Septembre 2023

Finance « décentralisée » ou « désintermédiée » (DeFi) : quelle réponse réglementaire ?

Synthèse des réponses à la consultation publique

Auteurs : Olivier Fliche, Julien Uri, Mathieu Vileyn
Pôle Fintech-Innovation

ACPR
BANQUE DE FRANCE

Résumé

Le document de réflexion de l'ACPR soumis à consultation proposait une description des risques spécifiques de la finance décentralisée ou désintermédiée (DeFi), en distinguant schématiquement les **trois grandes strates** qui la composent : **l'infrastructure blockchain, la couche applicative des « services »**, et les **dispositifs d'accès des utilisateurs** à ces services. Il notait également le **haut niveau de concentration** qui caractérise l'écosystème de la DeFi, ainsi que la **gouvernance parfois très centralisée** de ses applications.

Une partie des risques de la DeFi étant étroitement liés aux caractéristiques des technologies qui en font l'intérêt, le parti pris par le document de réflexion était de proposer des pistes réglementaires adaptées aux spécificités de la DeFi, sans se borner à répliquer les dispositifs encadrant actuellement la finance traditionnelle.

L'intérêt suscité par le document de réflexion et les réponses reçues lors de la consultation valident largement ces choix. La consultation a en outre permis d'éclairer ou d'approfondir certains des thèmes de réflexion.

Ainsi, s'agissant des **phénomènes de concentration** décrits dans le document de réflexion, la consultation apporte deux éléments de réflexion nouveaux. En premier lieu, **la concentration des acteurs de l'écosystème n'est pas nécessairement le reflet de l'immaturité de l'écosystème DeFi** ; elle pourrait bien être due au contraire – comme plus généralement dans le monde numérique – à l'existence de **rendements croissants**, aboutissant à des situations de **monopole** ou **d'oligopole**. Cette situation, déjà perceptible au niveau des infrastructures blockchain elles-mêmes, pourrait s'observer également au niveau de certains services fournis. Une réglementation future de la DeFi, pour être pertinente, devra naturellement prendre en compte cette tendance, si elle se confirme. En second lieu, certains répondants ont mis en lumière un **autre aspect de la concentration** dans la DeFi : celui de **l'infrastructure physique hébergeant les nœuds de la blockchain** et le rôle central joué par les fournisseurs de *cloud* à cet égard. Ce point, qui rejoint les préoccupations de résilience opérationnelle récemment traitées par le règlement DORA pour la finance traditionnelle, mérite effectivement considération.

Les principales pistes de réglementation évoquées dans le document de réflexion appellent, quant à elles, les commentaires suivants.

La très grande majorité des répondants soutient l'idée que **les blockchains publiques** peuvent abriter les activités DeFi, et l'éventualité d'une transition vers des blockchains privées suscite de fortes réserves (généralement au nom de la capacité à innover). Ce faisant, de nombreux acteurs admettent la nécessité de renforcer la résilience des blockchains publiques et s'accordent sur la nécessité d'auditer régulièrement leur fonctionnement, rejoignant ainsi l'idée promue par le document de réflexion de **fixer des standards de sécurité**. Les divergences sont grandes, en revanche, quant à la manière d'y parvenir. À cet égard, on notera l'importance d'intégrer dans la réflexion réglementaire les « surcouches » ou **solutions de *layer 2*** utilisées pour la gestion à grande échelle des transactions sur la blockchain. La consultation met ainsi en évidence une grande diversité de vues sur les risques liés à ces solutions, à mettre en relation avec la grande diversité des solutions techniques elles-mêmes, signe d'un **paysage technologique encore peu mature et très évolutif**.

L'idée que des autorités publiques gèrent des **nœuds d'archives** de certaines blockchains publiques, afin notamment d'aider à la restauration du registre après une attaque, est en revanche assez consensuelle parmi les participants.

Le principe d'**une certification des *smart contracts*** emporte un large assentiment. Le périmètre d'une telle certification ainsi que ses modalités pratiques font davantage débat ; plusieurs répondants avancent toutefois des pistes intéressantes en la matière (proportionnalité, « mode d'emploi » des *smart contracts*, remontée des incidents à une autorité centralisatrice etc.). On mentionnera également ici le concept – à explorer – de « **minimisation de la gouvernance** », développé par certains répondants comme un moyen de limiter les risques qu'une concentration trop importante des droits de vote pourraient faire peser sur les protocoles et les services « décentralisés » qu'ils fournissent.

Enfin, **l'encadrement des intermédiaires ou des interfaces avec les utilisateurs fait l'objet d'un large consensus** : toutefois, à l'inverse de certains commentaires reçus, cette piste réglementaire ne semble pas de nature à dispenser les autorités d'une réflexion sur un encadrement des deux autres couches de la DeFi. Un point d'attention réside dans la façon dont les interfaces décentralisées (en développement rapide) devront être encadrées en pratique, de nombreux retours de la consultation indiquant qu'elles ne peuvent l'être « de la même manière » que les intermédiaires centralisés.

Suites envisagées par l'ACPR

Comme annoncé lors de la publication du document de réflexion, **les enseignements tirés** de la présente consultation **viendront nourrir les contributions de l'ACPR à la réflexion** qui s'engage, au niveau européen, **quant aux suites à apporter au règlement MiCA**. En particulier, il apparaît possible et souhaitable d'édicter des mesures relatives à la fiabilité des infrastructures blockchain sur lesquelles la DeFi – ou d'autres formes de finance tokenisée – seraient amenées à se développer, d'élaborer des règles – par exemple de certification – adaptées à la nature et au fonctionnement des *smart contracts*, et de définir des règles de gouvernance et de conduite des opérations permettant d'assurer une protection adéquate des utilisateurs de la DeFi.

En outre, la consultation a montré l'intérêt d'**approfondir** les nombreuses questions que soulève le thème de **la certification des *smart contracts*** : cet approfondissement et des analyses complémentaires pourraient être menés dans les mois qui viennent, en mobilisant les expertises du secteur et des autorités concernées.

Enfin, au-delà de la veille technologique nécessaire sur des sujets encore évolutifs, **certains thèmes**, tels que la sécurité de certaines briques de l'infrastructure (*layer 2*), ou encore les moyens de limiter les phénomènes de concentration et les risques associés, pourraient probablement être plus efficacement **explorés par le monde de la recherche**. Le renforcement des liens existant déjà entre l'ACPR et la recherche serait un moyen possible d'éclairer ces sujets, toujours dans la perspective de promouvoir une réglementation adaptée au niveau européen. Des études de nature plus juridique, notamment sur les modalités de représentation des *organisations autonomes décentralisées* (DAO), pourraient utilement compléter ces travaux.

