduire cette volatilité. Par ailleurs, Bloomberg a pu relever que cette instabilité était caractéristique des débuts des nouvelles offres du numérique. À titre de comparaison et d'exemple, le cours de l'action Amazon a connu lui aussi, à l'origine, une forte volatilité de son cours. Celle-ci s'est réduite également, à l'image de celle du bitcoin qui se rapproche progressivement de la volatilité de l'action du géant américain.



Bloomberg - Évolution du cours du bitcoin et de l'action Amazon et de leurs volatilités respectives entre 1999 et 2022⁵⁹

Certains considèrent que le bitcoin ne pourra être une réserve de valeur, dans la mesure où il ne trouve pas de cas d'usage dans le monde physique. *A contrario*, l'or fait l'objet d'une fascination quasi homogène sur l'ensemble du globe. Il est utilisé pour la création de bijoux, ou autres ornements ayant contribué à exprimer la richesse et l'opulence des civilisations à travers les siècles.

Toutefois, un actif devient aussi une réserve de valeur, non pas seulement en raison de ses qualités intrinsèques, mais du fait de son adoption par une ou plusieurs sociétés comme telle. Anciennement Blockchain Partner, société spécialisée dans l'expertise blockchain et nouvellement associée au cabinet d'audit et de conseil KPMG, a dressé le parallèle entre l'or et le bitcoin permettant de comprendre l'assimilation de ce dernier comme réserve de valeur⁶⁰.

⁵⁹ Bloomberg Crypto Outlook - [Bitcoin making gold redundant?](#) - 03.2021

⁶⁰ Blockchain Partner by KPMG - [Cryptoactifs : vers une révolution financière](#) - 06.2021

S'agissant de l'or, il est relevé que son histoire et sa composition ont conduit une grande majorité des pays à l'exploiter et à le posséder pour ses qualités propres. L'or est, par ses qualités esthétiques, un signe ostentatoire de richesses et de pouvoir, considéré de manière uniforme et échangé partout dans le monde. En outre, il s'agit d'un métal qui peut être travaillé et transformé en bijoux, pièces de monnaie, ornements. Il est également divisible en de petits volumes afin d'assurer sa conservation ou son transport. Par ailleurs, l'or est l'un des métaux qui résiste le mieux à l'usure du temps. Enfin, il s'agit d'une ressource naturelle qui, *a priori*, est disponible en quantité limitée sur Terre. L'offre d'or reste rare malgré l'exploitation de ressources minières qui implique sa légère augmentation à travers les années. Pour toutes ces raisons, non exhaustives et qui ne reflètent pas la longue histoire de la place de l'or dans la société, ce métal est devenu une réserve de valeur privilégiée ainsi qu'un référentiel refuge lors des chocs économiques.

S'agissant du bitcoin, s'il peut devenir une valeur refuge, c'est moins en raison de la place qu'il occupe dans l'histoire que de ses qualités qui font de lui l'or numérique du XXI^{ème} siècle. Il n'aura certes jamais le caractère esthétique de l'or, mais il n'en est pas moins dénué d'usage. Précédemment évoqué, le bitcoin est un outil numérique de transfert de la valeur dans des conditions de sécurité optimale. Il est à la fois la devise et le réseau de paiement. Par conséquent, il n'est pas uniquement détenu pour y stocker de la valeur, il est aussi un instrument économique au service d'acteurs de l'économie réelle. Sa fongibilité et sa liquidité sont fortes. Par ailleurs, il est possible de diviser un bitcoin un grand nombre de fois, chacun étant composé de satohis⁶¹ et étant divisible jusqu'à 10^{-8} . Or, contrairement à l'or, dont le fractionnement nécessite un procédé industriel coûteux, le fractionnement du bitcoin résulte d'une simple transaction à hauteur du montant transféré. Par ailleurs, sa résistance n'est plus à prouver, le réseau Bitcoin n'a subi aucun hack ni d'interruption de service depuis son émission. Enfin, au même titre que l'or, l'offre totale de bitcoins est limitée à 21 millions de *tokens* et reproduit ainsi la rareté de certaines ressources naturelles.

Ces caractéristiques communes expliquent la métaphore de l'or numérique utilisée pour désigner le bitcoin comme réserve de valeur. Toutefois, de par sa nature intrinsèque, le bitcoin revêt des avantages qui dépassent largement celui de l'or physique.

⁶¹ Du nom du fondateur présumé du réseau Bitcoin, Satoshi Nakamoto.

Contrairement à l'or, le bitcoin n'impose pas d'infrastructure spécifique pour être stocké et déplacé. Du fait de sa forte liquidité, de son coût de transport extrêmement faible et un coût de stockage nul, il est bien plus accessible que l'or. Néanmoins, pour tout détenteur de crypto-actifs, il est nécessaire de se poser la question du stockage de ces derniers. Ainsi, la conservation de *tokens* via un portefeuille propre (*unhosted wallet*) n'induit pas les mêmes risques de perte ou de hack que lorsque la conservation est déléguée à un tiers, acteur centralisé. Ainsi, un arbitrage doit être réalisé entre la conservation auprès de tiers (notamment les *exchanges* ou acteurs dit « *custodians* »), la conservation en propre sur un stockage physique (*hardware wallet*) ou un stockage connecté (*software wallet*). En la matière, la société Ledger, première licorne française dans le domaine, est devenue le leader mondial des *hardware wallet*.

Outre la question du stockage, l'autre atout de bitcoin reste sa résistance à la censure qui découle directement de son caractère décentralisé. En effet, là où les stocks d'or sont généralement gérés par des prestataires spécialisés soumis à la réglementation, les bitcoins sont détenus sur le réseau éponyme, par nature insaisissable. Cette résistance à la censure est salutaire face à la répression issue de régimes autoritaires.

4. La place de Bitcoin dans la lutte contre le réchauffement climatique

Le présent rapport s'attache, dans les prochains développements, à traiter de la question des implications énergétiques de Bitcoin. En effet, il est indispensable de revenir sur les arguments et préjugés de ceux qui disqualifient les crypto-actifs par la seule question de la consommation énergétique issue de la « preuve de travail ». Par conséquent, il est question ici d'essayer de dresser un panorama objectif de la situation afin de mieux éclairer les pouvoirs publics.

a. Une consommation énergétique fortement critiquée

Avec l'envolée du cours du bitcoin, l'attention médiatique s'est peu à peu portée sur la consommation présumée du réseau Bitcoin en électricité. Ainsi de nombreuses voix, acteurs politiques, journalistes ou chercheurs, se sont élevées pour critiquer son empreinte carbone. Selon certains, ce réseau serait un contributeur substantiel aux émissions mondiales de CO₂. À tel point que Bitcoin pourrait être cité comme co-responsable de l'échec des politiques et objectifs environnementaux de l'Accord de Paris. En janvier 2022, Erik Thedéen, vice-président de l'Autorité

européenne des marchés financiers (ESMA) a annoncé envisager d'interdire pour cette raison les blockchains reposant sur le consensus de validation reposant sur la preuve de travail⁶² (en anglais, on parle de *proof-of-work* ou PoW)⁶³. À l'écriture de ces lignes, l'interdiction de la PoW est largement défendue par la gauche de l'hémicycle européen dans le cadre de la réglementation à venir MICA - *Market In Crypto Assets*. Ce sujet étant omniprésent dans le débat public, il convient de procéder à un état des lieux des thèses et études ayant trait à la consommation énergétique de Bitcoin.

Selon une étude de l'Université de Cambridge⁶⁴, la consommation annuelle de Bitcoin - au travers des opérations de minage nécessaires à la validation des blocs de la blockchain - serait comprise dans une fourchette de 130 à 147 TWh, soit environ 0,6% de l'électricité produite dans le monde. Cette consommation est comparable à celle de la Suède ou de l'Égypte. Cette estimation a toutefois été minorée par Galaxy Digital qui, dans un rapport paru en mai 2021⁶⁵, a eu l'occasion d'estimer la consommation énergétique de Bitcoin aux environs de 113,89 TWh par an.

Annual Electricity Consumption of the Bitcoin Network					
Miner Demand (GW)	Miner Electricity Consumption (kWh/yr)	Pool Electricity Consumption (kWh/yr)	Node Electricity Consumption (kWh/yr)	Total Electricity Consumption (kWh/yr)	Total Electricity Consumption (TWh/yr)
15.87	113,880,000,000	8,609,328	5,358,089	113,893,967,417	113.89

Galaxy Digital Mining - Consommation annuelle du réseau Bitcoin en énergie en 2020

Selon ses détracteurs, Bitcoin serait un « *gouffre énergétique et donc un désastre écologique* »⁶⁶. Par conséquent, il constituerait un obstacle à part entière à la transition écologique. Ce point a notamment été mis en lumière par la revue *Nature*⁶⁷, dans une étude relative aux activités de minage en Chine, publiée en avril 2021. Ses auteurs concluent que, sans intervention publique, la consommation

⁶² Pour plus d'informations, cf. [Rapport d'information n°1624](#) rendu dans le cadre de la mission d'information relative aux monnaies virtuelles de l'Assemblée nationale.

⁶³ Les Echos - [Bitcoin : l'Esma s'inquiète des méthodes de minage énergivores](#) - 19.01.2022

⁶⁴ University of Cambridge - [3rd Global Cryptoasset Benchmarking Study](#) - 09.2020

⁶⁵ Galaxy Digital Mining - [On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question](#) - 05.2021

⁶⁶ Reporterre - [Le Bitcoin, monnaie virtuelle mais gouffre environnemental réel](#) - 04.2021

⁶⁷ Nature - [Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China](#) - 06.04.2021

énergétique annuelle correspondant à l'activité Bitcoin en Chine culminerait, en 2024, à 296,59 Twh et générerait environ 130,5 millions de tonnes d'émissions carbone, soit l'équivalent de 5,41% des émissions liées à la production d'électricité.

Il ne s'agit pas ici de contester les chiffres avancés dans cette étude sérieuse mais d'y apporter certaines précisions et nuances. La « géopolitique du bitcoin » est par exemple un angle mort de cette publication. L'implantation de fermes de minage peut être tantôt perçue comme une nouvelle manne financière pour un gouvernement local et un moyen de construire des infrastructures produisant de l'énergie renouvelable, tantôt comme une menace pour l'équilibre énergétique à destination des populations civiles. Ces différents éléments doivent être pris en compte afin de pouvoir évaluer sans manichéisme la question.

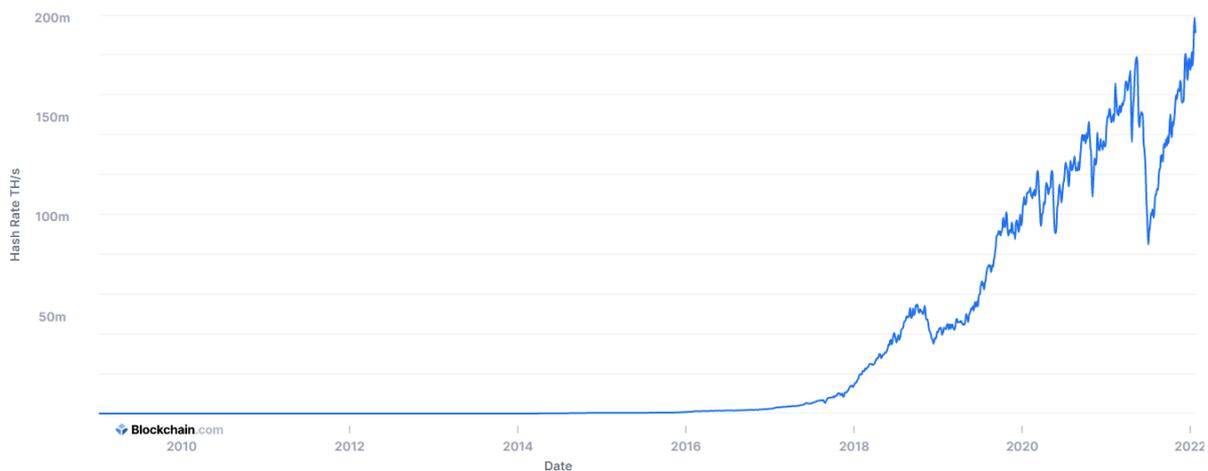
b. La consommation énergétique du réseau Bitcoin, un élément consubstantiel de sa valeur

Le Bitcoin, comme certains autres crypto-actifs, repose sur une technologie blockchain ayant comme méthode de validation des blocs la *proof-of-work*. Cette dernière implique la résolution d'un calcul mathématique complexe rendu possible par le travail de machines de minage, des ordinateurs disposant d'une capacité de calcul importante et qui sont chargés de résoudre cette énigme mathématique. Une fois qu'un bloc est validé par un mineur, celui-ci reçoit, en contrepartie de la puissance de calcul qu'il a déployée, une récompense en bitcoins⁶⁸ à laquelle s'ajoutent les frais payés par les utilisateurs du réseau Bitcoin lors de leurs transactions.

Or, avec l'augmentation continue du cours du premier des crypto-actifs, cette récompense n'a évidemment pas la même valeur en dollars au 15 mars 2019 (environ 4.000\$ pour un bitcoin) qu'au 15 novembre 2021 (environ 60.000\$), ni même au 25 janvier 2022 (environ 36.000\$). L'extraction de bitcoins constitue par conséquent une source de profit substantielle pour les détenteurs de machines de minage et en fait un secteur extrêmement compétitif. Cette « course à l'or numérique » a emmené avec elle de nouveaux mineurs en recherche de profits. La plupart se constituent en « pool » de mineurs et forment ainsi de véritables entreprises industrielles.

⁶⁸ Depuis le *halving* de mai 2020, cette récompense est désormais de 6,25 bitcoins.

L'afflux de nouveaux mineurs induit une augmentation de la puissance de calcul présente sur le réseau. De surcroît, cela a pour incidence d'accroître la rapidité de validation d'un bloc. Néanmoins, le protocole Bitcoin est pensé pour que la difficulté de l'énigme mathématique soit réévaluée afin qu'un bloc ne puisse être miné en moins de 10 minutes. Ainsi, la production monétaire de bitcoins se lisse sur la période, quelle que soit la puissance de calcul globale⁶⁹.



Blockchain.com - Évolution du hashrate total de Bitcoin entre 2009 et 2022⁷⁰

En parallèle, l'augmentation récente des cours du bitcoin a produit une augmentation substantielle de la rentabilité de l'activité de minage, conduisant notamment à un choc de la demande sur les micro-processeurs qui composent les ordinateurs. Ce choc de demande s'est plus précisément traduit sur le marché des cartes graphiques, dites GPU, dans un contexte Covid de fortes pénuries de micro-processeurs.

Il convient de préciser pour la bonne compréhension du lecteur, que la compétition entre les mineurs se joue sur trois terrains. Ces derniers constituent l'essentiel des facteurs relatifs à la compétitivité de l'activité de minage, le coût de l'électricité, les charges liées à l'investissement en matériel et sa productivité en fonction de la difficulté de minage à un moment donné, et enfin le prix du bitcoin sur les plateformes d'échange.

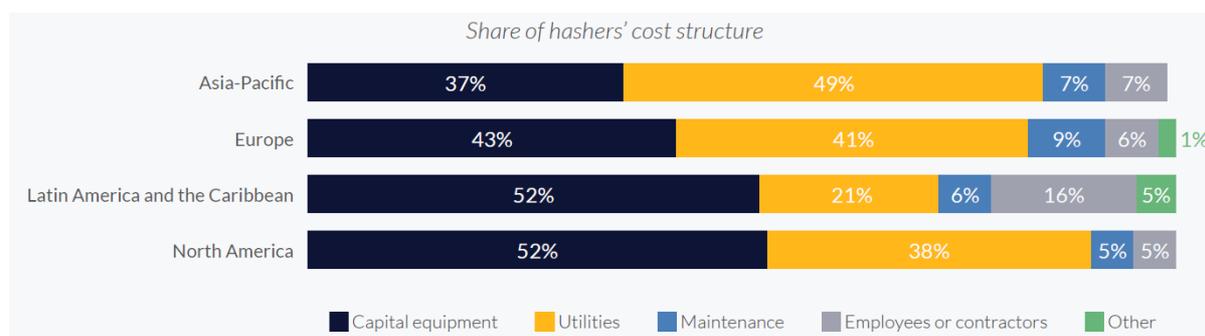
⁶⁹ On parle de *hashrate*.

⁷⁰ Blockchain.com - [Mining information – Total Hash Rate \(TH/s\)](#)

i. *L'électricité : la ressource clé des mineurs*

Au cœur du processus de validation des blocs par PoW se trouve l'électricité. Carburant indispensable au fonctionnement des composants électroniques, il représente l'investissement réel et physique nécessaire à la sécurisation de la blockchain Bitcoin. Ainsi, la structure économique du réseau incite les mineurs⁷¹ à fournir davantage de puissance de calcul lorsque les cours augmentent, avec la consommation d'énergie que cela suppose. En revanche, quand les cours baissent, la rentabilité de chacun des apporteurs de puissance au réseau baisse. Par conséquent, seuls ceux qui ont une énergie à bas coût et qui ont su maîtriser leurs charges liées à leurs investissements peuvent survivre. Le cours a donc une incidence sur le *hashrate* et celui-ci a réciproquement une incidence sur le cours du bitcoin.

Comme évoqué ci-dessus, la structure des coûts des mineurs s'articule entre les dépenses d'investissements (infrastructures, ordinateurs, etc ...) et les dépenses opérationnelles (qui sont pour l'essentiel des dépenses liées à l'électricité).



Université de Cambridge - Structure de coûts des mineurs selon les régions en 2019

À cet égard, on constate qu'il existe une vraie différence de stratégie entre d'une part les mineurs nord-américains et européens et d'autre part les mineurs asiatiques. En effet, les premiers consacrent une part plus importante de leur budget à l'acquisition de machines plus performantes et moins énergivores quand les seconds favorisent des machines de minage à bas coût, induisant une moindre efficacité énergétique. Ce choix est avant tout dicté par le contexte énergétique global. Lorsque les mineurs étaient encore admis en Chine, ils pouvaient bénéficier d'une électricité à très bas coût (notamment grâce à l'importante production de charbon et aux surplus hydroélectriques). Les fermes de minage étant extrêmement mobiles, les mineurs pouvaient se permettre de déplacer leurs activités en fonction

⁷¹ C'est-à-dire les personnes ou entités possédant et gérant des machines de minage, qu'ils soient professionnels ou non.

des coûts de l'énergie et donc de consommer davantage sans subir de hausse substantielle de leurs coûts de production.

En parallèle et pour optimiser leurs rendements, les mineurs ont tendance à rechercher les prix d'électricité les plus bas. Cela a conduit la grande majorité d'entre eux à ne plus payer les prix de l'électricité résidentielle, mais ceux, moins élevés, réservés aux entreprises contractant leurs tarifs avec les producteurs d'électricité.

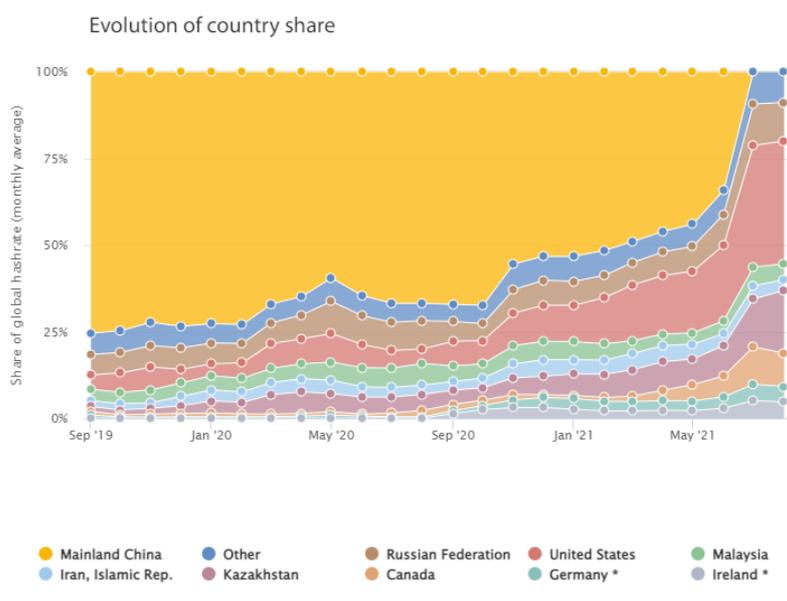
Au-delà des accords conclus avec les fournisseurs d'électricité, les coûts opérationnels des mineurs peuvent aussi être réduits *via* les aides ponctuelles des gouvernements. Ainsi, certains pays optent pour une politique incitative à l'endroit de cette nouvelle industrie, à l'aide de subventions ou d'exonérations fiscales. Elles sont toutefois relativement rares. Selon l'étude de Cambridge, seuls 23% des mineurs reçoivent un soutien financier de la part du gouvernement de l'État dans lequel ils exercent leurs activités. Il s'agit principalement du cas du Kazakhstan.

Toutefois, après avoir posé clairement ce constat et explicité le modèle de rentabilité du secteur, il ne s'agit pas de savoir si les mineurs de bitcoins consomment trop d'électricité, mais davantage de connaître l'origine de cette électricité. Contrairement aux rapports précédemment évoqués, il convient de s'intéresser à sa provenance et aux implications de l'activité de minage dans la production d'énergie. En effet, décrire l'industrie du minage à l'aune de sa seule consommation électrique brute serait faire preuve de myopie au regard de la complexité d'une industrie qui implique des incidences non négligeables sur le secteur de l'énergie.

ii. Une ressource aux origines diverses

La Chine a longtemps été la place forte du minage de bitcoins dans le monde. À elle seule, elle concentrait plus des deux tiers de cette activité. Sa politique industrielle l'a conduite à développer un mix énergétique basé sur le charbon et sur l'hydroélectrique. Cette dualité lui a permis de conserver une électricité à très bas coût toute l'année : hydroélectricité à la saison des pluies dans le sud du pays, centrales à charbon plus au nord le reste de l'année. La première étant souvent produite de manière excédentaire, la seconde demeurant l'une des énergies les moins onéreuses au monde.

Or, en mai 2021, la Chine a engagé une politique de répression et d'expulsion des mineurs. Cette décision a provoqué une chute drastique du *hashrate* et, par voie de conséquence, du cours du bitcoin⁷². Depuis, le *hashrate* a retrouvé ses plus hauts historiques. Quant aux mineurs, ils se sont réimplantés dans d'autres pays en abandonnant la Chine. Cette décision fut certainement motivée par l'hostilité des gouvernements à l'égard d'une monnaie décentralisée, alors même que le régime chinois s'emploie à centraliser les moyens monétaires du pays autour du e-Yuan. Les États-Unis ont été les grands gagnants de cette transhumance, multipliant leur production de puissance de calcul par dix depuis septembre 2019, et atteignant même en août 2021 plus du tiers de la production mondiale.



Université de Cambridge - Évolution de la répartition du hashrate total selon les pays de septembre 2019 à août 2021

Outre les États-Unis, les mineurs basés en Chine se sont également reportés sur le Kazakhstan, devenu deuxième puissance mondiale du *hashrate* dédié au réseau Bitcoin. Or, ce pays fait face à une crise énergétique majeure, se matérialisant par une succession de coupures d'électricité au niveau national⁷³ et par un doublement des prix des carburants. Cette crise, sans précédent, a entraîné une forte protestation populaire dans le pays. Le gouvernement, revenant aux anciennes doctrines de l'ordre soviétique, a réprimé avec force les manifestants, avec l'appui de Moscou⁷⁴. Or, selon plusieurs sources, la crise énergétique - eu égard aux

⁷² CNBC - [Bitcoin price falls after China calls for crackdown on Bitcoin mining and trading behavior](#) - 21.05.2021

⁷³ Le Monde - [Le Kazakhstan, le Kirghizistan et l'Ouzbékistan touchés par des coupures massives d'électricité](#) - 25.01.2022

⁷⁴ Le Figaro - [Kazakhstan: analyse d'un mouvement de protestation étouffé par les tanks](#) - 20.01.2022

récurrentes coupures d'électricité - serait due à l'implantation massive de mineurs de bitcoins près des centrales à charbon du pays.

En réalité, la situation est plus complexe. D'une part, l'infrastructure énergétique de cette ex-république soviétique se trouve dans un état de délitement qui l'empêche de fonctionner à la hauteur des besoins de la population. Par conséquent, il n'était pas rare d'observer des coupures d'électricité en raison de la vétusté de certains équipements. D'autre part, l'arrivée massive de mineurs de bitcoins - près de 12% du *hashrate* mondial en août 2021 - a entraîné une pression supplémentaire sur le réseau électrique du pays. D'évidence, les capacités énergétiques du pays n'étaient pas suffisantes pour fournir, dans le même temps, de l'électricité à la population et aux mineurs. Le gouvernement local a, vraisemblablement, choisi de privilégier les revenus financiers induits par l'implantation de fermes de minage à la fourniture de l'électricité des habitants. Les avantages fiscaux et budgétaires du gouvernement local le prouvent par ailleurs.

Lorsque la crise a éclaté, le bitcoin a été vu par beaucoup comme le coupable idéal, alors que la population payait surtout le prix de choix politiques des gouvernants. La question qui se pose alors est de savoir quelle politique publique mettre en œuvre à l'égard du minage de bitcoins, notamment au regard de la capacité énergétique du pays et quel est l'impact écologique de ces choix. Dans le cas du Kazakhstan, le mix énergétique du pays est fortement centré sur le charbon, donc le minage de bitcoins y est particulièrement polluant. En Chine, les fermes de minage alternaient entre une énergie basée sur le charbon - donc fortement carbonée - et une énergie basée sur l'hydraulique - donc faiblement carbonée, d'autant que les mineurs consommaient essentiellement des surplus qui auraient été autrement perdus. Il existe d'autres pays, comme le Canada ou la Suède, dont le mix énergétique est fortement construit autour des capacités hydroélectriques locales et sur lesquelles les mineurs se branchent.

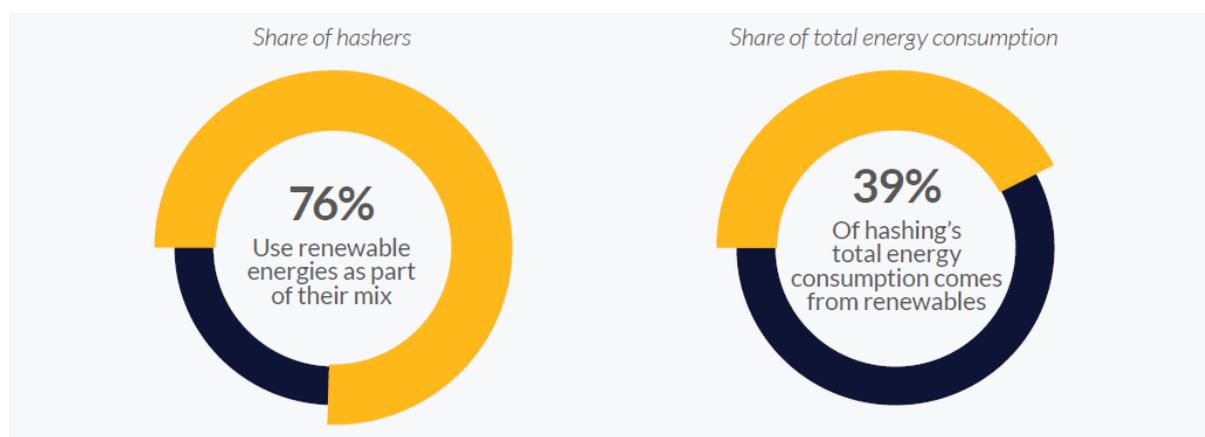
c. Bitcoin, un nouvel instrument au service de la transition écologique

Si l'extraction de bitcoins consomme effectivement beaucoup d'énergie, électricité parfois carbonée, elle peut également être une activité particulièrement efficace pour financer la transition écologique.

i. Un verdissement de l'activité de minage

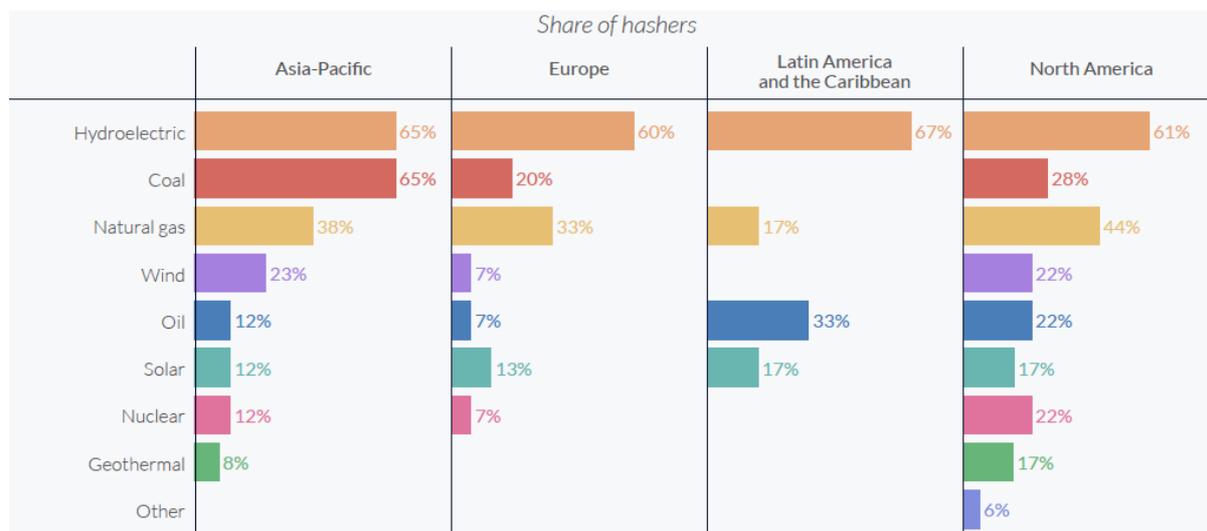
La réalité écologique de Bitcoin est disparate. L'enjeu n'est pas de déterminer si ce réseau est énergivore ou s'il consomme trop d'énergie par rapport au service rendu mais bien de savoir s'il pollue. Il est donc indispensable de faire un état des lieux relatif à la typologie des énergies utilisées par les mineurs à travers le monde.

Si, effectivement, les mineurs issus de Chine - nord du pays - ou ceux qui produisent à ce jour au Kazakhstan ont un mix énergétique principalement centré sur le charbon, il faut aussi rappeler que la tendance est au verdissement des sources énergétiques. Ainsi, l'étude de l'Université de Cambridge démontre que 39 % de la totalité de l'énergie utilisée pour le minage de bitcoins proviendraient de sources renouvelables en 2019 (contre 28 % en 2018), et que 76 % des mineurs utiliseraient des sources renouvelables dans le cadre de leur mix énergétique.



Université de Cambridge - Part du renouvelable dans le mix énergétique des mineurs en 2019

Néanmoins, ce verdissement de l'activité n'est pas homogène selon les différentes régions du monde. Le pourcentage médian des énergies renouvelables en Europe et en Amérique du Nord est relativement élevé, à environ 70 % et 66 % respectivement, tandis que la médiane est beaucoup plus faible en Asie, à 25 %.



Université de Cambridge - Part des différentes énergies dans les activités de minage par région en 2019

Ainsi, dès 2019, une large majorité des mineurs incluait dans son mix énergétique des sources d'énergie hydroélectriques. Néanmoins, les mineurs asiatiques se concentraient davantage sur le charbon. Issues d'un sondage réalisé en 2019, ces données prennent toutefois en compte les cas des mineurs chinois qui ont très largement quitté le pays depuis 2021.

Au-delà du seul prisme altruiste, les mineurs de bitcoins semblent se diriger naturellement vers des sources d'énergie renouvelables. En effet, la source d'énergie et, par conséquent, l'implantation des fermes de minage est un enjeu stratégique pour la viabilité de leurs modèles économiques. Obtenir l'énergie la moins chère possible est donc une question de survie pour les mineurs, car elle représente le poste de dépenses le plus important, après l'investissement en machine. La source d'approvisionnement énergétique doit être relativement stable et peu coûteuse.

Plusieurs éléments viennent soutenir le choix des énergies renouvelables. Premièrement, elles ont l'avantage d'être indépendantes des cours des hydrocarbures et autres minerais. Dans un contexte de flambée et de forte volatilité du pétrole et de nombreuses matières premières, l'indépendance aux gaz, charbons et hydrocarbures est un atout pour la viabilité du modèle économique des mineurs à moyen et long terme.

En outre, la nature de la production d'énergies renouvelables fait d'elles un choix de premier plan pour les mineurs. Leur production intermittente ne correspond pas toujours aux besoins à l'instant T des consommateurs. La production étant difficile à anticiper, elle induit régulièrement d'importants surplus quand les réseaux

de distribution ne sont pas suffisamment dimensionnés. Ainsi, la mauvaise répartition des réseaux de distribution et l'incapacité pour le secteur du renouvelable à stocker l'électricité produite est une aubaine pour les mineurs de bitcoins qui peuvent acheter de l'énergie à bas coût. Il s'agit d'une aubaine réciproque entre producteurs et consommateurs, cette énergie n'aurait pas trouvé preneur.

Le prix du bitcoin sur le marché mondial est une donnée importante à prendre en compte. Quand le bitcoin baisse, la rentabilité des mineurs diminue. L'activité de minage est par conséquent une activité extrêmement concurrentielle. Conséquence de l'augmentation naturelle et géopolitique du cours des matières premières, les mineurs, ayant localisé leur production dans des zones où l'électricité n'est pas issue du renouvelable, seront à terme contraints d'arrêter leur production dans la mesure où les produits des ventes des bitcoins minés ne couvriront plus les charges. Ainsi, la situation économique la plus précaire revient aux mineurs qui ne sont pas consommateurs d'énergie renouvelable.

Autre facteur endogène, la récompense issue du minage attribuée aux mineurs est réduite de moitié tous les quatre ans environ. Elle deviendra nulle en 2140. Or, puisqu'il est impossible d'anticiper le cours du bitcoin dans les prochains mois, voire dans les prochaines années, cette réduction va nécessairement avoir un impact sur le modèle économique des mineurs et donc sur leur structure de coûts. Cela pourrait notamment conduire ceux dont les rendements seraient devenus inférieurs au coût de l'électricité locale, à délocaliser leurs activités dans d'autres pays où l'électricité est encore moins chère.

Il y a donc un véritable pari des mineurs quant aux énergies renouvelables. Il amène certains d'entre eux à accompagner le développement de projets d'infrastructures vertes dans des régions principalement alimentées par des énergies carbonées. C'est notamment le cas du projet financé par BigBlock DataCenter consistant en la construction de plusieurs barrages hydroélectriques dans le parc national des Virunga, en République Démocratique du Congo. Principal objectif : réduire la dépendance énergétique de cette région du monde vis-à-vis du charbon de bois qui ravage l'écosystème local. En effet, l'implantation de fermes de minage près de sites de production émergents présente l'avantage de (i) consommer l'énergie produite par le site sans attendre son raccordement au réseau de distribution (le minage de bitcoins ne nécessitant qu'un accès internet et une source d'électricité), donc (ii) de fournir des revenus supplémentaires aux producteurs d'énergie et ainsi (iii) accroître les financements des projets d'infrastructures vertes. Ce cas d'usage a

également été répliqué en Nouvelle-Zélande. Une ferme de minage a été connectée à un barrage hydroélectrique pour consommer les surplus d'énergie produits⁷⁵. Pour les régions concernées, cela permet également de réduire le coût de financement des sites de production et ainsi d'aligner le prix de l'énergie verte nouvellement créée sur le prix de l'énergie carbonée préexistante.

En extrapolant le dispositif, le Bitcoin aurait la vertu de stocker l'énergie excédentaire en valeur. S'il est aujourd'hui utilisé pour capter l'énergie produite par une centrale non encore raccordée au réseau, le Bitcoin sera utilisé demain pour absorber les surplus produits par toutes sortes de centrales, et ainsi fournir une source de financement supplémentaire aux fournisseurs d'énergie pour l'entretien, le développement, l'optimisation du réseau, etc ...

Outre sa compatibilité avec le réseau électrique, les fermes de minage peuvent également avoir d'autres cas d'usage, plus spécifiques, avec par exemple la suppression des torchères des sites de production de pétrole. En effet, l'activité d'extraction de pétrole induit l'émission de méthane. Inutilisable, il est brûlé à 95% dans des torchères, produisant ainsi de grandes quantités de CO₂. S'il existe différentes méthodes pour transformer ce gaz en électricité, les sites de production de pétrole présents dans des zones éloignées des habitations sont rarement raccordés au réseau de distribution et ne peuvent par conséquent pas distribuer l'électricité produite. Certains mineurs aux États-Unis ont donc fait le pari de convertir ce gaz en électricité. Les fermes de minage étant mobiles et installées directement sur le site de production, aucune infrastructure de distribution n'est nécessaire afin d'acheminer l'électricité produite. Elle est donc consommée sur place. De cette manière, le Bitcoin s'est révélé être une nouvelle manne financière pour les producteurs d'énergie tout en réduisant drastiquement les émissions de gaz induites par l'exploitation pétrolière.

Ainsi, le Bitcoin peut donc s'avérer très polluant, mais il peut être un allié majeur dans la transition écologique en améliorant les modèles économiques de production énergétique et en participant au financement de nouvelles sources d'énergie verte.

ii. Une consommation excessive, mais relativement à quoi ?

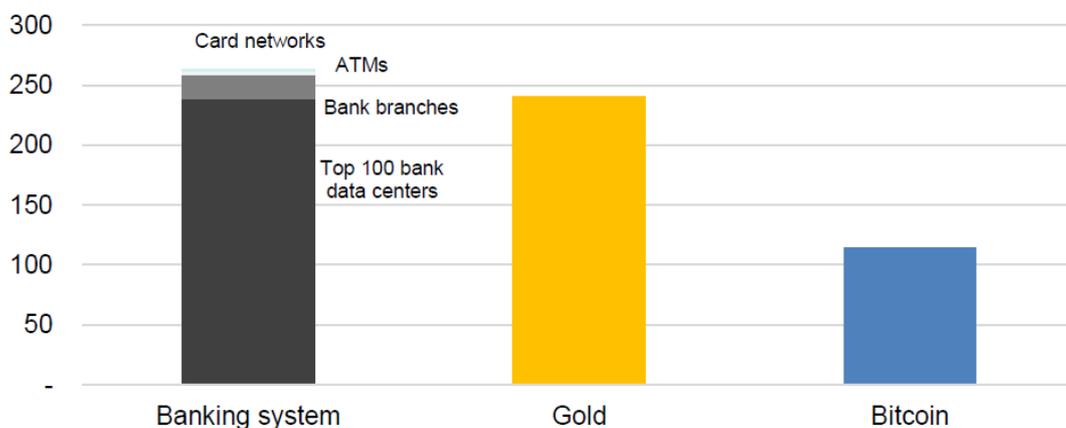
De nombreuses voix se sont élevées pour dénoncer une consommation excessive du réseau Bitcoin, la comparant même à la consommation énergétique de

⁷⁵ Contact Energy - [Contact Energy to supply 'flexible' renewable electricity for new data centre near Clyde Dam](#) - 31.08.2021

certaines pays. Face à cela, deux questions doivent se poser : (i) Bitcoin consomme-t-il davantage relativement aux secteurs connexes de l'économie traditionnelle ? (ii) Bitcoin vaut-il cette consommation en énergie ?

S'agissant de la première question, il convient de préciser que s'il est possible de comparer la consommation de Bitcoin avec d'autres ordres de grandeur, c'est parce que la technologie qui en est à l'origine le permet. En effet, la transparence est telle que l'on peut connaître avec une relative précision la consommation énergétique de ce réseau mondialisé. Notons qu'il s'agit en soi d'une prouesse technique. Or, cette transparence numérique est loin de trouver son pendant parmi les différentes industries dont les activités sont connexes à Bitcoin. Bien sûr, ce dernier est une technologie fondamentalement nouvelle qui ne remplace pas précisément un système existant. Il est donc particulièrement difficile de faire des parallèles. Toutefois, dans son étude, Galaxy Digital compare la consommation énergétique de Bitcoin à celle du système financier et de l'industrie aurifère, pariant que le Bitcoin exercera une influence sur l'un et sur l'autre.

Si le réseau Bitcoin consomme entre 113,89 TWh et 147 TWh, l'étude réalisée par Galaxy Digital estime la consommation énergétique du système financier et de l'industrie aurifère respectivement à 263,72 TWh et à 240,61 TWh environ.



Galaxy Digital - Consommation énergétique annuelle estimée du secteur bancaire, du secteur aurifère et du réseau Bitcoin en 2020⁷⁶

Si ces éléments de comparaison sont perfectibles, ils ont le mérite d'offrir un ordre de grandeur de la consommation énergétique des différents secteurs sur lesquels Bitcoin a, ou aura, une influence dans les prochaines années. Sans verser

⁷⁶ Galaxy Digital Mining - [On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question](#) - 05.2021

dans la critique systématique, ni dans l'angélisme béat, le Bitcoin et plus globalement la technologie blockchain peuvent représenter une formidable opportunité de modernisation de la société en commençant notamment par le système financier. Construit il y a plusieurs décennies déjà, ce dernier présente de nombreuses failles, dont son empreinte écologique, loin d'être neutre. Paradoxalement, les détracteurs de Bitcoin ne se posent que peu la question du système actuel. Ainsi, quid de la consommation des dizaines de milliers de distributeurs automatiques de billets à travers le monde qui consomment une énergie constante et ce à toute heure du jour et de la nuit ?

S'agissant de la question relative au ratio bénéfice/coût, il s'agit moins là d'une question statistique que d'une question purement politique. Bitcoin et les usages qui en découlent doivent-ils être considérés comme utiles à la société ? Certains voient en Bitcoin une forme numérique d'un capitalisme débridé dans la droite ligne de la crise des *subprimes*. D'autres considèrent Bitcoin comme l'un des remèdes face à un système monétaire et bancaire opaque. Force est de constater que toutes les innovations qui l'accompagnent peuvent être appréhendées comme une nouvelle évolution des cadres financiers et monétaires. À l'heure de la numérisation globale, amplifiée par la pandémie de la Covid-19, il ne faut pas perdre de vue les apports que pourraient représenter une adoption de masse de ces nouvelles technologies.

Par ailleurs, cette technologie n'est pas simplement un outil spéculatif. Mais, à l'instar de toute innovation, elle implique des paris sur l'avenir qui se modélisent notamment dans la spéculation. S'agissant de la question de l'apport social, cet outil est intrinsèquement protecteur face à toute forme de censure et d'oppression. Il ne juge pas du bien-fondé des choix politiques, il est un outil d'expression de la liberté attaché à la valeur. Il ne fait aucune distinction selon l'origine, la religion, ou les convictions de son utilisateur.

Face à l'interdiction réclamée par certains, ce rapport défend une vision selon laquelle les pouvoirs publics doivent mettre en œuvre une politique permettant d'orienter les mineurs vers les énergies propres et de récompenser ceux qui financent la transition écologique. Ils devraient également favoriser la conclusion de partenariats entre des producteurs d'énergie renouvelable (hydroélectrique) et des mineurs afin d'apporter aux premiers comme aux seconds une source supplémentaire de financements. Cependant, ces partenariats ne sauraient être conclus au détriment des populations et des acteurs locaux. Ils devront se concentrer sur les surplus d'énergie inutilisés, d'où le rôle central d'un État stratège, garant de l'intérêt général.

Proposition 11 : Accroître le financement de nouvelles sources d'énergie renouvelable en favorisant les partenariats entre les producteurs d'énergie et les mineurs de crypto-actifs, afin d'utiliser les surplus d'énergie autrement perdus.

