Finance « décentralisée » ou « désintermédiée » : quelle réponse réglementaire ?

(Avril 2023)

Questionnaire de consultation

Ce document reprend la liste des questions du document de réflexion soumis à consultation publique *Finance « décentralisée » ou « désintermédiée » : quelle réponse réglementaire ?*

Les réponses sont à envoyer à l'adresse fintech-innovation@acpr.banque-france.fr **avant le 19 mai 2023.**

Partie 1 du document – La *DeFi* : définition, cas d'usage et structure schématique

Q1 : Avez-vous des commentaires sur la définition de la *DeFi* retenue dans le document ? Le document rend-il correctement compte du niveau effectif de décentralisation des services ?

La définition requiert des connaissances minimales pour appréhender la famille de ces services. Les services sont uniquement digitaux (pas de réseau de distribution physique), nativement mondiaux. C'est un écosystème en rapide évolution du fait, entre autres, de sa construction en mode open source.

Q2 : À vos yeux, quels cas d'usage de la *DeFi* sont appelés à se développer à l'avenir ? Peuvent-ils servir l'économie réelle ?

La liste des cas d'usage pourrait être généralisée, les cas d'usages pouvant se développer dans tous les métiers de contrats financiers (assurance, financement etc.).

L'utilisation de la DeFi en assurance va se développer : échanges entre acteurs de l'éco-système (par exemple assureurs / réassureurs) ; besoin de couvertures assurantielles pour les acteurs de la DeFi (RC pro, vol, cyber), nouvelle classe d'actif pour les assureurs ; nouveaux produits pour les assurés (paramétrique) ; déploiement des processus de gestion des contrats d'assurance actuels ; assurance décentralisée, paramétrique ou non (via des DAO ?). La DeFi pourrait permettre de développer de nouveaux produits d'assurance basés sur la blockchain. Les primes d'assurance pourraient également être payées en cryptomonnaies, ce qui faciliterait les paiements transfrontaliers.

Dans le domaine financier, les entreprises pourraient utiliser la DeFi pour financer leurs opérations / investissements, une entreprise pourrait par exemple émettre des obligations sur une blockchain publique et les vendre directement aux investisseurs DeFi, sans avoir besoin de passer par le marché traditionnel. D'autres cas d'usage sont appelés à se développer à l'avenir : staking, tokénisation de l'immobilier, etc.

La DeFi est un outil qui sert déjà l'économie réelle, à une échelle modeste qui va toutefois se développer.

Q3 : Que pensez-vous des phénomènes de concentration décrits dans la partie 1-5 du document ?

La DeFi est un domaine émergent, ce qui se mesure par le faible nombre d'utilisateur, et les changements peuvent venir rapidement. De nouvelles blockchains innovantes et de nouvelles applications peuvent émerger et attirer rapidement les utilisateurs, anciens ou nouveaux, et des investisseurs, ce qui peut réduire le niveau de concentration existant.

La concentration peut aussi être vue comme un élément positif, susceptible de susciter la confiance des utilisateurs (anciens ou nouveaux) et celle des investisseurs qui auront plus de facilité à financer des projets DeFi déjà connus et réputés. L'augmentation de la liquidité, de la sécurité et de la durabilité des projets peut bénéficier à l'ensemble de l'écosystème DeFi. Les autres projets pourraient en parallèle se développer et bénéficier de cette tendance haussière du nombre d'utilisateurs pour se faire connaître. La concentration peut également contribuer à réduire le risque de fragmentation de l'écosystème DeFi (qui est encore fragile actuellement au vu du nombre d'utilisateur), ce qui peut faciliter la collaboration entre les différents projets et améliorer l'interopérabilité entre les blockchains et les applications DeFi.

Q4 : Avez-vous des commentaires à formuler ou des compléments à apporter sur la présentation schématique de la *DeFi* figurant en partie 1-6 ?

Non

Partie 2 du document – Les risques liés à la *DeFi*

Q5 : Avez-vous des remarques sur la description des risques liés à la gouvernance décentralisée (partie 2-1 du document) ?

Non, pour la description théorique des risques. Il manque toutefois un éclairage sur la dynamique temporelle (l'âge des protocoles et l'évolution de la décentralisation avec le temps) ainsi que sur la transparence nécessaire à l'appréciation des risques.

Q6 : Pensez-vous que les solutions de *layer 1* peuvent accroître les problèmes de sécurité de l'infrastructure blockchain ? Et pour les solutions de *layer 2* ? Selon vous, existe-t-il de ce point de vue d'importantes différences selon les solutions de *layer 2* considérées ?