Table des matières

Résumé 2
Suites envisagées par l'ACPR 3
Rappel du contexte 5
Participation à la consultation 5
Réponses à la consultation 6
I. Description et fonctionnement de la DeFi 7
1-1. Définition et périmètre de la DeFi 7
1-2. La question de la concentration dans l'univers DeFi 7
II. Les risques liés à la DeFi 9
2-1. Les risques liés à la gouvernance décentralisée 9
2-1-1. La persistance d'éléments de centralisation dans une gouvernance décentralisée 9
2-1-2. Les attaques par prêts instantanés sur la gouvernance des protocoles 10
2-2. Les risques liés aux infrastructures : des débats autour des solutions de *layer 2* 10
2-3. Les attaques informatiques sur les blockchains et les protocoles 11
2-4. Les risques de LCB-FT : la question du pseudonymat 12
III. Les pistes réglementaires 14
3-1. Assurer une résilience minimale de l'infrastructure blockchain 14
3-2. Proposer un encadrement adapté à la nature algorithmique des services 16
3-2-1. La certification des *smart contracts* 16
3-2-2. Le cas des oracles 18
3-2-3. Le cas des *stablecoins* 18
3-3. Règlementer la fourniture et l'accès aux services 19
3-3-1. La recentralisation potentielle de certaines activités 19
3-3-2. La réglementation des points d'accès 20

Rappel du contexte

La finance « décentralisée » ou « désintermédiée » (DeFi) désigne un ensemble de services sur crypto-actifs, comparables à des services financiers et effectués sans l'intervention d'un intermédiaire.

Malgré sa taille modeste et le nombre actuellement restreint de ses cas d'usages, la DeFi suscite l'intérêt par les **innovations technologiques** sur lesquelles elle est bâtie et par sa promesse fondamentale : remplacer la confiance entre les acteurs par du **code informatique tenant lieu de règle commune**. **L'intérêt pour la DeFi tient aussi à ce qu'elle pourrait préfigurer des transformations à venir de la finance.** L'intérêt du superviseur financier pour la DeFi tient évidemment aussi aux **risques** qu'elle présente, risques qui posent la question d'un **encadrement réglementaire**.

Après une série d'entretiens auprès d'acteurs de l'écosystème, l'ACPR a ainsi publié, en avril 2023, un **document de réflexion** consacré à l'encadrement de la DeFi. Ce document n'exprimait pas une position définitive de l'ACPR, mais visait plutôt à développer une première analyse des pistes règlementaires, en vue de les discuter avec les parties prenantes à l'occasion d'une consultation publique.

Cette **consultation publique**, qui s'est tenue en avril-mai 2023, a permis de vérifier la bonne compréhension par l'ACPR des principaux mécanismes de la DeFi, mais aussi de recueillir l'avis des participants sur les pistes réglementaires esquissées dans le document de réflexion.

Pour rappel, ces pistes de réflexion portaient sur les **trois grandes strates de la DeFi** et visaient, pour l'essentiel, à :

- S'assurer de la résilience des infrastructures blockchain qui servent de base à la DeFi, par exemple en imposant des standards de sécurité et en limitant les risques de concentration des capacités de validation des transactions dans les mains de quelques acteurs ;
- Renforcer la sécurité des *smart contracts*, en particulier via un mécanisme de certification portant sur la sécurité du code informatique, la nature du service fourni ou encore la gouvernance ;
- Mieux encadrer la fourniture de services et l'accès des utilisateurs à ces services, par exemple en instaurant un cadre de contrôle renforcé des intermédiaires assurant en pratique l'accès des utilisateurs aux services de la DeFi.

Au travers de l'ensemble de ces travaux, l'ACPR entend **nourrir les réflexions en cours, notamment au niveau européen**, dans le prolongement du règlement MiCA, qui prévoit, dans les 18 mois suivant son entrée en vigueur, la rédaction d'un rapport sur l'assujettissement de la DeFi à la réglementation européenne.

Participation à la consultation

Ouverte durant deux mois (avril-mai 2023), la consultation publique sur le document de réflexion de l'ACPR a **rencontré un large écho, en France et en Europe mais aussi dans le reste du monde,** permettant de recueillir **39 réponses**. Y ont participé des **acteurs diversifiés** : des institutions financières traditionnelles, des cabinets de conseil et d'audit, mais aussi des représentants des écosystèmes crypto et DeFi, dont certains leaders mondiaux du secteur (cf. tableau).

Au-delà du nombre, l'ACPR tient à saluer la **grande qualité** des réponses reçues, qui constituent une contribution précieuse aux nombreux débats concernant la DeFi.

Tableau : Répondants à la consultation publique

Catégorie	Total	France	UE hors France	Reste du monde
Particuliers	6	5		1
Banques, paiement	2	1		1
Conseil, audit	3	2		1
Associations professionnelles finance traditionnelle	5	3	1	1
Associations professionnelles DeFi / cryptos / DLT	5	1	3	1
PSAN	6	3	1	2
Ecosystème DeFi / cryptos / DLT	11	2		9
Capital-risque	1			1
Total	**39**	**17**	**5**	**17**

Source : ACPR

Réponses à la consultation

De manière générale, le document de réflexion a été **bien accueilli**. Même si toutes les analyses et les propositions faites ne sont pas unanimement partagées, nombreux sont les répondants qui saluent l'initiative prise par l'ACPR et la précision de son travail.

Au plan technique, la consultation a permis d'apporter des compléments utiles aux éléments exposés dans le document de réflexion (notamment sur certains aspects techniques des attaques informatiques sur les blockchains) : ceux-ci sont résumés dans la présente synthèse. Les réponses reçues **ne remettent toutefois pas fondamentalement en cause la compréhension du sujet par l'ACPR, qui en sort donc globalement confortée**.

Plusieurs des **pistes de réglementation** esquissées par le document de réflexion ont par ailleurs fait l'objet d'un **intérêt marqué de la part des répondants**. Si quelques-uns d'entre eux rejettent l'idée même d'une réglementation des activités DeFi, la plupart – y compris les acteurs du secteur des actifs numériques – reconnaissent la nécessité de mécanismes d'encadrement ou de limitation d'un certain nombre de risques.

Ce document retrace les réponses reçues lors de la consultation publique. Il a parfois été jugé utile d'inclure une brève discussion de celles-ci. **Ces propos ne représentent que les vues des auteurs, et n'expriment pas une position officielle de l'ACPR**.

La présente synthèse suit la structure du document de réflexion initial qui abordait (i) la description de la DeFi (définition, cas d'usage, structure), (ii) les risques (liés à la gouvernance, aux infrastructures, à la couche applicative et aux usages) et (iii) les pistes réglementaires.

I. Description et fonctionnement de la DeFi

1-1. Définition et périmètre de la DeFi

Synthèse des réponses

La définition retenue par l'ACPR de la finance décentralisée ou désintermédiée (« DeFi »), insistant sur son caractère imprécis et caractérisant plutôt cette activité au moyen d'un faisceau de critères, est saluée pour sa flexibilité par plusieurs répondants. D'autres répondants critiquent au contraire le choix opéré, et estiment que tout projet de réglementation de la DeFi suppose une définition précise.

De fait, plutôt que de participer aux nombreux débats visant à définir la « vraie » DeFi, le document de réflexion présentait un **écosystème dans son fonctionnement réel**, c'est-à-dire aussi dans ses interactions avec des **éléments centralisés** (*stablecoins*, conversion entre monnaie officielle et crypto-actifs etc.). Des participants à la consultation soulignent d'ailleurs que, au-delà des différentes briques composant l'écosystème, **certains éléments de centralisation demeurent aujourd'hui encore au cœur du fonctionnement des protocoles de DeFi** : oracles, dispositifs « multisig », mécanismes de mise à jour etc. C'est dire si la frontière entre une finance théoriquement centralisée (« CeFi ») et une finance théoriquement décentralisée (« DeFi ») paraît complexe à tracer.

Quant au **schéma présentant l'architecture applicative de la DeFi** (fin de la partie I du document de réflexion), certains répondants ont fait observer qu'il ne faisait pas apparaître l'ensemble des couches informatiques constituant la blockchain.