En outre, les récents débats au Parlement européen en marge du texte MiCa (Market in Crypto Asset) relatif à l'interdiction indirecte de la preuve de travail (Proof of Work ou POW) constituent une vraie rupture principielle. En effet, Bitcoin fait face pour la première fois à un débat politique non plus axé sur les usages d'une technologie mais sur son rapport coût énergétique / utilité sociale. Ainsi, le Bitcoin en tant que technologie devrait être interdit au seul motif que le protocole consommerait trop d'énergie. Si cette position peut se défendre sur le fond considérant que le débat relatif à la sobriété énergétique résulterait d'un choix politique, force est de constater que jamais la problématique n'a été abordée par cette approche. En ce sens, elle constitue une vraie rupture avec le principe de neutralité technologique alors même que la réponse à la question est plus complexe que ce que les débats au Parlement ont laissé à voir. Cette proposition a finalement été rejetée par les eurodéputés. À défaut, l'Union européenne se serait alors coupée d'une part non négligeable de crypto-actifs essentiels au développement de cet écosystème, dont le Bitcoin qui est l'étalon de tous les autres *tokens*.

Ainsi, cette restriction pure et simple représente un vrai danger pour l'écosystème européen et n'apparaît pas être la bonne méthode afin de limiter l'impact des crypto-actifs sur le climat. Cela est développé précédemment, il faut distinguer les crypto-actifs minés à partir d'une énergie carbonée de ceux minés à partir d'une énergie renouvelable. Si cette technologie peut induire des applicatifs qui s'avèrent polluant, ce n'est pas tant la technologie mais la façon dont elle est employée qui l'est en réalité. Ainsi selon ses modalités d'usages, elle peut être à la fois néfaste pour le climat ou au contraire contribuer à sa protection. Le rôle du politique est d'intervenir et créer les leviers économiques afin de faire en sorte que les acteurs du minage choisissent la seconde voie plus que la première. À cet égard, le Parlement européen aurait sûrement dû envisager l'interdiction du minage sur de l'énergie carboné afin d'accélérer la transition. Rappelons toutefois, que la production de bitcoins est très faiblement localisée en Europe et que lorsque les mineurs y opèrent, ils le font à base d'énergie renouvelable. Cela démontre les limites de ce débat, débat essentiellement idéologique.

En outre, il serait également pertinent d'adapter le régime des droits à polluer aux activités de minage, afin de favoriser les entreprises vertueuses. Ainsi, les

mineurs qui participeraient aux financements de nouvelles sources d'énergie renouvelable se verraient attribuer de nouveaux crédits carbone qu'ils pourraient alors monnayer sur les marchés.

Proposition 12 : Interdire le minage professionnel de crypto-actifs à partir d'énergies carbonées et adapter la réglementation applicable aux droits à polluer afin de l'appliquer aux mineurs professionnels de crypto-actifs, en attribuant des crédits carbone à ceux participant au financement de nouvelles sources d'énergie renouvelable.

En matière de politique publique, l'intérêt de la France et de l'Europe n'est pas seulement de limiter l'impact écologique de ces nouvelles activités, il est surtout de faire émerger de nouveaux champions capables de tirer le meilleur parti de ces ressources numériques. La France dispose déjà de plusieurs leaders en la matière tels que BigBlock Datacenter, Sesterce Mining et Just-Mining. Disposer de compétences en matière de validation de blocs par la méthode PoW s'avèrera nécessaire avec le développement de nouvelles blockchains à l'avenir et leur appropriation à des fins industrielles.

II. Au-delà de Bitcoin, de nouvelles formes de *tokens*

Le bitcoin s'est imposé comme l'étalon-or de ce nouvel écosystème. Néanmoins, d'autres *tokens* se sont progressivement développés et ont fédéré autour d'eux un écosystème propre. C'est évidemment le cas du réseau Ethereum, qui a donné naissance à la finance décentralisée. C'est aussi le cas d'autres réseaux comme Solana, Cardano ou Tezos, qui disposent chacun de leur propre *token*.

Or, l'appellation « crypto-actif », utilisée pour désigner l'ensemble de ces jetons, ne se limite pas uniquement aux *tokens* de réseau. En effet, depuis 2018 et l'éclatement de la bulle ICO majoritairement dominée par les « *utility tokens* », les « *security tokens* » ont également pris leur essor et représentent un des cas d'usage majeurs des crypto-actifs.

Plus encore, la période 2019-2022 a été une étape charnière dans le développement de la sphère des crypto-actifs, au point qu'ont émergé des *tokens* qui, s'ils sont bien des « crypto », ne sont toutefois pas des « actifs ». C'est le cas notamment des *stablecoins* et des monnaies numériques de banque centrale, qui

s'apparentent à de la monnaie numérique. C'est également le cas des *tokens* de gouvernance, qui confèrent à leurs détenteurs des droits politiques sur le protocole concerné. C'est enfin le cas des *non-fungible tokens* (ou NFT, en français on parle de « jetons non fongibles ») qui, par leur grande diversité, peuvent être tantôt un actif et tantôt un simple objet numérique.

1. L'essor des NFT, entre euphorie et révolution

Les NFT ont fait une irruption médiatique remarquée au cours de l'année 2020. Désormais, ils occupent une place importante accordée à l'écosystème des crypto-actifs dans les médias traditionnels. Leur première véritable apparition date de 2017, mais leur essor a largement profité du *bull run* de 2020 et 2021.

a. Un nouveau standard technologique encore limité au monde de la culture

La notion même de NFT est difficile à cerner tant ils sont à la fois similaires et différents les uns des autres. En effet, fort de la programmabilité absolue offerte par la blockchain, les NFT sont avant tout un standard technologique qui peut être utilisé pour un grand nombre de cas d'usage, le premier en ayant bénéficié étant le monde de l'art.

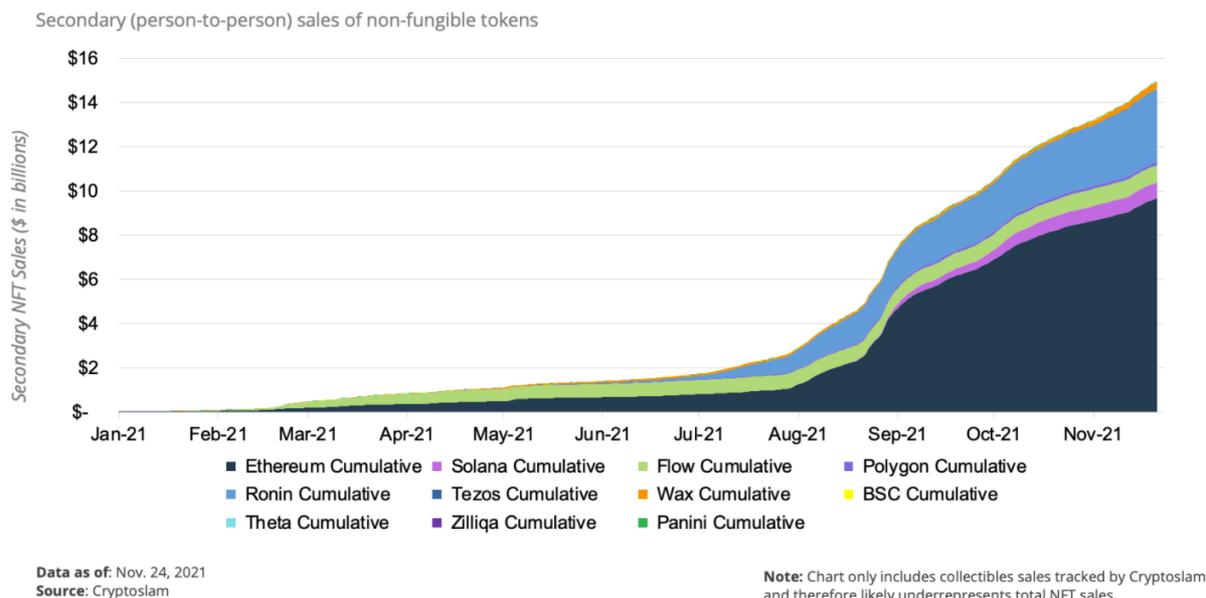
i. *Définition du jeton non fongible et caractéristiques*

La technologie du jeton non fongible est l'une des innovations majeures de la blockchain. Pourtant, cette technologie n'a pas encore déployé son plein potentiel et ne laisse entrevoir qu'une partie seulement de ses capacités. Mais, déjà, il n'y a aucun doute sur la pérennité de ces nouveaux objets qui, grâce à leur forte capacité d'évolution, auront un impact sur plusieurs pans de la société.

D'un point de vue strictement technique, un NFT est un *token* unique, certifiant la propriété d'un bien corporel ou incorporel au profit de son détenteur, enregistré sur le registre public de la blockchain⁷⁷. À l'écriture de ces lignes, l'essentiel des NFT est natif sur la blockchain Ethereum mais ils peuvent être émis sur d'autres blockchains dès lors que leur structure technologique le permet. Au-delà, un NFT correspond à un standard technologique et il semble, par conséquent,

⁷⁷ ADAN - [Les non-fungible tokens \(NFT\) : la rareté numérique](#) - 15.11.2021

que sa seule définition comme crypto-actif est trop restrictive et élude une part significative de ses enjeux.



Messari - Évolution du marché secondaire des NFT (en dollars) selon les blockchains d'origine entre janvier 2021 et janvier 2022⁷⁸

Par leur unicité, les NFT ne sont pas interchangeables ou remplaçables par un autre token quel qu'il soit (par exemple : un bitcoin, un ether, ou encore un autre NFT). Ce caractère unique découle du fait que les NFT ont une existence unique et précise, certifiée dans la blockchain. Leur propriété est assurée par la blockchain, il en va de même de son contenu, des droits qui en découlent et de son propriétaire indirectement. Les applications relatives au standard NFT constituent ainsi une véritable révolution dans le monde numérique.

Avec l'émergence d'Internet, ces nouveaux réseaux ont conduit à une dématérialisation des données et des œuvres intellectuelles de toutes natures. L'information est devenue plus facile à dupliquer, à partager et parfois même à s'approprier. Internet a été une révolution de l'information mais elle n'aura pas permis une juste protection de la propriété intellectuelle dans ce processus de démocratisation. Or, face à un Internet de plus en plus centralisé où toute information, image, ou vidéo est copiable à l'infini, les NFT permettent de créer de la rareté, jusqu'alors impossible à reproduire techniquement.

⁷⁸ Messari - [A Short, Non-Fungible Story](#) - 03.12.2021

Par conséquent, la technologie NFT est une nouvelle brique qui vient compléter l'édifice érigé depuis plus de vingt ans avec Internet. Cette évolution est particulièrement éloquente lorsqu'il s'agit des objets nativement numériques, au premier chef l'art numérique. Les NFT répondent aux deux enjeux de l'Internet contemporain. Le premier est la conséquence du monde fermé et centralisé des plateformes. Face aux conditions contractuelles prohibitives de ces dernières, il est difficile de rester maître de ses données personnelles, de sa production artistique ou de sa production intellectuelle. Le second est relatif à la preuve de la propriété dans un internet libre et ouvert. Les moyens d'apporter la preuve de propriété sont complexes, il en découle la difficulté de pouvoir être rémunéré pour ses productions comme tout contributeur l'est dans le monde physique. En effet, comment prouver être à l'origine d'une information si celle-ci se duplique au fur et à mesure qu'elle atteint de nouvelle personne ? Les NFT - en figeant une partie de l'information et notamment l'émetteur et l'horodatage de son émission dans un registre inviolable et immuable - apportent cette réponse.

En individualisant l'œuvre, en accordant un certificat d'authenticité et en apportant une preuve d'antériorité, l'artiste « numérique » peut effectivement exercer les droits qui découlent de la propriété d'une œuvre immatérielle. Cette propriété est évidemment exclusive, mais elle n'empêche pas une diffusion de l'œuvre par duplication. Dans ce cas, si un tiers revendique des droits sur l'œuvre, il se verra opposer le NFT en tant que certificat d'authenticité.

Par ailleurs, ces nouveaux standards permettent de superviser, dans le monde numérique, des biens corporels en assurant leur traçabilité et leur intégrité. Cette faculté à représenter numériquement, de manière unique, un bien physique est une révolution dont il est aujourd'hui difficile de distinguer les contours et usages. Ce cas d'usage est aujourd'hui partiellement développé, notamment, dans les chaînes logistiques et d'approvisionnement industrielles pour le suivi des marchandises.

ii. Au-delà de la mode, l'apparition des premiers cas d'usage

À l'instar de la blockchain et des ICO en 2018, les NFT sont au cœur d'un emballement médiatique depuis le début de l'année 2021. Et pour cause, le 11 mars 2021 s'est produite la vente la plus onéreuse de toute l'histoire des NFT : l'œuvre - numérique - « *Everydays : the first 5 000 days* » de l'artiste américain Beeple a ainsi été vendue pour 69,3 millions de dollars par la maison d'enchères Christie's. Cette

œuvre composite, rassemblant 5.000 autres œuvres de l'artiste, a propulsé ce dernier parmi les artistes les plus prisés de sa génération.

Selon Chainalysis⁷⁹, la valeur cumulée des transactions relatives aux NFT a dépassé les 44 milliards de dollars au terme de l'année 2021. La forte valorisation des œuvres a deux origines majeures. D'une part, les NFT ont, comme les ICO avant eux, bénéficié d'une forme d'euphorie. Cet enthousiasme a été amplifié par les valorisations exorbitantes induites par l'excès de liquidité dans l'écosystème. D'autre part, les NFT permettent de construire un sentiment de communauté autour des propriétaires d'une œuvre. En effet, détenir un NFT, et l'afficher comme tel, est devenu le témoignage d'une appartenance à un nouveau monde de la mode et de l'art digital. Ainsi de nombreuses personnalités ont sauté le pas et ont contribué à rendre les NFT populaires.

Cette dynamique des NFT a été alimentée, depuis deux ans, par différentes vagues fondées sur la volonté de collectionner des « œuvres » issue de la blockchain⁸⁰. Apparue en 2017, le crypto-art s'est développé autour de collections de personnages en « *pixel art* », générés aléatoirement par des algorithmes selon certaines caractéristiques (humains/animaux, masculin/féminin, couleurs, accessoires, postures, ...). Ces œuvres, issue davantage de la technologie que de l'humain, se sont démocratisées au travers de deux collections majeures : les « CryptoKitties » et les « CryptoPunks ». En parallèle de cet art « crypto », l'art numérique, plus traditionnel, a également alimenté cette croissance des NFT.

Or, en raison des fortes valorisations du marché « crypto » et du développement de nouvelles formes d'art, le secteur traditionnel de l'art s'est retrouvé impacté par l'essor des NFT. En 2021, ces derniers représentaient près des deux tiers de la valeur des ventes en ligne, soit 2% du marché de l'art en général, dans un contexte de dématérialisation des ventes en raison de la pandémie de la Covid-19⁸¹. Les NFT vont ainsi particulièrement révolutionner la manière dont fonctionne le marché de l'art. En effet, la technologie des NFT permettra à terme de construire des contrats intelligents qui, tant dans les échanges que dans la vie de l'œuvre, inventeront des nouveaux modèles de rémunération plus justes et décentralisés, dans lequel le consommateur sera directement le financeur de l'artiste. En outre, les collectionneurs fréquenteront de moins en moins les salles des ventes traditionnelles et de plus en plus les marchés dématérialisés, à l'image d'OpenSea.

⁷⁹ Chainalysis - [Report Preview: The 2021 NFT Market Explained \[UPDATED 1/13/22\]](#) - 13.01.2022

⁸⁰ Barthalois Cyril - Les ventes volontaires aux enchères publiques à l'heure des NFT - 01.2020

⁸¹ Franceinfo - [Les NFT dopent le marché de l'art contemporain](#) - 04.10.2021

Par ailleurs, le rapport annuel de Chainalysis sur les NFT montre ainsi que le succès des NFT s'étend à l'ensemble du globe (principalement en Amérique du Nord et en Asie du Sud-Est, dans une moindre mesure en Europe de l'Ouest et en Amérique Latine). Néanmoins, si plusieurs transactions ont représenté plusieurs centaines de milliers de dollars, voire plusieurs millions, le rapport tend à considérer que la grande majorité (environ 80%) des transactions réalisées sur NFT le sont à un prix inférieur à 10.000 dollars. Ainsi, alors que l'art traditionnel est davantage réservé à une catégorie aisée, voire très aisée, de la population, les NFT ont permis l'ouverture de ce marché à des personnes qui en étaient jusqu'alors exclues.

En parallèle du domaine artistique, les NFT ont également trouvé un second applicatif majeur dans le monde des jeux vidéo. La France compte d'ailleurs une licorne sur ce segment. La société Sorare édite ainsi une collection de cartes, sous forme de NFT, représentant des joueurs de football. En parallèle, ces dernières peuvent interagir entre elles sous forme d'un jeu de football en ligne. Elles sont valorisées selon la notoriété du joueur apposé sur la carte, mais aussi en fonction des performances de ce dernier. En parallèle, d'autres sociétés, comme Ubisoft, ont émis des NFT pour certains de leurs jeux, correspondant notamment à des avantages de *gameplay* ou à des éléments esthétiques.

Au-delà de la monétisation d'objets virtuels, la technologie NFT a permis l'invention de nouveaux modèles de jeu, transformant radicalement le rôle et la place du joueur. Ainsi, grâce à la blockchain, des sociétés ont inventé des jeux vidéo fonctionnant selon le système du « *play-to-earn* »⁸². Ces jeux, comme « Axie Infinity », permettent à leurs joueurs de rémunérer leurs actions dans le jeu. Moyennant parfois une mise de départ sous la forme d'un NFT, représentant un actif virtuel *in-game*, le joueur peut gagner, en fonction des modèles économiques, des crypto-actifs afin de rémunérer sa progression et son talent dans le jeu. Le modèle économique du jeu vidéo s'en trouve complètement bouleversé.

b. Les enjeux liés au développement des NFT

Comme cela a été évoqué, l'usage des NFT est aujourd'hui limité au monde de l'art, avec quelques incursions dans d'autres secteurs comme les jeux-vidéos. Toutefois, certains projets envisagent leur utilisation dans d'autres pans de

⁸² Système de jeu qui récompense le joueur en lui attribuant des biens ayant une certaine valeur pécuniaire, ici des NFT. En opposition, notamment, au « *pay-to-win* », qui est un système dans lequel les joueurs qui dépensent dans le jeu sont privilégiés par rapport aux autres joueurs.

l'économie. Ces nouveaux usages impliqueront des adaptations réglementaires pour garantir leur bon développement et le respect de l'ordre public.

i. De nouveaux objets numériques au potentiel disruptif

À l'instar de l'Internet des années 1990, le potentiel des NFT et de la blockchain est infini. Il est aujourd'hui difficile d'imaginer ce que seront les usages de 2030 grâce à cette technologie. Associées à l'œuvre musicale ou bien encore à la vidéo, les applications sont innombrables. Ainsi, s'il n'existe que peu de NFT représentant des œuvres musicales, cette tendance pourrait se généraliser au fur et à mesure. Par exemple, l'influenceur français ZeratoR a ainsi vendu sur la plateforme OpenSea un NFT de « La Lèpre », une reprise parodique de la chanson « La Bohème » de Charles Aznavour⁸³. Les NFT pourraient ainsi révolutionner le mode de rémunération des artistes, en évitant que pour le financement ou la distribution de leurs albums, ils ne soient contraints par les « *Majors* » de leur reverser une partie des droits. La consommation artistique entre le public et l'artiste serait donc désintermédiée. Les artistes, en diffusant leurs NFT auprès des plateformes de *streaming* décentralisées, percevront ainsi une rémunération à chaque écoute, achat, transfert en fonction des clauses prévues dans les *smart-contracts*.

Les NFT pourraient également repenser les interactions sociales sur Internet, en permettant aux utilisateurs de reprendre le contrôle de leurs données. La récente prise de conscience de la société sur l'enjeu autour du contrôle des données personnelles par les GAFAM a conduit à différentes initiatives afin de limiter leur usage. L'Union européenne a ainsi émis un Règlement général à la protection des données (RGPD) afin de réguler les données personnelles obtenues par les GAFAM. En parallèle, le propriétaire de l'OM, Frank McCourt, a créé une fondation visant - en partenariat avec Sciences Po et Georgetown University - à décentraliser Internet et le rendre à ses utilisateurs grâce au projet Liberty⁸⁴.

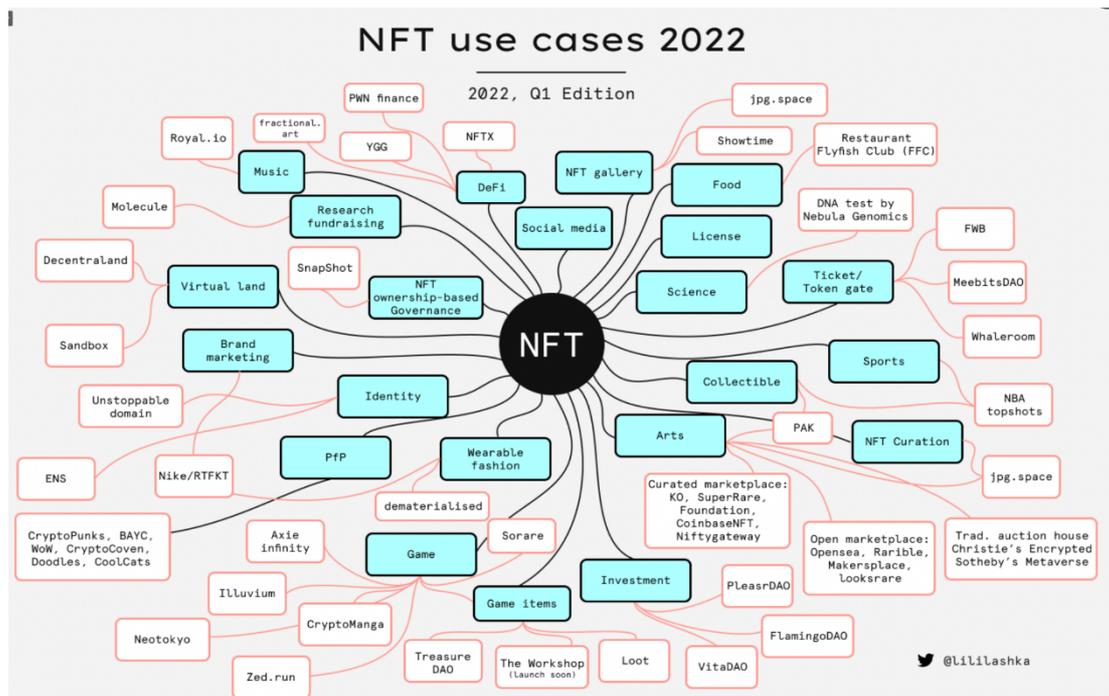
En outre, autre applicatif majeur, la création de modèles d'identité décentralisée (*Decentralized Identity* - DID) est une rupture majeure. Elle permettra à terme *via* la technologie NFT de prouver à un tiers son identité ou bien sa réputation, sans avoir à en donner les pièces justificatives. Ainsi, on peut imaginer aisément demain des systèmes de KYC qui permettront à un service de connaître

⁸³ OpenSea - ["La lèpre" Vidéo by ZeratoR](#)

⁸⁴ Projet Liberty - [Site officiel](#)

l'utilisateur, d'avoir la certitude de sa preuve d'identité et d'existence sans pour autant que l'utilisateur ne soit contraint de transférer son passeport.

En somme, la technologie laisse augurer une grande variété de cas d'usage des NFT dans la vie quotidienne des utilisateurs d'Internet. À ce jour, les NFT ne laissent entrevoir qu'une infime partie des usages qu'ils permettent intrinsèquement. Ainsi, des développements envisagent déjà le potentiel futur dans le monde réel. Des sociétés innovent afin de créer des NFT d'immeubles dans l'objectif de rendre ces derniers plus liquides et facilement cessibles. La tokenisation de biens immobiliers ne nécessitant pas nécessairement de rendre unique le *token* dans la blockchain, il est tout à fait possible de diviser la propriété d'un bien immobilier en un ensemble de *tokens* fongibles. Toutefois, la technologie NFT devient intéressante lorsqu'il s'agit de désigner une partie d'un immeuble (un appartement par exemple). Il devient donc possible de représenter, sur la blockchain, des lots de l'immeuble et de faciliter les transactions afférentes.



@Lililashka (Twitter) - Illustration de l'ensemble des projets relatifs aux NFT selon leur cas d'usage et en cours au premier trimestre 2022⁸⁵

⁸⁵ Twitter - @Lililashka

ii. *De nouveaux objets source d'interrogations réglementaires*

Du fait de leur récente apparition dans l'espace public, rares sont les réglementations spécifiques aux NFT à travers le globe. Face à la complexité de leur qualification, en tant que standard technologique, les NFT ne font l'objet que de quelques traitements fiscaux particuliers, sans autre implication juridique. Cette problématique n'échappe pas au droit français. Ainsi, un flou juridique existe quant au traitement juridique et fiscal de ces nouveaux objets.

Dans la mesure où ces nouveaux objets numériques vont modifier considérablement le rapport des citoyens à la propriété, à l'origine essentiellement fiduciaire - reposant sur la confiance d'un titre papier - ou plus directement physique, les NFT imposent un nouveau paradigme dont il faut se saisir. Si les NFT ne remplaceront pas tous les modes d'expression de la propriété qui existent aujourd'hui, ils auront néanmoins un impact significatif sur la propriété intellectuelle du XXI^{ème} siècle et l'exercice des droits qui en sont attachés.

Il semble par conséquent impératif que la France et l'Europe se dotent d'un cadre réglementaire qui crée de la clarté et de la confiance pour les acteurs de ce secteur. Ce cadre doit être suffisamment souple afin de permettre à l'innovation de prospérer sur le continent européen, tout en assurant un cadre protecteur aux utilisateurs de NFT. Mais, en même temps, cet impératif de protection ne doit pas pousser le législateur à sur-réguler. En effet, cette technologie étant particulièrement immature, elle est loin d'avoir exploré tous ses cas d'usage.

Cela a été évoqué, cette technologie implique des cas d'usage extrêmement variés. Il est inenvisageable de régir de la même façon en droit des NFT représentant des objets virtuels issus de jeux-vidéo et des NFT représentant des biens immobiliers. En outre, difficulté supplémentaire, il est impossible de prédire aujourd'hui ce que les NFT deviendront dans deux, cinq ou dix ans. Ce serait donc une erreur de venir contraindre plus que de raison ce nouvel outil numérique.

En droit français, les NFT sont généralement assimilés à des actifs numériques. En fonction de leurs activités, les prestataires de services sur NFT sont soumis à la réglementation applicable aux prestataires de services sur actifs numériques (PSAN). Toutefois, d'un point de vue empirique et technologique, il est permis de considérer que les NFT sont transparents et que le régime applicable aux NFT découle de l'actif qu'il représente⁸⁶. *De facto*, les NFT ne seraient plus des actifs numériques au sens de la définition légale héritée de la loi Pacte.

⁸⁶ ADAN - [Les non-fungible tokens \(NFT\) : la rareté numérique](#) - 15.11.2021

Dans un premier temps, le législateur doit par conséquent réfléchir à l'opportunité de définir les NFT en droit français. Cette définition devra avant tout porter sur la notion de standard technologique, et éviter de créer une définition juridique stricte et figée de l'objet NFT. Le principe à privilégier sera alors celui de la transparence juridique du véhicule technologique (le NFT) au profit du régime du sous-jacent (l'objet ou les droits identifiés dans le NFT). En effet, les NFT ne constituent pas en tant que tels une catégorie d'objets uniformes, un travail sera nécessaire afin d'étudier l'ensemble des sous-jacents et leurs cas d'usage recensés à ce jour. En fonction de ces derniers, il devra alors découler une ou plusieurs précisions juridiques encadrant les cas d'usage si tant est que rien ne s'y réfère en droit positif.

Au-delà de la transparence de l'objet NFT et de la nécessité d'interroger son sous-jacent plus que son enveloppe technologique en tant que telle, il sera nécessaire d'inscrire dans le droit civil une définition suffisamment large d'un « jeton non fongible », afin de couvrir l'ensemble du spectre des NFT existants ou pouvant émerger. Cette définition, dans le Code civil, s'impose pour deux raisons. D'une part, seuls les NFT représentant un actif financier correspondent à la définition qui est faite d'un actif numérique dans le Code monétaire et financier⁸⁷. D'autre part, la technologie du NFT est une nouvelle expression de la propriété. Ce postulat entre en résonance avec la genèse du Code civil de 1804. Il est par conséquent très éloigné de la notion de nouvel actif économique ou financier.

Proposition 13 : En droit civil, définir de manière large la notion de jeton non fongible afin de donner un statut juridique à ces nouveaux objets numériques et les dissocier de la notion d'actif numérique. S'assurer de la juste traduction des usages futurs et du sous-jacent de ces jetons en droit positif.

Les NFT sont une enveloppe numérique et un standard technologique créateurs de droits associés à un objet virtuel ou physique. Par conséquent, la réglementation relative à l'actif sous-jacent devrait l'emporter sur la qualification de NFT. Dans le cas d'une œuvre d'art représentée sous forme de NFT, l'ensemble du régime juridique applicable aux œuvres d'art devrait prévaloir. Toutefois, cette qualification devra se faire sous réserve de certaines adaptations inhérentes à la nature numérique du NFT.

⁸⁷ Article [L54-10-1](#) du Code monétaire et financier et, par renvoi, article [L552-2](#) du même Code.

Au regard de l'utilisation massive des NFT dans le monde de l'art, la question de la propriété intellectuelle apparaît comme la plus intéressante. S'agissant de la propriété littéraire et artistique, le droit d'auteur - principal outil en la matière - trouve son fait générateur lors de la création de l'œuvre sans formalité de dépôt. Aussi, le droit d'auteur s'exprime en réalité le plus souvent lorsqu'un auteur souhaite monétiser la propriété de son œuvre (soit en cédant ses droits cessibles, soit en agissant en contrefaçon). Dans le cas d'un litige, l'auteur doit alors apporter la preuve que son oeuvre est, d'un point de vue juridique, considérée comme « originale » et que cette dernière a été créée antérieurement à l'autre oeuvre litigieuse⁸⁸. Afin de donner date à cette création, l'auteur peut avoir recours à la solution de l'enveloppe Soleau⁸⁹, au dépôt de l'œuvre auprès d'un officier ministériel, ou aux services d'une société d'auteurs. Ainsi, il est possible d'imaginer que le NFT puisse s'ajouter à ces différentes solutions permettant (i) de donner date à la création de l'œuvre mais également (ii) de pouvoir assurer la bonne gestion de cette œuvre. En effet, au même titre que les titres de propriété industrielle, le recours aux *smart-contracts* permettrait d'automatiser les opérations liées aux droits patrimoniaux du droit d'auteur (par exemple : la perception de *royalties* lors de l'utilisation de l'œuvre ou de sa transmission).

S'agissant de la propriété industrielle, le NFT pourrait devenir un nouveau support pour l'ensemble des titres de propriété (brevet, marque, dessins et modèles). Ce recours aux NFT pourrait favoriser davantage encore la protection des entrepreneurs qui innovent. En effet, alors que les transactions se réalisent toujours plus *via* Internet, le recours aux NFT permettra d'associer la puissance des *smart-contracts*. Ces contrats intelligents permettront la mise en œuvre automatique d'opérations diverses, comme le recouvrement des droits d'exploitation issue d'une licence par exemple. En outre, le NFT (une marque par exemple) sera associé à des mécanismes de traque de la contrefaçon. La lutte contre ces pratiques pourra être automatisée. Il en ira de même pour l'ensemble des opérations sur titres de propriété industrielle (gestion des droits d'exploitation, gestion des licences, etc ...).

D'ores et déjà, en matière de preuve, la blockchain est un outil précieux. De nombreuses sociétés proposent de certifier et d'horodater des documents. C'est notamment le cas des sociétés Woleet, Ipocamp, ou encore Mailstone qui certifient les emails envoyés. Il semble opportun que le législateur se penche sur la question afin de renforcer dans de nombreux champs la valeur d'une preuve issue d'un enregistrement sur la blockchain. Alors que les solutions existantes pour faire

⁸⁸ INPI - [Le droit d'auteur](#)

⁸⁹ INPI - [La solution de l'enveloppe Soleau](#)

reconnaître ses droits en tant qu'auteur sont coûteuses et parfois lourdes en termes de formalités administratives, le recours aux NFT pourrait être une solution plus simple, moins coûteuse, opposable à tous, sans risque de fraude et sans coût en matière de gestion de données. Une question pourrait donc légitimement se poser : serait-il pertinent de lier l'attribution du droit d'auteur à une formalité de dépôt *via* NFT ? À l'écriture de ces lignes, la démarche prospective du présent rapport ne permet pas de répondre à cette question. Elle n'en reste pas moins pertinente pour imaginer l'avenir.

Proposition 14 : Modifier la réglementation applicable à la propriété intellectuelle afin d'intégrer les jetons non fongibles comme nouveau support. Adapter le droit de la preuve et reconnaître la force probante d'une preuve inscrite dans la blockchain.

Pour autant, la technologie NFT n'est pas le rempart ultime à la fraude. Ces interrogations s'imposent dès lors qu'une tierce personne revendique des droits sur une œuvre dont elle n'est pas l'auteur notamment en déposant un « faux » NFT. Si les NFT sont de formidables opportunités pour des propriétaires ou des auteurs de revendiquer leurs droits sur un objet physique ou numérique, ils constituent aussi des opportunités pour des contrefacteurs de s'arroger le mérite d'une œuvre d'un autre en publiant, sous son nom propre, un NFT. Ainsi, celui-ci ne proscriera pas totalement l'acte de fraude. Il existe des cas où l'artiste numérique publiant son œuvre sur des sites spécialisés afin de se faire connaître, voit cette dernière créée sous forme de NFT par des tiers⁹⁰. La problématique est d'autant plus délicate dans la mesure où la blockchain ne permet de revenir en arrière lorsqu'une fraude est intervenue et qu'il n'existe aucun moyen concret de contraindre le contrefacteur à restituer les droits qu'il prétend détenir ou a acquis de manière indue. Ainsi, les NFT, qui devaient être à l'origine un outil de rémunération des artistes, peuvent devenir un outil de leur dépouillement.

Face à cette menace, largement minoritaire, un travail de pédagogie est nécessaire auprès des acteurs concernés, notamment les artistes. Ce travail d'éducation est d'autant plus important que les NFT ont vocation à se démocratiser à grande échelle et s'imposeront à terme à tous. Permettre aux acteurs français de se familiariser d'ores et déjà avec cette technologie leur donnerait un avantage certain face aux pratiques frauduleuses. Cela leur permettrait également de réellement

⁹⁰ L'Express - [Arnaques, impostures... La face obscure des NFT agite le monde de l'art](#) - 31.01.2022

obtenir des droits sur leurs œuvres, donc de vivre de leur art et, *in fine*, favoriser le développement de ce dernier. Dans le cas des objets nativement numériques, l'émergence de cette menace impose un véritable changement de paradigme.

Proposition 15 : Organiser, de concert avec les sociétés de perception et de répartition des droits d'auteur, le ministère de la Culture et les représentants concernés, une politique de sensibilisation à l'égard des droits de propriété au sein de la technologie NFT et éduquer quant à la publication d'une œuvre sous ce format.

Au-delà de la question de la propriété intellectuelle, la question fiscale nécessite également quelques adaptations. Il n'existe aujourd'hui pas de consensus autour du fait que les NFT doivent être fiscalisés comme des actifs numériques ou comme des biens meubles. Ce débat est la conséquence d'une impréparation du droit face à l'irruption de ces nouveaux objets numériques. Ainsi, une clarification fiscale s'impose. Afin de définir le régime fiscal le plus adéquat possible, il faut revenir à la nature même du NFT. Comme cela a été évoqué, le NFT n'est qu'une enveloppe, une représentation numérique d'un bien virtuel ou physique. Aussi, il semble donc pertinent que le NFT soit transparent d'un point de vue fiscal et que la fiscalité s'impute sur l'actif sous-jacent, selon le régime applicable à ce dernier.

Or, exclure les NFT de la catégorie juridique des actifs numériques aurait une conséquence désastreuse pour l'écosystème. En effet, depuis la loi de finances pour 2019, les particuliers qui échangent des actifs numériques contre d'autres actifs numériques bénéficient d'un sursis d'imposition⁹¹, de sorte qu'ils ne fiscalisent pas leur plus-value à chaque échange. Or, l'exclusion des NFT de la catégorie des actifs numériques induirait, *in fine*, leur exclusion de ce régime de sursis d'imposition. Cela est problématique pour trois raisons principales. D'abord, cette mesure est avant tout une mesure de simplification fiscale et administrative. Elle évite que, à chaque échange de crypto-actifs, un contribuable ne soit contraint de tenir une comptabilité écrite pour la restituer fidèlement au moment du paiement de l'impôt. Ensuite, cette mesure permet d'éviter à un contribuable de payer un impôt sur une plus-value qu'il n'a pas toujours perçue. En effet, l'échange d'un crypto-actif contre un autre crypto-actif induit un transfert de propriété, fait générateur de l'impôt. Mais s'il a échangé deux crypto-actifs entre eux, le contribuable ne s'est pas réellement enrichi, puisque la plus-value alors constatée n'a pas été convertie en euros (ou autre

⁹¹ [Article 150 VH bis](#), II. A., du Code général des impôts.

devise ayant cours légal). Enfin, les NFT et les crypto-actifs sont intrinsèquement liés et les premiers représentent l'un des principaux cas d'usage des seconds. Aussi, supprimer cet aménagement fiscal, finalement assez naturel, entre ces deux catégories d'objets numériques serait une véritable erreur pour la compétitivité fiscale de la France. À ce titre, le rédacteur du présent rapport, soutenu par d'autres Députés, a porté un amendement d'appel dans le cadre de l'examen du projet de loi de finances pour 2022 afin d'alerter le Gouvernement sur ce sujet.

Proposition 16 : Fiscaliser les revenus tirés des jetons non fongibles selon le régime fiscal applicable à leurs sous-jacent et, en parallèle, instaurer un report d'imposition des plus-values générées à l'occasion d'un échange entre un jeton non fongible et un actif numérique.

Au-delà des sujets évoqués, les NFT auront des incidences directes sur d'autres branches du droit. Cette technologie, qui a connu un succès fulgurant en seulement deux ans *via* l'art numérique, aura certainement une influence sur l'ensemble de l'économie et de la société. Il s'agit là d'un nouveau champ à explorer. La France et l'Europe devront prendre toute leur part dans la naissance de ce nouvel écosystème.

2. L'émergence de nouveaux modes de financement tokénisés

Les crypto-actifs, au regard de leurs qualités intrinsèques, portent en germe les nouveaux outils du financement de l'économie réelle de demain. Certes encore immature, ils représentent une capacité de modernisation et de simplification inégalée.

C'est en 2017 que la technologie blockchain a servi pour la première fois comme mécanisme de financement de l'économie *via* les premières levées de fonds par émission de *tokens*. Les *Initial coin offering (ICO)* - émission de jetons au public - se sont développées à grande vitesse jusqu'à devenir une bulle à la fin de l'année 2017, qui a fini par éclater en 2018. A l'époque, n'importe quel projet d'ICO pouvait lever des dizaines de millions, alors que sans ce nouveau mode de levée de fonds, le financement bancaire ou capitalistique aurait été impossible. Les ICO étaient davantage alimentées par une euphorie ne reposant pas - toujours - sur une véritable logique économique.

Les ICO reposent sur l'émission d'*utility tokens*. Ces derniers confèrent à leur détenteur un droit d'usage sur un service futur développé par l'émetteur du token. Or, l'impréparation de certains projets et le manque de valeur ajoutée de nombreux projets ont conduit à un profond reflux de capitaux qui a entraîné une traversée du désert de l'écosystème jusqu'en 2020. En outre, la folie spéculative avait réussi à attirer de nombreux escrocs qui n'ont jamais développé les projets promis, ne laissant aucun recours aux investisseurs. *A contrario*, dans cette phase d'euphorie puis d'absolu marasme, quelques projets aux fondations solides ont réussi à se développer. Ils constituent aujourd'hui les premières places de l'écosystème.

Dans le même temps, si les ICO constituent un vecteur de liquidité, les caractéristiques des jetons émis se sont affinées afin de mieux correspondre à la logique d'investissement. D'une simple promesse d'un service futur, les *tokens* se sont développés en s'inspirant des instruments traditionnels. Les *security tokens offering* (STO - en français, on parle d'émission de titres financiers tokénisés au public) se sont développés. Dès lors, il n'était plus question de droits d'utilisation futurs sur un bien ou un service, (d'où la notion d'*utility token*) mais de propriété fractionnée avec les caractéristiques classiques que l'on attribue à un titre financier (droit de vote, dividendes, etc ...). Les *security tokens* apparaissent alors comme un outil et une voie toute tracée afin de moderniser la finance traditionnelle et le financement de l'économie réelle.

a. L'évolution des *security tokens*, de 2017 à aujourd'hui

En parallèle des jetons d'échange et des jetons d'utilité, les jetons de titres financiers (en anglais, on parle de *security tokens*) se sont progressivement développés et ont très rapidement attiré l'attention des régulateurs. Ainsi, il semble nécessaire de revenir brièvement sur la nature de ces jetons, avant d'en détailler l'évolution d'un point de vue économique.

i. *Notion et caractéristiques*

Les *security tokens* apparaissent comme une nouvelle évolution des modes de financement des entreprises. En résumé, un *security token* est une forme numérique, enregistrée dans la blockchain, d'un instrument financier traditionnel⁹². Ce jeton

⁹² S'il est surtout traité, dans la suite des développements, de la question des financements des entreprises *via* des actions ou des obligations, il est important de préciser que les *security tokens* peuvent porter sur un vaste champ d'instruments financiers qui ne concernent pas toujours le financement d'entreprise, à l'instar des dérivés sur matières premières ou des produits immobiliers titrisés.

reprend donc toutes les caractéristiques des instruments financiers et reproduit leur fonctionnement selon les mécaniques permises par la blockchain. Ces jetons permettent donc de faire bénéficier les titres financiers traditionnels de l'ensemble des avantages permis par la tokenisation, comme une réduction des coûts et des délais de transaction ou encore une gestion automatisée *via* les *smart-contracts*. La tokenisation des actifs traditionnels permet de rendre ces derniers encore plus liquides qu'ils ne le sont déjà.

Outre la grande simplicité d'échange qui les caractérise, les *security tokens* sont également échangeables avec des crypto-actifs qui n'ont pas les mêmes caractéristiques. En effet, dans le monde traditionnel, une obligation ou une action s'échangent quasi-exclusivement contre des devises ayant cours légal. Au contraire, le monde des crypto-actifs permet une parfaite liquidité entre différents actifs qui ne sont pas fongibles. Il devient dès lors possible d'échanger un titre financier tokenisé avec un jeton d'échange (comme le bitcoin), un jeton de protocole (comme l'éther), un jeton de gouvernance (comme le jeton Aave), etc ... Ainsi, la tokenisation, des titres financiers notamment, permet le décloisonnement de la valeur entre les différentes catégories d'actifs.

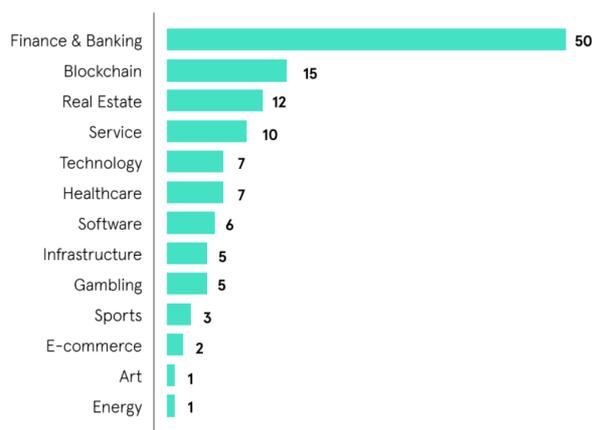
Outre une liquidité accrue avec d'autres catégories d'actifs, la tokenisation offre également une grande programmabilité de ces nouveaux jetons. Ainsi, un *security token* permet de répliquer, dans la blockchain, l'ensemble des caractéristiques d'un titre financier classique, mais il offre également la possibilité à son émetteur de construire son actif sur-mesure selon ses besoins. Semblables à ce qui peut déjà se faire en matière de société par actions, certains jetons offrent ainsi la possibilité de toucher des dividendes sans posséder une fraction de propriété de l'entreprise concernée, ou encore posséder une fraction de cette propriété mais sans disposer de droit de vote. Or, cette programmabilité doit s'envisager au regard de la variété des instruments financiers traditionnels qui existent aujourd'hui.

En parallèle, les *security tokens* doivent être distingués des *tokenized securities* qui, bien que très proches d'un point de vue sémantique et technique, revêtent une réalité différente. En effet, les *tokenized securities* ne sont que la représentation, sur la blockchain, de la propriété de titres financiers traditionnels. Concrètement, alors que les *security tokens* associent dans la blockchain la propriété du titre et les droits attachés, les *tokenized securities* ne portent que sur la propriété dudit titre, les droits continuant d'être gérés de manière traditionnelle.

L'ensemble de ces jetons de titres financiers sont émis dans le cadre de STO. Comparable à une fusion entre une introduction en bourse (*Initial Public Offering* ou IPO) et une ICO, les STO permettent notamment d'ouvrir le capital social d'une société à des investisseurs en délaissant les mécanismes traditionnels de levée de fonds au profit de la blockchain. En parallèle, les *security tokens* étant assimilés à des titres financiers, ces derniers sont soumis à la réglementation en vigueur applicable aux instruments financiers. Ainsi, leur émission et leur utilisation font d'ores et déjà l'objet d'une régulation protectrice des investisseurs.

ii. *Un développement encore limité et principalement tourné vers la finance*

Après l'éclatement de la bulle des ICO et la raréfaction de ce type d'opérations, les STO ont connu un regain d'intérêt. Toutefois, elles restent encore limitées dans l'écosystème, du fait des contraintes réglementaires qui pèsent sur ces nouveaux modes de financement. À titre d'exemple, le nombre de levées de fonds *via* STO est loin d'atteindre les records des ICO au cœur de la bulle de 2017. Plus de 2.500 ICO avaient été recensées par la société BlockState - une société suisse spécialisée dans les *security tokens* - contre seulement une trentaine de STO. En valeur, les ICO recensées cette année avaient permis de récolter plus de 11 milliards de dollars contre seulement 400 millions de dollars pour les STO⁹³.

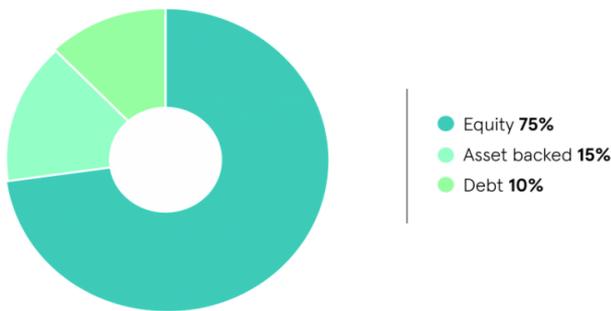


Parmi les 120 projets recensés par BlockState, la quasi-totalité (94%) fonctionnait sur la blockchain Ethereum. Or, cela n'est pas sans incidence sur la nature des projets qui y sont développés. En effet, la blockchain Ethereum est à la base des applications de finance décentralisée qui émergent depuis 2020. Il semble logique que près de la moitié des applicatifs de ces STO portent sur des services bancaires et financiers.

BlockState - Répartition des STO par industrie - 18.06.2019

⁹³ BlockState - [Global STO Study 2019](#) - 18.06.2019

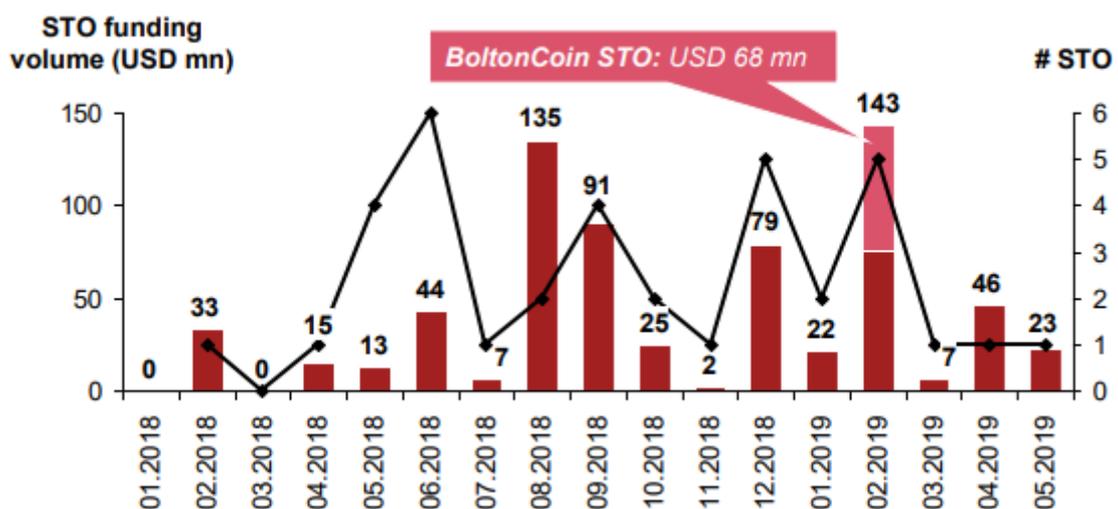
Or, si les *security tokens* peuvent porter sur tout type d'instruments financiers, il semble que le financement des capitaux propres des entreprises soit le cas d'usage



plébiscité par les investisseurs et les porteurs de projets. En effet, 75% de ces projets portaient, en 2018, sur la tokenisation du capital d'entreprises traditionnelles. Seulement 10% des STO concernaient l'émission d'obligations et 15% portaient sur des dérivés.

BlockState - Répartition des STO par classe d'actifs tokenisés - 18.06.2019

Le marché des STO est moins documenté que d'autres secteurs relatifs aux crypto-actifs comme la finance décentralisée ou les *stablecoins*. Les quelques études menées portent généralement sur un nombre restreint de projets. Il est par conséquent difficile d'avoir une vue d'ensemble de cet écosystème spécifique des *security tokens*. Le cabinet d'audit PwC, en partenariat avec l'association suisse Crypto Valley, a eu l'occasion de publier une série de rapports sur les levées de fonds *via* ICO, STO et IEO (abordées ultérieurement). Dans la cinquième édition de ce rapport, PwC indique que, de 2017 à 2018, les STO ont permis de lever 442 millions de dollars.



PwC - Évolution des levées de fonds par STO entre janvier 2018 et mai 2019⁹⁴

⁹⁴ PwC et Crypto Valley - 5th ICO / STO Report, A Strategic Perspective - Summer 2019 Edition

Cette faible dynamique peut s'expliquer par l'importante barrière réglementaire inhérente aux *security tokens*. En effet, si les *utility tokens* sont soit régulés par une réglementation spécifique comme en droit français, soit par aucune réglementation, les *security tokens* sont généralement régis par les règles afférentes aux titres financiers traditionnels. Ainsi, en Europe et davantage encore aux États-Unis, la nature du *token*, caractérisée par les droits pécuniaires ou de gouvernance qui en découlent, oblige l'émetteur du *security token* à respecter la réglementation sur les actifs financiers.

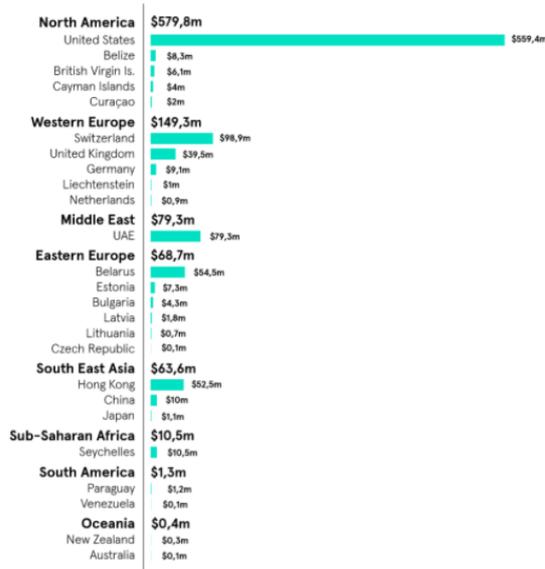
En outre, force est de constater que la frontière entre *utility token* et *security token* est parfois complexe à définir. Ainsi, il est préférable pour nombre d'acteurs du secteur de se réfugier derrière des *tokenomics* (modèle économique du jeton) qui permettent de ne pas être qualifié d'instrument financier.

En outre, la question des marchés secondaires est fondamentale. La répartition des projets selon les pays en est un révélateur. En effet, les États-Unis concentrent la majorité des projets de STO qui émergent depuis 2017. Ce fait est à souligner d'autant que la SEC a mis en place une politique particulièrement sévère ainsi qu'une qualification extrêmement large à l'endroit des *security tokens* et des STO. *De facto*, le régulateur les assimile facilement à des instruments financiers traditionnels et considère qu'ils représentent un risque systémique pour la stabilité financière. Toutefois, cette attractivité américaine s'explique par la vitalité de l'écosystème local et notamment par le développement de marchés secondaires, vecteur de liquidité. Si les États-Unis sont en tête sur ce marché, l'Europe est également une terre d'accueil prisée des projets de *security tokens*. En effet, en 2019, six des dix plus importantes STO sont des projets européens, notamment portés par des acteurs de premiers plans comme l'État autrichien, la Deutsche Bank ou encore la Société Générale avec sa filiale Forge. Selon la société BlockState, 53 des 120 projets recensés sont basés en Europe, contre 34 aux États-Unis. Toutefois, en termes de volumes des fonds levés, les opérations basées aux États-Unis ont permis de lever plus de 500 millions de dollars, contre seulement 200 millions pour les STO basées en Europe⁹⁵.

⁹⁵ PwC et Crypto Valley - 5th ICO / STO Report, A Strategic Perspective - Summer 2019 Edition

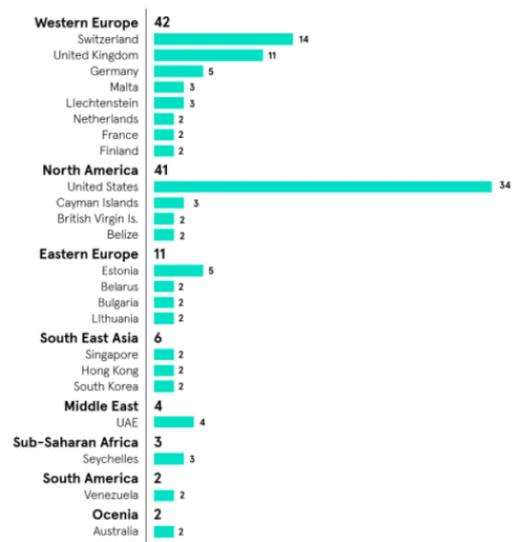
Amount raised by each country in USD*

Switzerland is the European champion, but still dwarfed by the US



Number of STOs per country*

The US is by far the leading country with 34 STOs



BlockState - Analyse géographique du marché des STO dans le monde - 18.06.2019⁹⁶

En France plus particulièrement, le marché des *security tokens* reste encore limité, mais bénéficie d'une tendance favorable. En effet, depuis l'ordonnance blockchain du 8 décembre 2017, la France permet l'inscription de titres financiers sur un dispositif d'enregistrement électronique partagé (DEEP), soit une blockchain. Il convient de souligner que cette réglementation était précurseur en la matière. Elle aura permis plusieurs expérimentations et développements. En mars 2020, l'AMF a recensé sept STO ayant abouti en France⁹⁷. Parmi ces projets, il convient d'évoquer l'opération menée par la Société Générale - Projet Forge - et ayant donné naissance à une filiale spécialisée du même nom. L'opération a consisté à émettre des *security tokens*, portant sur des obligations de financement de l'habitat, pour un montant de plus de 100 millions d'euros. Depuis, la société SG Forge a développé ses offres dans les marchés primaires et secondaires, ainsi que dans les services de conservation d'actifs. Cet élan est à saluer tant il est précurseur à l'échelle des banques françaises.

⁹⁶ BlockState - [Global STO Study 2019](#) - 18.06.2019

⁹⁷ AMF - [État des lieux et analyse relative à l'application de la réglementation financière aux security tokens](#) - 03.2020

b. Enjeux

Les *security tokens* portent en eux les bases d'une nouvelle finance, plus efficace, plus transparente et plus ouverte. Il importe alors de les réguler sans en compromettre le développement.

i. *Une innovation technique aux potentiels multiples*

La tokenisation des instruments financiers représente une nouvelle étape dans l'évolution de la finance mondiale. Plus encore qu'une énième évolution numérique, cette innovation est une véritable révolution du financement des entreprises.

La tokenisation des actions, des obligations ou des autres instruments financiers désintermédie l'ensemble du processus financier en organisant ce dernier sur une blockchain publique et transparente. Cette désintermédiation permettra de réduire massivement les délais de réalisation des transactions et, par voie de conséquence, leurs coûts de réalisation. Par ailleurs, le recours à des blockchains publiques librement distribuées - notamment la blockchain Ethereum - permet de conférer une portée mondiale aux titres tokenisés, là où actuellement ils ne sont listés que sur des bourses d'échange nationales ou régionales. Si les *security tokens* se différencient des *utility tokens* ou des *currency tokens* par leurs caractéristiques juridiques ou économiques, ils revêtent la même forme technologique. De ce fait, ils sont interchangeables avec pour seule limite l'interopérabilité des protocoles entre eux. Il est par exemple possible d'échanger un *utility token* contre un *security token* ou un *currency token* comme un *stablecoin*. Par conséquent, le marché des titres financiers deviendra à terme extrêmement liquide.

Autre apport majeur, la blockchain permet de détenir en compte propre ses actifs. Associés aux actions d'une entreprise, l'avancée est majeure car elle exclut le nécessaire recours à un tiers dépositaire afin de consigner ses titres financiers. Les titres sont gérés par leur propriétaire, à moindre coût. Ils sont rendus liquides car échangeables avec des actifs radicalement différents. En outre, ils peuvent être vendus sur une place de marché globale, unique, transparente et permanente.

Comme évoqué précédemment, la blockchain permet une grande programmabilité des *tokens* émis. Outre la nature des droits attachés à ces *security tokens*, elle permet ainsi de programmer et d'automatiser la gestion même de ces instruments financiers. Cette automatisation concerne notamment l'ensemble des procédures liées à la gestion de l'actionnariat des entreprises. A titre d'exemple, la société française Blockpulse a développé une gestion automatisée de l'actionnariat,

des transferts de propriété de titres ou encore des stipulations contractuelles entre associés *via* la blockchain et les titres tokenisés.

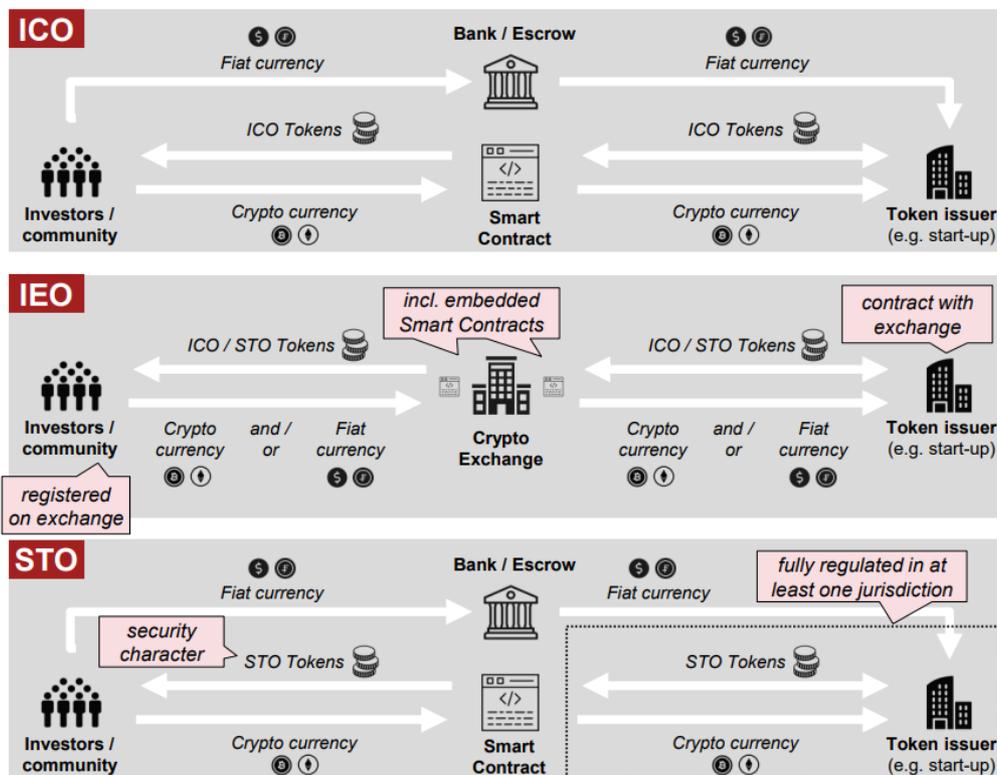
Il convient également de compléter l'exposé en évoquant, après les ICO et les STO, l'émergence des IEO. Ces opérations de IEO (*Initial Exchange Offering*) sont en réalité des ICO ou des STO (selon que le jeton émis est un *utility token* ou un *security token*) réalisées à partir de plateformes d'échanges comme Coinbase ou Binance. Apparues en 2017 au même titre que les ICO et les STO, les IEO n'ont pas connu d'essor significatif. En effet, il n'existe actuellement peu de IEO significatives dans l'écosystème. Celle de Bitfinex, en mai 2019, a néanmoins marqué les esprits dans la mesure où elle a permis de récolter un milliard de dollars, alors que la moyenne des IEO est de quelques dizaines de millions par opération.

Les IEO sont caractéristiques de l'institutionnalisation de l'écosystème. En effet, dans le cadre d'une IEO, les plateformes d'échanges agissent comme un premier filtre. Elles font le tri entre les projets qui leurs sont soumis, ce qui n'est jamais fait pour les autres modes de financement. Par ailleurs, la plateforme d'échanges offre la possibilité aux porteurs du projet de bénéficier de sa notoriété et de son portefeuille client. Il s'agit d'un gage de qualité - uniquement réputationnel dans la mesure où la plateforme engage seulement sa crédibilité - et de sécurité pour l'investisseur, là où aucune garantie n'était présente dans le cadre des ICO.

Les plateformes d'échanges supervisées par le régulateur apportent ainsi un gage de sérieux et de crédibilité à des projets qui ne disposent ni d'une reconnaissance économique (par l'écosystème) ni d'une reconnaissance réglementaire (comme ce qui peut exister en France). Elles permettent également de renforcer les conditions de sécurité dans lesquelles sont émis ces nouveaux jetons, en appliquant leurs propres standards à des projets qui, souvent, n'en disposent pas. En parallèle, elles prennent en charge les obligations de KYC liées aux politiques de lutte contre le blanchiment et le financement du terrorisme. En outre, l'IEO est un avantage pertinent pour les entrepreneurs dans la mesure où leur jeton est listé directement sur la plateforme. Cet atout est non négligeable dans la mesure où il permet au jeton d'être liquide et de bénéficier d'un volume conséquent dès son émission.

Ainsi, les plateformes d'échanges continuent d'élargir leur palette d'offres financières, en incluant les levées de fonds à leurs activités de *trading et*

d'investissement. Cette diversification progressive est symptomatique d'une mutation de ces plateformes en « crypto-banques » capables de traiter de tous les aspects de la sphère financière, allant du compte de dépôt et d'épargne au financement de l'économie.



PwC - Principes de fonctionnement des ICO, des IEO et des STO⁹⁸

ii. La nécessité d'une réglementation adaptée

Paradoxalement, les *security tokens* sont, parmi les objets issus de l'univers blockchain, ceux qui ont été soumis le plus tôt à une réglementation dédiée. En effet, en raison de leurs similitudes avec les instruments financiers traditionnels, les régulateurs ont adopté une jurisprudence visant à soumettre ces nouveaux objets à la réglementation financière actuelle. Durant la bulle des ICO des années 2017 et 2018, les principaux régulateurs ont manifesté des inquiétudes concernant les risques que faisaient encourir l'écosystème sur la stabilité financière, alors que de nombreuses levées de fonds recourant à ce qui était alors présenté comme des *utility tokens* - sans nature financière - se multipliaient et rassemblaient plusieurs dizaines de millions de

⁹⁸ PwC et Crypto Valley - 5th ICO / STO Report, A Strategic Perspective - Summer 2019 Edition

dollars. Ainsi, les régulateurs ont interrogé la nature réelle des jetons qui étaient émis.

Ainsi, la SEC a eu recours au test de Howey afin d'évaluer si un jeton constituait un instrument financier. En appliquant cette jurisprudence, l'autorité a sanctionné, à plusieurs reprises, des opérations de levées de fonds par émission de *tokens* qui, parce que qualifiés d'instruments financiers, auraient dû respecter le droit financier. Ce fut notamment le cas pour le projet The DAO présenté par Slock.it, une société allemande, qui avait levé en 2016 près de 150 millions de dollars. La société Telegram a été aussi condamnée à payer une amende 18,5 millions de dollars pour ne pas avoir respecté la réglementation applicable aux instruments financiers⁹⁹.

S'agissant de la vie - juridique - de ces jetons de nature financière en Europe, l'AMF a rendu, en mars 2020, un état des lieux et une analyse relative à l'application de la réglementation financière aux *security tokens*¹⁰⁰. L'autorité énumère l'ensemble des problématiques de nature juridique quant au développement des opérations de STO. Le régulateur financier distingue le traitement juridique des *security tokens* selon le stade de leur vie (émission, gestion, échanges sur les marchés secondaires).

Au stade de l'émission, les *security tokens* sont soumis aux dispositions du règlement (UE) 2017/1129 (dit règlement Prospectus). Ainsi, le rapport d'information relatif aux monnaies virtuelles évoquait déjà la nécessité d'aménager le règlement Prospectus pour les start-up, afin de prendre en considération des paramètres tels que la taille ou les revenus de l'entreprise (proposition 22). Cette proposition n'a toutefois pas été satisfaite. L'AMF considère que, malgré quelques difficultés pratiques pointées dans le rapport d'information, le cadre juridique n'empêche pas l'émission de *security tokens*.

L'enjeu majeur du développement des *security tokens* repose sur les marchés secondaires. Or, c'est sur ce point que la réglementation est la plus contraignante et impacte de manière significative le développement de ces nouveaux objets numériques. Le règlement-livraison des titres cotés impose, juridiquement, le recours à un intermédiaire agissant comme système de règlement de titres, alors même que cette technologie a pour principe de fonctionner sans recours à un tiers de confiance. Cette contrainte réglementaire, qui se justifie pleinement aux regards des

⁹⁹ Cryptoast - [Clap de fin : Telegram donnera 18.5 millions de dollars à la SEC](#) - 26.06.2020

¹⁰⁰ AMF - [État des lieux et analyse relative à l'application de la réglementation financière aux security tokens](#) - 03.2020

anciens mécanismes de règlement-livraison, est donc totalement incompatible avec le fonctionnement d'une blockchain. Eu égard aux avantages qu'offrent les *security tokens*, les marchés financiers traditionnels vont progressivement migrer vers ces nouveaux objets, permettant ainsi de fluidifier davantage les échanges, de réduire les coûts et de renforcer l'innovation financière. Il est donc fondamental que la réglementation prenne en compte l'évolution des technologies et permette de réaliser des expérimentations à grandes échelles dans les meilleures conditions.

À ce propos, l'Union européenne a commencé à agir. En décembre 2021, le Conseil européen a ainsi adopté la proposition de règlement relatif à un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués (dit « *régime pilote* »). L'objectif poursuivi est de construire un environnement propice au développement de ces innovations financières *via* la blockchain en apportant un cadre clair et simplifié. Contrairement à la proposition de règlement MiCa, le projet de régime pilote simplifie la réglementation avec l'objectif affiché de favoriser l'innovation. Le texte instaure un régime transitoire permettant aux projets qui en bénéficient d'être exemptés de certaines contraintes imposées par le règlement CSDR et les directives MIF2 et Finalité. Ce bac à sable permettra aux entrepreneurs européens de se consacrer davantage à la réussite de leurs projets qu'aux questions de nature réglementaire. Il s'agit là d'un point fondamental dans la compétition mondiale. Toutefois, cette largesse réglementaire n'est pas ouverte à tous, et notamment aux acteurs qui ne bénéficient pas, encore, des agréments nécessaires, ce qui est dommageable. Le Conseil a donc privilégié les acteurs bancaires et de marché au détriment de ceux qui innovent réellement sur le sujet. En outre, la réglementation impose de procéder au règlement-livraison directement en monnaie de banque centrale. Or, l'écosystème des crypto-actifs s'est construit sans devise en euro. Aussi, le développement d'une monnaie numérique de banque centrale destinée aux règlements-livraisons sur blockchain devient un impératif pour la modernisation des infrastructures financières.

PARTIE III - Souveraineté monétaire : entre rupture et continuité

Dans l'histoire de la monnaie, le concept juridique de souveraineté monétaire est récent. Il aura fallu attendre un arrêt de la Cour permanente de la Justice Internationale en 1929 sur les emprunts serbes afin d'en établir une définition juridique. Ce caractère nouveau de la souveraineté monétaire avait notamment été mis en lumière par le Doyen Jean Carbonnier : « le droit de battre monnaie est l'apanage exclusif de l'État moderne. C'est à lui - et à lui seul - qu'il appartient de choisir l'unité monétaire, le signe, qui va circuler sur son territoire : il va lui donner cours légal, voire cours forcé ... ».

S'il relève de l'apanage exclusif de l'État moderne de choisir les devises ayant cours légal sur son territoire, de battre monnaie ou bien encore de réglementer, les responsables politiques ont largement abandonné à des institutions indépendantes le soin de donner la direction à suivre s'agissant de la monnaie. Par exemple, il n'y a pas eu, au sein des parlements nationaux de l'Union européenne, de débat démocratique sur les choix - pourtant politiques - des banques centrales lors de la crise sanitaire, notamment ceux de la Banque Centrale Européenne. De la même manière, aucun débat démocratique n'a précédé ou accompagné la politique monétaire expansionniste de rachat d'actifs depuis 2015, au sein des différentes classes politiques nationales.

Pourtant, la politique monétaire, à bien des égards, a des conséquences directes sur le quotidien des citoyens, le modèle économique, le rapport entre le travail et le capital et *in fine*, la répartition des richesses.

Les crypto-actifs, dans leur construction ainsi que dans leurs applications, entrent en contradiction et parfois en opposition avec la vision moderne de la monnaie étatique. Dès 2015, et particulièrement en 2017, avec la capitalisation grandissante du bitcoin, de nombreux acteurs du débat public se sont alors interrogés sur le risque d'instabilité pour le système monétaire et économique international. Certains avaient même estimé que la « bulle » des crypto-actifs était en mesure d'avoir des impacts systémiques sur l'économie mondiale.

Ce n'est que dans un second temps que les banques centrales ont émis des réserves sur la possibilité que le bitcoin empiète dans le champ monétaire. Les débats sur la souveraineté étatique sont véritablement apparus lorsque le projet Libra a été annoncé par le consortium notamment mené par Facebook, aujourd'hui Meta. En

effet, le projet Libra consistait à émettre un *stablecoin* adossé à un panier de devises ayant cours légal. Dès l'annonce, les réactions ont été nombreuses et virulentes aux États-Unis comme en Europe. La fronde a été menée directement par le politique et les régulateurs qui y voyaient une profonde incartade à l'absolue souveraineté monétaire des États. En réaction, les sénateurs américains ont convoqué les représentants de Libra et notamment le président de Facebook, Mark Zuckerberg, le 23 octobre 2019 afin de leur témoigner de leur farouche hostilité à ce projet qui, selon eux, contrevenait sur plusieurs aspects aux intérêts américains. La représentation américaine s'est alors focalisée sur le panier de devises qui devait assurer la stabilité du *stablecoin* émis. Selon les parlementaires, un tel outil aurait conféré la faculté à Facebook de déstabiliser des monnaies légales à faible capitalisation. En outre, la taille du consortium, en termes de portefeuille clients, aurait permis à Libra d'atteindre rapidement une capitalisation supérieure à certaines monnaies officielles.

À l'écriture de ces lignes, le projet Libra, depuis renommé Diem, a été abandonné par le consortium, il n'en reste pas moins que le sujet monétaire est l'une des préoccupations majeures qui accompagnent l'émergence des crypto-actifs. Face à ce constat, ceux-ci peuvent être une chance de rebattre les cartes du système monétaire avec un objectif de démocratie et de transparence. Toutefois, le chemin emprunté par la puissance publique fait fi des évolutions et laisse seul le secteur privé maître des développements de cette technologie. L'État doit garder un rôle et la monnaie rester un bien public, gouverné de manière démocratique. Pour ce faire, elle ne peut être l'attribut unique d'un consortium d'entreprises au point où son émission et sa gestion ne seraient le fruit que de décisions privées et centralisées. L'enjeu pour l'État est tout simplement de conserver les prérogatives dépeintes par Jean Carbonnier et son droit à battre monnaie.

La question de la souveraineté monétaire ne peut être abordée uniquement sous l'angle de la concurrence entre les nouvelles « crypto-monnaies » issues des différentes blockchains - publiques (bitcoin) ou privées (Libra) - et les monnaies traditionnelles, ayant cours légal. Il ne s'agit là que d'une partie de l'équation que devront résoudre les décideurs publics. En effet, dans l'édification de la finance de demain, en parallèle de la finance traditionnelle et de la finance décentralisée structurée autour des crypto-actifs, les États se jouent une guerre monétaire. L'enjeu pour tous est d'imposer sa propre monnaie et ses standards dans ce nouvel écosystème afin de modifier les rapports de force en sa faveur.

Ainsi, la Chine a décidé de construire un nouvel ordre monétaire correspondant à son espace géographique et économique direct. La zone d'influence du renminbi¹⁰¹ ne cesse de s'étendre et l'émission prochaine, à grande échelle, du yuan numérique est la prochaine étape de cette ambition hégémonique. La Chine a pris le parti de se couper de la compétition mondiale sur les crypto-actifs afin de pouvoir recentraliser une technologie et des réseaux qui pourraient échapper au contrôle de l'État-parti chinois. Procédant comme elle l'avait fait pour Internet dès 2000, elle a interdit tout usage qui pourrait remettre en cause son contrôle sur les réseaux, construisant sa propre infrastructure monétaire et financière.

Non loin, les pays sous sanctions secondaires américaines (l'Iran et la Russie notamment) se pressent pour bâtir des standards d'échange de la valeur qui n'imposent plus de passer par les entités et les réseaux contrôlés par les Américains.

Les États-Unis, eux, depuis 2020 embrassent complètement la finance décentralisée. Si les sénateurs américains étaient frileux à l'idée qu'un GAFAM se lance sur la question monétaire, le régulateur - toujours pragmatique - contrôle *a posteriori* les nouveaux acteurs de la monnaie que sont les émetteurs de *stablecoins* (Tether et Circle notamment). Ainsi, le régulateur américain entend, par ces intermédiaires, imposer le dollar comme seule monnaie étatique dans la finance de demain et entrevoit déjà les futures banques autonomes décentralisées.

L'Europe, elle, est spectatrice de ces enjeux. Étant dans une posture au mieux attentiste, au pire hostile à la technologie et à ses possibilités, aucune stratégie n'émane de l'Union européenne. Faute d'intérêt des décideurs politiques, aucune ambition n'est portée outre celle du secteur privé. Aucune stratégie n'a été définie afin d'ériger un standard monétaire pluriel, robuste et compétitif face aux américains au-delà de l'invocation permanente d'un euro numérique de banque centrale. Malheureusement, le projet de règlement MiCa, pilier réglementaire de cet écosystème, est davantage pensé comme un outil d'interdiction que comme un outil de politique économique et monétaire, face à de grandes puissances rivales. Sur ces questions, l'Europe est tout simplement nulle part.

¹⁰¹ Renminbi est la dénomination officielle de la devise légalement reconnue en Chine.

Enfin, l'autre apport majeur de la technologie blockchain à ne pas sous-estimer est son impact sur le rôle des intermédiaires. En effet, l'intermédiation est au centre du paradigme monétaire, bancaire et financier. Chaque jour, toutes les transactions à travers le monde résultant des investissements ou de la consommation fonctionnent grâce à des tiers qui autorisent, administrent et distribuent la confiance dans le réseau. Demain, l'argent sera détenu en propre par l'individu et le tiers ne sera plus nécessaire afin de faire transiter la valeur en toute confiance entre des interlocuteurs ne se connaissant pas. Ce changement de paradigme va profondément modifier la nature des modèles économiques existants. S'il s'agit très certainement d'un progrès pour l'individu, dans sa quête de souveraineté personnelle et de socialisation, il reste que cela pose des problèmes de transition qui s'accompagnent de risques systémiques. Le responsable politique doit une nouvelle fois anticiper ces problématiques, non pas en interdisant ce qui va advenir mais en anticipant afin que la transition puisse se faire sans douleur.

I. La qualification controversée de Bitcoin comme monnaie

La question « Le bitcoin est-il une monnaie ? » est certainement celle qui, dans la littérature relative aux crypto-actifs, a fait l'objet du plus grand nombre de publications et de débats. Elle a ainsi opposé frontalement deux camps. D'une part, ceux qui voyaient en bitcoin une nouvelle monnaie, mondiale, libérée des manipulations discrétionnaires des États, plus protectrice des intérêts des particuliers. D'autre part, ceux qui ne voyaient en bitcoin qu'un nouvel eldorado spéculatif, qui ne remplissait pas les fonctions fondamentales de la monnaie telles qu'édictées depuis l'Antiquité par Aristote.

Le sujet a aujourd'hui été largement abordé et il n'est pas utile d'ajouter une énième strate à ce débat. Toutefois, un nouvel événement est venu bousculer les lignes et certaines certitudes : la reconnaissance par le Salvador du bitcoin comme monnaie officielle. Par une loi adoptée le 9 juin 2021, le plus petit pays d'Amérique centrale est devenu le premier - et à l'écriture de ces lignes le seul - pays au monde à intégrer un crypto-actif dans son système monétaire, aux côtés du dollar américain. Déflagration immédiate dans l'écosystème des crypto-actifs, mais aussi chez les décideurs politiques et penseurs économiques, cette décision concrétise ce que certains affirmaient depuis longtemps : le bitcoin peut être considéré comme monnaie. Il s'agit aujourd'hui d'une évidence.

Depuis qu'il est adopté par un large écosystème, le bitcoin est effectivement devenu un moyen d'échange de valeur et un moyen de paiement, principalement

entre spécialistes ou convaincus de la blockchain. La véritable problématique qu'impose la qualification du bitcoin comme une monnaie est la suivante : quels sont les cas de figure dans lesquels le bitcoin peut être pertinemment considéré comme une monnaie ?

Sur ce point, la réponse est beaucoup plus complexe. Le Parlement du Salvador a, lui, répondu que la situation de son pays amenait à considérer qu'il était pertinent d'imposer le bitcoin comme une monnaie officielle. Mais est-ce que cette réponse peut se transposer à tous les pays du monde ? Est-ce que la situation de ce petit État ne disposant même pas de sa propre monnaie, est comparable à celle de grandes puissances monétaires mondiales ?

À cette dernière question, la réponse est évidemment non. Pour comprendre cela, il est nécessaire de revenir brièvement sur la structure économique, financière et monétaire du Salvador. Dans ce pays, quatre personnes sur dix vivent dans la pauvreté et environ 20% du PIB est constitué par les fonds envoyés par la diaspora¹⁰². Dans le même temps, le pays a abandonné sa monnaie locale en 2001 pour adopter le dollar américain (le Salvador réalise environ 45% de ses exportations avec les États-Unis) et chaque transfert de fonds fait l'objet de frais prohibitifs, au détriment des destinataires salvadoriens¹⁰³. Ainsi, l'adoption du bitcoin comme monnaie officielle du Salvador relève d'une logique économique spécifique : obtenir un moyen d'échanges peu coûteux, fiable et rapide, permettant de renforcer l'inclusion financière et la croissance économique.

Cependant, si cette adoption résout la question d'un système financier défaillant, elle en soulève bien d'autres en contrepartie. En effet, la loi du 9 juin adoptant le bitcoin prévoit que les agents économiques salvadoriens ont l'obligation d'accepter ce dernier comme moyen de paiement dans le traitement de leurs opérations courantes. Or, au regard des infrastructures techniques et de la volatilité des cours, cette obligation a suscité de nombreuses inquiétudes de la part des commerçants locaux. Le Président de la République Nayib Bukele a alors été contraint de trouver un arrangement confus pour ne pas déstabiliser l'économie nationale¹⁰⁴.

Par ailleurs, les conséquences macroéconomiques à long terme de cette mesure inédite restent encore aujourd'hui inconnues. Quels seront les effets sur le chômage, la croissance et les autres grandes variables économiques d'une monnaie extrêmement volatile aussi bien à la hausse qu'à la baisse ? Le FMI met en avant les

¹⁰² Le Point - [Le Salvador, premier pays au monde à légaliser le Bitcoin](#) - 09.06.2021

¹⁰³ Direction générale du Trésor - Situation économique et financière du Salvador - 05.2019

¹⁰⁴ Le Monde - [Le jour où le Salvador s'est converti au Bitcoin](#) - 04.07.2021

conséquences qu'une telle adoption pourrait avoir, d'abord sur les prix et les salaires et, ensuite, sur les recettes fiscales et les finances publiques du pays. Ainsi, dans l'hypothèse où les citoyens du Salvador décidaient de payer leurs impôts en bitcoin, cela réduirait d'autant les réserves en dollars du gouvernement, utilisées notamment pour financer les dépenses publiques et, par conséquent, la dette publique. À cela s'ajoutent également les considérations environnementales précédemment évoquées.

Dès lors, si l'adoption du bitcoin par le Salvador marque une nouvelle étape dans l'histoire des crypto-actifs, cet événement ne provoquera probablement pas de contagion massive à d'autres pays avant qu'une analyse approfondie *a posteriori* soit faite. Il est encore moins probable que cette adoption s'étende à de grandes puissances monétaires, comme les États-Unis ou la zone euro, dont les monnaies représentent, au-delà de simples étalons et moyens d'échange, des objets politiques.

Néanmoins, outre le bitcoin, les crypto-actifs auront nécessairement une incidence sur le système monétaire et, *in fine*, sur les rapports de force entre grandes puissances monétaires. Or, cette incidence interviendra bien plus rapidement que certains ne le prévoient, dans la mesure où elle suit le rythme de l'innovation qui, dans cet écosystème des crypto-actifs, est l'une des plus fertiles au monde. Cette innovation, majeure au demeurant, a pris forme pour donner naissance à ce que l'on appelle aujourd'hui les *stablecoins*.

II. Les *stablecoins*, une représentation de la monnaie étatique dans le monde numérique

Depuis plusieurs années, les *stablecoins* sont devenus incontournables dans l'écosystème des crypto-actifs. À la frontière de la monnaie électronique et de la blockchain, ils associent le meilleur des deux mondes. Leur première apparition intervient en 2014, mais ils ne se généralisent qu'à partir de 2017. Afin de se couvrir face à la volatilité des actifs numériques (tels que le bitcoin, l'ether et autres *altcoins*), les agents économiques ont rapidement eu besoin de garantir leurs échanges avec un équivalent en monnaie fiduciaire dans l'écosystème des crypto-actifs. Ces représentations des devises traditionnelles dans le monde des crypto-actifs ont progressivement su s'imposer pour devenir indispensables.

Par leur aspect et leur nature, les *stablecoins* ont révolutionné la sphère financière des crypto-actifs. Par leur célérité et leur simplicité d'emploi, ils ont également attiré l'attention de grandes multinationales intéressées par la possibilité de dépasser les lenteurs, frictions et rentes du processus de paiements traditionnel.

Face à cela, les principales banques centrales (Fed et BCE notamment) ont affirmé la volonté d'émettre leur propre monnaie numérique de banque centrale (MNBC).

1. Brève définition

Afin de démontrer l'importance prise par les *stablecoins* depuis cinq ans et d'aborder leur fonctionnement, il est nécessaire d'en définir brièvement les contours.

Un *stablecoin* (en français, on parle de jeton stable) est un *token* qui présente une particularité qui le différencie substantiellement d'autres *tokens* comme le bitcoin ou l'éther : son cours, quelles que soient l'offre ou la demande de marché, reste stable autour d'une certaine cible. L'objectif premier de ces *tokens* est donc d'offrir une transcription des monnaies ayant cours légal dans le monde des crypto-actifs. Ainsi, un *token* de *stablecoin* doit avoir pour valeur un euro ou un dollar selon la devise à laquelle il est adossé.

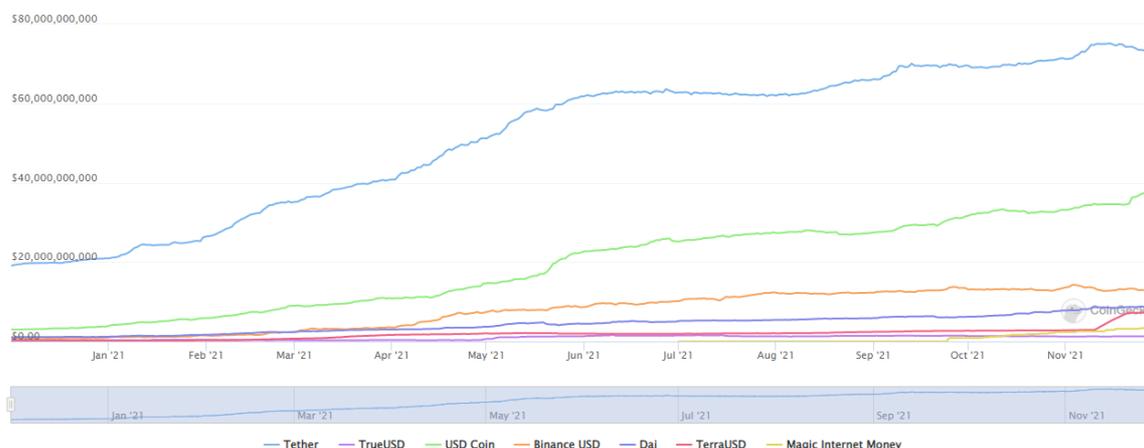
Toutefois, dans la mesure où ces *stablecoins* restent inscrits sur les marchés, quelques variations infimes peuvent tout de même intervenir en fonction de l'offre et de la demande ainsi que de la liquidité de ces derniers. Ainsi, la volatilité du cours d'un *stablecoin* peut évoluer faiblement. Certains mécanismes garantissent qu'elle se maintienne proche de zéro (comme détaillé ultérieurement). L'écart de volatilité d'un *stablecoin* n'est pas sensé excéder quelques dixièmes de pourcents, et ce même lors de fort mouvement du marché.