Discussion

Malgré la difficulté pratique à le faire, est-il exact qu'il faudra bien un jour tracer les contours de « la DeFi » ? Tout dépend en fait de la manière d'appréhender la réglementation relative aux actifs numériques. **Définir précisément le périmètre de « la DeFi » n'apparaît en effet nécessaire que si l'on souhaite élaborer une réglementation propre à ce mode de fourniture de services sur actifs numériques**. On peut à l'inverse imaginer une règlementation **homogène** – ce qui ne signifie pas forcément uniforme – couvrant l'intégralité des services sur actifs numériques, quel que soit leur mode de fourniture. Une telle réglementation pourrait par exemple prendre la forme d'un règlement « MiCA 2 ». Dans cette perspective, le besoin de faire apparaître un objet « DeFi » apparaît moins évident.

1-2. La question de la concentration dans l'univers DeFi

Synthèse des réponses

Le document de réflexion mettait en lumière la paradoxale concentration de l'écosystème DeFi, et ce à plusieurs niveaux (partie 1-5). Deux phénomènes distincts étaient soulignés : la **concentration économique** sur le marché DeFi d'une part, et **la concentration de la gouvernance** des blockchains et des applications d'autre part (sur ce second aspect, se reporter à la partie 2 de la présente synthèse).

Sur la **concentration économique**, un répondant fait d'abord remarquer que, s'agissant des protocoles de prêts-emprunts, les parts de marché des applications décentralisées peuvent être relativisées si l'on se souvient qu'elles subissent aussi la concurrence d'applications centralisées. Il n'en demeure pas moins que le constat dressé dans le document de réflexion est largement reconnu par les répondants

à la consultation : quelques blockchains et un nombre relativement restreint d'applications concentrent, en valeur, l'essentiel des actifs. Certains répondants remarquent en outre qu'il conviendrait d'ajouter **une troisième dimension** à ce constat d'un écosystème concentré : **l'infrastructure physique hébergeant les nœuds de la blockchain**. Ainsi, certains recensements indiquent qu'une majorité des nœuds Ethereum sont hébergés par des fournisseurs de *cloud*, dont une partie significative par Amazon Web Services (AWS). Ce point est d'autant plus intéressant à noter qu'il constitue un **facteur de risque si l'un de ces prestataires devait connaître une défaillance**. En outre, avec le développement des blockchains, les « nœuds complets »[1] du réseau auront probablement à stocker une quantité croissante d'informations à l'avenir ; ce risque devrait donc probablement perdurer, voire s'accroître.

Discussion

Il est d'abord utile de préciser que la concentration n'est pas forcément gênante en elle-même, notamment dans le domaine des infrastructures, marqué par l'importance des **effets de réseaux**[2]. En outre, si certains répondants tentent d'expliquer la concentration dans la DeFi par la relative jeunesse de l'écosystème, on peut au contraire formuler l'hypothèse inverse : que **l'univers de la DeFi, comme peut-être plus généralement celui des activités numériques, est un espace de rendements croissants**. Or, selon la théorie économique, une production à rendements croissants se traduit par une situation de **monopole naturel**, ou à tout le moins d'**oligopole**.

Ainsi, un protocole décentralisé de prêt-emprunt ne peut fonctionner sans une masse critique de liquidité, apportée par les utilisateurs. En retour, une liquidité abondante et un nombre élevé d'utilisateurs permettent au protocole de réaliser des **économies d'échelle**, et notamment de facturer certains services moins chers, ce qui rend le service **plus compétitif** et attire de nouveaux utilisateurs, et donc encore davantage de liquidité. En outre, toutes choses égales par ailleurs, plus d'utilisateurs et plus de liquidité génèrent davantage de **confiance**, ce qui contribue là encore à renforcer l'attractivité du service. Or contrairement à ce qui prévaut pour produire la plupart des biens et services du monde réel, des **investissements somme toute modestes** permettent généralement d'éviter que la hausse du nombre d'utilisateurs ne conduise à une **congestion** du service (ce point est possiblement différent au niveau des blockchains, *cf. infra* la discussion sur le passage à l'échelle, mais il affecte alors indifféremment tous les protocoles situés sur une même blockchain). En revanche, davantage d'utilisateurs et donc davantage d'actifs échangés peuvent aiguiser les appétits d'acteurs malveillants, et par conséquent conduire à une hausse des attaques informatiques contre le protocole, et donc à une baisse de la confiance des utilisateurs si le service n'est pas assez solide.

Finalement, la concentration économique constatée dans l'univers de la DeFi n'est donc peut-être **ni une surprise, ni le signe d'une immaturité de l'écosystème**. Au-delà d'enjeux classiques de concurrence, cette situation rend, en tout état de cause, **particulièrement critique la question de la résilience des infrastructures blockchains**, qu'il s'agisse du risque de panne ou du risque d'une prise de contrôle par des attaquants (*cf. infra*).

---

[1] En général, les nœuds complets stockent chacun une copie complète de l'historique de la blockchain (contrairement aux nœuds légers, qui ne conservent qu'une petite partie de l'historique). Il existe toutefois des exceptions : ainsi, sur la blockchain Ethereum, pour des raisons de taille, un nœud complet ne stocke que les 128 derniers blocs (des nœuds d'archive stockant les données plus anciennes). Dans tous les cas, l'opération d'un nœud complet nécessite de disposer d'une grande quantité de mémoire.

[2] Phénomène par lequel l'utilisation d'un bien ou d'un service par de nouveaux utilisateurs augmente sa valeur pour les utilisateurs existants. Cette externalité positive concerne en particulier les réseaux de communication.

II. Les risques liés à la DeFi

2-1. Les risques liés à la gouvernance décentralisée

2-1-1. La persistance d'éléments de centralisation dans une gouvernance décentralisée

Synthèse des réponses

Que cela passe par la concentration de la majorité des jetons de gouvernance dans les mains de quelques acteurs, par la conservation de clés d'administrateurs, ou encore via l'existence d'autres privilèges relativisant les mécanismes de vote, le document de réflexion montrait que la **gouvernance** de nombreux protocoles apparaissait **faussement décentralisée** (« *decentralised in name only* » ou DINO, *cf.* partie 2-1 du document de réflexion).

À cet égard, certains participants à la consultation avancent une idée intéressante : c'est peut-être moins la centralisation *de facto* de la gouvernance qui est gênante que son **éventuelle dissimulation** aux utilisateurs d'une blockchain ou d'une application DeFi. Ainsi, la détention de clés d'administrateur par quelques individus dotés de privilèges apparaît-elle moins problématique si elle est connue de tous, et si les conditions d'utilisation de ces clés sont fixées à l'avance (attaque informatique, nécessité de mettre à jour le protocole etc.).

Au-delà des efforts de transparence, la persistance d'éléments de centralisation au cœur du fonctionnement des protocoles DeFi (*cf.* la partie 1-1 de cette synthèse) constitue un risque, qui conduit certains répondants à plaider pour une « **minimisation de la gouvernance** ». Ce principe consiste à limiter au maximum le périmètre des actions que peut entreprendre l'instance de gouvernance pour modifier le protocole[3]. Avec une gouvernance réduite à son strict minimum, un protocole est **quasi-immuable** : les instances de gouvernance ne peuvent pas en modifier le fonctionnement profond, mais uniquement faire varier certains des paramètres, comme le niveau des frais prélevés pour chaque utilisation du service[4].

Discussion

En premier lieu, la **transparence** quant aux mécanismes de gouvernance en vigueur peut effectivement être admise comme un principe important. On peut d'ailleurs citer, parmi les efforts de transparence des protocoles DeFi, la publication fréquente, voire en temps réel, de données permettant au public de savoir qui détient les jetons de gouvernance.

S'ils sont bienvenus, les efforts pour améliorer la transparence ne constituent pas pour autant une réponse définitive à l'ensemble des risques émanant de la gouvernance faussement décentralisée. Tout d'abord **parce que la transparence n'est généralement pas complète sur les blockchains** : c'est le problème du pseudonymat (sur ce sujet, voir également le point 2-4 de cette synthèse, traitant de la lutte contre le blanchiment de capitaux et le financement du terrorisme). Ainsi, la publication de données sur les détenteurs des jetons de gouvernance d'une blockchain ou d'un protocole ne permet pas nécessairement de se représenter la concentration réelle des capacités de validation ou de

[3] Uniswap ou Liquity sont des exemples souvent cités de mise en œuvre de ce principe.

[4] Cette variation peut d'ailleurs elle-même être contrainte au sein d'une fourchette fixée « en dur », afin d'interdire par avance toute tentative de fixer des frais à un niveau confiscatoire.

décision, puisque les détenteurs sont seulement identifiés par leur adresse sur la blockchain ; or un même individu peut disposer de plusieurs adresses, tandis que des entités liées entre elles dans le monde réel (une maison-mère et une filiale par exemple) peuvent disposer d'adresses blockchain apparemment sans lien entre elles.

En second lieu, il paraît clair que la **persistance d'éléments de centralisation** dans des protocoles théoriquement décentralisés fait à tout moment peser un **risque d'arbitraire** sur la gouvernance, même lorsque ceux-ci sont encadrés ou précisés à l'avance. Ainsi, qui jugera de la réalité du danger planant sur un protocole, danger qui pourra être invoqué par un groupe d'individu pour utiliser ses clés d'administrateur ? Et même si la communauté des utilisateurs désavoue après coup l'intervention, il sera probablement difficile de revenir sur des décisions ayant déjà généré des évènements économiques. **Les risques découlant de la persistance d'éléments de centralisation peuvent ainsi être atténués, mais pas supprimés**.

Face à ces risques, le principe de **« minimisation de la gouvernance »** constitue une idée intéressante : il présente un intérêt certain en termes de sécurité et, à ce titre, il **pourrait faire partie des critères retenus pour la certification des *smart contracts*** (*cf. infra*). Il faut cependant noter que d'autres difficultés peuvent émerger du peu de pouvoir laissé aux instances de gouvernance : ainsi, comment effectuer des mises à jour de sécurité d'un protocole quasi-immuable, ou comment réagir en cas d'attaque informatique ?

2-1-2. Les attaques par prêts instantanés sur la gouvernance des protocoles

Synthèse des réponses

Le document de réflexion mentionnait (dans sa partie 2-1) le risque **d'attaques sur la gouvernance via des prêts instantanés** (*flash loans*), visant à emprunter d'importantes quantités de jetons de gouvernance afin de voter une décision nocive aux autres utilisateurs, avant de rembourser immédiatement la somme, une fois le méfait accompli. Certains répondants à la consultation ont indiqué que **ces attaques étaient devenues en pratique rares**, en raison des **mécanismes de protection** déployés dans de nombreux protocoles. Ainsi, il est généralement exigé que les votes soient d'abord envoyés au sein d'un premier bloc de transaction, avant que le vote lui-même n'ait lieu dans un bloc de transaction distinct (alors que le mécanisme des prêts instantanés requiert que l'emprunt et le remboursement s'effectuent au sein d'un même bloc). Des répondants indiquent aussi que les systèmes de gouvernance les plus courants prévoient un **délai significatif** entre le vote d'une proposition et sa mise en œuvre (trois jours pour le protocole Uniswap par exemple). La soumission d'une proposition et son vote étant des processus transparents, les parties prenantes peuvent savoir qui a voté en sa faveur. Le délai de mise en œuvre donne ainsi aux utilisateurs le temps nécessaire pour quitter une blockchain ou une application si une proposition qu'ils jugent malveillante a été votée.

2-2. Les risques liés aux infrastructures : des débats autour des solutions de *layer 2*

Synthèse des réponses

La consultation publique confirme que, en dehors des enjeux de gouvernance (*cf. supra*), les risques liés aux infrastructures blockchain ont essentiellement trait aux problèmes de **passage à l'échelle**

(*scalability*). À ce sujet, les répondants confirment que les **solutions de *layer 2*** (« surcouches »)[5] sont actuellement la voie principale utilisée par l'écosystème pour surmonter la congestion des réseaux. Les participants à la consultation indiquent aussi que l'ACPR a bien identifié les risques principaux des différentes solutions de *layer 2* : sécurité des ponts (*bridges*) reliant les blockchains entre elles, lorsque les *layer 2* sont d'autres blockchains (*sidechains* par exemple) ; importance du délai (7 jours en général) permettant de rendre les transactions finales dans le cas des *optimistic rollups* ; rôle critique d'opérateurs centralisés, risquant de conduire à des comportements frauduleux, dans le calcul des preuves sans divulgation de connaissance (*zero-knowledge proof* ou ZK), pour le cas des *ZK-rollups*.

Les réponses reçues lors de la consultation soulignent, en outre, la **grande diversité** des solutions de *layer 2* actuellement mises en œuvre, dans un univers technologique extrêmement évolutif. Cette diversité est aussi le reflet de la **grande hétérogénéité technologique** des blockchains de *layer 1*, dont les caractéristiques sont plus ou moins adaptées à chacune des solutions de *layer 2*. De plus, certaines questions techniques divisent largement les répondants à la consultation, qu'il s'agisse de savoir si les ZK-rollups réduisent la transparence de l'information pour les utilisateurs qui ne sont pas partie aux transactions, ou encore si les transactions se déroulant sur des *rollups*[6] doivent être considérées comme « *on-chain* » ou « *off-chain* »[7]. De manière encore plus cruciale, les réponses à la consultation font également apparaître une **grande diversité de vue sur les risques** induits par les solutions de *layer 2*, ainsi que sur les difficultés liées à l'interopérabilité des blockchains entre elles.

Discussion

La dispersion des solutions techniques retenues et la diversité d'appréciation des acteurs quant aux risques présentés par ces solutions **posent la question de la maturité de l'écosystème sur la question du passage à l'échelle**. Il paraît donc important de continuer à explorer cette question dans des études ultérieures.

2-3. Les attaques informatiques sur les blockchains et les protocoles

Synthèse des réponses

La consultation publique a permis de recueillir d'utiles compléments techniques quant aux risques d'attaques informatiques sur les blockchains et les protocoles DeFi. Ainsi, certains participants à la consultation ont remarqué que le document de réflexion ne mentionnait pas en tant que telles les **« attaques sandwich »** sur la *mempool* des blockchains, pourtant porteuses de risques importants.