2. Les *stablecoins* dans le paysage des crypto-actifs

Les *stablecoins* ont largement contribué à l'essor de l'écosystème des crypto-actifs en apportant de la stabilité dans un monde fortement marqué par la volatilité. Ils ont permis une mutation des acteurs et des pratiques, en offrant par ailleurs de nouvelles innovations financières et monétaires.

a. Le stablecoin, un crypto-actif spécifique

Les *stablecoins* ont connu, entre 2017 et 2021, un essor tel qu'ils sont aujourd'hui incontournables sur le marché des crypto-actifs. De janvier à décembre 2021, la capitalisation des *stablecoins* a cru de plus de 126 milliards, soit une progression de 466% sur l'année (contre 107% en 2019 et 439% en 2020)¹⁰⁵.



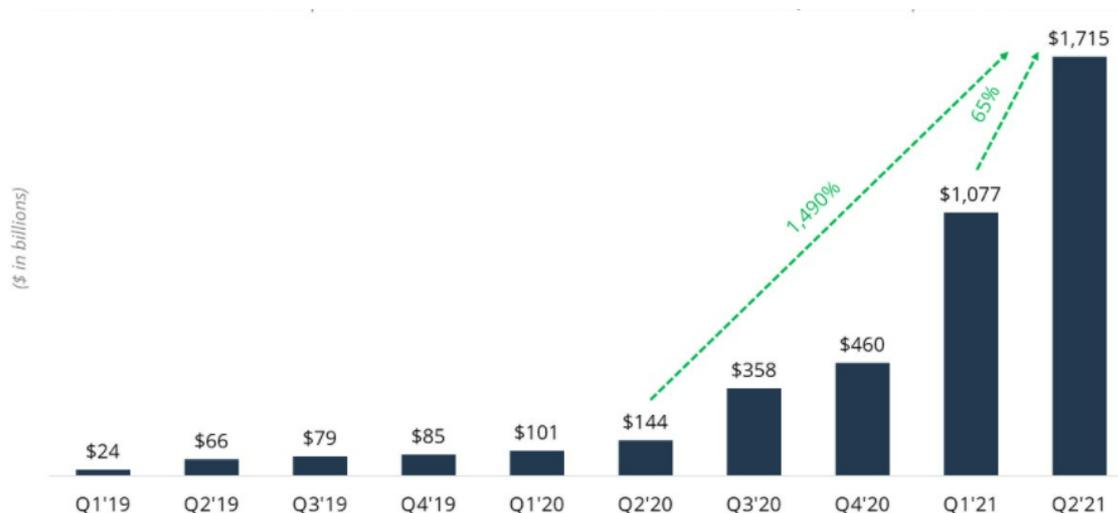
CoinGecko - Capitalisation de marché des stablecoins entre décembre 2020 et décembre 2021

À mesure que leur liquidité croissait, les *stablecoins* ont remplacé partiellement le bitcoin comme monnaie d'échange crypto-crypto. En outre, ils ont permis aux utilisateurs de la finance décentralisée (*decentralized finance* ou DeFi) de se couvrir face à la volatilité des autres crypto-actifs.

Cette bascule du bitcoin vers les *stablecoins*, pour les règlements de transactions, vient combler un vide qui existait jusqu'alors dans le monde des crypto-actifs. En effet, la valeur que les acteurs souhaitaient émettre pour régler une transaction (par exemple, l'acquisition de machines de minage) ou pour transférer des fonds (par exemple, le transfert de fonds en crypto-actifs au sein d'une même famille dispersée entre plusieurs pays) n'était jamais garantie dans sa totalité, en raison de la forte volatilité. Si une brusque chute des cours intervenait entre l'ordre de mouvement et la réception des fonds, une partie de la valeur s'était alors évaporée. Les *stablecoins* constituent donc un outil de règlement des transactions et de transfert de la valeur plus efficace et rassurant.

¹⁰⁵ CoinGecko - [Stablecoins by market capitalization](#) - 12.2021

À ce titre, les *stablecoins* ont participé à un nombre de transactions exorbitantes, avec plus de 1.700 milliards de dollars échangés au deuxième trimestre 2021 seulement (en hausse de 1.490% sur un an)¹⁰⁶.



Messari - Volume trimestriel des transactions en stablecoins - Juin 2021

Par ailleurs, cette logique de sécurisation de la valeur peut également s'appliquer aux fonds qui sont placés sur les applications DeFi. Souvent basées sur la *blockchain* Ethereum, ces dernières utilisent notamment des ethers. Il est fréquent pour leurs utilisateurs de conserver la valeur acquise depuis ces applications en ethers. Toutefois, et au même titre que le bitcoin, le cours de l'ether est sujet à une volatilité suffisamment importante pour induire une variation non négligeable de la valeur acquise à partir des applications DeFi. Or, en convertissant ces gains en *stablecoins*, leur valeur est sanctuarisée en équivalent monnaie ayant cours légal et n'est plus sujette aux variations de cours.

De cette manière, sur l'année 2020, les *stablecoins* ont progressivement été amenés à représenter régulièrement plus de 40 % du volume quotidien combiné des transactions en bitcoins et en ethers. De plus, en permettant aux investisseurs de conserver leurs gains en crypto-actifs sans risque de pertes sur les marchés, les *stablecoins* ont permis, par leur essor, de verrouiller plus encore une part importante des fonds placés sur les marchés des crypto-actifs et, ainsi, de renforcer la tendance haussière du second semestre 2020.

Ainsi, les *stablecoins* jouent, pour l'écosystème des crypto-actifs, (i) le rôle d'une monnaie qui est en mesure de conserver la valeur générée dans le monde

¹⁰⁶ Messari - Ryan Watkins et Roberto Talamas - [Q2'21 DeFi Review](#) - 13.07.2021

numérique, et (ii) le rôle d'étalon et de moyen de paiement pour les professionnels du secteur qui privilégient les crypto-actifs aux devises traditionnelles.

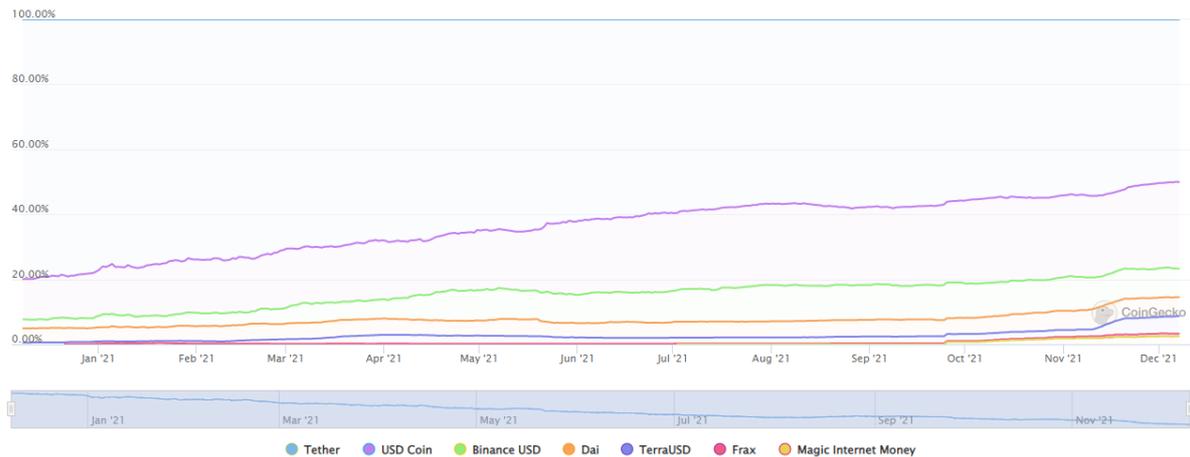
b. Diversification progressive du marché des *stablecoins*

Le marché des *stablecoins* est, depuis son émergence, un marché relativement concentré mais qui tend à se diversifier au fur et à mesure des développements de la finance décentralisée. En parallèle, la base monétaire des *stablecoins* n'a cessé de croître depuis 2017 et a particulièrement bénéficié du « *Summer DeFi* »¹⁰⁷, période pendant laquelle elle a connu une croissance de plus de 8 milliards de dollars, soit plus de 40% de hausse en à peine un trimestre.

Symbole de cette course aux sommets, l'offre de Tether (dont le *stablecoin* est le USDT) a été multipliée par quatre, tandis que celle de Circle (dont le *stablecoin* est le USDC) a été multipliée par dix sur l'année 2021. Le *stablecoin* décentralisé de MakerDAO, le DAI, a également connu une croissance fulgurante et a atteint, fin 2021, une capitalisation totale seize fois supérieure à sa valeur du premier semestre 2020.

Toutefois, cette augmentation impressionnante n'est en réalité pas répartie équitablement entre les différents *tokens* du marché. En effet, ce dernier reste largement dominé par l'USDT de Tether, qui concentre à lui seul plus de 50% de l'ensemble du marché des *stablecoins*, avec plus de 81 milliards de dollars de capitalisation. Il est néanmoins de plus en plus concurrencé par l'USDC de Circle, qui comptabilise plus de 51 milliards de dollars de capitalisation (avec une hausse de 42 milliards au cours de la seule année 2021), ainsi que par le BUSD, le *stablecoin* de Binance, et le DAI.

¹⁰⁷ Comme évoqué [ultérieurement](#).



CoinGecko - Répartition du marché des stablecoins entre décembre 2020 et décembre 2021¹⁰⁸

Si cette diversification progressive du marché interroge, elle semble surtout être la conséquence des choix des investisseurs de privilégier un *stablecoin* plutôt qu'un autre, en raison de leurs caractéristiques intrinsèques. En effet, le terme *stablecoin* est un terme générique pour catégoriser des *tokens* semblables mais non identiques, de telle sorte que des sous-catégories de *stablecoins* peuvent être identifiées selon leur structure et leur fonctionnement.

3. Typologie des *stablecoins*

Le terme de *stablecoin* décrit avant tout le principe de stabilité de ces *tokens* particuliers, auxquels la programmabilité de la blockchain permet de donner certaines caractéristiques particulières. Néanmoins, cette liberté implique également de faire certains choix ; Ces derniers ont donné naissance à une grande diversité de *stablecoins*, parmi lesquels des systèmes adossés à des actifs *off-chain*, des systèmes adossés à des actifs *on-chain* ou encore des systèmes basés sur une structure algorithmique.

a. Caractéristiques générales des *stablecoins*

Lors de la conception d'un *stablecoin*, son émetteur doit se poser la question des différentes caractéristiques qu'il souhaite lui faire revêtir pour en déterminer le fonctionnement. En effet, les *stablecoins* sont aujourd'hui construits autour de trois caractéristiques majeures : la disponibilité, la stabilité et la résistance à la censure.

¹⁰⁸ CoinGecko - [Stablecoins by market capitalization](#) - 12.2021

Toutefois, il n'en existe aujourd'hui aucun qui ait réussi à concilier en son sein, chacune de ces trois caractéristiques. A cet égard, les concepteurs de *stablecoins* doivent choisir de prioriser une caractéristique au détriment d'une autre.

Hypothèse 1 : *Stablecoin* centralisé émis par une société privée

Stablecoin centralisé et réglementé (exemple : USDC de Circle)

Ce *stablecoin* est émis par une entité privée centralisée, il peut s'agir d'une société traditionnelle. Cette dernière est soumise à la réglementation applicable, qui prévoit généralement la disponibilité des fonds conservés en garantie des *tokens* émis (afin de pouvoir prétendre au remboursement des dépôts). L'émetteur du *stablecoin* doit appliquer des ratios de fonds propres ainsi qu'une politique prudentielle stricte. Afin de protéger les avoirs des déposants, détenteurs d'une créance sur l'émetteur du *stablecoin*, la société doit respecter des règles prudentielles quant au placement de la réserve. En ce sens, ce mécanisme se rapproche du cadre légal relatif à la monnaie électronique prévue par la directive 2009/110/CE.

La stabilité du cours est assurée par des intervenants sur le marché appelés « *market maker* »¹⁰⁹ via la technique d'arbitrage. Ces opérateurs de marché apportent la liquidité nécessaire à la demande de *stablecoins*. La stabilité du cours est assurée par la certitude que la société émettrice remboursera en devise ayant cours légal l'intégralité des *stablecoins* émis.

En lien avec la réglementation relative à la lutte contre le blanchiment et le financement du terrorisme, l'État ou la société émettrice du *stablecoin* a la possibilité d'exclure une adresse publique contenant des *tokens* qui auraient été le fruit ou l'objet d'activités illégales. Il existe donc une capacité de censure des transactions et de la détention de *tokens*.

Stablecoin centralisé et non réglementé (exemple : USDT de Tether)

Le principe est le même mais la société est basée dans un pays n'imposant pas de réglementation relative aux *stablecoins*. L'absence d'intervention de l'État dans les affaires de l'émetteur de *stablecoins* réduit les risques d'ingérence publique. Toutefois, il existe toujours un **risque de censure** de la part de l'entreprise émettrice, même si le risque est limité.

¹⁰⁹ Leur rôle est explicité [ultérieurement](#).

En parallèle, l'absence de réglementation ne contraint pas toujours la société à garantir chaque *stablecoin* émis par un actif de même valeur dans un compte de cantonnement, ce qui conduit à un risque d'**indisponibilité** des fonds en cas de retraits massifs par les déposants. Certains *stablecoins* centralisés non régulés peuvent être transparents et respecter une politique de risque mais cette politique n'est pas une obligation légale.

La **stabilité** du cours du *stablecoin* est garantie par des mécanismes similaires à ceux régissant les *stablecoins* centralisés et réglementés.

Hypothèse 2 : *Stablecoin* émis de manière décentralisée (exemple : DAI de MakerDAO)

Le *stablecoin* décentralisé se différencie grandement de la première hypothèse en ce qu'il ne repose sur aucune entité « réelle », traditionnelle, ni aucun tiers de confiance. Ainsi, les mécanismes de la finance traditionnelle comme le séquestre des dépôts sur un compte de cantonnement sont impossibles. En réalité, dans ce cas de figure, chaque *stablecoin* émis est garanti en valeur par un algorithme, géré par des *smart-contracts*.

Contrairement à la première hypothèse, il est particulièrement difficile, si ce n'est impossible, de manipuler une blockchain publique décentralisée, de sorte qu'un *stablecoin* émis et géré par ce type de technologie apparaît comme impossible à censurer.

En parallèle, la disponibilité est garantie par l'investisseur lui-même, par le biais de *smart-contracts* qui assurent la collatéralisation des *stablecoins* émis avec ses propres actifs, ou qui maintiennent l'équilibre de prix en jouant sur l'offre et la demande parfois d'un second jeton utilitaire.

Le cours étant géré de manière automatisée, il peut être soumis à de fortes pressions à la hausse comme à la baisse lorsqu'une demande importante d'émission ou de retrait intervient, entraînant une plus ou moins légère instabilité.

Au-delà de leur structure de fonctionnement, il est également possible de classifier les *stablecoins* selon les réserves ou systèmes sur lesquelles ils sont adossés : il existe, d'une part, les *stablecoins* avec réserve, que cette dernière soit *off-chain* ou *on-chain*, et d'autre part les *stablecoins* algorithmiques.

b. Stablecoins adossés à des actifs off-chain

Les *stablecoins* avec réserve constituée par des actifs *off-chain* sont aujourd'hui ceux qui captent la plus grande part de marché. On parle alors de *stablecoins* centralisés, dans la mesure où leur gestion est assurée par des sociétés traditionnelles.

On parle de *stablecoin* avec réserve constituée par des actifs *off-chain* lorsque sa valeur est garantie par une réserve en actifs réels, traditionnels. Dans la majorité de ces *stablecoins*, les actifs réels sont constitués par des fonds libellés en devise officielle. Dans le cas de l'USDT de Tether ou de l'USDC de Circle, ces entreprises ont, en principe, un dollar placé en réserve en contrepartie de chaque USDT ou USDC émis. De cette manière, l'entreprise ne fait que donner une représentation numérique au dollar et se doit d'assurer la convertibilité de ses *stablecoins* en devises officielles à tout moment pour les investisseurs. Toutefois, pour se rémunérer, un émetteur de *stablecoin* centralisé doit pouvoir placer une partie de ses dépôts sur des actifs moins liquides et plus risqués afin de produire du rendement notamment dans le cas où les taux interbancaires sont négatifs (obligations, bons du trésor ou papier commercial). Ces placements font alors peser des risques sur le capital des déposants, ce qui rend la transparence des réserves d'autant plus importante. Circle, par exemple, publie chaque trimestre un état certifié de ses comptes, contrairement à Tether dont la gestion des réserves reste très opaque. Au dernier trimestre de l'année 2021, la société Circle précisait ainsi avoir 100% de ses dépôts en devises USD évitant tout risque de perte de capital pour les déposants.

Plus rarement, les *stablecoins* peuvent également être adossés à d'autres catégories d'actifs, comme les métaux précieux par exemple ou un panier de devises. Toutefois, ces *stablecoins* sont plus rares et moins sollicités par les investisseurs parce qu'ils sont plus difficiles à gérer et ils sont soumis à la volatilité du collatéral comme dans le cas de l'or. En outre, l'émission de nouveaux *stablecoins* de ce type requiert l'acquisition et le stockage de nouvelles matières premières. Digix Or (DGX) est un exemple de *stablecoin* adossé à des matières premières (en l'espèce l'or).

c. Stablecoins adossés à des actifs on-chain

En parallèle des *stablecoins* adossés à des actifs réels, il existe également des *stablecoins* adossés à des actifs *on-chain* : on parle de *stablecoins* adossés à des

crypto-actifs ou de *stablecoins* décentralisés. Le principe de ces *tokens* est similaire aux *stablecoins* centralisés. Toutefois, leur mode de fonctionnement est radicalement différent.

En effet, la gestion des émissions et des retraits de *stablecoins* n'est plus contrôlée par une société, mais par des *smart-contracts*. On parle alors de *Collateralized Debt Position* ou CDP. Ce type de « *smart-contract* » a été créé à l'origine pour le DAI de MakerDAO, un *stablecoin* dont la valeur cible correspond à un dollar. Ainsi, lorsqu'un investisseur souhaite acquérir un ou plusieurs DAI, ce dernier va interagir avec le protocole de MakerDAO, qui va créer un CDP spécifique à la transaction. Ce *smart-contrat*, le CDP, s'assure d'abord que l'investisseur fournisse le dépôt de garantie nécessaire à l'émission (en l'espèce, des crypto-actifs placés comme collatéral au sein du protocole), avant de procéder à la création puis à l'attribution des DAI.

Ainsi, lorsque l'investisseur souhaitera ultérieurement convertir ses DAI en d'autres crypto-actifs, le CDP afférent procédera au recouvrement de la créance en DAI et au règlement des frais afférents, puis à la restitution du dépôt de garantie. A la suite de quoi, le protocole clôturera le CDP.

Les *stablecoins* décentralisés sont adossés à des actifs dont la valeur est fluctuante. Ainsi, pour garantir la parité entre le dépôt de garantie et les *stablecoins* émis, le protocole exigera de sur-collatéraliser les dépôts qui doit être supérieur, en valeur et à l'instant T, à la valeur émise en *tokens* par le protocole.

Le niveau de ce dépôt de garantie est déterminé par le CDP, en fonction d'un ratio de liquidation¹¹⁰ minimal (exemple : le ratio de liquidation minimal est de 150% lorsque le collatéral est constitué d'éthers - au moins 150\$ en éthers sont donc nécessaires pour obtenir 100\$ en DAI). Lorsque la valeur de ces crypto-actifs diminue, le ratio diminue également jusqu'à atteindre son niveau minimal. Alors, le protocole procédera à la liquidation de la garantie. Cette liquidation prend la forme d'une vente aux enchères, pendant laquelle des acquéreurs potentiels vont utiliser leurs DAI pour acquérir les crypto-actifs constituant le dépôt de garantie. De cette manière, un niveau équivalent de DAI est liquidé avec le dépôt de garantie afin de maintenir l'équilibre général¹¹¹.

¹¹⁰ MakerDAO - [How Liquidation Works](#)

¹¹¹ Sur les différentes hypothèses d'enchères : Itovault - [How Dai Liquidation Work: MakerDAO's MCD System](#) - 10.12.2020

En parallèle, le protocole de MakerDAO peut également utiliser un mécanisme de rétroaction (*Target Rate Feedback Mechanism* ou TRFM) afin de stabiliser le cours du DAI autour de sa cible d'un dollar¹¹².

d. Stablecoins algorithmiques

En sus des *stablecoins* adossés à une réserve matérielle ou immatérielle, il existe des *stablecoins* dont la particularité est de n'être adossés à aucun collatéral : on parle alors de *stablecoins* algorithmiques. Ces derniers ont la particularité d'être décentralisés et contrôlés uniquement par un algorithme. Il est procédé à une régulation algorithmique des émissions afin de stabiliser le cours du stablecoin autour de sa cible.

Il est usuel dans l'écosystème des crypto-actifs qu'une même catégorie de *tokens* donne lieu à plusieurs réalités protéiformes et complexes. En effet, la gouvernance ainsi que les processus de fonctionnement différents au sein de chaque protocole peuvent radicalement changer leur aspect et leur qualification. *De facto*, l'usage ou le fonctionnement d'un *token* peut être radicalement différent d'un second, pourtant classé dans la même catégorie. Ainsi, il existe de multiples *stablecoins* algorithmiques dont la finalité est identique mais dont le fonctionnement est radicalement différent. Il est par conséquent impossible d'entrevoir l'exhaustivité des modes de fonctionnement sans étudier chacun des projets précisément. Aussi, le présent rapport prendra l'exemple du *stablecoin* Basis¹¹³ qui, bien qu'ayant disparu, a inspiré nombre de ses successeurs.

Afin de maintenir le cours aux environs d'un dollar, l'algorithme de Basis va jouer sur l'offre et la demande du marché pour induire des mouvements contracycliques. Ainsi, lorsque le cours est supérieur à la cible d'un dollar (c'est-à-dire lorsque la demande de *stablecoins* est supérieure à l'offre), l'algorithme émet davantage de *stablecoins*, de façon à accroître la masse monétaire et ainsi équilibrer l'offre et la demande de *stablecoins* (on parle de phase d'expansion monétaire).

À l'inverse, lorsque le cours est inférieur à la cible d'un dollar (c'est-à-dire lorsque l'offre de *stablecoins* est supérieure à la demande), l'algorithme va racheter - et donc sortir du marché - des *stablecoins* afin de réduire la masse monétaire et

¹¹² Pour plus d'informations : MakerDAO - [The Target Rate Feedback Mechanism: An Introduction](#) - 01.05.2020

¹¹³ Pour plus d'informations sur les *stablecoins* algorithmiques en général : Medium - Haseeb Qureshi - [A Visual Explanation of Algorithmic Stablecoins](#) - 27.04.2021

ainsi équilibrer le cours autour de sa cible (on parle de phase de contraction monétaire).

Techniquement, il existe en réalité plusieurs types de *tokens* qui servent à maintenir le cours autour de sa cible. En effet, lorsque l'algorithme souhaite contracter l'offre de *stablecoins* afin d'équilibrer avec la demande, il va en réalité émettre des *tokens* obligataires (en anglais, on parle de « *bond tokens* »). Ces derniers sont vendus sur les marchés et donnent droit à l'octroi d'un *stablecoin*, sous certaines conditions dans le futur (le plus souvent lorsque l'offre de *stablecoins* est inférieure à la demande). Ces *tokens* obligataires peuvent donc être acquis par les investisseurs directement sur les marchés et moyennant un prix inférieur à un *stablecoin* - soit, dans le cas de Basis, moins d'un dollar. De cette manière, l'algorithme permet de capter une partie des *stablecoins* en surplus, en échange d'une promesse d'en émettre davantage à l'avenir et de les distribuer d'une manière préférentielle.

En parallèle de ces *tokens* obligataires, il existe également des *tokens* actions (« *share tokens* »). À l'inverse des *tokens* obligataires, les *tokens* actions sont utilisés afin de répondre à un surplus de demande par l'émission de nouveaux *stablecoins*. Ainsi, ces *tokens* actions, dont le nombre est limité en volume, permettent à leurs détenteurs d'obtenir gratuitement des *stablecoins* dans les phases d'expansion monétaire, lorsque le protocole répond à un surplus de demande par de nouvelles émissions de *stablecoins*. À ce titre, on parle également d'actions de seigniorage (en anglais, on parle de « *seigniorage shares* »), notamment parce que ces dernières octroient à leurs détenteurs un revenu de seigniorage lorsque le protocole augmente sa masse monétaire, sans devoir fournir de contrepartie.

En parallèle des *stablecoins* algorithmiques basés sur une méthode de seigniorage, il existe également d'autres *stablecoins* algorithmiques basés sur la méthode dite de « *rebase* ». Il s'agit notamment du *stablecoin* Ampleforth¹¹⁴.

Son innovation est la suivante : maintenir son offre parfaitement élastique et appliquer les ajustements nécessaires à stabiliser le cours sur le solde de tous les détenteurs de *stablecoins*. Concrètement, cela implique que (i) si le cours croît au-delà d'un dollar, l'algorithme émet de nouveaux *stablecoins* afin de réduire le niveau du cours et le rapprocher de sa cible - ainsi chaque détenteur de *stablecoins* va en recevoir une partie, proportionnellement à la quantité qu'il possède déjà ; et (ii) si le

¹¹⁴ Pour aller plus loin : Gemini - [Ampleforth: An Algorithmic Rebase Cryptocurrency](#) - 22.07.2021

cours décroît en deçà d'un dollar, l'algorithme va retirer des *stablecoins* en circulation afin d'augmenter le niveau du cours et l'approcher de sa cible - ainsi chaque détenteur de *stablecoins* verra son solde diminuer proportionnellement à la quantité qu'il possède déjà.

Le lecteur le comprendra aisément à la lecture de ces lignes que ces mécanismes complexes impliquent des modélisations et des équilibres financiers poussés. Ils confèrent à ces outils une part d'expérimentation indéniable à date. Ils conditionnent les *stablecoins* algorithmique à une catégorie à part qui ne saurait pas être confondue avec l'intégralité du marché des *stablecoins*. Ainsi, si ces derniers essaient de trouver le meilleur moyen d'équilibrer leurs cours, ils sont expérimentaux et comportent des risques comme la démontré le cas de l'UST récemment.

4. Les *stablecoins*, un objet technologique aux nombreux enjeux

Jamais la monnaie n'a eu autant de formes diverses et de fonctionnements différents. Aussi, comprendre ce que sera la monnaie du XXI^{ème} siècle implique de comprendre, outre les mécanismes qui assurent la stabilité de ces nouvelles monnaies, les problématiques et les enjeux qu'apporte l'innovation monétaire.

L'un des enjeux majeurs de la monnaie est celui de la confiance. Une monnaie ne peut prospérer si ses utilisateurs ne lui ont pas accordé leur confiance. Pour les monnaies traditionnelles, la confiance des citoyens à leurs endroits émane de la banque centrale, plus globalement, l'État. Dans le cadre des crypto-actifs, la confiance des utilisateurs résulte d'un ensemble complexe en fonction de la nature de l'objet mais tous partagent une confiance dans la technologie qui repose sur un immense registre transparent et inviolable, garantit la fiabilité du système.

Dans les cas des *stablecoins* centralisés, adossés à des actifs *off-chain*, l'objectif est avant tout de créer les conditions de la confiance vis-à-vis du collatéral adossé aux *stablecoins* émis. L'émetteur recherche alors la confiance de l'utilisateur qui souhaite conserver la valeur de son dépôt.

L'USDT, émis par la société Tether, est aujourd'hui le *stablecoin* le plus important du marché en termes de capitalisation, représentant plus de 81 milliards de dollars, contre 51 milliards pour l'USDC¹¹⁵. Toutefois, la société Tether est aussi

¹¹⁵ CoinGecko - [Stablecoins selon la capitalisation du marché](#) - 28.03.2022

connue pour l'opacité de ses réserves mettant en doute sa capacité garantir l'ensemble des *stablecoins* émis. Plusieurs enquêtes menées par la justice américaine ont ainsi démontré qu'une partie de la trésorerie de Tether avait été utilisée afin de prêter à la société Bitfinex pour lui permettre de couvrir des dettes ponctuelles. En outre, en 2019 à la suite d'une enquête du procureur général de New York, Tether a révélé que seuls 75% des *stablecoins* en circulation étaient garantis par des dollars liquides. Dès lors, l'opacité des placements des actifs en réserve pose une problématique de confiance. La question se pose : Tether garantit-il la valeur d'un USDT pour un dollar ? Tether a répondu en affirmant qu'il existait bien une parité entre ses réserves et ses émissions, les réserves de la société étant constituées de dollars liquides mais aussi de créances et autres actifs moins liquides. Si cela s'avère exact, le caractère liquide de ses placements et la capacité de Tether à répondre à de brusques demandes de remboursement n'a pas été certifié.

Cette problématique de la confiance est un enjeu majeur pour l'écosystème des crypto-actifs, d'autant plus que Tether est l'un des acteurs incontournables de cette économie numérique. Pour la seule année 2020, le nombre d'USDT en circulation a augmenté de 500%. Cette croissance place, à l'écriture de ces lignes, Tether en position dominante sur le marché des *stablecoins* et en fait le quatrième *token* le plus capitalisé au monde. Tether est par conséquent devenu un acteur systémique dans l'écosystème des crypto-actifs, dont l'absence de transparence devient un sujet de préoccupation majeur. Dans l'hypothèse où cette société deviendrait insolvable et serait dans l'incapacité d'échanger ses *stablecoins* contre des dollars, cette crise ponctuelle emporterait avec elle tout un écosystème naissant. Il est important de ne pas négliger ce risque.

Toutefois, force est de constater que les déboires de Tether n'ont eu qu'un impact limité sur sa popularité auprès de l'écosystème. Ceci s'explique par deux avantages inhérents à sa position et aux effets de réseau que cela induit. D'une part, il est l'un des premiers *stablecoins* à avoir été émis à grande échelle, permettant à des centaines de milliers d'utilisateurs de neutraliser la volatilité liée aux crypto-actifs. D'autre part, cette antériorité et la stabilité qu'il procure ont permis à Tether de se constituer une base très large d'utilisateurs. Ainsi, l'USDT étant accepté par une large part de cet écosystème, il bénéficie d'effets d'entraînement qu'un tel réseau lui procure et constitue ainsi un *token* particulièrement liquide.

Cet impact limité précédemment évoqué s'est toutefois matérialisé par l'émergence d'autres *stablecoins* et le détournement d'une part des utilisateurs de l'USDT vers ces derniers. L'un d'eux a notamment profité des affaires entourant Tether : l'USDC, émis par Circle. Ce dernier est tout à fait similaire à l'USDT mais

présente néanmoins une différence de taille, il est le premier à avoir accepté le jeu de la transparence. Cette stratégie a fonctionné puisque l'USDC, qui représentait moins de 10% des parts du marché des *stablecoins* en juin 2020, en représente plus du quart au premier trimestre 2022. La position dominante de l'USDT s'érode ainsi progressivement passant de 85% à moins de 50% en deux ans seulement¹¹⁶.

L'essor d'un *stablecoin* pourtant très semblable à l'USDT résulte en réalité d'une demande de réglementation et de stabilité. La société Circle audite de manière indépendante, ses comptes à intervalles réguliers et publie les rapports qui en découlent, permettant à chaque investisseur de connaître la structure des réserves utilisées comme garantie¹¹⁷. En parallèle, la société Circle s'est assurée du soutien des autorités réglementaires américaines, qui l'ont appuyé dans sa démarche. Cela a vraisemblablement participé à sa rapide progression. Les failles de l'USDT ont également incité la société Paxos à émettre un autre *stablecoin* adossé au dollar : l'USDP. Sa particularité est d'offrir une complète parité entre ses réserves disponibles et les *stablecoins* émis, Paxos garantissant l'émission de ses *tokens* avec des réserves en dollars et des bons du Trésor américain.

Le second enjeu majeur posé par les *stablecoins* est celui de la régulation. Dans l'écosystème des crypto-actifs, la décentralisation est devenue un *leitmotiv*. Elle permet en outre de contourner les cadres traditionnels et de disposer de nouveaux modèles économiques plus justes et plus transparents. C'est dans cette optique qu'ont émergé les *stablecoins* adossés à des actifs *on-chain* et les *stablecoins* algorithmiques. Libérés de toute pression physique, ces derniers doivent être en mesure d'accompagner la mue de la valeur vers une totale décentralisation. Or, cette décentralisation totale n'est pas sans poser quelques problématiques.

La décentralisation implique de nouveaux modèles afin d'assurer la stabilité monétaire. Alors même que les protocoles exigent fréquemment une surcollatéralisation des actifs afin de garantir le *stablecoin* décentralisé – ce qui implique une perte d'efficacité du capital, les dispositifs chargés d'assurer le maintien de la valeur sont soumis souvent à rude épreuve notamment lors des épisodes de crash comme cela a pu être constaté lors de l'épisode du « jeudi noir » de mars 2020. Avec la propagation de la pandémie de Covid-19, l'ensemble des marchés, y compris ceux des crypto-actifs, ont subi un reflux massif. Le jeudi 12 mars 2020, l'ether a perdu plus de la moitié de sa valeur en l'espace d'une journée.

¹¹⁶ CoinGecko - [Stablecoins selon la capitalisation du marché](#) - 28.03.2022

¹¹⁷ Communiqué de presse de Circle - [Greater Transparency for USDC Reserves](#) - 20.07.2021

Or, le *stablecoin* DAI étant principalement adossé à l'ether, la chute brutale du cours de ce dernier a entraîné une vague de liquidation sans précédent des dépôts de garantie de plusieurs centaines de milliers d'investisseurs. En une seule journée, 5,67 millions de DAI n'étaient plus garantis. On estime qu'entre le 12 et le 13 mars 2020, environ 8,32 millions de dollars de crypto-actifs ont été vendus aux enchères par le protocole de MakerDAO, pour une offre nulle ou quasi-nulle émise par un individu ayant exploité les failles du système.

Autre fait marquant, le 9 mars 2022, le *stablecoin* algorithmique UST émis sur la blockchain Terra a vu sa parité avec le dollar, techniquement assurée grâce à un jeton parallèle appelé Luna, se rompre pendant plusieurs jours entraînant une perte de plus de 85% de sa valeur par rapport à sa cible d'un dollar. À ce jour, les événements n'ont pas encore permis d'élucider totalement les circonstances de marché ayant conduit à cette rupture de la parité. Selon certains observateurs attentifs, il semblerait qu'un fonds d'investissement traditionnel doté de plusieurs milliards de dollars ait mis en œuvre une stratégie afin de déstabiliser la confiance des utilisateurs dans l'UST, produisant ainsi une spirale infernale en quelques heures. L'UST, normalement stabilisé autour d'un dollar, a perdu jusqu'à 99% de sa valeur et a atteint 0,02\$, avec les conséquences financières que cela implique sur ses détenteurs. Force est de constater que les *stablecoins* algorithmiques peuvent se révéler être des cibles fragiles face à des attaques financières ou lors de conditions de marché extrême. Cette question est d'autant plus préoccupante que ces nouveaux outils fonctionnent de manière quasiment automatisée et sans réelle responsabilité humaine. Il se pose une nouvelle fois la question de la régulation de ce type d'objet.

En outre, la décentralisation de ces mécanismes implique également l'absence totale de contrôle extérieur de la stabilité du système et d'audit de la technologie afin de déceler d'éventuelles failles dans le code. Elle implique enfin que, si les créateurs du *stablecoin* décentralisé le décident ainsi, aucune assurance n'est accordée à l'investisseur en cas de crise sur les marchés.

Par ailleurs, la décentralisation induit également que, dans l'hypothèse d'une future adoption généralisée, les États ne puissent disposer de leviers afin de diriger l'action monétaire en conformité avec leurs actions budgétaires, les privant ainsi d'un outil de politique économique majeure pour leur développement. Cela implique également, dans le cadre de *stablecoin* centralisé, un risque de censure monétaire décidée depuis l'étranger. Ainsi, dans le cas de l'USDC, les régulateurs et le pouvoir politique américains seraient, par exemple, en capacité (i) d'influencer les émissions

de *stablecoins* au profit, ou au détriment, de certains acteurs américains, ou européens ; (ii) d'influencer les transactions qui pourraient être réalisées avec ces *stablecoins* ; ou (iii) geler leur usage et les garanties qui y sont afférentes. Cette hypothèse du gel des avoirs numériques s'est produite, en août 2021, lorsque Tether a gelé et rendu indisponibles près de 33 millions d'USDT suite à un piratage de plus de 600 millions de dollars. Dans le cas d'espèce, la société Tether avait pris la décision de geler ces USDT, objet du délit. Si cette intention était louable, elle démontre également qu'une entité privée à elle seule peut contrôler de manière absolue plus de 80 milliards de dollars numériques aujourd'hui en circulation.

En somme, les *stablecoins* privés représentent des opportunités mais posent un grand nombre d'enjeux. Par conséquent, les États ne devront pas rester immobiles alors que se construit sous leurs yeux les futures formes de monnaies ainsi que les nouveaux moyens de transfert de la valeur. Ils devront trouver un équilibre afin d'éviter les risques systémiques liés à ces nouveaux acteurs tout en travaillant à ne pas perdre leurs leviers de politique monétaire. Or, dans ce contexte de compétition monétaire, l'Europe doit impérativement penser une nouvelle ambition. Elle doit prendre pleinement la place qui est la sienne dans cette guerre monétaire qui se joue davantage entre les États et leurs devises qu'avec les entreprises privées.

Cette ambition peut se matérialiser par le développement d'un euro numérique de banque centrale. Toutefois, ce nouvel outil public ne se suffit pas à lui-même. Alors que les devises issues d'émetteurs privés règnent en maître sur ce nouvel écosystème, l'Europe doit favoriser l'émergence de *stablecoins* en euros afin d'y imposer sa marque et gagner en souveraineté. Cette stratégie est d'autant plus urgente dans la mesure où l'émission d'un euro numérique de banque centrale n'interviendrait pas avant plusieurs années.

Proposition 17 : Favoriser le développement de *stablecoins* en euros privés afin de défendre la souveraineté monétaire européenne dans ce nouvel écosystème.

III. La tokenisation de la monnaie : l'émergence des monnaies numériques de banque centrale

Depuis quelques années seulement, les monnaies numériques de banque centrale (MNBC - en anglais, *Central Bank Digital Currency ou CBDC*) sont au cœur des débats qui agitent l'écosystème des crypto-actifs. En effet, de nombreuses banques centrales ont annoncé des travaux de réflexion, voire de développement, de leur propre MNBC. Or, si les banques centrales semblent déterminées à faire aboutir ces projets, le débat qui les entoure reste très technique et esquive toutes les problématiques politiques.

Le concept de MNBC est pluriel. L'ensemble de ces attributs et choix techniques peuvent radicalement modifier la nature de la monnaie traditionnelle ainsi que son usage. Par conséquent, un travail de prospective doit être engagé sur les différentes composantes d'une MNBC. Toutefois, avant de résoudre ces caractéristiques techniques, les banques centrales devront faire des choix de nature politique. Ces décisions induiront des conséquences substantielles allant jusqu'à modifier le paradigme d'émission monétaire. C'est pourquoi, au-delà des considérations techniques, économiques et juridiques, un débat doit s'ouvrir en Europe sur les conséquences politiques d'une telle monnaie.

1. Brève introduction

Principe consubstantiel à sa création, le réseau Bitcoin s'est fondé sur la volonté de retirer le pouvoir monétaire des mains des banques centrales. Jugées insuffisamment démocratiques, n'ayant pas su encadrer les excès financiers des banques commerciales, les banques centrales et les États devaient renoncer à leur pouvoir de battre la monnaie. Ce bien public qu'est la monnaie devait être libéré du joug des technocrates et rendu aux citoyens. Grâce au progrès technologique permis par la blockchain, la monnaie devait être basée sur des règles strictes et démocratiques, confondues dans le code informatique. Ces règles devaient permettre la transparence tant sur l'émission monétaire que sur son pouvoir de contrôle. Ce dernier devait en outre reposer sur un principe de décentralisation. Cette vision libérale, quasi libertarienne, de la monnaie a largement infusé dans l'écosystème, notamment parmi ses premiers défenseurs.

Néanmoins, avec la démocratisation du bitcoin et son adoption progressive dans le monde, la motivation politique s'est peu à peu muée en une finalité financière. Toutefois, la vision originelle perdure encore. Les pionniers de cet

écosystème sont avant tout des esthètes de la décentralisation. La promesse originelle a, par conséquent, toujours guidé les développements de ce nouveau monde. Cela se constate encore aujourd'hui avec les prémices de la finance décentralisée.

Conscient des antagonismes et arguant de risques systémiques au-delà de la seule question de la souveraineté monétaire des États, les banques centrales se sont emparées de ces nouveaux objets pour y faire respecter l'ordre constitutionnel qui prévaut aujourd'hui sur le terrain monétaire.

a. Un outil monétaire entre la devise officielle et le crypto-actif

Il convient de noter au préalable qu'une MNBC est, au même titre que le terme « *stablecoin* », une appellation générale pour désigner une diversité de réalités.

Cette diversité résulte du fait qu'il n'existe, à date, aucune MNBC pleinement opérationnelle à l'échelle d'un pays ou d'une région du monde. Et, au même titre que les *stablecoins*, les MNBC sont totalement programmables selon les souhaits de leurs émetteurs et ne revêtiront peut-être pas les mêmes traits selon leur pays d'origine (MNBC de détail¹¹⁸ - adressée aux particuliers ; MNBC de gros¹¹⁹ - adressée aux intermédiaires financiers ; etc ...) ¹²⁰. Aussi, il n'est possible que d'en donner une définition relativement générale : est une MNBC une représentation exclusivement numérique d'une devise ayant cours légal et émise par la banque centrale elle-même.

Par ailleurs, les MNBC sont apparues dans le sillage des crypto-actifs, basés sur la *blockchain*. Or, si environ 88% des projets de MNBC utilisent la *blockchain* comme technologie sous-jacente¹²¹, certains projets explorent également des pistes technologiques plus traditionnelles. La *blockchain* reste globalement privilégiée dans la mesure où elle permet une plus grande programmabilité et interopérabilité des *tokens* qui seront émis, tout en garantissant la sécurité de la propriété de ces derniers et le partage efficace de la valeur. Par ailleurs, les banques centrales pourraient ainsi avoir l'opportunité de concevoir des *smart-contracts* sur ces

¹¹⁸ Ou « *retail Central bank digital currency* » (r-CBDC).

¹¹⁹ Ou « *wholesale Central bank digital currency* » (w-CBDC).

¹²⁰ Cryptoast - [Monnaies numériques de banque centrale \(MNBC\) - C'est quoi et comment fonctionnent-elles ?](#) - 20.07.2021

¹²¹ PwC - [CBDC global index \(1st edition\)](#) - 04.2021

protocoles blockchain afin d'organiser ce nouveau système monétaire tout en l'optimisant dans son fonctionnement.

Lorsque l'on parle de MNBC, la première question qui se pose est celle de savoir ce qui distingue ce nouvel objet monétaire de la monnaie déjà existante sous forme numérique sur les comptes bancaires, utilisable avec les cartes de paiement et les *smartphones*.