La *mempool* est le lieu de stockage temporaire où les transactions sont mises en attente sur la blockchain, jusqu'à la création d'un bloc de transactions qui les incorporera. La *mempool* est généralement publique : tous les utilisateurs de la blockchain peuvent voir quelles sont les transactions en attente, et quels sont les frais que les utilisateurs ont consenti à payer pour leur validation. De ce fait, un utilisateur malveillant – généralement un robot spécialisé sur cette tâche – peut rechercher

[5] Type de solution de passage à l'échelle des blockchains, dont le principe est de traiter une partie des transactions hors chaîne, en n'enregistrant que le minimum d'informations dans la chaîne principale (*layer 1*).
[6] Les *rollups* sont la solution de *layer 2* la plus répandue aujourd'hui, consistant à « enrouler » un groupe de transactions en une seule opération (d'où son nom), et à compresser l'information en envoyant uniquement les données strictement nécessaires à l'inscription définitive de ces transactions sur la blockchain.
[7] Ce débat pourrait poser des questions en termes de périmètre réglementaire, les crypto-actifs étant notamment définis comme des actifs dont la valeur est transférée au moyen de la technologie blockchain.

des transactions de montant élevé en attente. Prenons l'exemple d'un utilisateur X ayant envoyé une transaction visant à acquérir une certaine quantité d'un crypto-actif A. Le robot malveillant qui a repéré cette transaction va alors chercher à intercaler un second ordre d'achat du même actif A *avant* la transaction envoyée par X (*front run*). Pour cela, il lui suffit généralement de payer des frais de transaction plus élevés que ceux de la transaction initiale, la plupart des blockchains validant les transactions par ordre décroissant des frais (*gas* sur Ethereum). L'achat du crypto-actif A par le robot malveillant fait monter son prix, et conduit donc X, lorsque sa transaction est validée, à acheter l'actif A à un prix supérieur au prix initialement fixé, ce qui représente une perte pour lui. Enfin, la phase finale de l'attaque consiste pour le robot à vendre son stock de l'actif A, mais cette fois à un prix supérieur au prix d'achat (le cours de A ayant été poussé à la hausse par les deux précédentes transactions). Là encore en fixant de manière appropriée les frais de transaction, le robot peut parvenir à faire valider cette transaction juste après la transaction de l'utilisateur X (*back run*) : la transaction initiale est finalement encadrée par deux nouvelles transactions malveillantes, l'une positionnée juste avant et l'autre juste après (d'où le nom d'attaque « sandwich »). Le robot empoche ainsi un profit au détriment de l'utilisateur X, grâce à la capacité d'observer la *mempool*[8].

Plusieurs répondants montrent que le risque de l'attaque « sandwich » **pose fondamentalement la question du type de *mempool* à privilégier** sur les blockchains de *layer 1*, mais également dans les solutions de *layer 2* (où sont également validées des transactions). Aujourd'hui, la plupart des *rollups* utilisent un modèle de « séquenceur unique », c'est-à-dire qu'une seule entité reçoit les transactions en attente, les ordonne et en fait des blocs. Or, si la *mempool* publique fait courir le risque d'attaques « sandwich » (largement répandues), le modèle de la *mempool* privée ou permissionnée ne va pas non plus sans poser de difficultés, puisque les tiers ne peuvent pas voir les transactions en attente, ni vérifier le respect des règles de séquençage. Le séquenceur a ainsi la possibilité d'ordonner les transactions selon un processus arbitraire, y compris en insérant ses propres transactions en vue d'en tirer un profit.

2-4. Les risques de LCB-FT : la question du pseudonymat

Synthèse des réponses

Le document de réflexion faisait état des débats entourant le **pseudonymat** en vigueur sur la plupart des blockchains. Certes, le pseudonymat n'est pas l'anonymat : il permet une certaine traçabilité des transactions, ce qui conduit à des formes d'auto-régulation sur les blockchains. Toutefois, **l'absence d'identification des utilisateurs[9] est susceptible d'affaiblir la lutte contre le blanchiment de capitaux et de financement du terrorisme (LCB-FT)**. A l'inverse, l'insertion dans une blockchain publique de l'identité des participants à chaque transaction risquerait de contrevenir aux exigences de **protection de la vie privée** (partie 2-4-4 du document de réflexion).

[8] Ce type d'attaque repose également sur les mécanismes de tolérance quant à la variation du cours des crypto-actifs à échanger entre l'envoi de la transaction et sa validation (*slippage*) : les utilisateurs fixent à l'avance le *slippage* maximum qu'ils consentent. Le risque d'attaques « sandwich » peut ainsi être atténué par la fixation d'un *slippage* plus faible, au risque toutefois que certaines des transactions envoyées par un utilisateur pour validation soient *in fine* annulées en cas de dérapage excessif des cours, ce qui peut poser d'autres difficultés.

[9] Et ce d'autant plus que les applications DeFi fonctionnent pour la plupart sans contrôle d'accès : la participation nécessite uniquement la connexion à un portefeuille numérique (*wallet)*, et une partie de ces portefeuilles peuvent être ouverts sans vérification d'identité ni contrôle de l'origine des fonds déposés.

Plusieurs répondants à la consultation estiment que des innovations technologiques récentes pourraient apporter une solution à cet épineux problème. Des **solutions d'identité numériques** ont en effet été développées au cours des dernières années. Reposant sur les progrès réalisés dans les techniques de preuve cryptographiques (en particulier de preuve à divulgation nulle de connaissance), elles permettent théoriquement de fournir une identification vérifiable, évolutive, utilisable par tous, interopérable entre différents systèmes, et garantissant aux individus que seule la quantité minimale nécessaire d'informations personnelles est partagée. Ces solutions d'identité numérique pourraient faciliter la mise en œuvre directe, sur la blockchain, des obligations de connaissance du client (« *Know your customer* » ou KYC)[10]. Elles permettraient ainsi de **concilier l'identification des personnes impliquées dans les transactions sur blockchain, pour les besoins de la LCB-FT, avec les exigences de protection de la vie privée**.

Discussion

L'utilisation de solutions d'identité numérique constitue une piste technologique intéressante. Pour garantir une lutte efficace contre le blanchiment de capitaux et le financement du terrorisme, ce type de dispositif nécessite toutefois que les données relatives à l'identification des protagonistes soient d'abord **recueillies de manière certaine**, qu'elles soient ensuite **dûment vérifiées**, et qu'elles soient enfin **accessibles à l'ensemble des entités ayant besoin d'identifier les bénéficiaires effectifs des transactions**. En effet, la mise en place de solutions d'identité numérique dont le contenu ne serait pas fiable pourrait paradoxalement faciliter l'exécution de transactions illicites.

[10] Un répondant mentionne par exemple la possibilité, après avoir enrôlé un utilisateur et effectué les procédures de vérification, d'émettre un jeton personnel (non transférable) servant de « certificat de KYC » à celui-ci.

III. Les pistes réglementaires

3-1. Assurer une résilience minimale de l'infrastructure blockchain

Synthèse des réponses

L'idée de recourir à des **blockchains privées** (scénario B de la partie 3-1 du document de réflexion) est largement critiquée par les répondants à la consultation. Les blockchains privées sont en effet jugées moins sûres que les blockchains publiques en ce qu'elles présentent, comme tous les éléments centralisés, un risque de point de défaillance unique (« *single point of failure* »). Surtout, les répondants estiment qu'elles n'induisent pas les mêmes effets de réseaux que les blockchains publiques, et sont donc moins efficaces.

Une large majorité des participants à la consultation plaide donc pour l'utilisation de **blockchains publiques** (scénario A du document de réflexion), tout en reconnaissant généralement la nécessité de **renforcer leur résilience**. Certains répondants **s'opposent toutefois au principe même d'une régulation de l'infrastructure**, en invoquant généralement l'exemple d'internet[11]. Un autre argument fréquemment invoqué contre le principe d'une règlementation est que le niveau actuel des connaissances sur la DeFi n'est pas suffisant pour réguler correctement les blockchains, ou même l'ensemble de l'écosystème. Un répondant propose ainsi la création d'un observatoire de la DeFi, qui aurait pour mission de rassembler des connaissances sur les blockchains et les protocoles, et pourrait ainsi alimenter la réflexion sur les formes de supervision à mettre en œuvre.

S'agissant des **moyens** pour renforcer la résilience, de nombreux répondants s'accordent sur la nécessité **d'auditer régulièrement le fonctionnement des blockchains**. De ce point de vue, une standardisation des pratiques est largement mentionnée (voir le point 3-2-1 de la présente synthèse sur cette question). Elle rejoint l'idée de fixer des **standards de sécurité** aux blockchains, qui est généralement approuvée. En revanche, les répondants divergent sur la manière d'élaborer ces standards. L'idée la plus fréquemment mentionnée est une élaboration conjointe par les acteurs de marché et les autorités publiques (une suggestion également présente dans le document de réflexion).

L'introduction de standards minimums de sécurité pour les blockchains pourrait cependant constituer un **obstacle à l'entrée de nouveaux acteurs** sur ce marché, ceux-ci disposant souvent de moyens réduits pour appliquer la réglementation. Certains répondants proposent ainsi que les standards de sécurité ne soient pas obligatoires mais seulement volontaires. L'idée sous-jacente est un mécanisme incitatif : les acteurs les plus importants souhaiteraient respecter les standards de sécurité afin d'accroître la confiance de leurs clients et d'en attirer de nouveaux ; les nouveaux entrants auraient quant à eux le temps d'atteindre une certaine taille avant de décider de se conformer aux standards. Pour renforcer l'incitation, certains participants proposent que les superviseurs financiers puissent décider si les institutions qu'ils supervisent ont le droit d'interagir avec telle ou telle blockchain, selon l'évaluation du niveau de sécurité de cette dernière.

Le document de réflexion indiquait également que des superviseurs publics pourraient surveiller en temps réel la **concentration des capacités de validation** sur les blockchains publiques, et communiquer en cas de dépassement de certains seuils. Ces propositions font largement débat parmi les répondants à la consultation. Certains d'entre eux pointent les initiatives de certaines blockchains pour limiter le risque de concertation entre validateurs (voire de prise de contrôle), par exemple via des mécanismes

[11] Régulation centrée sur les sites internet, l'infrastructure de communication à proprement parler n'étant que peu règlementée.

de **sélection aléatoire** des validateurs d'un nouveau bloc. D'autres, favorables au contraire au principe d'une surveillance, proposent de **s'inspirer de la réglementation applicable au capital des sociétés cotées** – par exemple s'agissant du franchissement de certains seuils – pour encadrer la concentration des capacités de validation.

Enfin, l'idée que des autorités publiques puissent opérer des **nœuds d'archive** de certaines blockchains publiques, afin d'aider à la restauration du registre après une attaque, ou éventuellement au transfert des informations vers une autre blockchain en cas de corruption définitive, fait largement consensus parmi les participants.

Discussion

Les deux principaux arguments contre l'utilisation de **blockchains privées** paraissent susceptibles d'être relativisés. Sur le sujet de la **sécurité**, en premier lieu, la défaillance d'une brique centralisée devenue systémique – et donc confrontée pour cette raison à des attaques informatiques régulières – constitue en effet un risque non négligeable. Il faut cependant noter que nombre de blockchains publiques ont également connu des défaillances, notamment en raison des attaques dont elles ont pu faire l'objet. Surtout, ce danger doit être **mis en balance avec l'ensemble des risques** liés au fonctionnement des blockchains publiques (voir la partie 2-2 du document de réflexion sur ce point). En second lieu, l'argument des **effets de réseaux** a probablement du sens lorsqu'il s'agit de comparer les blockchains publiques et les blockchains privées dans leurs formes actuelles. Toutefois, si une blockchain privée pan-européenne (voire mondiale), abritant l'essentiel des activités liées aux actifs numériques, devait un jour être créée – par exemple pour des raisons réglementaires –, ses effets de réseaux seraient certainement considérables.

S'agissant des **blockchains publiques**, et du principe même de leur encadrement, la comparaison effectuée par certains répondants avec le fonctionnement d'internet présente une limite de taille : **contrairement aux blockchains, le réseau internet ne permet pas par lui-même d'échanger, de stocker et de prouver directement la propriété d'actifs financiers**. Les risques induits pour les utilisateurs – notamment les particuliers –, voire à terme pour la stabilité financière, ne sont donc pas comparables.

Sur la résilience des blockchains publiques, il est clair que le problème potentiel de **concurrence** qui résulterait de la mise en place de standards de sécurité invite à envisager des formes de **proportionnalité** dans la mise en œuvre de ce type d'obligation. Les différentes propositions formulées par les répondants invitent en tout état de cause à clarifier un point : **il serait de toute façon difficile au superviseur financier de réguler lui-même le fonctionnement des blockchains**. **Son action se limiterait donc nécessairement aux institutions qu'il supervise**, même s'il n'est pas exclu que d'autres acteurs publics puissent contribuer à l'encadrement – voire à l'opération directe –, des blockchains.

S'agissant de la surveillance des capacités de validation par des autorités publiques, il faut dans tous les cas insister sur le fait qu'un **contrôle efficace suppose de remplir deux conditions** : d'une part que, sur la blockchain, les adresses puissent être efficacement reliées à l'identité des utilisateurs (au moins pour l'autorité en charge de la surveillance), afin d'identifier les multiples adresses d'une même personne ; d'autre part que, dans le monde réel, les autorités de contrôle disposent de suffisamment d'informations pour relier entre eux des individus ou des sociétés (maison-mère et filiale par exemple) susceptibles de se concerter sur la blockchain.

Il paraît clair, en tout cas, que pour les autorités publiques puissent exercer une **surveillance efficace** des activités liées aux actifs numériques, il leur faut disposer d'une bon niveau d'information. De ce

point de vue, la constitution de **bases de données** alimentées régulièrement – voire en temps réel – et permettant de suivre l'activité sur les blockchains, constitue une **étape essentielle**. Dans le même objectif, le **superviseur financier pourrait opérer un « nœud de supervision »**, doté de privilèges spécifiques.

3-2. Proposer un encadrement adapté à la nature algorithmique des services

3-2-1. La certification des *smart contracts*

Synthèse des réponses

Les répondants à la consultation reconnaissent très majoritairement que les *smart contracts* présentent trop souvent des dangers pour les utilisateurs, notamment les particuliers peu avertis. De ce fait, ils se montrent généralement **favorables au principe d'une certification**.

Les répondants insistent d'ailleurs sur l'existence **d'initiatives du marché** pour assurer ou renforcer la sécurité des *smart contracts*. La pratique des *bug bounties*[12], tout d'abord, est souvent jugée efficace. Des outils permettant d'explorer automatiquement le code des *smart contracts* existent également sur le marché. S'agissant des techniques d'audit, les répondants indiquent que les **méthodes formelles** sont pour l'heure peu employées, du fait de leur coût élevé, et ce malgré un potentiel jugé significatif. Enfin, un certain nombre de répondants mettent en avant les promesses portées par le **développement de l'intelligence artificielle (IA)** en matière d'audit informatique.