Si ces deux types de devises sont effectivement numériques, elles ne sont pas émises par la même entité. On distingue traditionnellement la monnaie dite de « banque centrale » (c'est-à-dire les pièces et les billets, mais aussi les MNBC et la monnaie interbancaire) et la monnaie dite de « banque commerciale » (c'est-à-dire la monnaie disponible sur les comptes bancaires principalement). Il s'agit d'un fait largement méconnu par les citoyens mais la seule créance qu'ils détiennent sur la banque centrale est issue des pièces et billets qu'ils possèdent. S'agissant du reste de la monnaie en circulation, elle constitue une créance sur les banques commerciales, entités sous gestion privée. Ainsi, leurs dépôts ne sont que partiellement assurés pour un montant maximal de 100.000 euros par la BCE. Dans le cadre d'une MNBC, le paradigme est différent. En effet, émis par la BCE, la MNBC sera garantie par l'institution elle-même, contrairement à la monnaie hébergée sur le compte bancaire, qui supporte un risque de crédit.

En outre, la différence d'émetteur implique que la monnaie utilisée sous forme numérique est principalement une monnaie créée et hébergée sur les réseaux des banques commerciales. Cette monnaie transite notamment *via* les infrastructures de paiement mises à disposition par les sociétés intermédiaires de paiement. Ainsi, l'activité de paiement nécessite l'implication de nombreux acteurs : un acheteur et un vendeur naturellement, mais aussi les banques de chacun ainsi qu'un ensemble de prestataires de services de paiement chargés de l'authentification et de l'autorisation de la transaction. En outre, les transactions doivent transiter *via* des infrastructures complexes nécessitant d'importantes bases de données dans l'objectif de contrôler et d'exécuter les flux. Dans le cadre d'une MNBC, l'ensemble de cette infrastructure complexe et coûteuse est remplacé par une blockchain, dont la décentralisation est à la discrétion de la banque centrale. Ce mécanisme permet de supprimer les intermédiaires traditionnels, d'automatiser certaines opérations et d'assurer une absolue sécurité des données.

L'apport de la MNBC est donc triple : (i) elle modifie la substance même de la relation entre l'utilisateur et la monnaie, en supprimant le risque de crédit ; (ii) elle remet en cause l'existence et le modèle d'affaires des intermédiaires bancaires,

financiers et de paiement ; et (iii) elle réduit les coûts de transaction et accroît l'efficacité du réseau. Il convient de préciser en outre que ce dernier ne souffre d'aucune interruption de service résultant d'une intervention humaine.

Force est de constater que les MNBC empruntent davantage leurs caractéristiques aux crypto-actifs qu'aux monnaies électroniques traditionnelles. Néanmoins, en raison de leurs philosophies radicalement différentes des premiers crypto-actifs libertariens, il existe des divergences majeures dans leur conception. D'une part, contrairement aux blockchains publiques comme Bitcoin ou Ethereum, les MNBC fonctionneront sur des blockchains fermées dont la détention d'un nœud sera soumise à une autorisation de la part de la banque centrale. D'autre part, (i) contrairement aux crypto-actifs, dont la valeur dépend uniquement de l'offre et de la demande et n'offre aucune contrepartie physique, et (ii) contrairement aux *stablecoins*, dont la plupart sont garantis par des réserves réelles ou numériques, les MNBC sont soutenues par une autorité publique, représentée par la banque centrale. Leur valeur, stable, dépend donc de la confiance que les utilisateurs placent dans cette autorité.

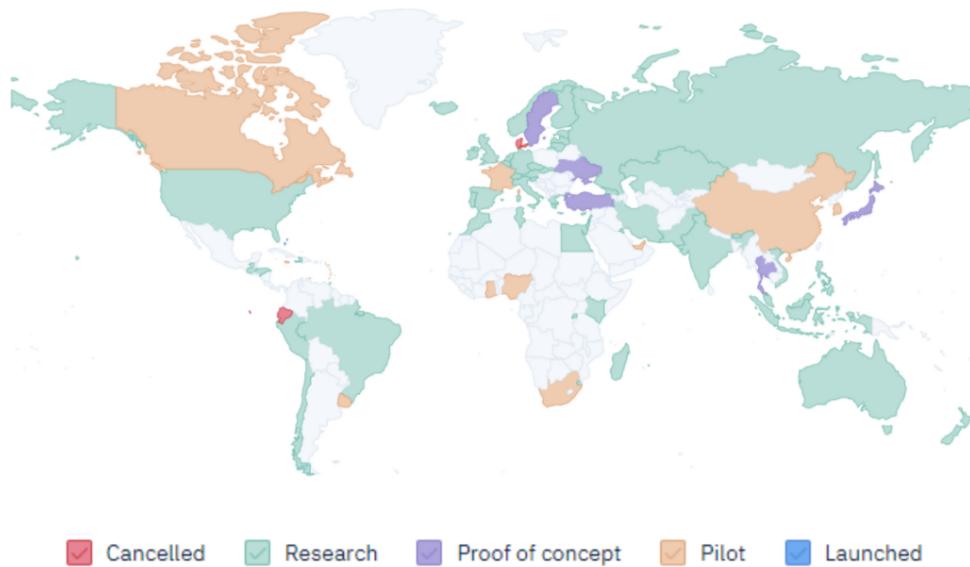
Ainsi, la grande hétérogénéité de ces nouveaux objets ne permet pas encore d'entrevoir clairement ce qu'ils deviendront dans les décennies à venir. Aussi, l'observateur attentif ne pourra que se limiter à observer les différentes directions qui sont prises par chacune des banques centrales sans pour autant déterminer ce que seront exactement ces objets dans le futur.

b. Une grande diversité de MNBC

Comme évoqué précédemment, la plupart des MNBC sont, à l'écriture de ces lignes, au stade de projet. Leur avancement est très inégal selon les pays. Or, selon un rapport de la Banque des règlements internationaux (BRI), publié en janvier 2021¹²², 86% des banques centrales ayant répondu au sondage¹²³ travaillent actuellement sur un projet de MNBC.

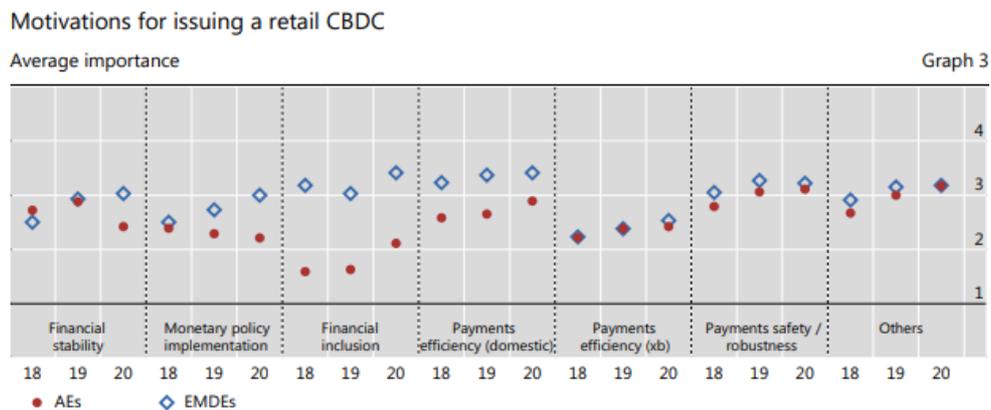
¹²² Banque des règlements internationaux - BIS Papers No 114 - Ready, steady, go? – [Results of the third BIS survey on central bank digital currency](#) - Janvier 2021

¹²³ Les banques centrales ayant répondu au sondage, au nombre de 65, sont principalement situées en Amérique, en Europe et en Asie du sud-est.



CBDC Tracker - Today's Central Bank Digital Currencies Status - Novembre 2021¹²⁴

Le rapport de la BRI met également en évidence les motivations des banques centrales à émettre une MNBC, qui diffèrent selon leur statut économique au niveau international. Ainsi, les pays émergents ont tendance à rechercher les bénéfices d'une inclusion financière accrue et une meilleure efficacité des systèmes de paiements, tandis que les pays avancés économiquement sont préoccupés par la stabilité financière et la sécurisation des moyens de paiement.



(1) = "Not so important"; (2) = "Somewhat important"; (3) = "Important"; (4) = "Very important".

Source: BIS central bank survey on CBDCs.

BRI - Les motivations des pays avancés (AEs) et des pays émergents (EMDEs) économiquement - Janvier 2021

¹²⁴ Source : [CBDC Tracker](#)

Ainsi, ces motivations vont participer du choix de la forme finale que revêtira la MNBC. En effet, dans la mesure où ils souhaitent renforcer l'inclusion financière de leurs citoyens, les pays émergents font le choix de développer une MNBC de détail à destination de l'ensemble des citoyens. A l'inverse, les pays développés, eux souhaitent optimiser et moderniser leurs systèmes financiers, sont incités à émettre une MNBC de gros, réservée aux seuls organismes financiers. On retrouve cette dichotomie des objectifs poursuivis dans les différents travaux des banques centrales les plus avancées sur ces questions.

2. Les différents projets de MNBC à travers le monde

Parmi les différents projets de MNBC qui se développent à travers le monde, certains retiennent davantage l'attention que d'autres, que ce soit en raison des possibilités qu'ils offrent, de leur niveau d'avancement ou de leur impact futur.

Ainsi, le présent rapport évoquera successivement le projet de MNBC de détail le plus avancé aujourd'hui - le Sand Dollar, le projet conjoint de MNBC de gros de Hong Kong et de la Thaïlande, ainsi que la MNBC qui devrait modifier substantiellement les rapports de force monétaires dans les années à venir, le yuan numérique.

a. La première MNBC de détail : le Sand Dollar des Bahamas

Le Sand Dollar¹²⁵ est aujourd'hui le projet de MNBC le plus avancé au monde, selon le cabinet d'audit PwC¹²⁶. Dirigé par la Banque centrale des Bahamas, ce projet a vocation à créer une version numérique du dollar des Bahamas (B\$) ainsi qu'à développer une infrastructure de paiements pour accueillir ce nouvel outil.

Or, ce pays de plus de 400.000 habitants et de plus de 700 îles est confronté à une problématique importante : celle de l'inclusion financière des populations éloignées de la capitale, Nassau. À elle seule, cette ville abrite plus de la moitié des habitants du pays (plus de 250.000), les autres étant répartis parmi les 30 autres îles habitées. Dans ces conditions, il est difficile d'assurer la bonne connexion de tous les citoyens aux infrastructures financières, ne serait-ce que pour faire circuler les espèces entre les différentes îles.

¹²⁵ Banque centrale des Bahamas - [Sand dollar](#)

¹²⁶ PwC - [CBDC global index \(1st edition\)](#) - 04.2021

Face à cette contrainte géographique, la numérisation de la finance offre une voie salutaire dans l'objectif d'inclure l'ensemble de la population dans les structures financières traditionnelles. C'est donc à cette fin que la Banque centrale des Bahamas travaille à la mise en œuvre d'une MNBC nationale, pour que l'ensemble des citoyens ait accès à la monnaie officielle et à un système de paiements efficace.

En outre, le Sand Dollar a été pensé de telle manière à ce qu'il puisse être utilisé par l'ensemble des citoyens, qu'ils soient avertis aux nouvelles technologies ou non. La MNBC des Bahamas est par conséquent disponible aussi bien sur *smartphone* que sur des cartes à puce, afin d'être utilisable sans support complexe.

Dans le même temps, le développement d'une telle infrastructure numérique permettrait de réduire les coûts des transactions. En effet, un écosystème financier national insuffisamment développé peut impliquer une dépendance des acteurs locaux vis-à-vis d'acteurs étrangers. Ces derniers peuvent imposer des conditions tarifaires importantes sur les transactions du quotidien. Dès lors, la création d'une structure nationale des paiements permet d'inclure l'ensemble de la population tout en réduisant le poids de ces acteurs dans les échanges économiques.

Par ailleurs, le Sand Dollar serait aussi une solution avantageuse afin de solutionner des problèmes plus spécifiques à ce type de pays, comme les épisodes météorologiques qui frappent régulièrement les Caraïbes. Dans ces circonstances, la numérisation de la chaîne de valeur permettrait de préserver les intérêts économiques des populations et des entreprises locales, tout en permettant une meilleure reprise des activités une fois les difficultés météorologiques éloignées et les dégâts constatés.

b. Le paiement transfrontalier tokenisé : la MNBC de gros de Hong Kong et de la Thaïlande

Parmi les différents projets de MNBC, le projet conjoint de la Hong Kong Monetary Authority (HKMA) et de la Banque de Thaïlande (BOT) est l'un des plus avancés. Ce projet, appelé « Inthanon-LionRock », vise à développer une MNBC de gros permettant de réduire les coûts, financiers et matériels, des paiements transfrontaliers.

Ce projet vise à permettre aux banques commerciales de Hong Kong et de Thaïlande d'effectuer des transferts de fonds et des transactions de change *via* des *smart-contracts*. Dès lors, l'objectif est de remplacer le système traditionnel, reposant sur une succession de couches opérationnelles, par un système automatique,

reposant sur la blockchain et permettant des paiements en temps réel à tout instant. En septembre 2021, les initiateurs du projet Inthanon-LionRock ont été rejoints par la BRI, le Digital Currency Institute of the People's Bank of China¹²⁷ et la Banque centrale des Émirats Arabes Unis. Le projet, renommé « mBridge », vise désormais à construire une plate-forme multi-MNBC au service des paiements internationaux.

Cette plateforme, aujourd'hui à l'état de prototype, a ainsi pu procéder à quelques expérimentations encourageantes. Selon un rapport de la BRI, mBridge a pu effectuer des transferts internationaux en quelques secondes contre plusieurs jours dans le système actuel. En parallèle, ce dispositif est développé de manière à fonctionner 24h/24 et 7j/7, dans la mesure où il est construit sur une blockchain partagée dans le monde entier et indépendante des fuseaux horaires. Enfin, l'automatisation des processus a permis de réduire les coûts de transaction de près de moitié. La BRI estime ainsi que les projets dits de « mCBDC », c'est-à-dire regroupant de multiples MNBC de gros sur des plateformes interopérables communes, offrent le plus grand potentiel pour dépasser les limites des systèmes actuels et permettre un service plus efficace et moins coûteux¹²⁸.

Les deux projets précédemment étudiés, qui figurent parmi les plus avancés au monde, représentent les principaux apports des MNBC à l'économie et à la finance. Néanmoins, ils ne prennent part à ce stade que dans des zones géographiques, monétaires et politiques restreintes et ne sont donc pas à même d'influer sur les rapports de force économiques mondiaux. À l'inverse, la Chine s'est lancée pleinement dans cette nouvelle course à l'armement monétaire et est désormais l'un des pays les plus avancés. Cela aura nécessairement des conséquences sur la stabilité monétaire internationale.

c. L'émergence précipitée du yuan numérique

Le yuan numérique, aussi appelé e-CNY¹²⁹, est le fruit d'un long travail de réflexion engagé par la Banque populaire de Chine (People's Bank of China ou PBoC) depuis 2014.

En effet, selon le *whitepaper* du e-CNY¹³⁰, le groupe de travail initié en 2014 a débouché, en 2016, sur les premiers prototypes conceptuels et, pour encadrer leur

¹²⁷ Organisme de recherche sous l'égide de la PBOC (la banque centrale chinoise) qui se concentre sur la recherche et le développement de monnaies numériques et de blockchain - Source : [China Banking News](#)

¹²⁸ BRI - Annual Economic Report, [CBDCs: an opportunity for the monetary system](#) - 23.06.2021

¹²⁹ CNY est le code désignant la devise officielle chinoise selon la norme internationale des codes des monnaies.

¹³⁰ PBoC - [Progress of Research & Development of E-CNY in China, Working Group on E-CNY Research and Development of the People's Bank of China](#) - 07.2021

développement, un Institut de la monnaie numérique a été créé. Depuis le dernier trimestre 2019, la Chine est passée à l'étape supérieure en lançant des pilotes de e-CNY dans certaines des plus grandes villes du pays, notamment : Shenzhen, Suzhou, Chengdu, puis en 2020 Shanghai, Hainan et Xi'an.

Dans le cadre de ces expérimentations, les autorités ont souhaité mettre à l'épreuve le yuan numérique dans des conditions très variées, afin d'étudier sa pénétration dans l'économie et les effets bénéfiques comme néfastes qu'il pourrait engendrer. En procédant à des *airdrops*¹³¹, en ajoutant cette MNBC à des distributeurs automatiques de billets¹³² ou en permettant le règlement des transactions ou des salaires directement en e-CNY¹³³, la Chine a accéléré le développement et le déploiement du yuan numérique depuis le début de 2020.

Selon les chiffres fournis par le gouvernement et la banque centrale chinoise, le *whitepaper* du e-CNY a précisé, en juillet 2021, que plus de 20 millions de portefeuilles personnels et plus de 3,5 millions de portefeuilles d'entreprises avaient déjà été ouverts. Le e-CNY avait déjà été utilisé pour régler pour plus de 34 milliards de renminbi de transactions. Début novembre 2021, la PBoC évoquait 140 millions de portefeuilles, dont 10 millions de portefeuilles d'entreprises, ouverts à des fins de transactions *via* le e-CNY¹³⁴.

L'objectif de la Chine est clair : profiter des avantages d'une monnaie numérique tout en appliquant des contrôles de capitaux. Cette nouvelle monnaie a ainsi pour objectif d'accompagner la numérisation de l'économie, mais aussi d'inclure financièrement des populations rurales jusqu'ici exclues de ces considérations numériques. L'e-CNY permettrait de raccrocher 200 millions de personnes mal connectées voire débancaarisées au système financier¹³⁵.

En outre, la banque centrale chinoise vise deux autres objectifs : d'une part, accompagner la diminution du recours aux espèces qui, comme en Europe, s'est fortement accrue avec la pandémie de la Covid-19 ; d'autre part, suivre la numérisation progressive des solutions de paiement et adapter la monnaie nationale aux nouveaux comportements de la population. Ces deux tendances concomitantes ont renchéri le coût du paiement de détail par rapport aux espèces. Ainsi, cette MNBC de détail a vocation à accompagner le déclin des espèces traditionnelles et, dans le même temps, à accompagner la mutation des moyens de paiement en

¹³¹ Cryptoast - [La Chine organise un airdrop massif du yuan numérique dans une ville pilote](#) - 05.12.2020

¹³² Cryptoast - [La Chine intègre le yuan numérique à des distributeurs automatiques](#) - 14.01.2021

¹³³ Cryptoast - [La Chine déploie plus de 3 000 ATMs dédiés au yuan numérique à Pékin](#) - 19.06.2021

¹³⁴ Bloomberg - [China's PBOC Says Digital Yuan Users Have Surged to 140 Million](#) - 03.11.2021

¹³⁵ Forbes - [Hong Kong Seeks Financial Inclusion With Digital Currency](#) - 01.11.2021

réduisant les coûts des transactions.

Ce sont ces objectifs qui vont conduire la banque et l'État centraux à définir les caractéristiques intrinsèques de cette MNBC, selon les besoins de l'économie nationale et selon les ambitions politiques du Parti. Parmi les caractéristiques anticipées du e-CNY, certaines doivent être détaillées pour comprendre le projet du yuan numérique.

D'abord, le yuan numérique fonctionnera sur un système à deux niveaux : (i) le premier niveau sera celui de la banque centrale, qui émettra les *tokens* à destination des intermédiaires financiers, (ii) le second niveau sera celui de ces intermédiaires qui seront chargés de distribuer lesdits *tokens* à la population. La PBoC souhaite ainsi favoriser l'adoption de cette nouvelle forme de monnaie en profitant des réseaux des banques commerciales et des habitudes de la population auprès d'elles. Néanmoins, il semblerait que la volonté de la PBoC soit de ne pas corréler les *wallets* e-CNY avec les comptes bancaires traditionnels.

Ensuite, la PBoC a annoncé que des *smart-contracts* pourront être déployés sur cette nouvelle forme de monnaie, notamment pour permettre l'émergence des paiements auto-exécutés dans des conditions prédéfinies par les parties à la transaction.

Par ailleurs, il est envisagé d'émettre différents types de *wallets*, selon les circonstances d'utilisation du e-CNY et selon les clients. Ainsi, il existe déjà des *wallets* destinés aux particuliers et des *wallets* destinés aux entreprises. Parmi ceux destinés aux particuliers, certains pourront être ouverts sans fournir d'identité, mais leur usage sera bien plus restreint s'agissant des opérations pouvant être effectuées ou la valeur transférée¹³⁶. Plus encore, il sera possible d'établir un *wallet* principal ainsi que des *wallets* secondaires, qui répondront à des caractéristiques différentes du premier (notamment en matière d'identification de l'utilisateur). Enfin, la PBoC envisage, en supplément des *wallets* disponibles par *smartphones*, d'émettre des *hardwallets*, afin que les populations non encore connectées à une infrastructure numérique puissent utiliser cette nouvelle forme de monnaie comme elles utilisent actuellement les espèces physiques.

Enfin, la PBoC met en avant le principe de l'anonymat « pour les petits montants » et de la traçabilité « pour les montants élevés » et annonce « attacher une grande importance à la protection des données personnelles et à la vie privée ». C'est notamment pour cette raison, et pour reproduire l'anonymat des espèces physiques

¹³⁶ L'ouverture de compte est possible en fournissant uniquement un numéro de téléphone. Dès lors, les transactions journalières seraient limitées à 5.000 yuans et les transactions annuelles à 50.000 yuans.

traditionnelles, qu'un *wallet* accessible sans identification est disponible pour les petits montants. Néanmoins, sur ce point particulier, le développement d'un e-CNY pose question quant à la restriction des libertés fondamentales en Chine. Il ouvre plus généralement des questions légitimes relatives à la protection des données personnelles ainsi que de droit à la vie privée pour chaque détenteur de cette MNBC à travers le monde. En effet, dans le cadre de la politique de centralisation et de renforcement du contrôle de l'État-Parti sur l'économie, le développement et l'adoption généralisée d'un e-CNY offrirait des moyens exorbitants aux autorités chinoises afin de contrôler et diriger les acteurs économiques nationaux. Cette centralisation des moyens et des données issus du pouvoir économique serait amplifiée par les nouvelles technologies telles que l'intelligence artificielle et facilité par le recul progressif des espèces physiques traditionnelles.

En parallèle, l'essor de cette nouvelle monnaie pourrait également avoir de graves conséquences sur les libertés individuelles des citoyens. En effet, dans le cadre des expérimentations réalisées sur le crédit social, la numérisation de la monnaie ainsi que la transparence des données permise par la blockchain pourraient permettre au gouvernement chinois de renforcer sa politique de contrôle des citoyens. Car, s'il existe des possibilités permettant au citoyen de conserver sa vie privée, il semble évident que ces cas de figure représenteront une petite minorité des usages de cette nouvelle monnaie. La plupart des citoyens seront contraints de s'identifier et il sera alors possible, pour l'État, de connaître précisément leurs habitudes de consommation et de pénaliser celles qui ne correspondent pas aux normes du Parti. À cet égard, la sinologue Chloé Froissart appuyait le propos dans un article du journal *Le Monde* : « La Chine ne reconnaît pas le principe d'égalité des citoyens. Les individus ont l'obligation de se conformer aux attentes de l'État sur ce que signifie être un bon citoyen. Sinon, ils sont rétrogradés dans la citoyenneté. »¹³⁷. La monnaie deviendrait par conséquent l'ultime outil permettant de compléter le graphe social de l'État-Parti.

Par ailleurs, il convient de regarder avec prudence ce que pourrait devenir le e-CNY au-delà des frontières chinoises. Si aujourd'hui la Chine pratique une politique de contrôle stricte des capitaux, le développement de cette nouvelle forme de monnaie pourrait servir à Pékin pour contrer la domination du dollar américain faisant du yuan numérique une forme de monnaie bien plus efficace pour des acteurs économiques étrangers. *A fortiori*, et comme cela est déjà arrivé avec le dollar (notamment au Salvador), certains pays dans la sphère d'influence chinoise pourraient se tourner progressivement vers cette monnaie, avec les conséquences

¹³⁷ *Le Monde* - [En Chine, le « crédit social » des citoyens fait passer les devoirs avant les droits](#) - 16.01.2020

déjà évoquées plus haut. Une diffusion du yuan numérique, en Europe notamment, représenterait une perte supplémentaire de souveraineté économique, en particulier s'agissant de la diffusion des données économiques et personnelles auprès d'une puissance étrangère.

Face à ces enjeux, l'Europe ne peut rester sourde à l'idée d'émettre une monnaie capable de rivaliser avec les monnaies privées venant d'Amérique ou d'un yuan numérique au service du Parti communiste chinois.

3. Le positionnement de l'Europe : entre défiance et tâtonnements

L'Europe, puissance monétaire mondiale, est l'une des zones les plus actives en matière de recherches sur les MNBC. En effet, la Banque centrale européenne (BCE), bien que prudente à l'idée d'émettre un euro numérique, a lancé une série de réflexions sur un éventuel e-euro en interne et avec les banques centrales nationales.

En parallèle, la Banque de France est certainement l'une des banques centrales les plus en pointe sur les questions de MNBC de gros. Depuis septembre 2020, elle a lancé neuf expérimentations visant à développer une MNBC de règlement entre intermédiaires financiers. Cette stratégie visant à moderniser la monnaie de gros est le résultat d'une observation selon laquelle il existe une tendance à la tokenisation des actifs numériques (exemple : les droits sociaux avec les *tokens securities*) mais aussi des actifs de règlement (exemple : les *stablecoins*).

a. Les expérimentations de la Banque de France

Dans un rapport publié en novembre 2021¹³⁸, la Banque de France fait le point sur les différentes expérimentations menées jusqu'alors, sept sur neuf ayant d'ores et déjà abouti. Les expérimentations ont porté sur deux cas d'usage principaux : (i) d'une part, le développement d'un système de règlement-livraison plus efficace et transparent, tout en conservant la place essentielle de la monnaie de banque centrale, et (ii) d'autre part, l'amélioration des paiements transfrontaliers et interdévises.

Ainsi, les expérimentations de la Banque de France ont exploré des solutions techniques permettant de régler directement sur la blockchain les opérations de livraison contre paiement des actifs tokenisés, sans passer par les structures

¹³⁸ Banque de France - [Wholesale central bank digital currency experiments with the Banque de France](#) - 11.2021

existantes de règlement-livraison. Ces nouvelles méthodes permettent ainsi de renforcer la transparence et le suivi des différentes transactions réalisées, mais aussi d'en réduire drastiquement les coûts tout en assurant la disponibilité du service à tout instant du jour et de la nuit.

En parallèle, l'autre objectif de la Banque de France était d'expérimenter des situations dans lesquelles une MNBC de gros permettrait de créer une interopérabilité entre des systèmes de règlement-livraison blockchain distincts et déconnectés les uns des autres. En effet, les développements actuels autour de la blockchain peuvent laisser penser que plusieurs systèmes distincts vont émerger dans les années à venir, ce qui aurait pour conséquence de fragmenter la liquidité des titres. Aussi, *via* une monnaie de banque centrale commune, cette fragmentation pourrait être limitée en permettant des règlements harmonisés sur les différentes plateformes tokénisées.

De plus, la migration des opérations de règlement-livraison sur blockchain permet à ces derniers de bénéficier de l'automatisation permise par les *smart-contracts*. En effet, en programmant ces derniers, il est possible de réaliser de manière automatique des opérations complexes qui nécessitent aujourd'hui un travail opérationnel parfois long et coûteux (exemple : règlement conditionnel).

La Banque de France a dès lors mené une série d'expérimentations visant à améliorer le système actuel de transferts de fonds internationaux en procédant de différentes manières : (i) émission de plusieurs MNBC compatibles entre elles, (ii) émission de plusieurs MNBC interconnectées, et (iii) création d'un système unique regroupant plusieurs MNBC. En parallèle, la Banque de France a également envisagé l'hypothèse d'un système avec MNBC interopérable avec un système traditionnel, sans MNBC ou blockchain.

Ces expérimentations, réalisées en à peine une année alors que le sujet des MNBC est encore très jeune, placent la France parmi les pays les plus actifs dans le développement de ces nouveaux objets monétaires. La Banque de France a réussi à donner un cap clair en associant les acteurs institutionnels de la monnaie et les acteurs privés spécialistes de la blockchain et des crypto-actifs. Cette initiative doit désormais prendre de l'ampleur et devenir un véritable programme au service du développement de la finance française et européenne.

Néanmoins, elles ne représentent qu'une partie des potentialités offertes par les MNBC et ne répondent pas aux enjeux de souveraineté monétaire posés par l'apparition de nouveaux objets. La tokénisation de la finance ne peut être

complètement réussie sans tokenisation de la monnaie à l'échelle de l'ensemble de l'économie.

b. L'émission d'un euro numérique, entre sauvegarde de la souveraineté et nécessaire modernisation de l'outil monétaire

Dans un rapport publié en octobre 2020, la BCE a imaginé les contours d'une future devise euro numérique. Le 14 juillet 2021, le Conseil des gouverneurs de la BCE a décidé de lancer une phase d'enquête, d'une durée de deux ans, afin d'examiner l'émission éventuelle d'un euro numérique.

Si l'émission d'un euro numérique reste à ce stade hypothétique, la communication officielle de la Banque Centrale Européenne est intervenue dans un contexte d'inquiétude des banques commerciales, détentrices d'un quasi-monopole sur l'émission de monnaie électronique. Cette inquiétude a été renforcée par l'apparition de projets tel que celui du consortium « Libra » mené notamment par Facebook. Face à l'apparition de projets de *stablecoin*, ayant comme finalité la mise en œuvre d'un système et des moyens de paiement semblables à la monnaie électronique, les régulateurs se sont saisis de la question monétaire dans ce nouvel espace des crypto-actifs.

La création d'un euro numérique répond à la nécessité de modernisation de l'outil monétaire étatique, afin de ne pas être supplanté par des nouveaux objets privés. Il permettrait de répondre à une demande de simplicité et d'efficacité de la part des citoyens et suivrait ainsi les évolutions numériques de l'ensemble des agents économiques. Néanmoins, comme toute innovation majeure, l'euro numérique pose certaines interrogations fondamentales. Quelle serait la nature précise de cette monnaie numérique de banque centrale ? Serait-elle une monnaie de gros, uniquement réservée aux échanges entre institutions financières ou au contraire une monnaie de détail, accessible à tous les citoyens et à toutes les entreprises européennes ? Sera-t-elle une monnaie de détail accessible à chacun aux fins de paiement et de réserve de valeur et, le cas échéant, qu'en serait-il de la tenue de compte normalement dévolue aux banques commerciales ?

Ainsi, l'émission d'un euro numérique aura nécessairement pour conséquence de modifier l'architecture du système monétaire moderne. Il impactera aussi indirectement l'activité et le rôle même des banques commerciales et autres prestataires de paiement. Ces considérations sont tout à fait fondamentales pour ne pas mettre en péril la fragile stabilité du système bancaire et financier actuel, mais

elles ne doivent pas écarter les enjeux relatifs à la sauvegarde de la souveraineté étatique en matière monétaire.

Face à la concurrence internationale croissante, et notamment l'émergence rapide du yuan numérique, le temps n'est plus aux interrogations sur l'opportunité ou non d'émettre un euro numérique. Il est devenu nécessaire de faire émerger ce nouvel outil afin d'incarner la continuité de la monnaie de banque centrale, publique et d'intérêt général, dans ce nouvel espace de la nouvelle finance permis par les crypto-actifs.

Fort de ce constat, la question fondamentale pour la BCE est la suivante : quelle structure l'euro numérique doit-il adopter pour embrasser la modernité des crypto-actifs tout en s'inscrivant dans le cadre des institutions bancaires et financières traditionnelles ?

La conception de la structure de l'euro numérique dépendra avant tout des fonctions que ce dernier remplira dans l'économie et du modèle que l'on souhaite pour cette nouvelle forme de monnaie. Plus encore qu'un nouvel outil monétaire adapté à l'innovation, il devra être une extension de la souveraineté européenne dans la sphère numérique et, plus encore, à l'international. C'est pourquoi cette monnaie doit être avant tout un acte politique d'une Union européenne conquérante sur le terrain économique et monétaire.

i. Première fonction : offrir de nouvelles opportunités technologiques et économiques aux entreprises et citoyens européens

Le développement d'une MNBC européenne, de gros ou de détail, permettrait d'offrir de nouvelles opportunités technologiques aux acteurs de la zone euro et accroîtrait la digitalisation de l'économie.

Dans l'hypothèse d'une MNBC de gros, cette dernière bénéficierait donc exclusivement aux acteurs du système bancaire et financier. En particulier, un euro numérique basé sur la blockchain permettrait de créer un système fiable, rapide et peu coûteux de règlement des transactions entre les différents acteurs bancaires.

Plus encore, cela permettrait de compléter le dispositif prévu par le projet de régime pilote¹³⁹ visant à créer un cadre réglementaire favorable au développement

¹³⁹ Proposition de règlement du Parlement européen et du Conseil sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués - COM/2020/594

des instruments financiers tokenisés. En effet, le projet pilote prévoit une série d'exemptions réglementaires liées au régime des valeurs mobilières. L'objectif poursuivi est l'amélioration des outils de financement des entreprises (notamment les actions et les obligations) en les émettant et en les gérant directement sur une blockchain (juridiquement désignée par la notion de « technologie de registres distribués », en anglais « *distributed ledger technology* » ou DLT). Cette mutation technologique permettrait ainsi de réduire les coûts d'émission et de gestion des valeurs mobilières qui existent déjà sous forme numérique mais gérées *via* des mécanismes plus complexes.

Or, les opérations sur valeurs mobilières sont aujourd'hui réalisées sur une plateforme dite « *Target2 - Securities* » (T2S)¹⁴⁰, qui gère les opérations de règlement-livraison des titres en monnaie banque centrale. Dans cette hypothèse, la seule digitalisation des titres ne suffit pas à rendre le système plus efficace. Il est donc nécessaire que la BCE émette une MNBC de gros accessible aux dépositaires centraux pour régler les transactions de titres directement sur la blockchain, sans avoir à naviguer d'une plateforme à une autre et d'une technologie à une autre.

À défaut de MNBC émise par la BCE, il est possible d'imaginer un autre mode de règlement-livraison des titres qui utiliserait des monnaies privées type *stablecoins*. Néanmoins, cette hypothèse n'est pas à privilégier dans la mesure où ce type de monnaie numérique suppose, en raison de sa structure d'émission, un risque de crédit qui pourrait s'avérer néfaste pour le système financier en cas de choc négatif.

Proposition 18 : Émettre une MNBC de gros, à destination des acteurs du système bancaire et financier, afin de compléter la modernisation des marchés financiers *via* la blockchain.

Dans l'hypothèse d'une MNBC de détail, elle serait mise à la disposition de l'ensemble des acteurs de l'économie, des citoyens aux entreprises européennes voire internationales. Le champ des utilisateurs serait dès lors beaucoup plus large et engendrerait un plus grand nombre de problématiques mais aussi de potentialités. En effet, si la MNBC de gros permet une plus grande optimisation des processus

¹⁴⁰ Pour aller plus loin : [Banque de France - Target2 - Securities](#)

financiers et monétaires, la MNBC de détail transforme profondément le rapport des citoyens à la monnaie et aux échanges.

Tout d'abord, l'euro numérique constitue une réponse face à la diminution constante de l'usage des espèces. En effet, depuis quelques années, les Européens délaissent progressivement les pièces et billets au profit de moyens de paiement numérisés comme les cartes de paiement ou les paiements par *smartphone*. Cette tendance s'est d'ailleurs accentuée avec la pandémie de Covid-19. Les citoyens européens sont de plus en plus exposés aux solutions développées et contrôlées par des acteurs étrangers, en l'espèce les principaux prestataires de services de paiement. Or, si dans le même temps, l'Union européenne s'est saisie des enjeux liés à l'oligopole du marché des paiements, le renforcement de sa souveraineté pourrait impliquer le développement d'un nouvel outil de paiement, organisé et géré par l'Eurosystème au même titre que les espèces.

En outre, un euro digital aura la capacité de mettre fin à l'absence d'accès à un compte bancaire dont souffre une partie non négligeable des citoyens à l'échelle européenne. En effet, *via* l'utilisation d'un *smartphone* ou tout autre mécanisme ayant la capacité de lire un registre distribué, il est possible de concevoir des modèles où le citoyen ne dépendrait plus d'un acteur commercial afin de pouvoir être bancarisé.

En parallèle, dans le sillage de la démocratisation du bitcoin, de nouveaux moyens de paiement ont émergé afin de permettre l'utilisation des crypto-actifs directement *via* une carte de paiement dans les commerces. Si ce mouvement reste encore limité en France, il a tendance à se développer progressivement. En outre, les acteurs du paiement traditionnel ont fait le choix de développer des solutions de paiement en crypto-actifs (soit par conversion préalable des *tokens*, soit par leur transfert direct). Sur ce marché, et comme évoqué précédemment, le spécialiste français des paiements, Worldline, a entamé un programme permettant le recours aux crypto-actifs pour le règlement de transactions du quotidien auprès de plusieurs dizaines de milliers de commerçants suisses. Récemment encore, Visa a annoncé travailler à des solutions afin d'intégrer l'USDC, le *stablecoin* dollar de la société Circle. Cette dernière travaille notamment à la construction d'une nouvelle technologie afin de continuer à intermédiaire le paiement en crypto. Les sociétés Stripe et Paypal ont aussi sauté le pas et proposent à leurs utilisateurs américains des produits de paiement *via* crypto-actifs ou *stablecoins*.

Face à ce constat, l'euro numérique pourrait être la clé de voûte d'une nouvelle économie numérisée. Il pourrait être interopérable dans le Web 3.0. Mais, si ce nouvel outil doit servir la souveraineté économique et monétaire de l'Union, il doit aussi s'adapter aux contraintes propres à la société.

La première contrainte est celle de l'accessibilité. En France et plus globalement en Europe, de nombreux publics restent trop éloignés de ces nouveaux outils du fait de la fracture numérique. Cette dernière sera accrue dans la mesure où l'utilisation d'un euro numérique ne sera pas toujours naturelle.

Il ne peut y avoir d'euro numérique efficace et juste sans inclusion. Demain, les populations les plus éloignées des outils numériques devraient pouvoir conserver des alternatives, ce postérieurement à l'implémentation d'un euro numérique. En ce sens, il ne paraît pas opportun de prêcher pour un euro numérique venant remplacer l'intégralité des moyens traditionnels. En outre, les caractéristiques techniques d'un tel outil devraient comprendre des possibilités d'utilisations similaires à celle des espèces traditionnelles. Ainsi, si l'euro numérique peut être échangé *via smartphone* ou carte de paiement, il doit aussi pouvoir être échangé sans infrastructure spécifique et sans connexion au réseau. À défaut, il exclurait *de facto* une part importante de la population au-delà des seuls cas d'usage hors réseau.

Cette exigence d'opérationnalité sans prise en compte de la couverture numérique du territoire est l'un des défis majeurs de l'euro numérique. S'il devait pouvoir fonctionner hors ligne, il doit alors pouvoir reposer sur des *hard-wallets* opérant sans connexion internet. Ces derniers pourraient alors être chargés *via* internet (depuis un ordinateur ou un *smartphone*) ou depuis des bornes de recharges fonctionnant sur un modèle similaire aux distributeurs automatiques de billets.

La seconde contrainte est celle de la confidentialité. Cette question représente un dilemme majeur et une condition essentielle à l'acceptation d'un euro numérique.

Cela a été précédemment évoqué s'agissant du réseau Bitcoin, la caractéristique première d'une monnaie n'est ni sa reconnaissance légale, ni même la vérification des propriétés énoncées par Aristote. Une monnaie n'est monnaie que par la confiance qu'on lui accorde. Un objet ne devient monnaie que si ses détenteurs ont confiance dans son objet et dans les droits qui en découlent.

Afin que l'euro numérique soit adopté par une large partie des citoyens, ceux-ci doivent être assurés de sa sécurité, en tant que moyen d'échange et de stockage de la valeur, mais aussi de la confidentialité associée à leurs données personnelles. A cet égard, un grand flou règne sur le projet de la Banque centrale Européenne.

Le risque pour l'Europe serait d'emprunter un chemin similaire à celui de la Chine. Il était particulièrement éloquent de constater que, à l'occasion de la lutte contre la Covid-19, les nouvelles technologies ont été un atout pour les régimes autoritaires dans leur volonté d'imposer une extrême centralisation des informations. En outre, des usages impensables hier deviennent rapidement des normes liberticides acceptées de tous. Or, dans cette société contemporaine, les libertés individuelles sont souvent bradées au profit de services ou d'usages gérés par des entités technologiques mondiales, comme les GAFAM, le consommateur devenant lui-même l'objet de consommation. Cet avenir ne peut être celui du rapport entre les citoyens et leur monnaie.

A cet égard, si le contrôle et la supervision politique des citoyens chinois semble être la finalité en matière de politique monétaire en Chine, l'Europe érige le principe de sécurité face à la lutte contre le blanchiment et au financement du terrorisme comme mantra de sa politique financière et monétaire. Si ces règles, dans leurs principes, sont nécessaires partout afin d'assurer la sécurité et l'ordre public, force est de constater que certaines de ces politiques confinent parfois à l'absurde. Pour une extrême minorité d'actes répréhensibles, l'intégralité des concitoyens sont entravés dans leur propre possession. Le nécessaire équilibre entre les droits découlant de la propriété privée et l'ordre public n'est pas toujours respecté.

Parfois, certains dispositifs vont au-delà du raisonnable. L'exemple du projet de règlement européen relatif aux transferts de fonds dit « Transfer of Funds Regulation » (*TFR*) est significatif. La version actuelle du texte implique la suppression automatique du pseudonymat issu des adresses publiques lors de l'utilisation d'un "*unhosted wallet*" vers un prestataire de services sur crypto-actifs. Si les règles imaginées vont au-delà des recommandations du GAFI, l'absence d'intervention du juge judiciaire est un problème majeur pour les libertés individuelles. Car, conséquence de la transparence inhérente aux blockchains publiques, ce projet de réglementation conduit à identifier toute personne utilisant des crypto-actifs et permettra d'en connaître tous les flux monétaires quels qu'ils soient. Pire encore, le projet induira demain la transmission automatique à l'autorité publique de toutes les transactions antérieures ainsi que le solde du compte dès une transaction supérieure à 1.000 euros.

Ce projet de règlement entre pleinement en contradiction avec le Règlement général sur la protection des données (*RGPD*), sans parler de l'absence d'équilibre dans la répartition des prérogatives entre le juge judiciaire, gardien des libertés fondamentales, et des prérogatives confiées à une simple autorité administrative indépendante ou non de l'État. Si demain la levée ponctuelle et encadrée du pseudonymat paraît être indispensable afin de faire régner l'ordre public, elle ne devrait pouvoir se faire sans l'intervention d'un juge judiciaire. En outre, d'un point de vue économique, l'euro numérique devra, qu'il s'agisse des prestataires de services utilisant l'euro numérique, des banques centrales ou des banques commerciales, protéger les données économiques personnelles des citoyens européens. Ces dernières ne devront pas être captées afin de construire des campagnes ciblées.

Ainsi, dans la droite ligne du RGPD, la BCE devra construire l'architecture de l'euro numérique afin de préserver la vie privée des citoyens lors de l'usage de cette nouvelle forme de monnaie. Sur ce point, les blockchains publiques permettant le pseudonymat sont une source d'inspiration. Loin d'être un refuge financier pour les criminels et les terroristes, les crypto-actifs permettent de tracer les fonds échangés. Ces transactions sont consignées dans chaque bloc de la blockchain, chacun étant immuable. Le pseudonymat apparaît alors comme le corollaire indispensable à la transparence de principe de la blockchain, *a contrario* des autres systèmes d'information existants.

S'il est avéré que les cas d'usage illicites sont plus rares dans l'écosystème des crypto-actifs que ce que les détracteurs des crypto-actifs aiment le répéter¹⁴¹, l'Eurosystème et les autorités des différents États membres de l'Union Européenne doivent avoir la capacité de retracer l'origine des fonds ainsi que les auteurs des actes. Tout l'enjeu réside donc dans la recherche d'un subtil équilibre entre respect de la vie privée des citoyens et lutte contre les activités illégales, face à une technologie parfaitement transparente.

C'est pourquoi, afin de préserver l'ordre public et la sécurité de tous, le pseudonymat s'impose comme standard pouvant être levé dans les cas prévus par une loi. Chaque citoyen devrait pouvoir bénéficier d'un compte libellé en « euro numérique » représenté dans une blockchain publique par une clé publique. Un processus de KYC pourrait être mis en œuvre préalablement. Les données en résultant (identités ainsi que les clés publiques concordantes) ne devront pas être stockées au sein d'une seule et même entité. La réunification des informations

¹⁴¹ Chainalysis - The 2022 Crypto Crime Report - 02.2022

nécessaires à la levée du pseudonymat ne pourrait alors se faire qu'après décision judiciaire.

Aussi, si les potentialités de cette nouvelle technologie monétaire sont immenses notamment afin de créer de nouveaux leviers de politique monétaire et budgétaire. Il est primordial de rester prudent et sage quant à la définition du fonctionnement d'un euro numérique car ses usages pourraient se révéler aussi bénéfiques que dévastateurs.

ii. Deuxième fonction : renforcer la souveraineté monétaire de l'Union européenne et créer les ponts vers la finance crypto

Outre la modernisation de l'économie, un euro digital n'a de sens que s'il permet de défendre la place de l'euro, en Europe d'abord, mais aussi dans le monde. La succession des crises récentes notamment, depuis la crise de la dette en 2015 et davantage encore depuis la crise sanitaire en 2020, a révélé l'importance de la politique monétaire dans les choix politiques, économiques et budgétaires des États membres.

Or, sans évoquer les débats portant sur l'intégration parcellaire qu'implique une monnaie commune sans politique budgétaire unifiée, les programmes à répétition visant à relancer tant bien que mal l'inflation et à faire baisser la pression sur les taux dans la zone euro n'ont pas été sans conséquence sur l'économie continentale. En parallèle, le dollar reste maître des échanges internationaux et réserve de valeur de référence, tandis que la Chine déploie à grande vitesse un yuan numérique qui pourrait être utilisé - à terme - comme devise de référence dans le commerce mondial. Par conséquent, l'euro doit se moderniser et s'adapter aux nouveaux usages qui deviendront prépondérants dans un avenir proche. Une monnaie qui ne répond pas aux exigences techniques de l'économie est une monnaie de moins en moins échangée, affaiblissant *de facto* la souveraineté de l'émetteur.

Si l'hypothèse d'une généralisation des *stablecoins* et MNBC à l'échelle mondiale comme nouveau standard monétaire reste encore lointaine aujourd'hui, ces derniers trouveront rapidement une application concrète dans les échanges transfrontaliers. Il est urgent, d'un point de vue politique mais aussi monétaire, d'envoyer un signal fort : l'euro doit anticiper les nouvelles données de l'économie numérique. Ce signal est indispensable au-delà de la seule question des crypto-actifs afin de renforcer la place de l'Europe dans l'économie mondiale. Toutefois, l'effet d'une telle annonce sur le secteur bancaire n'est pas sans conséquence. En effet, la

création, par la BCE, d'un euro numérique à destination des citoyens européens et des acteurs économiques de la zone euro modifie profondément le mode d'émission monétaire.

Afin de renforcer la souveraineté de la devise européenne, il convient d'appréhender l'euro numérique, non comme un substitut aux crypto-actifs ou autres *stablecoins* privés, mais comme un pont vers cette nouvelle finance. Au-delà des seules caractéristiques définies en amont, un euro numérique constitue un moyen de paiement dans un monde où les devises traditionnelles ne peuvent être utilisées. Ainsi, ce nouvel outil monétaire serait un atout pour le secteur de la finance des crypto-actifs dans la mesure où il rendrait plus simple l'interopérabilité avec le monde traditionnel.

L'absence de volonté du secteur bancaire d'épouser clairement cette nouvelle vague constitue à long terme une erreur de jugement qui risquerait d'être préjudiciable pour l'ensemble de l'économie. Ainsi alors que même des banques commerciales étrangères (notamment américaines, comme Goldman Sachs ou Morgan Stanley) commencent déjà à adapter leurs services aux crypto-actifs et que les *exchanges* développent de nouvelles offres financières afin de devenir les crypto-banques de demain, les banques françaises sont déjà supplantées sur le terrain de la valorisation. En outre, ces acteurs systémiques ne se priveront pas, dans un futur proche, de déployer des offres les rapprochant de plus en plus du métier des banques traditionnelles.

À titre d'illustration, Coinbase, l'un des plus importants *exchanges* au niveau mondial, a annoncé en juillet 2021 vouloir émettre un produit d'épargne à destination des particuliers, rémunérant leurs placements avec un taux de rendement de 4%, bien supérieur aux produits d'épargne traditionnels. Ces produits d'épargne fonctionneraient sous la forme d'un dépôt de fonds, convertis en *stablecoins* ultérieurement prêtés sur les protocoles DeFi, réputés fournir des taux de rendement importants. Le 13 septembre de la même année, la SEC a déclaré vouloir poursuivre en justice Coinbase s'ils émettaient ce nouveau produit d'épargne à destination des particuliers¹⁴². Ce cas d'espèce démontre que la SEC est consciente des conséquences systémiques que pourraient avoir le développement d'une offre alternative et concurrente en matière d'épargne sur l'ensemble des acteurs bancaires.

En effet, l'offre d'un produit d'épargne disponible à tous présentant un faible niveau de risque et une rentabilité jusqu'à 8 fois supérieure aux produits d'épargne traditionnels pourrait avoir pour conséquence d'assécher les dépôts auprès des

¹⁴² L'Agefi - [Coinbase abandonne son programme de prêt crypto](#) - 21.09.2021

banques commerciales. Il est certain que ce type de produit pourrait trouver, en Europe et plus particulièrement en France, une clientèle. Or, l'adage est bien connu des économistes : « les dépôts font les crédits ». L'intégralité du financement de l'économie pourrait être affaiblie.

Parmi les hypothèses de structure de l'euro numérique de détail, l'une envisage l'hébergement et la gestion des comptes utilisateurs par la BCE elle-même. Dans ce cas de figure, et dans l'hypothèse d'une adoption progressive de l'euro numérique par la population, une part non négligeable de l'épargne aujourd'hui détenue auprès des banques commerciales serait ainsi réorientée vers les comptes de la banque centrale. La banque d'affaires américaine Morgan Stanley a même estimé, en juin 2021, que dans l'hypothèse où la BCE hébergerait elle-même les comptes en euro numérique des citoyens (en les plafonnant à 3.000 euros), cela entraînerait une perte de liquidités d'environ 8% des dépôts aujourd'hui détenus par les banques commerciales européennes¹⁴³. Par conséquent, il paraît complexe que l'euro numérique n'intègre pas les problématiques des banques commerciales dans sa structure globale de fonctionnement.

Or, à ce jour, qu'il s'agisse des travaux de la BCE ou des banques centrales nationales, les réflexions engagées n'ont pas encore abouti et les choix structurants peinent à se dessiner.

iii. Troisième fonction : moderniser les politiques publiques avec de nouveaux outils plus performants

L'émission d'une MNBC à l'échelle de la zone euro n'implique pas seulement un changement de paradigme dans la structure monétaire actuelle. Elle permet aussi de mettre en œuvre des politiques ou des outils qu'il était difficile, voire impossible, d'appliquer auparavant. L'euro numérique sera le premier outil rendant possible l'automatisation de la monnaie.

Modernisation des outils fiscaux - Parmi les applications que l'on peut déjà entrevoir, l'usage des *smart-contracts* dans la collecte des impôts et taxes est l'une des plus novatrices. En effet, à titre d'exemple, dans le cadre de transactions recourant à l'euro numérique, il pourrait être décidé de rendre compatible la monnaie avec des *smart-contracts* afin de collecter automatiquement la TVA lors de la vente

¹⁴³ Reuters - [Digital euro might suck away 8% of banks' deposits](#) - 16.06.2021

de biens ou de services. Ce mécanisme permettrait d'améliorer la collecte de l'impôt et simplifierait les démarches administratives.

Outre la collecte de la TVA, l'euro numérique permettrait également de lever les difficultés juridiques et techniques liées au prélèvement à la source. En effet, les *smart-contracts* permettront d'automatiser le prélèvement de l'impôt sur le revenu, prélevé à la source, en supprimant le coût administratif supportés par les employeurs. Ainsi la lourdeur administrative et les coûts afférents ne seront plus supportés par les entreprises mais par la blockchain. De cette manière, l'euro numérique viendra soulager les agents économiques de leurs obligations déclaratives et comptables. En parallèle, il donnera à l'administration fiscale un nouvel outil extrêmement efficace afin de lutter contre la fraude fiscale, par son automatisme, sa transparence et son inviolabilité.

Toutefois, et comme évoqué précédemment, cette automatisation des prélèvements fiscaux ne peut prospérer sans la confiance des contribuables envers ces nouveaux outils. Cette confiance découlera du respect, par l'administration fiscale et les acteurs économiques, de la confidentialité des données économiques personnelles des contribuables. Ainsi, la question s'était notamment posée lors de l'entrée en vigueur du prélèvement à la source au sujet de la transmission, à l'employeur, des données personnelles du contribuable salarié concernant ses revenus et son patrimoine personnel. Différents mécanismes avaient alors été imaginés afin de permettre le respect de la confidentialité de ces informations, mais au prix d'une moindre efficacité du dispositif.

A l'avenir, la programmabilité de la monnaie, avec l'introduction des *smart-contracts*, permettra de mettre en œuvre des dispositifs efficaces tout en préservant la vie privée des citoyens. Ainsi, ces nouveaux mécanismes pourraient fonctionner en deux temps : (i) les informations personnelles des contribuables nécessaires à la fiscalisation de l'opération (achat/vente d'un bien ou d'un service, versement du salaire, etc ...) sont transmises au *smart-contract* correspondant par le biais d'un oracle¹⁴⁴ ; (ii) puis, il procède de manière automatique à la fiscalisation de l'opération en répartissant directement les fonds entre le Trésor public et le contribuable.

Ainsi, dans le cas d'un traitement d'une opération soumise à TVA, l'enjeu repose sur les informations qui seront transmises par le *smart-contract* au Trésor public. Il serait dès lors attentatoire à la vie privée des contribuables s'il était

¹⁴⁴ Le concept de « oracle », dans le contexte de l'écosystème des crypto-actifs et de la blockchain, est explicité ultérieurement.

transmis à l'administration fiscale les habitudes de consommation de tel ou tel contribuable. C'est pourquoi, qu'il s'agisse d'une opération soumise à TVA ou d'une opération distincte, seules les informations impérativement nécessaires au traitement fiscal de l'opération concernée devront être transmises au Trésor.

Néanmoins, si une grande partie de la collecte des taxes et des impôts dépendait à l'avenir de ces *smart-contracts*, une attention particulière devrait être portée à la sécurité de ces derniers et à leur bon fonctionnement. En effet, dans l'hypothèse d'un déploiement de ces nouveaux outils numériques à grande échelle, l'État se doit de développer des moyens afin d'assurer leur maintenance et pour conserver leur intégrité face aux nouvelles cyberattaques.

Afin de faire face à ces nouvelles exigences, les personnes publiques doivent monter en compétence sur ces sujets en dotant l'ANSSI ainsi que les administrations concernées des moyens techniques et humains nécessaires.

Modernisation des outils monétaires - En parallèle de la modernisation des outils fiscaux, l'euro numérique est également une opportunité sans précédent permettant de moderniser les outils de politique monétaire.

Toujours *via* la blockchain et les *smart-contracts*, cet euro numérique permettrait de mettre en oeuvre d'une manière simple et efficace une politique de monnaie hélicoptère¹⁴⁵, en complément des différentes mesures de politique monétaire déjà mises en oeuvre. Or, chacun peut le constater depuis la crise financière de 2008, la politique accommodante menée par la BCE n'a pas vraiment permis de porter le niveau d'inflation au niveau de sa cible de 2%. Il aura fallu attendre la reprise de l'économie après les premières vagues de la Covid-19 pour retrouver cette inflation, accentuée par la guerre en Ukraine et la crise énergétique.

Pourtant, la politique d'assouplissement quantitatif (en anglais, on parle de *quantitative easing*) mise en oeuvre l'a été dans des proportions telles que les liquidités ont abondé les marchés financiers et ont gonflé les prix de plusieurs classes d'actifs, les actions et l'immobilier au premier chef. Parmi les différentes causes, la plus notable est certainement le manque d'efficacité dans la transmission de la politique monétaire par le biais du système financier qui, pour plusieurs raisons,

¹⁴⁵ La monnaie hélicoptère est un type de politique monétaire consistant à créer, *ex nihilo*, de la monnaie pour, ensuite, la distribuer directement aux agents économiques (ménages et entreprises) sans passer par le secteur financier. Il s'agit donc d'une distribution directe de monnaie, de la banque centrale aux agents économiques.

préfère investir une partie de ces fonds nouvellement créés sur les marchés plutôt que de le rediriger vers une économie réelle apparaissant alors comme moribonde.

Aussi, selon plusieurs économistes, une politique de monnaie hélicoptère permettrait de contrebalancer ce manque d'efficacité en injectant directement les liquidités nouvelles créées auprès des ménages et des entreprises. De cette manière, ces derniers se trouveraient en situation de surplus d'épargne ou de trésorerie et seraient incités à consommer et investir. Ce faisant, la relance de la consommation et de l'investissement à production égale favoriseraient le retour de l'inflation et de la croissance.

S'il n'est pas question, dans le présent rapport, de juger de l'opportunité de la mise en œuvre d'une telle mesure, l'apport de l'euro numérique dans l'application concrète d'une politique monétaire semble indéniable au regard des pratiques existantes. Dans l'hypothèse où chaque citoyen dispose d'un *wallet* euro numérique auprès de la BCE, celle-ci n'aura qu'à procéder à une opération sur la blockchain pour créditer les *wallets* de l'ensemble des ménages et entreprises concernées.

Plus encore, la programmabilité de l'euro numérique pourrait permettre de flécher toute politique monétaire en direction des acteurs qui en ont le plus besoin, ou encore d'en restreindre l'usage dans des utilisations avec un fort effet de levier pour l'économie européenne. De cette manière, il serait possible de sectoriser la politique monétaire, qui deviendrait alors plurielle, et de faire bénéficier certaines catégories de la population ou certains pans de l'économie d'un effet de levier monétaire qu'il est impossible de reproduire aujourd'hui.

L'émergence de ce nouvel outil monétaire reste, pour le moment, une perspective lointaine. Par ailleurs, il ne peut être fait usage d'un tel outil sans prudence ; celle-ci oblige, une nouvelle fois, l'ensemble des parties prenantes à considérer les opportunités qu'offre l'euro numérique, sans dogmatisme ni préjugé.

Qu'il s'agisse des administrations de l'État, des services de la Commission européenne ou de la BCE, des grands prestataires de paiement et des grandes banques européennes, tous les acteurs doivent collectivement penser au futur rôle de cette monnaie numérique. Cette révolution de la monnaie s'accompagnera d'une autre révolution, celle de la finance, qui apparaît comme le cas d'usage le plus naturel des crypto-actifs et qui promet de bouleverser les usages et les produits financiers traditionnels.

Proposition 19 : Émettre un euro numérique de détail, à destination de tous les particuliers et de toutes les entreprises, dont certains prérequis auront fait l'objet, au préalable, d'une réflexion approfondie :

(i) Accessible partout et par tous, que l'on soit connecté au réseau centralisé ou non, que l'on soit équipé de matériel informatique ou non ;

(ii) Confidentiel s'agissant des données personnelles des citoyens, avec la possibilité d'identifier les personnes et les transactions dans le cadre de la lutte contre le blanchiment et le financement du terrorisme, sous le contrôle de l'autorité judiciaire ;

(iii) Dont la structure repose sur les acteurs bancaires traditionnels afin que ces derniers puissent diffuser l'euro numérique à travers les différentes couches de la population et sans que cela ne crée un risque systémique pour la stabilité financière ;

(iv) Dont la structure permet de faire face aux risques de dysfonctionnements et d'attaques sur les *smart-contracts* chargés de collecter l'impôt - les services de l'État doivent monter en compétence d'un point de vue technique sur les possibilités offertes par la blockchain ; et

(v) Dont la structure permet de développer des applications innovantes relatives à la collecte de l'impôt et à la politique monétaire.

PARTIE IV - La finance numérique de demain

Les crypto-actifs sont, aujourd'hui encore, définis par leurs détracteurs comme des outils spéculatifs déconnectés des réalités du monde et tournés uniquement vers une recherche de profit désincarné. Il y a encore quelques années, il était en effet difficile d'identifier de manière tangible les véritables cas d'usage des crypto-actifs, si ce n'était celui de numériser et de faire transiter la valeur. Ainsi, les premiers crypto-actifs ont longtemps été des objets dont la fonction première était de vérifier la faisabilité d'un dispositif technique (on parle de *proof of concept* ou PoC). Parmi les premiers usages économiques, sont apparus les ICO à partir de 2016. Cette innovation et l'apport de liquidités qui en a résulté a conduit à la première bulle de l'histoire des crypto-actifs. Depuis 2019 et l'avènement de protocoles permettant de répliquer des mécanismes de finance traditionnelle de manière décentralisée, un vent nouveau souffle sur l'écosystème qui, jusqu'alors, semblait manquer de réels usages. Cette nouvelle manière d'entrevoir la finance a apporté son lot d'innovations permettant de développer de nouveaux modèles d'affaires qui très certainement remettront en cause les rentes des acteurs de la finance traditionnelle.

Il ne sera pas question, ici, de juger si les valorisations de ces nouveaux protocoles et services financiers sont justifiées ou non. Le présent rapport s'attachera à décrire ce que sont les véritables apports de la finance décentralisée, leurs cas d'usage, leur fonctionnement et les enjeux qui accompagnent leurs développements. Cette partie se veut pédagogique et prospective, tant le potentiel transformateur de cette nouvelle grappe d'innovations pourrait révolutionner, voire déstabiliser, les fleurons financiers français et européens.

I. La finance décentralisée, un nouveau modèle

La finance décentralisée constitue un secteur à part au sein de l'écosystème des crypto-actifs. Ce secteur revêt en réalité une grande diversité d'applications qui restent liées entre elles par des caractéristiques communes. Secteur émergent, il n'a pas encore atteint sa maturité, mais il propose déjà une pluralité de cas d'usage.

1. Notion et enjeux

La finance décentralisée (en anglais *decentralized finance* ou « DeFi ») est une nouvelle forme de finance basée sur la technologie blockchain. Bénéficiant des

avantages de cette technologie, elle permet notamment de créer des applications financières décentralisées.

Le terme de DeFi est une appellation composite afin de désigner une grande variété d'applications aux objectifs et modes de fonctionnement divers. Néanmoins, celles-ci partagent plusieurs caractéristiques communes. Ainsi, les protocoles DeFi (i) sont hébergés sur des blockchains publiques (pour l'immense majorité, la blockchain Ethereum), (ii) fonctionnent sans opérateur central, (iii) de manière automatisée à partir de *smart-contracts* et (iv) ne sont pas soumis aux contraintes horaires des marchés financiers traditionnels. Par ailleurs, la DeFi est, contrairement à la finance traditionnelle, un écosystème transparent et facile d'accès. En permettant à toute personne disposant d'un simple accès au réseau Internet d'utiliser ces applications, et en protégeant ses données personnelles grâce au pseudonymat, les protocoles DeFi offrent un nouvel horizon financier aux personnes débancarisées ou discriminées.

Du fait de l'état de développement de ces technologies, la DeFi est confrontée aux mêmes problématiques inhérentes à la technologie blockchain que celles déjà évoquées. Ainsi, les enjeux relatifs au pseudonymat, la volatilité des actifs, le piratage des *smart-contracts* sont autant de défis auxquels les acteurs de la DeFi doivent faire face. Toutefois, l'essentiel des problématiques de la DeFi sont liées à la jeunesse de ce secteur qui a réellement émergé durant l'été 2020. En outre, du fait de la nature inédite de ces activités, le législateur ainsi que le régulateur n'ont pas encore imaginé les nouveaux leviers d'une réglementation financière. À ce jour, aucune règle ne protège les investisseurs, ni n'encadre les activités des prestataires.

Toutefois, il ne serait pas juste d'affirmer que la DeFi est un *far-west* numérique dans lequel règne la cupidité et la férocité. D'une part, parce que la DeFi s'est construite d'abord sur une opposition à la finance traditionnelle centralisée en proposant un système simplifié et transparent, au même titre que Bitcoin s'est construit en opposition aux monnaies officielles des banques centrales. D'autre part, parce que la DeFi est un écosystème dans lequel des dizaines d'innovations apparaissent chaque semaine. Le secteur, extrêmement agile, innove sans cesse afin de développer de nouvelles offres. Il est difficile dans ce contexte d'établir une réglementation pérenne et stable.

Si l'importance d'une évolution technologique devait se quantifier *via* ses impacts sociétaux, nul doute que la DeFi sera considérée comme une rupture majeure à l'échelle du progrès technologique. Or, à l'instar de toute rupture technologique induisant une destruction-créatrice schumpétérienne, elle entraînera sans doute la

disparition d'anciens acteurs n'ayant pas su se renouveler au profit d'autres ayant saisi cette opportunité technologique.

Ainsi, on comprend aisément que les acteurs traditionnels soient réticents envers cette finance nouvelle et qu'ils en appellent même à barrer son développement. Néanmoins, ces acteurs seraient sages et avisés de s'en inspirer et d'améliorer leurs propres systèmes à l'aune de ces innovations. A contrario, la difficulté qu'éprouve le secteur de la DeFi vis-à-vis du monde bancaire traditionnel et l'incapacité de ce dernier à voir le potentiel de ces nouvelles technologies impliqueront nécessairement les mêmes conséquences que celles vécues lors de la naissance d'Internet et l'explosion du numérique. Il appartient donc à ces acteurs de se saisir de ces opportunités afin ne pas connaître le même sort que des entreprises comme Kodak, leader dans le secteur de la photographie, ou encore les *majors* du disque face à l'apparition du *streaming*.

2. Un secteur encore émergent

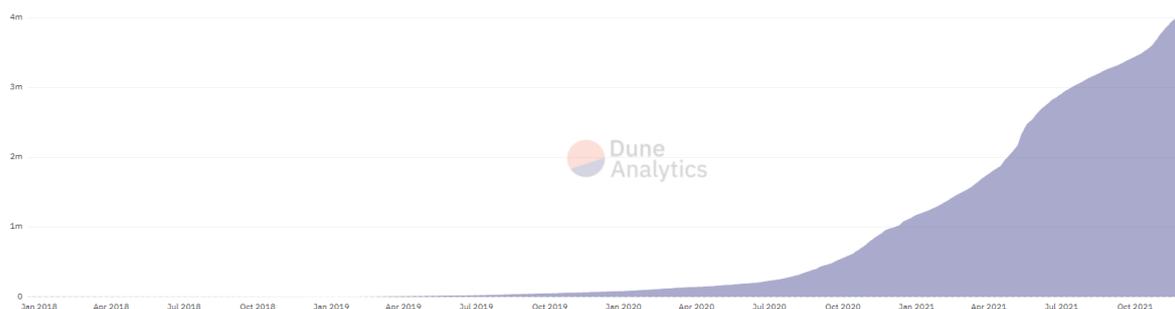
La finance décentralisée n'est plus un sujet de niche au sein de l'écosystème des crypto-actifs. Aujourd'hui capitalisée à hauteur de 112 milliards de dollars¹⁴⁶, la DeFi a vu le nombre de ses utilisateurs croître rapidement. Ainsi, sur la blockchain Ethereum, fer de lance de cette nouvelle finance, elle représente à elle seule quatre millions d'utilisateurs, soit quatre fois plus qu'il y a un an¹⁴⁷.

Si la DeFi n'est finalement encore qu'une goutte d'eau dans l'océan de la finance traditionnelle, elle n'en reste pas moins le principal cas d'usage des crypto-actifs. Dans de nombreux protocoles de DeFi, la valeur sous-jacente du crypto-actif n'est plus l'unique résultante d'une conjonction entre une offre et une demande. En effet, de nombreux protocoles de DeFi produisent des revenus et dépendent aussi de nouveaux produits financiers traditionnels ou innovants disposant d'une vraie logique économique sous-jacente.

¹⁴⁶ DefiLlama - [Total value locked \(USD\) in DeFi](#) - 13.05.2022

¹⁴⁷ Dune Analytics - [Total DeFi users over time](#) - 06.12.2021

Total DeFi users over time
Users = unique addresses. Since a user can have multiple addresses the numbers below are overestimates. Source: @richardchen39



Dune Analytics - Progression du nombre d'utilisateurs DeFi entre janvier 2018 et décembre 2021

La DeFi est apparue dix ans après l'émergence du réseau Bitcoin. Mais l'essor de ce nouveau secteur financier n'est intervenu qu'avec le « *Summer DeFi* ». Cette période, correspondant aux environs de l'été 2020, a vu croître de 700% la capitalisation des protocoles DeFi en seulement trois mois, passant d'un milliard à plus de huit milliards de dollars en termes de capitalisation. Ce *momentum* fut le point de départ d'une course à la liquidité qui alimente encore les développements DeFi et attire de nombreux utilisateurs.

Cette croissance exponentielle est consécutive à la découverte de nouveaux cas d'usage pour les crypto-actifs. Les protocoles DeFi permettent ainsi de faire fructifier, par le biais de mécanismes traditionnels comme le prêt, des crypto-actifs dont le principal intérêt résidait jusqu'alors dans leur valorisation et la spéculation qui en découlait. De cette manière, les investisseurs peuvent prêter leurs *tokens* et percevoir, en contrepartie, une rémunération sous forme, elle aussi, de crypto-actifs.

Plus encore, des nouveaux types de *tokens* sont apparus avec l'émergence de protocoles décentralisés. Si la promesse voulait que le service fourni à l'utilisateur soit décentralisé, il était nécessaire que la gouvernance dudit service le soit également. L'apparition des organisations autonomes décentralisées, traitées ultérieurement dans ce rapport, répondent à cette exigence. Ainsi, de nouveaux *tokens* ont émergé, dont l'objet est de décentraliser la prise de décision, non pas de fournir un service ou d'être utilisé à des fins monétaires. Distincts des *utility tokens* ou des *security tokens*, les *tokens* de gouvernance servent au bon fonctionnement des organisations décentralisées et permettent la prise de décision selon des règles prédéterminées.

La DeFi a également fait apparaître de nouveaux mécanismes financiers rendus possibles par la dématérialisation et l'automatisation permises par la

blockchain, tels que les *flashloans* ou le *yield farming*. L'ensemble de ces nouveaux cas d'usage seront développés ultérieurement.

Depuis l'épisode du « Summer DeFi », la valeur des actifs placés sur les protocoles DeFi a considérablement augmenté. Les sept milliards de dollars de capitalisation ont été multipliés par dix en moins de six mois. Avant le krach du mois de mai 2021, elle avait même atteint la somme record de 170 milliards de dollars. Outre les mécanismes innovants, la DeFi est avant tout portée par le marché des crypto-actifs, lui-même porté par le principal d'entre eux : le bitcoin. En effet, même si la décorrélation interviendra sûrement à terme, le cours de ce dernier a une incidence directe sur le comportement des investisseurs et les placements sur les protocoles DeFi. Toutefois, il convient de noter que la corrélation entre le cours du bitcoin et la capitalisation totale de la DeFi est moindre que celle observée entre le bitcoin et les autres crypto-actifs. Par conséquent, l'attrait des investisseurs pour ces nouveaux cas d'usage devrait se prolonger de manière durable et stable, indépendamment des évolutions du marché à court terme.



Messari (haut) - Évolution du cours du bitcoin en dollars entre décembre 2020 et décembre 2021
DeFiLlama (bas) - Évolution de la capitalisation en dollars des protocoles DeFi entre décembre 2020 et décembre 2021

Cet afflux massif de liquidités au profit de la DeFi a représenté une incitation importante au développement de nouveaux protocoles. Elle a renforcé l'innovation avec l'émergence de nouvelles offres qui répondent soit à des améliorations d'offres existantes, soit à des réponses à certaines problématiques qui ont émergé avec la DeFi. En résulte alors une grande diversité de protocoles qui constituent ce que l'on appelle aujourd'hui la finance décentralisée.

3. Un secteur particulièrement varié et innovant

La finance décentralisée n'aurait pu voir le jour sans le développement de la blockchain et des *smart-contracts*. Elle bénéficie de deux atouts majeurs : l'automatisation et la modularité. Dans la finance traditionnelle, les processus sont souvent longs et coûteux pour faire fonctionner ensemble plusieurs services dont les normes et les standards diffèrent entre eux. La création de ponts entre les infrastructures de différents acteurs financiers et l'intermédiation importante du secteur est un frein à sa scalabilité, sa transparence, son efficacité et surtout à la baisse des coûts pour ses utilisateurs. La DeFi passe outre ces difficultés techniques en imposant un même langage à tous les services : celui de la blockchain.

À sa naissance, la DeFi s'est tout d'abord développée sur la blockchain Ethereum. Grâce à elle, les développeurs sont en capacité, *via* des *smart-contracts* fonctionnant sur ce protocole, de concevoir des ponts automatiques et directs entre les différents services hébergés sur cette blockchain, de les combiner pour faire émerger des offres nouvelles et d'automatiser le fonctionnement de l'ensemble.

a. Les plateformes d'échanges décentralisées

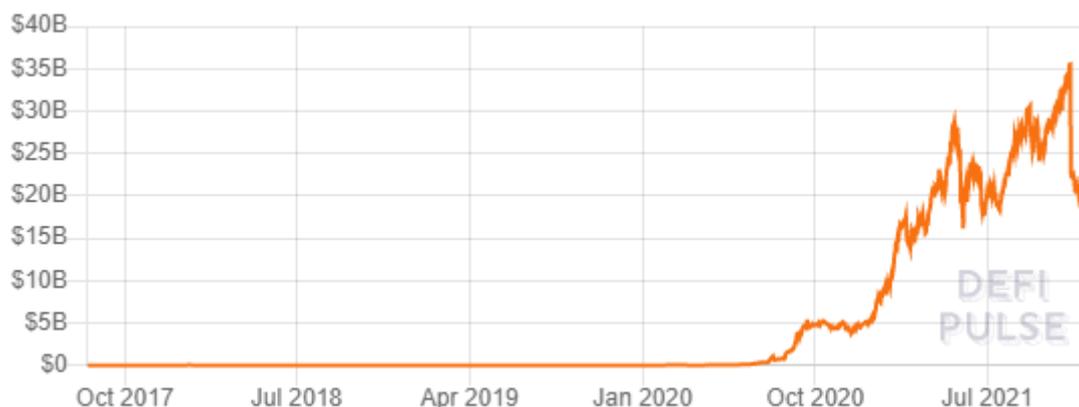
i. Notion de plateforme d'échanges décentralisée

Le monde des crypto-actifs est porté par une ambition de décentralisation ultime. Alors que l'écosystème s'est bâti autour d'acteurs centralisés devenus pour certains des géants, est apparu en parallèle une offre de services décentralisés agréant les différentes fonctionnalités induites par cette nouvelle finance. Afin que la promesse soit complètement tenue, les développeurs devaient répondre aux contraintes techniques de la DeFi. L'apparition des plateformes d'échanges décentralisées (*decentralized exchange* ou « DEX ») est le premier élément de réponse au besoin d'échanger ses crypto-actifs sans intermédiaire. Elles proposent une alternative aux plateformes d'échanges traditionnelles.

Un DEX s'oppose au concept de plateforme d'échanges centralisée (ou *centralized exchange* ou « CEX »). Un DEX est un protocole ayant la vocation d'organiser un marché de pair-à-pair où les transactions se réalisent directement entre les acheteurs et les vendeurs de crypto-actifs. Fonctionnant à partir d'une blockchain, ils offrent la sécurité des échanges tout en excluant le recours à un tiers de confiance.

Les DEX représentent aujourd'hui plus de trente milliards de dollars de capitalisation. Étant les premiers protocoles à avoir émergé, ils ont le plus bénéficié du *Summer DeFi* à l'été 2020, leur capitalisation passant d'une centaine de millions de dollars à plus de cinq milliards en seulement deux mois.

Toutefois, les DEX sont aujourd'hui une partie minoritaire du volume transactionnel induit par les plateformes d'échanges de crypto-actifs. En effet, alors que le volume de transactions journalier de la société Binance est estimé à environ seize milliards de dollars¹⁴⁸, le volume de transactions journalier de l'ensemble des DEX est de l'ordre de cinq milliards de dollars avec, en tête, le protocole Uniswap qui assure à lui seul deux milliards de dollars de transactions par jour¹⁴⁹.



DeFi Pulse - Évolution de la capitalisation en dollars des DEX entre août 2017 et décembre 2021

Fondamentalement, les DEX se distinguent des plateformes d'échanges centralisées par plusieurs aspects. Tout d'abord, elles proposent une variété bien plus importante de *tokens*. De plus, grâce à l'utilisation des *smart-contracts*, les DEX sont autonomes. Ainsi dans le cas des CEX, il est du rôle de la plateforme centralisée que de faire rencontrer l'offre et la demande *via* la tenue d'un carnet d'ordre. Dans le cas des DEX, ces dispositifs sont automatiques. Les revenus générés par le

¹⁴⁸ CoinGecko - [Top Cryptocurrency Exchanges Ranking by Trust Score / Spot](#) - 13.12.2021

¹⁴⁹ CoinGecko - [Top Decentralized Exchanges on CoinGecko by Trading Volume](#) - 13.12.2021

protocole sont majoritairement reversés à l'utilisateur *via* la détention d'un jeton du DEX contrairement aux CEX qui ne répartissent pas le profit.

Cette disparité des DEX entre eux et leurs profondes différences avec les acteurs centralisés entraînent également plusieurs difficultés majeures. D'une part, le caractère décentralisé de ces entités implique qu'il est particulièrement difficile d'y transposer les réglementations aujourd'hui applicables au secteur financier - ce qui n'est d'ailleurs pas souhaitable. En conséquence, aucun superviseur ou aucune autorité publique ne contrôle le bon fonctionnement des protocoles ou encore la licéité des *tokens* admis à l'échange. D'autre part, ces protocoles ne réalisent pas ou peu les diligences qui incombent normalement à un acteur traditionnel de marché. C'est le cas, notamment, pour la cotation de *tokens* dont le projet a été audité et dont le sérieux a été prouvé (contrairement aux nombreux cas de fraude qu'a connu l'écosystème des crypto-actifs dans le passé). Il en est de même pour les diligences en termes de KYC, globalement absentes de la DeFi et qui peut, par conséquent, conduire à l'utilisation de *tokens* dans le cadre d'activités de manipulation de marché, de fraude, de financement de terrorisme ou de blanchiment d'argent.

Si leur utilité est identique, c'est-à-dire fournir un pont unique entre différents *tokens* et différents services de la DeFi, ces dernières années ont pourtant vu l'émergence de plusieurs DEX qui offrent chacun des caractéristiques et des modes de fonctionnement différents.

ii. Fonctionnement

Il convient tout d'abord de noter que la nature décentralisée des DEX a une incidence sur leur mode de fonctionnement. Contrairement aux plateformes centralisées comme Coinbase, Bitpanda ou Coinhouse, les DEX sont nativement numériques et n'ont pas d'existence physique. Par conséquent, ils ne possèdent ni compte bancaire pour accueillir les fonds des clients, ni base de données ou système d'informations outre que la blockchain pour enregistrer les transactions. Cela implique deux choses : (i) les DEX ne permettent pas, à l'écriture de ces lignes, d'échanger des devises ayant cours légal contre des crypto-actifs, ne conservent pas les fonds des clients lors des transactions, mais (ii) enregistrent l'ensemble des transactions qu'ils réalisent directement sur la blockchain.

L'impossibilité d'interagir directement avec ces plateformes en utilisant de l'euro ou du dollar ajoute une couche supplémentaire qui renforce la complexité de

cet écosystème déjà très inaccessible pour la majeure partie de la population. La nécessité de devoir acheter, en amont, des crypto-actifs sur des plateformes d'échanges centralisées puis de les transférer sur un portefeuille propre afin de les utiliser sur des DEX implique un niveau de connaissance et un coût d'entrée important pour la plupart des utilisateurs néophytes. Cette réalité semble être de nature à donner un avantage majeur aux CEX dans la démocratisation des crypto-actifs à court terme.

Toutefois, si cette complexité n'est pas abordable facilement sans une connaissance du secteur, elle implique une sécurité à laquelle les plateformes d'échanges centralisées ne peuvent prétendre qu'à un prix très élevé en matière d'organisation interne et de moyens techniques. Ainsi, l'hébergement des données relatives aux transactions directement sur la blockchain permet une totale transparence ainsi qu'un niveau de sécurité de haut niveau lorsqu'il s'agit de blockchains publiques telles que Ethereum. Plus encore, le fait que les DEX ne conservent pas eux-mêmes les fonds de leurs utilisateurs réduit d'autant la concentration de richesse en un point donné et donc les risques de tentatives de piratage.

Par ailleurs, ces protocoles sont souvent *open source*. Ainsi, la plupart des applications fonctionnent sur des programmes librement accessibles - et reproductibles - par chacun. Ainsi, il est usuel qu'une application DeFi soit copiée et modifiée pour y inclure de nouvelles fonctionnalités. Cela a notamment été le cas avec le code du DEX Uniswap, qui a été copié et modifié pour donner naissance aux DEX Sushiswap et Pancakeswap. Cette transparence totale permise par la blockchain est un atout qui favorise l'innovation et le développement de nouveaux cas d'usage.

De plus, la structure même du fonctionnement de ces plateformes d'échanges décentralisées est impactée par la nature purement numérique de ces nouvelles applications. Ainsi, comme évoqué précédemment, si certaines d'entre elles fonctionnent encore sur des mécanismes similaires aux plateformes d'échanges traditionnelles ou centralisées de crypto-actifs, utilisant des carnets d'ordres, les DEX ont inventé un système reposant uniquement sur des *smart-contracts* et des pools de liquidités : on parle de *Automated Market Makers* (AMM).

En finance traditionnelle, les *markets makers* sont les acteurs privés qui assurent la liquidité d'un ou de plusieurs marchés. Il s'agit communément d'une organisation centralisée qui intervient sur ledit marché en achetant et en vendant

massivement des actifs, tout en se rémunérant sur la différence de prix entre l'achat et la vente. De cette manière, ils assurent le bon fonctionnement du marché en assurant à un acheteur de trouver, à un prix donné, un vendeur - et réciproquement.

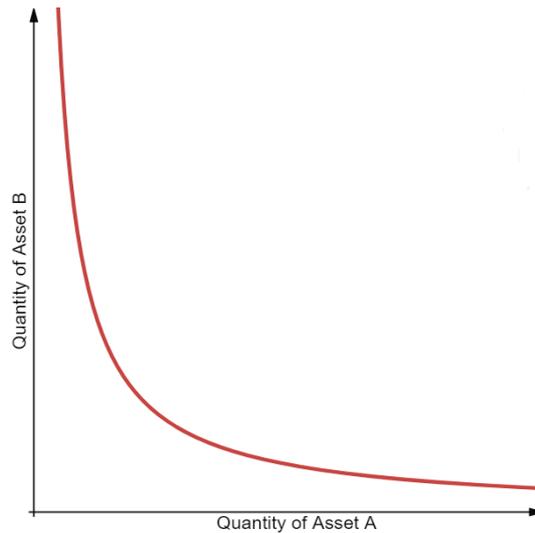
La DeFi a désintermédié cette fonction en introduisant le concept d'AMM. Ceux-ci fonctionnent *via* des pools de liquidités sur la base desquelles des *smart-contracts*, appuyés par des oracles, définissent le taux de change entre deux crypto-actifs. Ainsi, ces pools fonctionnent par paire de crypto-actifs (par exemple une paire bitcoin-ether). Ces paires de liquidités sont alimentées par des apporteurs de liquidité (en anglais, on parle de *liquidity providers*). Ces particuliers ou institutionnels, détenteurs de crypto-actifs souhaitant mettre ces derniers à contribution au sein d'un protocole, sont rémunérés pour le dépôt de leurs liquidités au sein du protocole *via* des frais prélevés au moment de l'échange. Ces frais sont constitutifs d'un revenu versé sous forme de *tokens*. *In fine*, lorsque le fournisseur de liquidités souhaite sortir du pool, il lui suffit de rendre les LP *tokens*¹⁵⁰ qu'il a obtenus en guise de preuve de dépôt afin de retrouver sa mise initiale ainsi que les intérêts.

Ce mécanisme de conversion automatique est lui-même régi par une formule mathématique qui assure l'équilibre entre le prix du premier actif, le prix du second actif et les quantités de ces derniers placées dans les réserves de liquidités. Ainsi, la grande majorité des DEX, tels que Uniswap, fonctionnent sur la base d'une simple équation : $x*y=k$ (où x représente la valeur de l'actif A, y désigne la valeur de l'actif B et k est une constante). Les *smart-contracts* vont alors définir, automatiquement, le taux de change d'équilibre au sein du pool de liquidités en fonction des quantités échangées, du prix auquel elles sont échangées et des quantités restantes dans le pool¹⁵¹.

Dans la mesure où le prix de chaque actif est déterminé selon les pools de liquidités du DEX, il est possible qu'il existe des différences avec le prix de marché déterminé issu des plateformes d'échanges centralisées. Par exemple, lorsque qu'un ou plusieurs investisseurs décident d'acheter, dans un laps de temps restreint, une grande quantité de l'actif A, cela entraînera une chute brutale du prix de l'actif B dans le pool de liquidités. En effet, cela impliquerait un retrait significatif, dans le pool, de l'actif A (dont le prix augmenterait substantiellement) et un apport de même nature de l'actif B (dont le prix chuterait de manière réciproque).

¹⁵⁰ Les *tokens* LP apparaissent alors comme une créance du fournisseur de liquidité sur le protocole.

¹⁵¹ CoinDesk - [What Is an Automated Market Maker?](#) - 20.08.2021



Dmitriy Berenzon - Représentation graphique de l'équation $x*y=k$ ¹⁵²

Ces différences entre prix de marché et prix spécifique au pool de liquidités permettent à certains investisseurs d'arbitrer en acquérant à moindre frais un actif sur un DEX pour finalement le revendre à meilleur prix sur une bourse centralisée, ou vice-versa. Cette stratégie de l'arbitrage doit, en théorie, permettre de rééquilibrer rapidement les pools qui ont récemment subi des variations de volumes importantes, en incitant certains investisseurs à acheter l'actif subissant la décote et donc à en réduire le poids dans la réserve.

Exemple

Hypothèses :

Un protocole permet la conversion entre des bitcoins (actif A) et des ethers (actif B).

Est donc organisé un pool de liquidités présentant la paire bitcoin-ether.

Fonctionnement :

Lorsqu'un utilisateur souhaite obtenir un bitcoin, il va apporter la somme correspondante en ethers au sein d'une pool de liquidités et en retirer ledit bitcoin.

Le pool comportera donc moins de bitcoins mais plus d'ethers.

Le *smart-contract* va alors rééquilibrer la pool (*via* l'équation $x*y=k$) en modifiant le prix de chacun des actifs.