Toutefois, la majorité des répondants reconnaît que les **mécanismes existants d'audit ne sont souvent pas suffisants**, pour deux raisons principales. D'une part, l'audit des *smart contracts* se concentre généralement sur les seuls aspects de sécurité informatique – certes essentiels –, mais aborde peu les fonctionnalités économiques, la gouvernance, ou encore la conformité à la réglementation. D'autre part, les techniques d'audit centrées sur l'examen du code informatique prennent difficilement en compte les aspects systémiques de la sécurité informatique, en particulier les vulnérabilités liées à l'utilisation des fonctionnalités d'un autre *smart contract*.

Les répondants insistent également **sur la grande hétérogénéité des pratiques** en matière d'audit des *smart contracts*, et **plaident pour une certaine standardisation en la matière**. Cette idée est très proche d'une des principales propositions du document de réflexion : un mécanisme de certification des *smart contract*.

Si le principe de la certification est largement admis, ses **modalités** font en revanche l'objet de débats parmi les répondants et, en premier lieu, sur **le champ des *smart contracts* à certifier**. Ainsi, l'un des répondants suggère-t-il, comme mesure de proportionnalité, de **n'imposer la certification que pour les plus gros projets** et de requérir seulement un audit de sécurité, plus léger, en dessous d'une certaine taille. Il propose à cette fin d'établir une typologie des *smart contracts* risqués ou complexes à certifier (expérimentaux, interactifs, complexes, évolutifs, etc.) Un autre répondant note, quant à lui, que le recours exclusif à des composants audités pourrait nécessiter l'audit de l'ensemble des logiciels

[12] Ou *bounty reward*. Mécanisme visant à faire tester un programme informatique par une communauté de développeurs et d'utilisateurs avertis, en offrant des récompenses à ceux qui parviennent à en révéler les défauts de conception ou les vulnérabilités.

de la blockchain ou des tokens compatibles avec la machine virtuelle Ethereum, ce qui lui semble hors de portée.

S'agissant ensuite de l'interaction avec les ***smart contracts* non certifiés**, de nombreux participants à la consultation plaident pour que celle-ci soit seulement découragée[13]. Un répondant propose ainsi que les institutions financières supervisées ne puissent interagir avec un tel *smart contract*, mais que les autres entités le puissent. L'idée sous-jacente est que la moindre liquidité qui en résulterait constituerait une incitation à la certification.

D'autres **difficultés pratiques** sont évoquées. Ainsi en est-il, par exemple, de la difficulté de définir un changement significatif du code en pratique, ou encore du risque qu'une exigence de certification renouvelée après un tel changement ne décourage les développeurs de mettre à jour les *smart contracts*. Un autre répondant observe qu'un *smart contract* peut être utilisé d'une manière que les créateurs n'avaient pas anticipée, à moins que des restrictions n'aient été incluses dans le code informatique.

Certaines réponses à la consultation contiennent enfin des suggestions quant à la mise en œuvre ou la surveillance de la certification des *smart contracts*. On mentionnera ainsi l'idée d'exiger un **renouvellement de certification quand une nouvelle vulnérabilité générale** a été détectée[14] et celle de **remonter les vulnérabilités détectées lors des audits et certifications à une autorité centrale**, qui aurait également pour rôle de certifier les certificateurs ou auditeurs, en reconnaissant leur expérience dans le domaine.

Discussion

S'agissant des interactions avec les *smart contracts* non certifiés, des mécanismes de désincitation plutôt que d'interdiction pourraient effectivement aller dans le sens d'une meilleure proportionnalité. Ils poseraient toutefois un problème de principe : si la sécurité, la gouvernance ou le principe même d'un *smart contract* n'étaient pas suffisamment conformes à des normes communément acceptées – empêchant sa certification –, il paraîtrait étrange de n'interdire les interactions qu'à certaines catégories d'acteurs (d'autant plus si les acteurs ainsi préservés sont des professionnels, les particuliers étant laissés sans protection). Au contraire, les dangers d'un tel *smart contract* justifieraient **une interdiction des interactions pour l'ensemble des utilisateurs**.

Le fait qu'un *smart contract* puisse être utilisé d'une manière non prévue par ses créateurs mérite effectivement considération. Cela pourrait conduire, dans une éventuelle réglementation, à demander aux développeurs de *smart contracts* de fournir **un mode d'emploi de leur outil, qui fixerait notamment le périmètre des utilisations considérées comme légitimes**. Les effets éventuellement défavorables d'une telle mesure sur l'innovation devraient naturellement être soigneusement étudiés si une telle piste réglementaire était retenue.

Plus généralement, l'intérêt suscité par la certification des *smart contracts*, la diversité des situations à considérer et la richesse des commentaires reçus montrent que le sujet est loin d'être épuisé et **mériterait des travaux d'analyse complémentaires, en lien avec les professionnels et les experts du secteur**.

---

[13] On peut préciser que la proposition faite concerne uniquement les interactions avec les *smart contracts* non certifiés, pas la production de ces objets ou leur existence.

[14] Cette idée est proche – mais distincte – de l'idée développée dans le document de réflexion d'une certification pour une durée limitée (point *a* de la partie 3-2-2).

3-2-2. Le cas des oracles

Synthèse des réponses

Les participants à la consultation reconnaissent largement le caractère critique de la fourniture de données dans la blockchain, et donc le **rôle crucial joué par les oracles** dans le bon fonctionnement du système. De ce point de vue, un répondant estime que des données de qualité constituent un élément important d'atténuation des risques financiers, ce qui justifie selon lui de **réserver leur fourniture à des entités centralisées spécialisées dans le métier de la donnée**. D'autres répondants plaident au contraire pour des **modèles plus décentralisés**, les seuls à même de garantir, selon eux, que les données fournies soient exemptes de conflits d'intérêts.

Des participants à la consultation contestent d'ailleurs la classification des oracles établie implicitement dans le document de réflexion. Ils estiment en particulier que le modèle d'**oracle décentralisé** qui y est décrit[15] serait plutôt à classer comme oracle centralisé. Ces modèles, comme celui de Chainlink, ne sont décentralisés que dans la mesure où plusieurs entités (souvent sous pseudonymes) participent à la soumission des valeurs. Or, selon ces répondants, de véritables oracles décentralisés seraient plutôt ceux reposant intégralement sur des données accessibles au public, et donc vérifiables de manière indépendante, comme l'oracle *Time Weighted Average Price* (TWAP) d'Uniswap.

En tout état de cause, les répondants reconnaissent que **tous les oracles**, quel que soit leur degré de (dé)centralisation, **peuvent être manipulés** (à un coût variable selon les spécifications de l'outil). Face à ce problème, des répondants mentionnent des tentatives, sur certains protocoles de prêts-emprunts, de fonctionner **sans recours aux oracles**, afin de limiter les risques. Pour l'heure, ce type de modèle ne semble toutefois que peu répandu. D'autres répondants évoquent l'idée de créer des **oracles de service public**, ce qui constitue une piste intéressante. En l'état actuel du fonctionnement de la DeFi, cependant, une majorité des répondants juge opportuns le principe d'une **certification des oracles décentralisés**, d'une part, et d'un **contrôle du fonctionnement de l'ensemble des oracles** d'autre part[16].

3-2-3. Le cas des *stablecoins*

Synthèse des réponses

Le document de réflexion proposait notamment **d'étendre le cadre applicable aux *Electronic money tokens* (EMT) du règlement MiCA à l'ensemble des crypto-actifs ayant pour objectif de répliquer la valeur d'une monnaie officielle**. Ainsi, un jeton se référant à une monnaie officielle, même émis par un protocole décentralisé, aurait à appliquer les exigences de MiCA sur les EMT, en particulier : droit de remboursement à la valeur faciale, et gestion d'une réserve constitué d'actifs liquide libellés dans la même devise. Cette proposition a fait l'objet de **nombreuses réactions**.