¹⁵² Dmitriy Berenzon (Medium) - [Constant Function Market Makers: DeFi's "Zero to One" Innovation](#) - 23.04.2020

D'une part, la réduction de la quantité de bitcoins dans la pool sera compensée par une augmentation de son prix - la valeur de l'actif A reste donc identique.

D'autre part, l'augmentation de la quantité d'ethers dans la pool sera compensée par une diminution de son prix - la valeur de l'actif B reste donc identique.

Le mécanisme évoqué ci-dessus, dit à fonction constante, est le plus simple mais aussi le plus répandu parmi les différents DEX qui existent aujourd'hui. Il existe toutefois d'autres fonctions mathématiques utilisées afin d'équilibrer les pools de liquidités. Par exemple, la plateforme Balancer¹⁵³ a réussi à faire coexister jusqu'à huit *tokens* différents au sein d'un même pool en réalisant la moyenne géométrique pondérée des réserves de chacun des crypto-actifs considérés. D'autres fonctions, plus élaborées encore, fonctionnent sur la base d'une formule hybride, reprenant plusieurs mécanismes différents¹⁵⁴.

En parallèle du pool de liquidités, les DEX sont également constitués autour d'une entité autonome décentralisée. Ces dernières ont la responsabilité d'assurer la gouvernance du protocole et décident, notamment, d'engager des spécialistes pour auditer le code du protocole pour en garantir la sécurité ou de modifier les frais de transaction prélevés sur chaque transaction. Pour composer cette DAO, les protocoles émettent des jetons de gouvernance, qui sont attribués selon certains critères (par exemple : être un fournisseur de liquidités). Le présent rapport traite plus précisément sur la question des DAO ultérieurement.

b. Les protocoles de prêt décentralisés

i. *Notion de protocole de prêt décentralisé*

Les protocoles de prêt (en anglais, on parle de *lending*) sont certainement le cas d'usage le plus abouti de la finance décentralisée, dans la mesure où ils permettent de faire travailler des *tokens* qui, jusqu'alors, n'avaient pas d'autre intérêt que leur valorisation.

¹⁵³ Balancer - [Balancer Pools](#)

¹⁵⁴ Exemple : [Mécanisme d'équilibre de Shell Protocol](#)

Aujourd'hui capitalisés à plus de cinquante milliards de dollars, les protocoles de prêt ont connu une augmentation de plus de 130% au cours de l'année 2021, principalement portés par les protocoles Maker et son stablecoin DAI, Aave et Compound.



DeFi Pulse - Évolution de la valeur totale hébergée sur les protocoles de prêt en 2021

Les protocoles de prêt représentent une réelle révolution. En effet, la décentralisation permet de faire aujourd'hui des choses impossibles jusqu'alors dans la finance traditionnelle. D'une part, elle désintermédie, comme cela est évoqué dans les prochains développements. D'autre part, elle automatise et simplifie l'ensemble des processus.

En effet, elle automatise chacune des opérations (du dépôt à l'emprunt en passant par le versement d'intérêts), ce qui permet des gains de temps et des réductions de coûts non négligeables. Elle automatise également la détermination des taux d'intérêt pour qu'ils représentent fidèlement l'état du marché à l'instant T. Par ailleurs, on constate que les taux présentés par les protocoles de prêts sont nettement supérieurs aux taux pratiqués dans la finance traditionnelle. Cet état de fait résulte en effet de l'efficacité économique de ces protocoles par rapport aux systèmes bancaires et financiers traditionnels ainsi que de la demande croissante de liquidités sur ces nouveaux marchés.

La décentralisation est également source de simplification. D'une part, elle offre une transparence qui n'est pas possible aujourd'hui en raison de l'opacité et de la fragmentation du secteur financier traditionnel. Cette transparence, déployée à grande échelle, représente un véritable atout, en ce qu'elle permet un meilleur contrôle par la société des activités de ce secteur systémique mais aussi une meilleure vision des décideurs économiques et politiques sur l'état de l'économie. Dans une période d'incertitude aussi grande, où la BCE, notamment, doit prendre des

décisions qui marqueront aussi bien l'avenir des produits d'épargne que les budgets des États membres, la blockchain serait une alliée utile au service du bien commun. D'autre part, outre les considérations macroéconomiques, la décentralisation permet également de garantir un juste accès à cette nouvelle finance. Dans la mesure où l'unique condition est l'accès à internet, cela permettrait d'éradiquer toutes les discriminations liées notamment à l'origine, au genre, à la religion et d'inclure des populations qui ne peuvent pas accéder à de tels services dans la finance traditionnelle.

Néanmoins, si la décentralisation des emprunts et des prêts représente une révolution majeure, elle induit également des risques qu'il est important de ne pas négliger, en raison du manque de maturité de cet écosystème.

Le premier risque majeur est celui inhérent à tout mécanisme fonctionnant à partir de crypto-actifs : le risque de volatilité. En effet, cette volatilité a deux conséquences structurelles : la première impacte les taux d'intérêts offerts par les protocoles, la seconde concerne les garanties déposées par les emprunteurs.

Dans le premier cas, et comme cela a été évoqué, les *smart-contracts* procèdent à la détermination automatique des taux d'intérêt selon les conditions de marché. Dans l'hypothèse où le marché subit de fortes baisses, cela entraînera une contraction équivalente des taux d'intérêt et réciproquement. Or, eu égard à la corrélation entre la DeFi et le cours du bitcoin, cette instabilité se répercute directement sur les positions des déposants et des emprunteurs. Ces derniers souffrent également de cette volatilité lorsqu'ils placent des crypto-actifs volatiles en garantie de leurs emprunts (comme cela est évoqué ultérieurement).

Le second risque majeur est celui relatif à la sécurité du protocole, face aux anomalies dans le code et aux piratages. Ces exemples ont été nombreux. Des protocoles dont le niveau de sécurité n'était pas suffisant ont subi des attaques visant à voler des fonds sous forme de crypto-actifs. Or, dans la mesure où les protocoles de prêts sont basés sur des pools de liquidités regroupant plusieurs millions voire plusieurs milliards de dollars, ils représentent des cibles privilégiées pour des pirates informatiques. Ces attaques sont, le plus souvent, le résultat d'une faille des protocoles, insuffisamment audités et testés. La sécurité représente donc l'enjeu essentiel du développement et de l'essor de ces protocoles à de plus grandes échelles.

Avec le succès planétaire du *lending*, les services de prêt sur crypto-actifs ont également attiré l'attention des plateformes d'échanges centralisées, qui y voient la suite logique du développement de leur activité. Néanmoins, partant d'une entité centralisée, ces services de prêt fonctionnent dans des conditions assez similaires aux prêts fournis par des banques traditionnelles. En effet, l'exécution des prêts et la conservation des actifs sont directement assurées par la plateforme, selon des conditions prédéfinies par elle (par conséquent moins flexibles que celles déterminées par les protocoles décentralisés).

ii. *Fonctionnement*

Fondamentalement, les protocoles de prêt décentralisés ressemblent trait pour trait aux services qui peuvent être fournis par des établissements bancaires. Néanmoins, la décentralisation, ici encore, en modifie les contours grâce à leur désintermédiation.

La décentralisation a permis de remplacer les intermédiaires financiers par des *smart-contracts* chargés de la bonne exécution des opérations. Dans la finance traditionnelle, cette fonction était assurée par un tiers de confiance (généralement une banque commerciale) chargé d'assurer le dépôt des fonds de clients, leur conservation et leur circulation (par l'intermédiaire des prêts notamment). Dans la finance décentralisée, toutes ces opérations sont automatisées.

Chaque utilisateur d'un protocole DeFi peut connecter son portefeuille directement au protocole, *via* la blockchain, et déposer ses fonds au sein d'un pool de liquidités. À partir de cette réserve, le protocole pourra octroyer des prêts à des demandeurs, si et seulement si ces derniers disposent d'une garantie suffisante pour assurer le remboursement de leur prêt. En effet, afin d'assurer la confiance des utilisateurs dans le protocole, un système de garantie est mis en place et contraint les demandeurs de prêt à bloquer une certaine somme (on parle de collatéral) dans le protocole, qui sera liquidée lorsque sa valeur sera inférieure à un certain seuil. Le collatéral, déterminé par le protocole, doit généralement être d'une valeur supérieure à la dette contractée, de manière à garantir l'équilibre du système. En raison de la forte volatilité des cours des crypto-actifs, il peut arriver que la valeur empruntée devienne supérieure à la valeur déposée en garantie. Dans ce cas de figure, l'emprunteur n'a plus intérêt à rembourser son prêt et en résulte une perte de valeur pour le protocole. Afin de compenser ces effets, le protocole est programmé de manière à demander un collatéral d'une valeur supérieure à la valeur empruntée. On parle alors de sur-collatéralisation.

Par ailleurs, la confiance que les utilisateurs placent dans le protocole ne dépend pas seulement de la garantie apportée par l'emprunteur, mais aussi dans la certitude que celle-ci n'échappera pas à la collectivité des déposants. Ici encore, les *smart-contracts* jouent un rôle prépondérant pour l'équilibre du système. En accordant le prêt et en bloquant concomitamment le collatéral dans le protocole, et en liquidant celui-ci lorsque sa valeur diminue sous un certain seuil, les prêteurs - c'est-à-dire ceux qui fournissent la liquidité - sont assurés de ne pas perdre leurs fonds dans l'opération.

Le processus de liquidation, quant à lui, procède selon la même logique au sein des principaux protocoles de prêt de l'écosystème DeFi, bien que quelques différences doivent être notées. D'une manière générale, il repose sur un système d'équilibre entre le niveau de dette contractée et le niveau de collatéral déposé auprès du protocole. Ce niveau d'équilibre correspond à un certain seuil en deçà duquel le collatéral est liquidé, comme c'est le cas pour le DAI de MakerDAO. Si, dans ce dernier protocole, le collatéral est liquidé *via* une mise aux enchères, ce n'est toutefois pas le cas de tous les protocoles. Par exemple, qu'il s'agisse de Compound ou de Aave, la liquidation ne porte que sur la moitié seulement de la dette et n'est pas soumise à une enchère mais librement saisie par n'importe quel liquidateur. Ce dernier va alors payer le montant du collatéral liquidé et percevra en contrepartie le collatéral liquidé augmenté d'une pénalité de liquidation prélevée directement sur le collatéral.

Cette liquidation reposant sur un ratio collatéral/dette est ainsi de nature à assurer l'équilibre entre l'offre et la demande de liquidités sur le marché, mais elle permet aussi d'écarter tout risque de surendettement qui pourrait peser sur un utilisateur. En effet, ce dernier ne pourra jamais emprunter plus que ce qu'il possède, en raison de la surcollatéralisation.

En parallèle, les déposants sont rémunérés comme s'ils déposaient leurs fonds sur un produit d'épargne traditionnel. Lorsqu'ils déposent des crypto-actifs, ces derniers quittent leurs portefeuilles personnels afin de rejoindre le pool de liquidités du protocole. En contrepartie, ils reçoivent un titre de créance, sous forme de *tokens* dérivés¹⁵⁵, sur le protocole. Les intérêts, qui peuvent être fixes ou variables et toujours déterminés par le marché, sont ainsi ajoutés régulièrement au portefeuille

¹⁵⁵ Un *token* dérivé est un *token* représentant la créance de l'utilisateur sur le protocole.

Exemple : lorsqu'un utilisateur souhaite déposer des DAI sur le protocole Aave, il recevra en contrepartie des aDAI, correspondant à sa créance.

de l'utilisateur sous forme de *tokens* dérivés identiques à ceux reçus lors du dépôt. Dans certains cas, les déposants reçoivent également des *tokens* de gouvernance.

En parallèle des prêts traditionnels permis par ces protocoles, ont émergé des prêts éclair (en anglais, on parle de *flashloans*), qui sont rendus possibles uniquement par la dématérialisation et l'automatisation de la blockchain.

Un prêt éclair ou *flashloan* est un emprunt instantané sans risque de contrepartie, qui ne demande aucune garantie, à condition d'être remboursé dans une seule et même transaction sur Ethereum¹⁵⁶. Ainsi, l'investisseur peut se servir de cette nouvelle technique d'ingénierie financière afin de bénéficier d'opportunités d'arbitrage sur une période très courte et empocher des gains sans mobiliser de capital.

Si ces nouveaux types de prêts permettent d'exploiter au mieux les différences de prix qui peuvent exister sur le marché, ils peuvent également servir à déstabiliser des protocoles entiers par la brutalité du choc qu'ils entraînent. Notamment, cette technique a été utilisée en 2020 pour influencer un vote concernant la gouvernance de MakerDAO. En effet, une des personnes intéressées au vote a utilisé un *flashloan* pour acquérir une grande quantité de *tokens* de gouvernance de MakerDAO, afin d'influer sur le vote qui devait, à l'origine, lui être défavorable¹⁵⁷.

Encore une fois, ce cas est la représentation parfaite qu'une technologie n'est pas, en elle-même, bienveillante ou malveillante mais qu'elle peut être détournée de son objectif initial par celui ou celle qui la contrôle ou qui abuse de ses failles. D'autres exemples de ce type, ayant notamment entraîné des préjudices financiers, sont déjà intervenus sur différents protocoles. C'est le cas notamment de la récente chute du *stablecoin* algorithmique UST suite à une attaque financière. Le manque de résilience et de maturité des outils de la DeFi et le fait que les concepteurs de ces protocoles n'aient pas toujours imaginé les failles rendent les protocoles DeFi vulnérables. Ainsi dans le cas de l'UST, l'absence de régulation n'a pas permis de protéger le protocole attaqué des mêmes garanties prévues au titre de la finance traditionnelle. Aussi, s'il faut évidemment condamner de tels usages, la question qui se pose réellement est celle de la sécurité et de la vulnérabilité des protocoles face à ces attaques.

¹⁵⁶ Cryptoast - [Qu'est-ce qu'un flash loan ? Un mal nécessaire](#) - 21.11.2020

¹⁵⁷ Bitcoin.com - [Uncollateralized Power: A Makerdao Governance Vote Was Swayed by a Defi Flash Loan](#) - 02.11.2020

c. L'optimisation automatisée des rendements

Avec le développement de la finance décentralisée, une nouvelle activité est apparue quand ont émergé de nouveaux services financiers décentralisés. Présentée au sein de l'écosystème comme de l'agriculture de rendements (en anglais, on parle de *yield farming*), cette pratique vise à générer des revenus, *via* le versement d'intérêts en capital, en exploitant l'ensemble des briques de la DeFi et en les faisant fonctionner ensemble.

L'objectif est simple : investir ses crypto-actifs de manière à bénéficier des meilleurs rendements offerts par les différentes applications DeFi. Plusieurs techniques sont possibles et reposent principalement sur des arbitrages entre les différentes offres de rendement de chaque protocole. Ainsi, l'investisseur souhaitant optimiser ses rendements va comparer les intérêts perçus sur les différents protocoles, qu'il s'agisse des protocoles de prêt décentralisés ou des DEX.

Sur la base de ces applications précédemment étudiées, se sont développés de nouveaux services d'optimisation automatisés des rendements de DeFi. Le plus connu, Yearn finance, est une application de finance décentralisée qui, à l'aide de *smart-contracts*, compare les rendements des autres protocoles de DeFi et permet à son utilisateur de maximiser ses gains pour un capital donné. Yearn finance a notamment développé un produit appelé *vault* (en français, on parle de coffre-fort). Comme son nom l'indique, il s'agit d'une réserve dans laquelle les investisseurs vont placer leurs fonds sous forme de crypto-actifs (notamment, des *stablecoins*). Ces derniers vont alors être gérés par des *smart-contracts*, de manière automatique, afin d'optimiser les gains qu'il est possible d'en retirer. Par exemple, le *smart-contract* place les *tokens* dans un pool de liquidités de Curve et en retire des intérêts, les récompenses liées aux transactions *via* Curve ainsi que des *tokens* de gouvernance¹⁵⁸. Outre l'optimisation des rendements, ce nouveau service permet également à ses utilisateurs d'économiser les frais de transactions (notamment ceux du réseau Ethereum devenus exorbitants) et de simplifier les changements de stratégie, qui sont gérés automatiquement par les *smart-contracts*. Néanmoins, ces mouvements de fonds réguliers, visant à optimiser les rendements, présentent un risque accru de volatilité. En effet, il est fréquent, dans l'écosystème des crypto-actifs, que les rendements les plus élevés soient offerts par les projets les plus

¹⁵⁸ Pour aller plus loin : Yearn finance - [The Vaults at Yearn](#) - 05.11.2021

risqués. Cela n'est pas sans conséquence sur le risque de pertes des fonds qui y sont placés automatiquement par Yearn finance.

En parallèle, il est également possible, à condition d'avoir une connaissance suffisamment poussée du secteur, de combiner les rendements offerts par les différentes applications de finance décentralisée. Certains investisseurs peuvent, par exemple, apporter des fonds à un pool de liquidité d'un DEX. En contrepartie, ils seront rémunérés par des intérêts et des *tokens* de gouvernance. Ils peuvent alors utiliser ces *tokens* obtenus pour les déposer dans des protocoles de prêt, pour en retirer davantage de gains tirés des taux d'intérêts. En effet, les *tokens* de gouvernance sont recherchés par certains pour leur valeur (représentant la valeur du protocole aux yeux de l'écosystème, à l'image d'une action d'une entreprise traditionnelle) ou pour les droits qu'ils confèrent dans la gouvernance de ce même protocole. Ils sont donc intéressés à payer des intérêts pour en disposer, ce qui rémunère l'investisseur qui les met à disposition.

d. Les actifs synthétiques

Les actifs synthétiques sont des dérivés tokénisés d'autres actifs traditionnels. Ils permettent ainsi de reproduire, dans le monde numérique, des actifs qui existent dans le monde traditionnel. Leur intérêt est indéniable, en ce qu'ils permettent de numériser la finance traditionnelle portant sur des actifs tangibles. Ils ont la vertu de rendre interopérable ces actifs dans l'environnement DeFi et donc d'y apporter les avantages de la blockchain.

En cela, ils ressemblent globalement aux différents dérivés existant déjà sur les marchés traditionnels, tels que les contrats à termes. Ils reflètent alors, dans l'écosystème des crypto-actifs, les performances des actions, devises et matières premières.

L'avancée la plus notable, en matière d'actifs synthétiques, découle de la tokenisation des actifs immobiliers. De toutes les classes d'actifs qui existent, ces derniers sont certainement les actifs les moins liquides. La tokenisation de ces actifs, qui sont difficilement échangeables par leur nature et leur réglementation, permet de simplifier et d'améliorer la valorisation et l'échange des biens immobiliers.

D'une part, la tokenisation permet de fragmenter un bien immobilier en une multitude de *tokens* représentant chacun une part du bien. Ainsi, un immeuble qui, traditionnellement, se vend d'une manière indivisible ou par lot, pourra être fragmenté en autant de *tokens* que souhaité, afin de le rendre davantage liquide. En

procédant de la sorte, les différents *tokens* auront *de facto* les mêmes droits (notamment pour la perception des loyers). Ainsi, la tokenisation permettra de démocratiser l'investissement immobilier au profit de certaines catégories de la population qui en sont aujourd'hui exclues, mais permettra aussi à terme d'assouplir les conditions de la propriété immobilière et rendre les biens plus liquides. Sur cette question, la start-up française Equisafe a développé, en 2020, une offre de *tokens* représentant les parts d'une société civile de placement immobilier (SCPI). Cette technique permet de reproduire les résultats de la société dans la sphère des crypto-actifs.

D'autre part, la tokenisation simplifie les transactions immobilières. En effet, si un immeuble est représenté, dans la blockchain, par une multitude de *tokens*, ces derniers pourront passer de main en main sans que cela ne pose de problématique quant à sa gestion. Par ailleurs, la question de la traçabilité de la propriété immobilière est écartée *de facto* par la technologie, du fait de ses caractéristiques intrinsèques notamment sa transparence et son inviolabilité. Il est aisément envisageable que dans le futur, par l'intermédiaire des *smart-contracts*, les loyers soient directement perçus par les différents propriétaires de *tokens* et que la part relative à l'impôt soit versée automatiquement au Trésor public. D'une manière générale, la tokenisation du foncier permettra de fluidifier les transactions immobilières, d'en simplifier la réalisation et par conséquent d'en réduire les coûts tout en augmentant la liquidité des biens immobiliers.

Par ailleurs, le développement de cette nouvelle catégorie d'actifs a incité l'émergence d'actifs synthétiques basés sur des actifs crypto-natifs.

Sont apparus les *wrapped coins*, c'est-à-dire des *tokens* représentant d'autres *tokens* fonctionnant sur une blockchain différente. Le plus connu d'entre eux est le WBTC, pour Wrapped bitcoin. L'objectif de ce dernier est simple : rendre les bitcoins (*tokens* hébergés sur le réseau Bitcoin) compatibles avec des *tokens* basés sur la norme ERC-20 et hébergés sur le réseau Ethereum. Ce nouveau *token*, qui est un dérivé de bitcoin, fonctionne dans une logique similaire à un *stablecoin*. La règle qui régit son émission impose une parité stricte entre les *tokens* dérivés et les *tokens* sous-jacents. Ainsi, un WBTC ne peut être émis que lorsqu'un bitcoin est collatéralisé. De la même manière, le cours du WBTC reproduit (quasi) fidèlement le cours du bitcoin, afin d'exporter la valeur qu'il représente dans les réseaux dans lesquels il n'est pas compatible. Par ailleurs, l'émetteur des WBTC assure une parfaite transparence des bitcoins tenus en réserve afin d'apporter la preuve de la

parité, donc des *tokens* émis. Là encore, la transparence de la blockchain est un atout majeur pour préserver la crédibilité du système, en justifiant à chaque instant des *tokens* émis lors de la réception des bitcoins et des *tokens* brûlés lors de leur restitution.

En parallèle, d'autres actifs synthétiques ont émergé, reproduisant notamment la puissance de calcul nécessaire à la validation de blocs de blockchain reposant sur la preuve de travail. Il existe ainsi des *tokens* qui représentent des machines de minage et dont la valeur reproduit le rendement de ladite machine. Alors que le minage de crypto-actifs est une activité particulièrement difficile et volatile, ces nouveaux outils permettent ainsi d'en ouvrir les portes à des non-spécialistes disposant de capitaux.

e. L'assurance décentralisée

Comparée à d'autres secteurs économiques émergents, la DeFi est caractérisée par une forte progression capitaliste sur un court laps de temps. L'attrait des capitaux vers ce nouveau secteur, s'il est louable en ce qu'il permet à l'écosystème de se développer, a eu un effet pervers. Victime de son succès, la DeFi a attiré des convoitises parfois malveillantes.

Résultant de *smart-contracts* peu voire pas audités, plusieurs problèmes techniques sont rapidement apparus sur différentes applications DeFi. Ces difficultés relevaient de failles dans le code des *smart-contracts*. L'un des derniers exemples en date est la mise à niveau du protocole de Compound qui, en raison d'une faille dans le code, a conduit à la distribution involontaire de plus de 90 millions de dollars du *tokens* de gouvernance du protocole. Ce type de problème technique, résultant d'un manque de rigueur dans le développement et la vérification de la mise à niveau, peuvent avoir de graves effets sur l'écosystème du protocole en question, et sur la DeFi dans son ensemble. Dans le cas de Compound, cela a eu un effet sensible sur le cours du *token* de gouvernance, mais également sur l'équilibre du rapport de force au sein de la DAO (280.000 *tokens* de gouvernance avaient alors été distribués), donc sur l'équilibre du protocole dans son ensemble. Cette situation est d'autant plus embarrassante dans la mesure où, s'agissant d'un protocole opérant sur une blockchain publique - ici Ethereum - il n'est pas possible de procéder à un rappel de fonds. En effet, les transactions sont inscrites dans les blocs ajoutés à la blockchain, et il n'est pas possible de défaire ces blocs sans « attaquer » la blockchain en contrôlant la majorité des validateurs de blocs. La seule solution était alors de faire

appel au « civisme » des bénéficiaires de cette faille pour qu'ils restituent les fonds obtenus¹⁵⁹.

Au-delà de ces anomalies, il existe également d'autres failles qui, une fois détectées, sont exploitées afin de subtiliser des crypto-actifs des protocoles au détriment d'autres investisseurs. Ces attaques informatiques sont en réalité peu fréquentes dans l'écosystème, mais elles sont fortement médiatisées en raison des montants qui sont dérobés par les pirates. En août 2021, a eu lieu l'attaque informatique la plus lucrative, mais aussi la plus insolite, de l'histoire de la DeFi. Le 10 août, le protocole Poly Network (dont l'objet consiste à assurer l'interopérabilité entre différentes blockchains) a été la cible d'une attaque ayant conduit au vol de plus de 600 millions de dollars de crypto-actifs, répartis entre différentes blockchains¹⁶⁰. Toutefois, des spécialistes en cryptographie ont pu remonter les traces - numériques - du voleur et ont réussi à établir un contact avec ce dernier. Deux jours plus tard, le pirate informatique avait restitué les fonds à Polygon Network, en refusant de conserver une partie comme négocié avec Poly Network (le voleur ayant déclaré qu'il n'avait jamais eu l'intention de garder l'argent, prétextant être un *white hat*, un hacker dont l'unique objectif est de révéler les brèches dans un système informatique).

Si cette affaire s'est finalement soldée par une restitution des fonds, cela n'en reste pas moins exceptionnel. Dans la plupart des cas, les victimes ne retrouvent jamais les fonds qu'elles ont perdu et aucune réglementation ni aucun mécanisme ne permet aujourd'hui cette indemnisation. Pour répondre à cette difficulté majeure, certains protocoles mettent en place des réserves qui seraient mobilisables pour indemniser en cas de faille ou d'attaque du protocole. Néanmoins, à grande échelle, cette pratique n'est pas satisfaisante pour assurer la sécurité des placements de l'ensemble des utilisateurs de la DeFi.

Dans le même temps, des applications d'assurance décentralisée ont émergé. L'objectif est ainsi de protéger les souscripteurs qui utilisent la DeFi contre les pertes résultant d'une faille informatique ou d'un piratage. Le plus connu d'entre eux est Nexus Mutual, une assurance décentralisée qui offre une protection contre les défaillances des *smart-contracts* et contre les piratages de DEX.

Nexus Mutual fournit différentes couvertures permettant à ses utilisateurs d'assurer leurs *tokens*, notamment contre : (i) la défaillance ou le piratage d'un

¹⁵⁹ CNBC - [DeFi bug accidentally gives \\$90 million to users, founder begs them to return it](#) - 01.10.2021

¹⁶⁰ Cryptoast - [Le pirate de Poly Network rend les fonds volés et refuse une prime de 500 000\\$](#) - 13.08.2021

protocole, ou (ii) le piratage ou le verrouillage de *tokens* placés en conservation auprès d'un tiers. Ainsi, ce protocole fonctionne sur la base d'un pool de liquidités qui garantit la valeur des polices d'assurance achetées par les utilisateurs.

Concrètement, si un utilisateur veut se couvrir contre un risque de perte de ses *tokens* sur un protocole en particulier, il peut acquérir une police d'assurance auprès de Nexus Mutual. Le protocole réalise alors une évaluation du risque - par des auditeurs - pour estimer les besoins nécessaires pour financer ladite couverture. Ce financement sera comblé, pour la majorité, par des apporteurs de liquidités ; s'agissant du reste, il est financé par les demandeurs d'assurance eux-mêmes lors de l'achat d'une couverture.

L'ensemble du système fonctionne sur la base d'un *token* unifié et spécifique au protocole : le *Nexus Mutual token* (appelé NXM). Le rôle du NXM est central, puisque c'est avec ce jeton qu'est constitué le pool de liquidités, que sont rémunérés les auditeurs et les apporteurs de liquidités. Le prix de ce *token*, qui n'est disponible que sur la plateforme de Nexus Mutual, est déterminé en fonction du besoin de financement du protocole, afin de garantir l'ensemble des risques qui sont couverts par celui-ci.

Aussi, l'assurance décentralisée repose sur un subtil équilibre entre les liquidités apportées, le nombre de couvertures fournies et les incitations liées au jeton en lui-même.

S'agissant de la mise en œuvre de cette assurance, plusieurs points sont à noter. Lors de l'achat d'une police d'assurance par un utilisateur, les apporteurs de liquidités et les auditeurs perçoivent une récompense équivalente à 50% du prix de la police, répartie proportionnellement et payée en NXM. Ensuite, lorsque le risque se réalise, l'assuré doit émettre une réclamation, prouvant la réalité de son préjudice. Cette réclamation donne lieu à une décision des membres qui participent au pool et qui évaluent le bien-fondé de la réclamation. Lorsque la réclamation aboutit, l'assuré reçoit un paiement correspondant à sa couverture. Dans ce cas de figure, les *tokens* qui ont été placés dans le pool par les apporteurs de liquidités sont perdus par ces derniers. Alors, si l'aboutissement d'une réclamation entraîne une perte pour les apporteurs de liquidités, ils n'ont toutefois pas vocation à empêcher toutes les réclamations d'aboutir. En effet, ce comportement aurait deux conséquences : d'une part, elle conduirait à un vote frauduleux, ce qui est réprimé par le protocole en supprimant les *tokens* placés dans le pool ; d'autre part, cela détruirait la confiance

que les utilisateurs placent dans le protocole, et donc serait une perte bien plus importante encore pour l'apporteur de liquidités.

f. Les protocoles d'infrastructure de données

La DeFi n'est pas seulement une succession d'applications purement financières. Ces dernières sont aussi accompagnées d'autres protocoles qui répondent à un besoin davantage structurel et qui ont vocation à organiser le transfert de données du monde physique - traditionnel - vers le monde virtuel, celui de la blockchain : ce sont les oracles. En parallèle, il devient également possible de se tourner vers des réseaux décentralisés pour y stocker une quantité importante de données, sans risque de perte ou de contrôle de ces dernières par une entité tierce.

i. Les oracles, passerelle entre le monde physique et le monde virtuel

Un « oracle » est une source d'informations qui permet d'intégrer des variables issues du monde réel dans des *smart-contracts*¹⁶¹. En agissant comme un pont entre le monde physique et le monde virtuel, il permet aux données extérieures à la blockchain (dites « *off chain* ») d'être prises en compte dans l'automatisation des processus permise par les *smart-contracts*. En effet, ces derniers, par nature, ne peuvent intégrer dans leurs programmes que des données issues de la blockchain (dites « *on chain* »), nativement numériques, résultant des différentes transactions entre utilisateurs.

Le développement de ces oracles est une étape importante dans le développement de l'écosystème des crypto-actifs dans son ensemble, et en particulier de la finance décentralisée. Les oracles représentent la première pierre du pont reliant monde physique et monde virtuel, indispensable à ce dernier pour pouvoir se développer et ne pas fonctionner en vase clos. Il existe plusieurs protocoles de ce type, les plus connus étant Chainlink ou encore Band Protocol. Afin de décrire clairement le fonctionnement de ces applications, le présent rapport prend l'exemple du fonctionnement du protocole Chainlink.

¹⁶¹ Cryptoast - [Qu'est-ce qu'un Oracle ? Blockchain et monde réel](#) - 05.09.2018

Chainlink est le premier projet d'oracle à avoir vu le jour. Il est aujourd'hui le plus connu et est notamment utilisé par de nombreuses applications de finance décentralisée déjà évoquées, telles que Aave ou Compound.

Il s'agit d'un oracle décentralisé. En procédant de manière distribuée, la collecte d'informations par le protocole ne repose pas sur les mêmes entités centralisées, qui peuvent être soumises à des pressions de toute nature ou à des défaillances. Le mécanisme privilégie la diversité des sources¹⁶².

Le service de transfert de données du monde physique vers le monde virtuel est composé de deux infrastructures distinctes : (i) une première qui agit *off chain*, c'est-à-dire qui n'est pas directement intégrée à la blockchain et (ii) une seconde qui agit *on chain*, c'est-à-dire qui est connectée à la blockchain et qui échange directement avec les *smart-contracts*.

La structure *off chain* est constituée d'un réseau de nœuds qui a vocation à collecter les données du monde physique, avant de les transmettre à la structure *on chain*. Chaque nœud d'oracle (*oracle node*) correspond en réalité à une personne ou entité qui se met à disposition afin de collecter et transmettre l'information demandée par l'utilisateur du protocole oracle. L'ensemble de ces nœuds est connecté à un nœud central (dans le cas de Chainlink, il s'agit du *Chainlink Core*) qui est chargé de traduire ces données pour que ces dernières soient compréhensibles par la blockchain avant de les lui transmettre.

La structure *on chain* se matérialise elle par un *smart-contract* spécifique - un *oracle contract*. Il traitera les demandes d'informations des utilisateurs et les transmettra aux oracles chargés de collecter l'information dans la structure *off chain*. Cet *oracle contract* est lui-même un assemblage d'autres *smart-contracts* qui ont chacun un objectif spécifique, comme vérifier l'intégrité de l'oracle qui a collecté l'information ou encore déterminer le prix de l'opération.

L'ensemble des deux structures fonctionne ainsi en deux, voire trois, étapes distinctes : (i) l'utilisateur formule sa requête et détermine certains paramètres afin de la préciser, (ii) la requête est transmise aux nœuds d'oracle, qui se chargent de collecter l'information demandée, (iii) les informations collectées par les nœuds d'oracle sont transmises à l'utilisateur qui choisit alors celle qui lui convient. Lorsque ces dernières sont différentes les unes des autres, le protocole fournit une réponse complexe, précisant chacune des informations obtenues en les pondérant

¹⁶² Cryptoast - [Qu'est-ce que le ChainLink \(LINK\) ?](#) - 16.04.2021

selon le nombre d'occurrences, mais aussi en fonction de la réputation des oracles ayant répondu.

Afin d'assurer une parfaite fiabilité du protocole, les oracles sont soumis à un système de notation, qui s'apparente à une réputation. Cette réputation est l'agrégat de l'ensemble des notes que reçoivent les oracles lorsqu'ils répondent à la requête d'un utilisateur. Si la réponse fournie n'est pas la bonne, l'utilisateur peut sanctionner l'oracle en lui attribuant une mauvaise note, qui sera visible de tous. Ce système de notation est particulièrement important puisqu'il est lié au système de rémunération.

L'ensemble du protocole fonctionne autour d'un *token ad hoc* : le LINK. Ce *token* est nécessaire, pour les utilisateurs, afin de régler les frais liés à l'opération qu'ils demandent. Ainsi, les LINK payés en contrepartie de la prestation de collecte d'informations sont distribués, notamment aux oracles qui effectuent l'opération. Or, si l'un d'eux ne bénéficie pas d'une bonne réputation, il ne sera jamais choisi par les utilisateurs et son activité ne produira donc aucun revenu. Une fois encore, la transparence de la blockchain se met au service de l'efficacité du protocole.

ii. *Le stockage décentralisé, outil de démocratisation des données*

Avec l'essor de la société numérique, accentué avec la pandémie de la Covid-19, la question des données devient de plus en plus cruciale pour la souveraineté des États. L'Europe en a pris conscience et a notamment adopté le RGPD¹⁶³ afin de protéger les données personnelles des européens. Mais, au-delà de la question de la vie privée des citoyens, la question de la protection des données revêt un fort enjeu de stratégie économique et industrielle. Or, aujourd'hui, l'essentiel des sociétés qui assurent le stockage et la conservation des données sont étrangères, le plus souvent américaines. En tête, Amazon et Google qui sont devenues des méga-corporations dont l'influence égale celle de certains États, avec le risque d'arbitraire que cela implique.

Conforme à sa volonté de décentraliser l'économie et la société en général, l'écosystème de la blockchain a vu émerger des solutions de stockage de données distribuées, en concurrence des solutions traditionnelles centralisées.

¹⁶³ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Différents réseaux ont émergé, comme Storj ou Arweave. Néanmoins, le plus connu d'entre eux est le réseau de stockage Filecoin, dont le projet vise à créer une place de marché du stockage distribué. L'objectif est simple : permettre à des personnes ou entités, disposant de grandes capacités de stockage de données, de les mettre à disposition moyennant rétribution. Le système est identique à certaines applications bien connues, selon lequel des particuliers peuvent mettre à disposition un appartement ou une voiture à des tiers en échange de paiement. Néanmoins, ce n'était jusqu'alors pas possible de le faire pour les données en raison de la complexité technique du projet, tant pour assurer l'intégrité des données et leur conservation dans le temps long. Or, il semble que cette nouvelle offre ait répondu à un réel besoin. En effet, fin 2021, le réseau Filecoin stockait plus de 30 pétaoctets de données (contre 5 au début de la même année) et revendique plus de 3500 fournisseurs de stockage.

Filecoin repose sur le protocole InterPlanetary File System (IPFS). Ce dernier est un protocole réseau similaire au protocole HTTP utilisé sur internet, avec la particularité qu'il fonctionne sur un réseau décentralisé de pair à pair, plus rapide et plus efficace. Sur cette base, Filecoin constitue un réseau qui permet de stocker et de partager des données de manière décentralisée¹⁶⁴.

À la base de ce réseau, se trouvent ceux que l'on appelle des « mineurs de stockage ». Ce sont des personnes ou entités disposant d'une grande capacité de stockage et qui souhaitent la mettre à disposition contre rémunération. Ces mineurs doivent, au préalable et afin de justifier de leur bonne foi, déposer en garantie une certaine quantité de *tokens* FIL - le *token* natif de Filecoin - afin de permettre le stockage de données sur leurs serveurs. En parallèle de cette garantie, les mineurs sont également redevables d'une preuve de bonne conservation des données sur une durée déterminée (en anglais, on parle de *Proof of Spacetime* ou PoSt) et d'une preuve de conservation effective de la donnée confiée (on parle de *Proof of Replication* ou PoRep). Cette dualité de garanties, l'une pécuniaire et l'autre probatoire, doit assurer la bonne conservation des données en respectant leur intégrité sur le long terme.

Cette nouvelle capacité de stockage distribuée permet ainsi de stocker des données qui n'ont pas nécessairement trait aux crypto-actifs ou à la blockchain. En effet, si des *smart-contracts* sont hébergés sur ce réseau (tels que des séquestres ou des enchères automatiques), on y trouve également la base de données de Wikipedia

¹⁶⁴ Cryptoast - [Filecoin \(FIL\), la blockchain au service du stockage décentralisé et du Web 3.0](#) - 04.01.2021

ou encore celle du Projet Gutenberg, qui a vocation à numériser et rendre accessible à tous de nombreux ouvrages tombés dans le domaine public.

Les utilisateurs versent alors des *tokens* FIL afin de rémunérer les mineurs, c'est-à-dire les personnes ou entités qui mettent à disposition leurs capacités de stockage. Il est question de mineurs parce que ces derniers reçoivent des récompenses proportionnelles à la quantité de données qu'ils hébergent, d'une manière semblable aux mineurs de bitcoins qui reçoivent des récompenses selon la puissance de calcul qu'ils allouent au réseau. Cette particularité fait qu'il n'y a pas de réelle barrière à l'entrée pour les nouveaux arrivants et que seule la compétitivité prix des acteurs entre en ligne de compte. Cela permet ainsi à Filecoin de proposer des coûts de stockage jusqu'à 15 fois moins élevés qu'un stockage standard sur Amazon ou Google¹⁶⁵.

II. La place de la finance décentralisée dans le système financier traditionnel

La finance décentralisée est un secteur qui construit peu à peu sa maturité. Toutefois ses cas d'usages, parfois expérimentaux, sont d'ores et déjà dynamiques et variés. Avec la numérisation et la décentralisation, le paradigme actuel du mode de fonctionnement de la finance s'en trouve interrogé et potentiellement transformé. L'irruption de la blockchain et des crypto-actifs dans le domaine financier permettra, demain, de le rendre plus efficace tant en termes de coûts, de transparence, d'ouverture et de sécurité.

La DeFi a émergé avec la promesse de concurrencer et de remplacer le modèle financier traditionnel. Cet antagonisme de nature politique est à la racine même du développement de la technologie blockchain. Elle ne doit pas pour autant cacher le véritable enjeu de l'émergence de cette nouvelle finance : le développement de la finance du XXI^{ème} siècle.

1. Les apports de la blockchain à la finance

La principale révolution de la blockchain est évidemment sa promesse d'absolue décentralisation. Croire en la blockchain, c'est croire en un outil qui permet d'avoir confiance en un interlocuteur pourtant totalement inconnu. La blockchain est alors, en même temps, créatrice et vectrice de confiance entre les individus. Toutefois, la nature décentralisée de ces outils va à l'encontre de tous les

¹⁶⁵ Blockchain Partner et KPMG - [Cryptoactifs : vers une révolution financière](#) - 06.2021

modes d'organisation classiques de l'Humanité. La centralisation a de tout temps été nécessaire afin de s'assurer de l'efficacité du système de confiance et de gouvernance. Avec la blockchain, ce n'est plus le cas. La structure de cette technologie implique une universalité sans pareil dans les systèmes traditionnels. Ainsi, quelle que soit l'origine, la couleur de peau, la croyance culturelle ou la nationalité de l'utilisateur, ce dernier pourra avoir y accès à n'importe quel service sans aucune discrimination de la part du protocole. Chaque personne est égale en droits devant les protocoles décentralisés. La blockchain a réussi là où les institutions publiques avaient échoué : instaurer une véritable universalité des services financiers sans contrainte entre les différents pays.

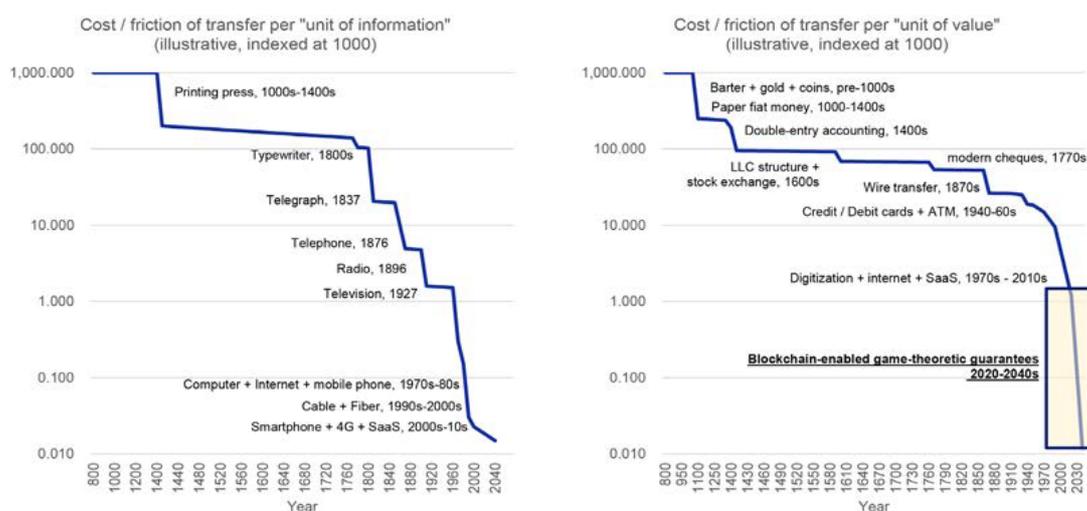
Naturellement, cette universalité de fait ne résiste pas toujours à la censure ou aux directives coercitives des juridictions et des gouvernements nationaux qui souhaitent empêcher leur développement sur leurs territoires. Le meilleur exemple est celui de la Chine qui, parallèlement au développement de sa propre MNBC, a mené une vaste offensive réglementaire afin de bannir le recours aux crypto-actifs parmi sa population. Néanmoins, la censure d'un tel réseau s'avère particulièrement difficile tant il est insaisissable et distribué au niveau mondial.