Elle est favorablement accueillie par un certain nombre de répondants, qui soulignent que cette approche permettrait de **limiter les risques** identifiés dans le document de réflexion (potentiel de déstabiliser de nombreuses applications DeFi et vecteur potentiel de transmission des chocs de

[15] Typiquement : plusieurs parties ou nœuds proposent une valeur actualisée du cours du bitcoin, et la médiane des valeurs soumises est publiée sur la blockchain, puis utilisée par des *smart contracts.*

[16] Par exemple sur le modèle du règlement européen « Benchmark », comme le proposait le document de réflexion.

l'écosystème DeFi vers la finance traditionnelle) et apporterait de la **clarté juridique**. Un répondant a précisé que le protocole décentralisé à l'origine de l'émission d'un *stablecoin* pourrait inclure dans son code l'information permettant son identification en tant qu'EMT.

D'autres répondants estiment au contraire peu opportun d'étendre le cadre des EMT à tous les *stablecoins*, car ceux émis par des applications décentralisées ont un **fonctionnement fondamentalement différent** : en l'absence d'émetteur centralisé, la réserve repose généralement sur un mécanisme de dépôt de collatéral, éventuellement assorti de mécanismes algorithmiques d'ajustement. Des répondants estiment toutefois que l'émission décentralisée de *stablecoin* pourrait *a minima* requérir un **devoir de conseil** vis-à-vis des utilisateurs, permettant à ces derniers de faire des choix éclairés entre les EMT et les autres crypto-actifs se référant à une monnaie officielle.

Certains répondants formulent une autre proposition : soumettre les *stablecoins* émis par des protocoles décentralisés au **régime des « autres crypto-actifs »** du titre II de MiCA. Cela aboutirait notamment à l'obligation de mettre à disposition des utilisateurs un livre blanc ; cette obligation pèserait sur l'émetteur ou, à défaut, sur l'intermédiaire permettant l'acquisition de ce type de *stablecoin*.

Discussion

Ces propositions alternatives **ne résolvent pas la question de la promesse de stabilité et de sécurité faite aux utilisateurs** par les émetteurs d'un *stablecoin*, fût-il décentralisé. En outre, elles pourraient créer une difficulté, pour les utilisateurs, à **distinguer les vrais jetons de monnaie électronique régis par MiCA d'autres crypto-actifs moins sûrs**.

3-3. Règlementer la fourniture et l'accès aux services

3-3-1. La recentralisation potentielle de certaines activités

Synthèse des réponses

Certains répondants se montrent favorables à l'idée d'une recentralisation obligatoire des activités dans certains cas : il est par exemple proposé de recentraliser les protocoles DeFi dès lors que ceux-ci se livrent à des activités financières régulées de finance traditionnelle, et ce afin d'assurer des conditions de concurrence équitables. Toutefois, dans leur grande majorité, les répondants se montrent réservés sur la possibilité de recentraliser certaines activités, au nom du respect de la gouvernance décentralisée des protocoles DeFi. Beaucoup estiment qu'une sécurité accrue passe par **davantage de décentralisation**, et non par des éléments de centralisation, en cohérence avec leur évaluation du risque (*cf. supra*).

Discussion

Il existe au moins deux situations dans lesquelles les formes actuelles prises par nombre de protocoles de DeFi posent des difficultés excessives : **l'engagement de la responsabilité**, civile ou pénale, notamment à l'égard des utilisateurs ; le **besoin d'interactions, ponctuelles ou régulières, avec des autorités publiques**, par exemple les superviseurs financiers. Ces deux situations nécessitent, selon les cas, **de disposer d'une organisation constituée ou de représentants désignés**.

Sans préjudice des propositions que pourra faire le Haut Comité Juridique de la Place financière de Paris (HCJP) en la matière[17], il paraît théoriquement possible de trouver une **voie moyenne**, puisque les exigences d'organisation ou de représentation n'entrent pas nécessairement en contradiction absolue avec la volonté d'un fonctionnement largement décentralisé. Ainsi, les décisions d'administration d'un protocole peuvent se prendre à l'issue de votes de la communauté (sans domination ou influence excessive d'un individu ou d'un groupe d'individus), mais ce protocole peut dans le même temps disposer de statuts ou de représentants. Selon les territoires concernés, les statuts à appliquer pourraient déjà exister, ou être créés pour l'occasion.

3-3-2. La réglementation des points d'accès

Synthèse des réponses

Le **principe d'une réglementation des points d'accès**, notamment en vue de protéger les utilisateurs, **fait l'objet d'un très net consensus** parmi les participants à la consultation. Cette ample approbation recouvre cependant des opinions divergentes quant au rôle joué par cette mesure au sein du dispositif d'ensemble : pour certains répondants, la réglementation des points d'accès constitue un élément certes nécessaire mais aussi suffisant, qui doit conduire à s'abstenir de toute autre forme d'encadrement de la DeFi.

Si le principe d'une réglementation est largement admis**,** l'idée d'un régime réglementaire s'appliquant à **l'ensemble des intermédiaires**, éventuellement au moyen d'une extension des obligations du règlement MiCA (partie 3-3-2 du document de réflexion), est majoritairement rejetée par les répondants. Le détail des réponses montre cependant que la proposition avancée dans le document de réflexion manquait sans doute de clarté (*cf. infra*).

Le document de réflexion suggérait également de **conditionner la distribution de certains produits** à la démonstration par les clients de leurs **aptitudes financières**. Cette proposition fait l'objet de quelques critiques. Pour certains répondants, l'essentiel serait de fournir une information transparente afin de laisser toute liberté de choix à l'utilisateur. Cette opinion se double parfois d'une critique des dispositifs européens existant dans la finance traditionnelle : il n'existerait pas de bonne manière de tester la compréhension de la clientèle, et la réglementation aboutirait à une exclusion *de facto* des épargnants les moins aisés.

Discussion

S'agissant d'abord d'un régime commun à tous les intermédiaires, l'idée avancée dans le document de réflexion n'était pas d'introduire exactement les mêmes obligations pour l'ensemble des points de contact permettant l'interaction des utilisateurs avec les protocoles de DeFi. Il était plutôt proposé d'établir un **régime de protection minimal des utilisateurs basé sur la nature du service fourni et non sur le type d'entité qui le fournit** (entités centralisées, simples *front-ends* des applications décentralisées etc.). Certains mécanismes de protection du consommateur applicables aux intermédiaires centralisés pourraient ainsi être étendus aux points d'accès décentralisés, avec au besoin certaines adaptations techniques.

[17] Le HCJP a été saisi, en 2022, d'une réflexion sur les questions que pose la DeFi en droit français. Celle-ci portera notamment sur le statut juridique des DAO.

S’agissant ensuite de conditionner la distribution de produits à la démonstration des aptitudes financières des clients, le document de réflexion rappelait des principes de protection de la clientèle généralement appliqués dans le secteur financier en Europe. De ce point de vue, les réponses reçues lors de la consultation **ne paraissent pas démontrer en quoi, pour des services comparables à ceux de la finance traditionnelle, la DeFi présenterait une spécificité justifiant l’élaboration de principes de protection entièrement différents**.