L'universalité et l'ouverture, fondements même de la blockchain, ont également des conséquences sur son propre développement. Si chacun peut l'utiliser, chacun peut également voir son fonctionnement et peut même le copier grâce à l'*open source*. Du principe d'ouverture découle donc le principe de transparence et de libre disponibilité de l'infrastructure. Ces deux principes favorisent ainsi (i) la confiance puisque chacun peut voir le code à la racine du protocole et s'assurer qu'il est bien conçu et qu'il ne présente aucune faille ou ne permet aucune fraude, mais aussi (ii) l'innovation, puisque chacun peut accéder à la structure informatique de la blockchain pour en proposer une nouvelle, modifiée en tout ou partie et qui serait alors plus efficace que la version originale (comme cela s'est produit avec l'émergence de Bitcoin cash, version amendée de Bitcoin et qui permet de réaliser davantage de transactions à un coût plus faible).

Cette transparence permet également une meilleure sécurité des protocoles qui sont utilisés pour fournir ces services financiers décentralisés. En effet, puisque leur code peut être consulté librement, il peut être audité et analysé par d'autres acteurs de l'écosystème afin d'en détecter les failles. Cette transparence est donc saine parce que, d'une part, elle favorise l'innovation à partir des protocoles existants et, d'autre part, elle permet un contrôle permanent de l'écosystème sur son fonctionnement.

Toutefois, cette transparence ne représente pas nécessairement une preuve suffisante de sécurité des protocoles. Le plus efficace reste évidemment de procéder à des audits répétés et spécialisés avant le lancement du service, réalisés par des spécialistes dont la compétence est reconnue. Certains protocoles en prennent l'initiative - leur nature décentralisée n'étant pas un obstacle à la réalisation de prestations d'audits par une société traditionnelle - afin de délivrer une structure informatique parfaitement fiable et non sujet à manipulation.

En parallèle des progrès effectués en matière de résilience des infrastructures basées sur la blockchain, le développement de cette dernière permet également des progrès en matière de réduction des coûts des opérations. En effet, au même titre que le développement d'internet a permis de réduire drastiquement le coût du partage de l'information, la blockchain réduit significativement le coût du partage de valeur, et constitue la suite logique de l'évolution financière.



Maple Leaf Capital - Estimation de l'évolution du coût de transfert par unité d'information (gauche) et par unité de valeur (droite) entre 800 et 2040¹⁶⁶

¹⁶⁶ Blockchain Partner et KPMG - [Cryptoactifs : vers une révolution financière](#) - 06.2021

En permettant de désintermédier les échanges, mais également une grande partie des activités financières telles que le prêt ou l'assurance, la blockchain permet de réduire le recours à une grande partie des activités dites de *back office* au sein des institutions bancaires et financières. Elle permet de rationaliser les organisations de ces entités, d'améliorer leurs procédures, de les rendre plus lisibles et plus efficaces, et d'en réduire le coût. Elle permet également de réduire le temps de réalisation des opérations.

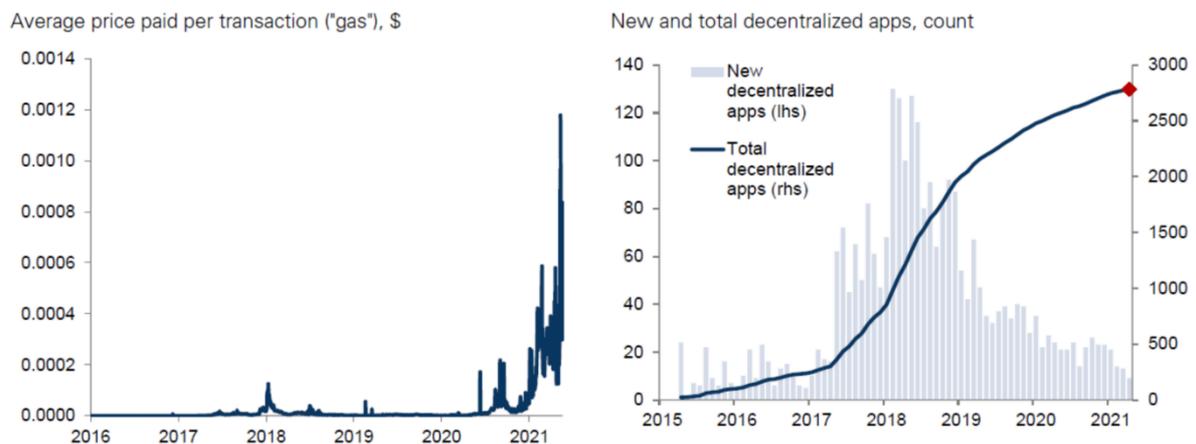
Évidemment, il serait inexact d'arguer que les services basés sur la blockchain pourraient remplacer, dès aujourd'hui ou à court terme, les institutions bancaires et financières. Les services de la finance décentralisée, pour beaucoup immatures, sont confrontés à des problématiques de stabilisation de leur infrastructure propre (qu'il s'agisse de la sécurité du code, de l'équilibrage de la gouvernance, etc ...) qui ne permettent pas encore d'assurer leur pleine démocratisation. Confrontés à de sérieuses problématiques de scalabilité et de congestion des réseaux, l'adhésion du grand public n'interviendra pas sans un réel changement des usages.

À l'écriture de ces lignes, la majorité des protocoles DeFi sont bâtis sur la blockchain Ethereum. Cette dernière est l'un des réseaux de seconde génération qui dispose de la plus grande communauté de développeurs. Organisée au sein d'une fondation, la communauté travaille en permanence à l'évolution et à la mise en œuvre du protocole Ethereum. Ce dernier devrait d'ailleurs progressivement migrer vers une version 2.0 permettant de fonctionner sur un consensus de preuve d'enjeu (en anglais, on parle de *proof-of-stake* ou PoS) en remplacement du consensus de *proof-of-work* actuel. Il s'agit d'un enjeu essentiel pour la blockchain Ethereum afin de pouvoir dépasser ses limites intrinsèques et permettre à la DeFi de continuer son essor.

Afin de comprendre ces limites, il est nécessaire d'expliquer brièvement la blockchain Ethereum. Les opérations réalisées sur ce réseau consomment du *gas* (ou gaz en français¹⁶⁷), qui correspond à une unité de mesure propre au réseau et que les utilisateurs achètent en contrepartie d'éthers. Si un utilisateur souhaite procéder à une transaction sur la blockchain, il doit au préalable acquérir du gaz, qui opère alors comme frais de transaction, afin que celle-ci puisse être inscrite dans un bloc de la blockchain. Ces frais servent ainsi à rémunérer les mineurs pour la preuve de travail fournie.

¹⁶⁷ Il s'agit d'une métaphore visant à comparer le réseau Ethereum avec une industrie traditionnelle qui fonctionne à partir de matières premières.

Toutefois, Ethereum, confronté au succès de la DeFi, fait l'objet d'un plus grand nombre de transactions que ce qu'il est capable de traiter. Il en découle un problème de scalabilité. Cette difficulté se répercute alors sur le prix du gaz, régi par la confrontation de l'offre (la capacité du réseau à valider un certain nombre de transactions en un seul bloc) et de la demande (les utilisateurs qui réalisent ces transactions). Ainsi, si la demande est élevée et que certains utilisateurs acceptent de payer un prix supérieur afin que leur transaction soit traitée dans des délais plus courts, cela entraîne une hausse généralisée du prix du gaz. Ainsi est-il devenu fréquent que le coût de transaction d'une opération soit supérieur à la valeur de cette dernière, ce qui la rend absurde d'un point de vue économique. Cette problématique majeure découle directement de la jeunesse du réseau et de la difficulté de mise à l'échelle des protocoles blockchain face à la nécessaire promesse de démocratisation de ces outils.



Glodman Sachs - Évolution des frais sur le réseau Ethereum entre 2016 et 2021 (gauche) et évolution des applications décentralisées (Dapps) sur le réseau Ethereum entre 2015 et 2021 (droite)

Cette problématique de la congestion du réseau Ethereum pose, de manière plus urgente, la problématique de l'interopérabilité des différentes blockchains. Avec la démocratisation des crypto-actifs et de la finance décentralisée, l'interopérabilité est un enjeu majeur. Il s'agira de l'un des prochains défis que le secteur aura à relever. Si la concurrence entre les protocoles dit de « layer 1 » est féroce, l'écosystème doit permettre une communication entre les différentes blockchains afin de pouvoir continuer à se démocratiser.

Si le rapport d'information relatif aux monnaies virtuelles posait la question de la suprématie d'un protocole sur les autres, il est fort à parier que l'avenir sera fait d'une multitude de protocoles ayant chacun leurs propres caractéristiques et communiquant entre eux. Tout comme Internet s'est structuré autour de protocoles, le monde de la blockchain et plus généralement le Web 3.0 sera sans doute un monde dans lequel coexisteront plusieurs protocoles en fonction des usages et de leurs potentialités propres. Peu à peu, les prémices de l'interopérabilité semblent poindre. Ainsi cela est déjà partiellement le cas avec les applications DeFi, qui s'implante progressivement sur différentes blockchains à la fois, en faisant fi des écosystèmes en silos tels qu'ils ont été conçus à l'origine, permettant ainsi une meilleure allocation des ressources.

2. La nécessaire rencontre de la finance traditionnelle et de la finance décentralisée

L'émergence de la finance décentralisée a posé les jalons d'une nouvelle manière de partager la valeur et de faire travailler le capital, de manière numérique et décentralisée. Considérer qu'il ne s'agit que d'une niche ou d'un effet de mode qui a vocation à s'estomper avec le temps, est méconnaître l'ampleur du mouvement qui adviendra.

Certaines institutions financières traditionnelles ont déjà pris part à cette mutation de la finance mais elles restent largement minoritaires. Si les fonds d'investissement américains se battent pour financer les futures licornes du secteur, les fonds d'investissement français et européens se montrent plus frileux. En effet, rares sont ceux qui décident de s'aventurer dans les opérations de levées de fonds des acteurs de cet écosystème, davantage par méconnaissance de ce dernier que par une réelle aversion aux crypto-actifs. L'institutionnalisation du bitcoin ne profite pas encore aux autres pans de cet écosystème si diversifié.

L'essor de la finance des crypto-actifs représente un risque pour la finance traditionnelle. Si ces deux finances ne fusionnent pas, si elles ne s'associent pas, cela donnera lieu à un affrontement qui fragilisera nécessairement l'une d'entre elles, jusqu'à potentiellement entraîner sa chute. Or, La conciliation entre les deux mondes devrait également être la volonté des décideurs publics afin d'éviter tout risque de déstabilisation systémique des secteurs bancaire et financier.

À défaut, si l'on se dirige vers une concurrence entre ces deux mondes, elle débouchera nécessairement sur une captation par cette nouvelle économie, d'une part importante de la valeur initialement hébergée par le secteur bancaire. En effet, avec la démocratisation grandissante des crypto-actifs, le développement d'une offre de services similaires aux services bancaires est la suite logique du développement des plateformes d'échanges centralisées. Celles-ci ne se limiteront pas à leurs activités initiales d'échanges de crypto-actifs, elles ont vocation à devenir des crypto-banques dans les années à venir.

Dans un contexte alliant des taux bas et un retour de l'inflation, les particuliers sont en demande de produits peu risqués et rémunérant davantage que les produits d'épargne des banques traditionnelles. Ce risque de concurrence a parfaitement été anticipé par la SEC qui s'est opposée brutalement à la société Coinbase lorsque cette dernière a souhaité émettre un produit d'épargne en *stablecoins* adossés aux dollars, comme évoqué précédemment. Cet épisode démontre une fois encore l'anticipation des régulateurs américains face à la concurrence à venir de ces nouveaux acteurs et ont vite perçu le risque de fuite de l'épargne des particuliers, aujourd'hui placé dans des produits traditionnels peu rentables. Cela pourrait poser, à terme, des difficultés quant à la solvabilité des banques si l'épargne de leurs clients était attirée par des rendements quatre à dix fois supérieurs aux produits bancaires que l'on connaît aujourd'hui. Qu'il s'agisse de Coinbase qui a procédé à son introduction en bourse, ou de Aave qui a obtenu une licence britannique afin d'opérer avec des monnaies traditionnelles et de proposer des services de paiement, l'irruption de ces nouveaux acteurs dans le quotidien des citoyens n'est plus qu'une question de temps.

Alors, le présent rapport souhaite insister sur le fait que cette nouvelle finance ne doit pas être vue comme une menace mais comme une nouvelle opportunité pour le système traditionnel. L'association des compétences de la finance traditionnelle avec les innovations technologiques permises par la blockchain permettrait à la finance d'entrer dans une nouvelle ère. Par ailleurs, l'ère technologique qui s'ouvre représente une réelle opportunité de faire émerger une finance davantage inclusive et transparente, mais aussi plus juste. Cette technologie permettra à l'ensemble de la société de mieux observer les fonctionnements du marché et de pointer du doigt les comportements déviants de certains acteurs financiers. Il ne s'agira plus de compter uniquement sur des lanceurs d'alerte, employés par les mis en cause, mais sur un ensemble d'acteurs indépendants et compétents qui assureront une veille constante des marchés. La promesse de cet écosystème ne consiste pas en une finance débridée, plus prédatrice, mais une finance plus durable, plus juste et à la portée de tous.

Cette transparence bénéficiera également aux pouvoirs publics en capacité de mieux orienter leurs politiques économiques, de contrôler et de prévenir les comportements délictueux sur les marchés. Pour autant, la suite et les futurs enjeux interrogent davantage encore. En toile de fond de cette transparence permise par la blockchain, se pose une fois encore la question de la confidentialité des données qui sera, assurément, l'un des thèmes majeurs du XXI^{ème} siècle.

Aussi, il est urgent de ne pas sur-réguler cet écosystème encore naissant. En la matière, le projet de règlement MiCa pose le principe que les protocoles DeFi sont des prestataires de services non conformes (ne disposant pas d'établissement physique au sein de l'Union européenne) et donc soumis à des règles particulières définies par l'ESMA. Cette position est problématique pour deux raisons : d'une part, il semble illusoire de penser que des protocoles dématérialisés se conforment à un règlement européen, puisque par définition ils n'ont pas d'assise territoriale ; d'autre part, cela envoie un signal particulièrement négatif à tous les développeurs qui innovent dans cet écosystème et à ses utilisateurs. Si la France et l'Europe souhaitent voir éclore des projets européens, elle doit adopter une logique dite du « bac à sable », consistant à laisser se développer les projets dans un cadre réglementaire minimal, à l'image du régime organisé par le projet de règlement dit « régime pilote ». Ce régime, nécessairement transitoire, doit permettre de ne pas brider l'innovation tant qu'une réglementation pertinente et protectrice se soit développée sur le sujet.

Proposition 20 : Modifier la réglementation applicable, actuelle et à venir, aux protocoles de finance décentralisée afin de développer un régime de « bac à sable », sous la supervision des autorités de régulation compétentes.

Le présent rapport met également en garde contre les tentatives de généralisation et de transposition aveugles des réglementations nationales et internationales de lutte contre le blanchiment et le financement du terrorisme, aux protocoles de la finance décentralisée. En effet, le GAFI considère que les utilisateurs ou les développeurs de ces protocoles pourraient être assimilés à des prestataires de services sur crypto-actifs. Ils se retrouveraient donc personnellement soumis à la réglementation applicable en la matière. L'idée sous-jacente consiste à dire que l'inexistence d'une personne morale derrière un protocole reviendrait à décaler la réglementation sur ses développeurs, quels qu'ils soient, ou à défaut sur

ses utilisateurs, partout dans le monde. Raisonement totalement illusoire.

La structure décentralisée de cette nouvelle finance impose donc de construire un nouveau paradigme réglementaire capable de réglementer efficacement ces nouvelles entités étherées. Ceci ne peut s'accomplir en transposant seulement l'existant applicable à des banques. Il implique une réflexion plus approfondie ainsi qu'une meilleure connaissance du fonctionnement des systèmes décentralisés. Ces réflexions doivent être le fruit d'un travail de concertation entre les acteurs de l'écosystème, les acteurs bancaires et financiers, les régulateurs et les autorités politiques.

Proposition 21 : Organiser une consultation publique à l'échelle européenne regroupant les acteurs de l'écosystème, les acteurs bancaires et financiers, les régulateurs et les autorités politiques afin de définir les lignes directrices d'une réglementation efficace et protectrice des utilisateurs, applicable aux entités de la finance décentralisée.

III. La DAO, une nouvelle forme de gouvernance

Parmi les innovations fondamentales permises par la technologie blockchain, on retrouve les organisations autonomes décentralisées. Elles s'organisent autour d'un mode de fonctionnement horizontal, totalement à rebours des modes d'organisation traditionnels. Ces nouvelles caractéristiques posent, de nouveaux enjeux en matière de régulation et de transposition avec l'existant.

1. Principe et fonctionnement

Une organisation autonome décentralisée (en anglais, on parle de *decentralized autonomous organization*, ou DAO) est un mode d'organisation de la prise de décision basé sur une blockchain et répondant aux principes de la décentralisation. Les règles de gouvernance sont déterminées en amont dans le code et inscrites de manière transparente dans le protocole. Les mécanismes qui assurent le bon fonctionnement des prises de décision et le respect des règles édictées sont régis par des *smart-contracts*, directement intégrés dans le protocole et qui procèdent de manière automatique.

Les DAO's sont particulièrement importantes dans l'écosystème des crypto-actifs, et notamment dans la finance décentralisée, puisqu'elles permettent de décentraliser la prise de décision et de la confier aux utilisateurs de l'écosystème - tout du moins, ceux qui en possèdent le droit. Comme évoqué, la quête de décentralisation ne s'arrête pas à la structure du service mais il modifie également sa gouvernance. Ainsi, la gouvernance d'un DEX est souvent couplée à une DAO afin de s'assurer que le service ou le produit, ainsi que la prise de décision soient décentralisés.

Les DAO assurent la gouvernance des protocoles décentralisés. En ce sens, elles ont vocation à prendre des décisions sur l'évolution des protocoles, tant du point de vue technique (par exemple : faire auditer la sécurité du protocole) qu'économique (par exemple : ajouter un nouvel actif empruntable dans un protocole de prêt).

Contrairement aux modes d'organisation centralisés, la gouvernance d'une DAO est constante et ne dépend pas de réunions convoquées régulièrement ou exceptionnellement. À tout instant, une personne éligible peut soumettre une proposition à la collectivité, qui statuera alors dans les conditions préalablement définies. Seuls les détenteurs de *tokens* de gouvernance sont éligibles à participer aux votes soumis à la DAO. Le principe est qu'un *token* équivaut à une voix. Les *tokens* de gouvernance ont émergé avec le développement des applications décentralisées et notamment la DeFi. Si ces objets d'un nouveau genre sont souvent comparés avec des parts sociales ou des actions de sociétés traditionnelles, ils en sont toutefois différents.

D'une part, contrairement aux droits sociaux, ces *tokens* ne représentent pas un titre de propriété équivalent à une fraction du protocole. Par conséquent, ils ne donnent pas de droit particulier sur le protocole en lui-même. Ce dernier fonctionne selon des règles préétablies et de manière automatique.

D'autre part, ils sont constitués, avant tout, de droits politiques qui s'expriment lors des décisions relatives à l'évolution du protocole. Malgré tout, il est devenu fréquent que des droits pécuniaires soient attachés aux *tokens* de gouvernance. Assimilés à des dividendes, ils peuvent avoir deux origines distinctes : (i) ils servent à récompenser le détenteur pour son investissement (financier ou en compétence) auprès du protocole, ou (ii) ils reflètent les résultats du protocole et s'apparentent alors à des droits sociaux traditionnels. C'est pourquoi la qualification de ces *tokens* est complexe : dans certains cas, ils ne confèrent qu'un droit de vote

(et peuvent être assimilés à de simples *utility tokens*), dans d'autres, ils sont similaires à des actions d'entreprise traditionnelle (et peuvent être assimilés à des *security tokens*). Parfois, il est même possible qu'ils ne correspondent à aucune de ces deux catégories, notamment lorsque la rémunération n'est qu'une incitation à participer aux votes.

Les DAO présentent certaines caractéristiques qui diffèrent des modes d'organisation traditionnels et qu'il est opportun de relever.

D'abord, et au même titre que la DeFi, la DAO écarte toute problématique de discrimination. Le pseudonymat permet d'effacer les caractéristiques personnelles de l'utilisateur lors de ses échanges avec d'autres utilisateurs. Celles-ci ne seront donc pas prises en compte lors de l'intégration au sein de la DAO - qui procède seulement de l'acquisition de *tokens* de gouvernance - mais aussi lors des dépôts de propositions ou lors des votes. Sur ces deux derniers points, seul le fond de la proposition est étudié par la collectivité et permet d'ignorer les préjugés que chacun pourrait avoir. Cet état de fait est aussi vertueux qu'efficace pour le protocole.

Ensuite, le corollaire de cette neutralité technologique induit une relative imperméabilité aux événements extérieurs à la DAO. En effet, alors que divers événements - notamment politiques - viennent entraver le fonctionnement et l'évolution des entreprises traditionnelles, la DAO est largement insensible à la censure et aux faits extérieurs. *De facto*, elle continuera de fonctionner et d'évoluer de manière déconnectée.

Enfin, la DAO rend le processus décisionnel collectif particulièrement efficace. Selon les règles qui déterminent son fonctionnement, lorsqu'une décision est prise, cette dernière est implémentée dans le protocole, soit immédiatement après le vote, soit dans un court laps de temps après. Aucun utilisateur mécontent ne peut en contester le résultat ou essayer de revenir en arrière de manière unilatérale. Dans cette dernière hypothèse, cela nécessiterait de voter pour revenir à l'état initial, ce qui nécessitera à nouveau des délibérations.

D'un point de vue plus politique, certains, au sein de l'écosystème, considèrent la DAO comme la forme la plus pure de la démocratie. En l'état actuel, cette assertion semble toutefois contestable, dans la mesure où le droit de vote résulte majoritairement de la détention capitaliste. Les individus qui possèdent un capital important peuvent décider d'acquérir un nombre de *tokens* de gouvernance suffisant

pour exercer une influence sensible sur le résultat du vote. *A contrario*, une personne disposant de peu de moyens verra son influence limitée. En cela, cette « démocratie » se rapprocherait d'un modèle de droit de vote serait censitaire. Il ne prendrait pas en compte le point de vue des petits porteurs à la valeur de leur individualité mais seulement de leur capital. Néanmoins, en raison des vastes possibilités offertes par la programmabilité des blockchains et des *smart-contracts*, cette difficulté pourrait être surmontée. Rien n'empêche par conséquent que les futurs modèles partisans ou associatifs soient construits sur des DAO. Bien au contraire, cela pourrait même être souhaitable. Modèle d'organisation collective, vecteur de vertu, plus efficient et plus transparent, les DAO donneraient à chacun des droits et des obligations dans l'exercice de leur responsabilité individuelle. Par ailleurs, elles supprimeraient sans doute la part d'incarnation individuelle qui peut dans certains domaines être un frein à l'équilibre d'un modèle. En outre, la modularité des dispositifs de gouvernance est sans limite et laisse augurer des équilibres en matière de gouvernance totalement novateurs dans les années à venir.

2. Enjeux

La grande majorité des applications de DeFi fonctionnent sur la base d'une DAO. Si ces protocoles sont totalement numériques et décentralisés, le sujet n'est pas dépourvu d'enjeux géographiques et de souveraineté. La domiciliation des développeurs de DAO sur le territoire français et plus largement le territoire européen représente un intérêt stratégique majeur. D'une part s'agissant des compétences, ces développeurs participent généralement au développement de plusieurs projets, qu'ils soient décentralisés ou non, et ces derniers représentent un atout majeur pour l'innovation en France. Au même titre que d'autres chercheurs ou spécialistes, la France et l'Europe se doivent de leur offrir un cadre réglementaire et économique à la hauteur de leur talent afin qu'ils puissent associer la société à leur réussite. D'autre part, ces projets décentralisés, s'ils sont aujourd'hui déconnectés du réel, sont amenés à se territorialiser, notamment en se conformant aux différentes réglementations qui leur permettront de toucher un public plus large et de se développer davantage encore. La question de l'implantation géographique est donc autant un enjeu pour ces nouvelles structures que pour les pays d'accueil, qui bénéficieront des retombées économiques de ces nouveaux acteurs financiers.

Pour ces raisons, le sujet de la DAO est certainement la porte d'entrée la plus pertinente afin d'envisager la réglementation de ces acteurs, et ainsi offrir un cadre clair et protecteur pour les utilisateurs et les développeurs.

L'essor d'entités décentralisées impose un changement de paradigme dans la réglementation des acteurs économiques. Le sujet est passionnant tant le champ des interrogations et des innovations juridiques est large. En droit positif, le respect de la règle de droit impose un sujet sur lequel elle s'applique, disposant de la personnalité juridique. Néanmoins, dans le cas des entités décentralisées, il est parfois impossible d'identifier un responsable, qu'il soit personne physique ou personne morale. Pourtant, cette entité n'est pas une coquille vide, elle s'organise et évolue par elle-même. Par conséquent, l'existence de la DAO comme objet doté d'une personnalité juridique devra à terme être reconnue.

Cela implique d'abord de reconnaître, en droit, les DAO comme des entités à part entière et de leur attribuer une personnalité « numérique ». Cette reconnaissance pourrait résulter d'une déclaration - comme c'est le cas pour les sociétés - ou d'une procédure d'enregistrement - comme c'est le cas pour les PSAN. Quoiqu'il en soit, préalablement à cette reconnaissance, la DAO devra se soumettre à des obligations réglementaires qui garantissent le bon fonctionnement de l'économie et préviennent les abus de toutes natures. La réglementation pourrait ainsi exiger de la DAO qu'elle soit constituée selon des règles de gouvernance équilibrées. Elle pourrait également rendre obligatoire la divulgation de l'identité des détenteurs de *tokens* de gouvernance exerçant une certaine influence dans les prises de décision (comme c'est le cas pour certains associés disposant d'une part importante du capital d'une société). De plus, elle pourrait imposer la réalisation d'audits réguliers afin de prévenir d'éventuelles failles dans le protocole, ou encore des attaques informatiques. Elle pourrait également prévoir une réserve prudentielle, à l'image de ce qui est imposé aux acteurs bancaires, afin de prévenir tout risque d'effondrement suite à un retournement de marché.

Ces obligations ne sont que des exemples, mais elles préfigurent les pistes afin de construire une prochaine réglementation. L'objectif ne serait pas de brider la créativité et la liberté qu'offrent ces nouveaux outils mais de garantir un standard minimal afin d'assurer la stabilité de la gouvernance du protocole, la sécurité de son code informatique et l'équilibre du système financier. Il s'agira de protéger les citoyens tout en conservant à l'esprit l'impérieuse nécessité de soutenir l'innovation et la compétitivité dans une logique de décentralisation.

Demain, apparaîtront des entreprises constituées sous la forme de DAO mais pas seulement. En effet, il est fort probable que ce type de structure siéra à la création d'associations, d'ONG, de partis politiques. De par la souplesse qu'elles permettent dans leur gouvernance et la simplicité qu'elle engendre dans leur fonctionnement, les DAO seront très certainement une forme juridique et économique incontournable dans le futur.

Proposition 22 : (i) Permettre aux DAO d'obtenir la personnalité juridique afin de reconnaître leur existence juridique et leurs donner le pouvoir de nouer des relations contractuelles à l'instar d'autres personnes morales. (ii) Développer un cadre réglementaire afin prendre en compte leur gouvernance, d'assurer leur stabilité financière notamment afin de protéger leurs membres et de garantir leur sécurité informatique.

Synthèse des propositions

Droit au compte

Proposition 1 : Supprimer la procédure de droit au compte dédiée aux acteurs crypto au profit de la procédure de droit commun.

Proposition 2 : Rendre systématique l'imposition d'une sanction pécuniaire, sous forme d'astreinte, lorsqu'un établissement de crédit attribué par la Banque de France en vertu du droit au compte ne se conforme pas à ses obligations.

Proposition 3 : Permettre aux acteurs enregistrés comme PSAN d'obtenir les services bancaires nécessaires à l'exercice et au développement de leurs activités. En parallèle, confier à l'ACPR la mission de contrôler la mise en œuvre régulière de ces services et, à défaut, d'imposer une mesure d'astreinte.

Proposition 4 : Approfondir les travaux engagés par le groupe de travail sur l'accès des PSAN aux comptes bancaires et, sur cette base, confier à l'ACPR le développement de lignes directrices à destination des établissements de crédit et des acteurs de l'écosystème des crypto-actifs.

Fiscalité

Proposition 5 : Instaurer un sursis d'imposition, limité à trois ans après l'opération faisant l'objet d'une imposition, pour les échanges d'actifs numériques réalisés par des entreprises et professionnels.

Proposition 6 : Instaurer un régime de faveur similaire au régime de l'apport-cession pour les apports d'actifs numériques à des sociétés traditionnelles.

Proposition 7 : Instaurer la possibilité, pour le contribuable, de reporter les moins-values sur cession d'actifs numériques sur les plus-values de même nature, jusqu'à trois ans après leur constatation.

Proposition 8 : Instaurer un régime fiscal similaire au régime des attributions gratuites d'actions (AGA) aux attributions gratuites d'actifs numériques (AGAN) réalisées par une entreprise émettrice de jetons à ses salariés.

Proposition 9 : Repenser le système fiscal et déclaratif lié aux paiements en crypto-actifs afin de lever les frictions fiscales afférentes.

Proposition 10 : Centraliser le traitement des dossiers relatifs aux crypto-actifs auprès d'équipes spécialisées au sein de la Direction générale des finances publiques.

Crypto-actifs et climat

Proposition 11 : Accroître le financement de nouvelles sources d'énergie renouvelable en favorisant les partenariats entre les producteurs d'énergie et les mineurs de crypto-actifs, afin d'utiliser les surplus d'énergie autrement perdus.

Proposition 12 : Interdire le minage professionnel de crypto-actifs à partir d'énergies carbonées et adapter la réglementation applicable aux droits à polluer afin de l'appliquer aux mineurs professionnels de crypto-actifs, en attribuant des crédits carbone à ceux participant au financement de nouvelles sources d'énergie renouvelable.

Jetons non fongibles (NFT)

Proposition 13 : En droit civil, définir de manière large la notion de jeton non fongible afin de donner un statut juridique à ces nouveaux objets numériques et les dissocier de la notion d'actif numérique. S'assurer de la juste traduction des usages futurs et du sous-jacent de ces jetons en droit positif.

Proposition 14 : Modifier la réglementation applicable à la propriété intellectuelle afin d'intégrer les jetons non fongibles comme nouveau support. Adapter le droit de la preuve et reconnaître la force probante d'une preuve inscrite dans la blockchain.

Proposition 15 : Organiser, de concert avec les sociétés de perception et de répartition des droits d'auteur, le ministère de la Culture et les représentants concernés, une politique de sensibilisation à l'égard des droits de propriété au sein de la technologie NFT et éduquer quant à la publication d'une œuvre sous ce format.

Proposition 16 : Fiscaliser les revenus tirés des jetons non fongibles selon le régime fiscal applicable à leurs sous-jacent et, en parallèle, instaurer un report d'imposition des plus-values générées à l'occasion d'un échange entre un jeton non fongible et un actif numérique.

Souveraineté monétaire

Proposition 17 : Favoriser le développement de *stablecoins* en euros privés afin de défendre la souveraineté monétaire européenne dans ce nouvel écosystème.

Proposition 18 : Émettre une MNBC de gros, à destination des acteurs du système bancaire et financier, afin de compléter la modernisation des marchés financiers *via* la blockchain.

Proposition 19 : Émettre un euro numérique de détail, à destination de tous les particuliers et de toutes les entreprises, dont certains pré-requis auront fait l'objet,

au préalable, d'une réflexion approfondie :

- (i) Accessible partout et par tous, que l'on soit connecté au réseau centralisé ou non, que l'on soit équipé de matériel informatique ou non ;
- (ii) Confidentiel s'agissant des données personnelles des citoyens, avec la possibilité d'identifier les personnes et les transactions dans le cadre de la lutte contre le blanchiment et le financement du terrorisme, sous le contrôle d'une autorité administrative indépendante et d'une autorité judiciaire ;
- (iii) Dont la structure repose sur les acteurs bancaires traditionnels afin que ces derniers puissent diffuser l'euro numérique à travers les différentes couches de la population et sans que cela ne crée un risque systémique pour la stabilité financière ;
- (iv) Dont la structure permet de faire face aux risques de dysfonctionnements et d'attaques sur les *smart-contracts* chargés de collecter l'impôt - les services de l'État doivent monter en compétence d'un point de vue technique sur les possibilités offertes par la blockchain ; et
- (v) Dont la structure permet de développer des applications innovantes relatives à la collecte de l'impôt et à la politique monétaire (monnaie hélicoptère).

Finance décentralisée

Proposition 20 : Modifier la réglementation applicable, actuelle et à venir, aux protocoles de finance décentralisée afin de développer un régime de « bac à sable », sous la supervision des autorités de régulation compétentes.

Proposition 21 : Organiser une comitologie publique à l'échelle européenne regroupant les acteurs de l'écosystème, les acteurs bancaires et financiers, les régulateurs et les autorités politiques afin de définir les lignes directrices d'une réglementation efficace et protectrice des utilisateurs, applicable aux entités de la finance décentralisée.

Proposition 22 : (i) Permettre aux DAO d'obtenir la personnalité juridique afin de reconnaître leur existence juridique et leurs donner le pouvoir de nouer des relations contractuelles à l'instar d'autres personnes morales. (ii) Développer un cadre réglementaire afin prendre en compte leur gouvernance, d'assurer leur stabilité financière notamment afin de protéger leurs membres et de garantir leur sécurité informatique.

Remerciements

AMAR Mickaël – Associé de Chainaccelerator

AMBROISE Mélodie – Directrice Stratégie et Relations institutionnelles de l'ADAN

BALVA Claire – Directrice blockchain & crypto-actifs de KPMG France

BARTHALOIS Cyril – Secrétaire général de l'Académie des beaux-arts de Paris

BENCHEMLED Mounir – CEO de Paraswap

BLOCH Raphaël – Cofondateur et rédacteur en chef de TheBigWhale

BORDET Hugo – Responsable des affaires réglementaires de l'ADAN

BOUTELOUP Julien – CEO de Stake Capital Group

CADIGNAN Gilles – CEO de Woleet

CANTU Nicolas – Associé de Chainaccelerator

CASELLES-DUPRÉ Hugo – CEO de Obvious

CHARLET David – Président de l'ANACOFI

CHARPIAT Victor – Avocat de Kramer Levin

CHOUEIFATY Yves – CEO de Tobam

COMAIR Jad – CEO de Melanion Capital

DELAMARE DEBOUTTEVILLE Alexis – CTO de NFT Factory

DELORME d'ARMAILLÉ – Directrice générale de l'OCBF

DESSERTINE Domitille – Directrice pôle innovation de l'AMF

EL MANSSOURI Youcef – CEO de Sesterce Mining

ENTREMONT Pierre – CEO de Frst

FAVIER Jacques – Auteur

FEDAK Gilles – CEO de iExec

FILALI Nadia – Directrice programmes blockchain de la Caisse des dépôts

FIGLIO Frédéric – CEO de Logical Pictures

FLEURET Faustine – Présidente et Directrice générale de l’ADAN

FOURNEL Morgane – Legal counsel de Ledger

FRANCE Thomas – CEO de Cygni Labs

GAUTHIER Pascal – CEO de Ledger

GOUSPILLOU Sébastien – CEO de BigBlock Datacenter

GRANGE Benjamin – CEO de Dentsy Consulting

GRAPINET Gilles – PDG de Worldline

GRUNTHALER Arnaud – Avocat associé de Fieldfisher

HABABOU Hervé – CEO de BTU Protocol

HEUVRARD Fabrice – Expert-comptable

INGELAERE Thibaut – CEO de Blockpulse

JULIA Nicolas – CEO de Sorare

De LASTOURS Ivan – Pilote blockchain de Bpifrance

LAURANT Dominique – Avocat associé de Laurant Michaud Duceux

LEBEAU Sandrine – Directrice compliance de Coinhouse

LOURIMI Alexandre – Avocat de ORWL Avocats

LOUVET Nicolas – CEO de Coinhouse

LUZU Paul-Arthur – Avocat associé de Ferdowsi Legal

MARÉCHAL Anne – Directrice des affaires juridiques de l’AMF

MAZZOLINI Giulia – Responsable France de Bitpanda

McCOURT Frank – CEO de McCourt Global

De MOMBYNES Yorick – Auditeur de la Cour des comptes

MORIZOT Pierre – CEO de Waltio

De NICOLAY Jean – CEO de NFT Labs (Pierre Bergé & Associés)

NIVOT Julien – Head of European affairs de Ledger

O’RORKE William – Avocat associé de ORWL Avocats

PAVAO Cédric – Avocat de Fieldfisher

POLROT Simon – Responsable affaires européennes de l’ADAN

RAYMOND Grégory – Cofondateur et rédacteur en chef de TheBigWhale

RODRIGUEZ Philippe – CEO de Avolta Partners

SABBAGH Cyril – Responsable ETF de Melanion Capital

SABBAN Axel – Avocat

SIMONIN Owen – CEO de Just Mining

SOUBIRAN Ambre – CEO de Kaïko

STACHTCHENKO Alexandre – Directeur blockchain & crypto-actifs de KPMG France

TAKKAL BATAILLE Adli - Entrepreneur

TCHAKERIAN Anthony – CFO de Sesterce Mining

TÉQUI Clément – Deputy CEO de Ternoia

VALES Antoine – Co-founder de Aleno

VEYRAT Pablo – Core contributor de Angle Protocol

VIAUD Astrid - Docteur en Sciences politiques, consultante en conformité

YATES Oliver – CEO de Sheeldmarket

ZERAH Hadrien – CEO de Nomadic Labs

ZEROUALI Medhi – Responsable blockchain de Sigma Prime

Abréviations

AMF - Autorité des marchés financiers

ACPR - Autorité de contrôle prudentiel et de résolution

BCE - Banque centrale européenne

BRI - Banque des règlements internationaux

CGI - Code général des impôts

ETF - *Exchange Traded Fund* (en français : fonds négocié en bourse)

FBF - Fédération bancaire française

Fed - Federal Reserve System (banque centrale des États-Unis d'Amérique)

FMI - Fonds monétaire international

KYC - *Know your client* (processus de contrôle de l'identité des clients)

LCB-FT - Lutte contre le blanchiment d'argent et le financement du terrorisme

PBoC - *People's Bank of China* (banque centrale de la République populaire de Chine)

Rapport d'information relatif aux monnaies virtuelles - Rapport d'information déposé en application de l'article 145 du règlement, par la commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale, en conclusion des travaux d'une mission d'information relative aux monnaies virtuelles, n° 1624

SEC - Securities and Exchange Commission (organisme de contrôle des marchés financiers des États-Unis d'Amérique)

Glossaire relatifs aux crypto-actifs

Airdrop - Distribution gratuite de *tokens* à destination du public (réservé ou non)

Altcoins - Crypto-actifs alternatifs au bitcoin (exemple : ether)

Centralized exchanges (CEX) - Plateforme d'échanges de crypto-actifs centralisée

Decentralized Autonomous Organization (DAO) - Organisation autonome décentralisée¹⁶⁸

Decentralized Finance (DeFi) - Finance décentralisée¹⁶⁹

Decentralized exchange (DEX) - Plateforme d'échanges de crypto-actifs décentralisée¹⁷⁰

Données off-chain - Données issues du monde physique, non compréhensibles par la blockchain

Données on-chain - Données nativement numériques, résultant de l'activité de la blockchain

Flashloan - « Prêt éclair » consistant en un emprunt instantané sans risque de contrepartie, qui ne demande aucune garantie, à condition d'être remboursé dans une seule et même transaction sur Ethereum¹⁷¹

Halving - Division de moitié de la récompense offerte en contrepartie de la validation d'un bloc de la blockchain Bitcoin, au-delà des frais de transaction

Hardware wallet - Portefeuille physique permettant d'y stocker des crypto-actifs en dehors de tout réseau connecté à Internet, réputé davantage sécurisé qu'un portefeuille en ligne (*software wallet*)

Hashrate - Puissance de calcul fournie par des ordinateurs et autres composants informatiques permettant de résoudre les problèmes mathématiques nécessaires à la validation de blocs d'une blockchain fonctionnant selon un consensus PoW

Initial coins offering (ICO) - Méthode de levée de fonds par l'émission puis l'offre au public de *utility tokens*

¹⁶⁸ Cf. « III. La DAO, une nouvelle gouvernance »

¹⁶⁹ Cf. « PARTIE IV - La finance numérique de demain »

¹⁷⁰ Cf. « a. Les plateformes d'échanges décentralisées »

¹⁷¹ Source : Cryptoast - [Qu'est-ce qu'un flash loan ? Un mal nécessaire](#) - 21.11.2020

Initial exchange offering (IEO) - Méthode de levée de fonds par l'émission puis l'offre au public de *tokens* (*utility tokens* ou *security tokens*) par le biais d'une plateforme d'échanges de crypto-actifs

Monnaie numérique de banque centrale (MNBC) - Monnaie de banque centrale émise et fonctionnant selon les principes de la blockchain¹⁷²

Oracle - Source d'informations permettant d'intégrer des variables issues du monde réel dans des *smart-contracts*¹⁷³

Proof-of-stake (PoS) - Processus de validation de blocs et de sécurisation de la blockchain par la mise en séquestre d'un capital en crypto-actifs

Proof-of-work (PoW) - Processus de validation de blocs et de sécurisation de la blockchain par la résolution d'un problème mathématique généré par un algorithme

Smart-contract - Programme ou code informatique dont l'exécution ne nécessite pas l'intervention d'un tiers de confiance ; dans le contexte de la blockchain, il s'agit d'un programme qui s'active automatiquement sur un réseau distribué lorsque certaines conditions sont remplies sur le registre partagé¹⁷⁴

Stablecoin - *Token* dont le cours est adossé à (i) un ou plusieurs actifs ou à (ii) un algorithme permettant d'assurer sa stabilité¹⁷⁵

Security tokens - Jeton accordant à son propriétaire des droits, sur l'émetteur, similaires à ceux offerts par la détention de titres financiers traditionnels

Security tokens offering (STO) - Méthode de levée de fonds par l'émission puis l'offre au public de *security tokens*

Token - « Jeton » ou actif numérique pouvant être transféré (et non copié) entre deux parties sur Internet et sans nécessiter l'accord d'un tiers

Utility token - Jeton accordant à son propriétaire une créance sur un bien ou un service proposé par l'émetteur

Vault - « Coffre-fort » correspond à un compte numérique dans lequel sont stockés et sécurisés des crypto-actifs

Wallet - Portefeuille numérique ou physique permettant de stocker des crypto-actifs

¹⁷² Cf. « III. La tokenisation de la monnaie : l'émergence des monnaies numériques de banque centrale »

¹⁷³ Source : Cryptoast - [Qu'est-ce qu'un Oracle ? Blockchain et monde réel](#) - 05.09.2018

¹⁷⁴ Source : Cryptoast - [Qu'est-ce qu'un smart contract ou contrat intelligent ?](#) - 09.11.2020

¹⁷⁵ Cf. « II. Les stablecoins, une représentation de la monnaie étatique dans le monde numérique »

Whitepaper - « Livre blanc » destiné à détailler les objectifs, moyens et caractéristiques techniques d'un projet blockchain

Yield farming - « Agriculture de rendements » consistant à optimiser les différents rendements offerts par les applications DeFi¹⁷⁶

¹⁷⁶ Cf. [c. L'optimisation automatisée des rendements](#)