Q7 : L'utilisation de *rollups* ou de solutions similaires est-elle selon vous de nature à réduire la transparence de l'information pour un observateur ?

Q8 : Avez-vous des remarques quant à la description des risques liés à la couche applicative de la *DeFi* (partie 2-3) ?

Le caractère public des smart contracts peut rendre ces derniers plus vulnérables aux attaques, mais ce point reste discutable. Car le caractère public permet à la fois une plus grande transparence et la mise en œuvre d'une plus grande responsabilité des développeurs de smart contracts, grâce à des audits avant déploiement. La qualité et la fiabilité des données (internes ou externes via les oracles) sont également essentielles. Il faut sans doute y ajouter une dimension de sécurité temporelle : la garantie d'un fonctionnement en temps long nécessaire à l'assurance (mutualisation temporelle) vs le temps court en finance.

Q9 : Avez-vous des commentaires à formuler au sujet du recensement des risques de la *DeFi* pour la clientèle particulière (partie 2-4-1) ?

Q10 : Avez-vous des remarques ou des compléments à apporter sur la description (partie 2-4-2) des fragilités systémiques de l'écosystème *DeFi* (endogénéité des placements, importants effets de levier, rôle des mécanismes de liquidation automatisée des positions) ?

Q11 : Êtes-vous d'accord avec la proposition s'agissant de la réglementation à appliquer aux *stablecoins* émis par des protocoles *DeFi* ? (*Cf.* partie 2-4-3 : « *dès lors qu'un service décentralisé prétend créer ou utiliser un crypto-actif ayant pour référence une monnaie officielle, ce crypto-actif doit obligatoirement être un EMT au sens de MiCA (ou un actif équivalent)* »)

☐Oui

☐Non

Pour quelles raisons ?

Q12 : Avez-vous des remarques à formuler quant à la description des risques que la *DeFi* peut faire peser dans la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) (partie 2-4-4) ?

Q13 : Voyez-vous d'autres risques à prendre en considération, qui ne seraient pas évoqués (ou insuffisamment) dans le document ?

Il manque la mention de risques lié aux actions étatiques : les évolutions réglementaires divergentes suivant les zones régionales et l'effet extraterritorial de certaines d'entre elles ; les évolutions techniques, en particulier le risque de séparation d'une partie des nœuds suite à un contrôle régional d'internet (assimilable à un fork). Manque également la mention du risque temporel lié à la durabilité / stabilité des dispositifs, nécessaire à la mutualisation temporelle des risques et à leur assurabilité.

Partie 3 du document – Les pistes d'encadrement réglementaire

Partie 3-1 – Assurer une sécurité minimale de l'infrastructure

Q14 : Les blockchains publiques devraient-elles faire l'objet d'un encadrement ou de standards minimaux de sécurité (cf. partie 3-1, schéma de régulation A) ?

☒Oui

☒Non

Si oui, de quelle façon ? Sinon, pourquoi ?

Oui, pour apporter de la confiance aux utilisateurs, sous réserve de ne pas brider l'innovation et de conserver un "level playing field"
Non, les blockchains publiques bénéficient déjà de l'auto-régulation par les acteurs du marché. La régulation pourrait limiter les possibilités technologiques en termes d'innovation. Il est préférable que la réglementation vise à améliorer la transparence des informations transmises par les acteurs spécialisés pour favoriser l'auto-régulation.

De plus, imposer des normes de sécurité strictes favorise la concentration et créé un environnement où seuls les grands acteurs avec des ressources importantes sont en mesure de se conformer.

Q15 : Les autorités publiques devraient-elles superviser la concentration des capacités de validation sur les blockchains publiques ? Si oui, par le biais de quelles actions ?

☐Surveiller la concentration en temps réel

☐Fixer des plafonds à cette concentration

☐Communiquer publiquement en cas de dépassement de certains seuils de concentration

☐Engager d'autres actions (préciser lesquelles)

Q16 : Partagez-vous l'analyse qui est faite dans le document quant aux avantages et inconvénients des blockchains privées (partie 3-1, schéma de régulation B) ? Les blockchains privées opérées par des opérateurs privés devraient-elles, le cas échéant, être soumises à un cadre de surveillance ?

☐Oui

☐Non

Pourquoi ?

Q17 : Des acteurs publics devraient-ils gérer directement les blockchains servant d'infrastructure à la *DeFi* ?

☐Oui

☐Non

Pourquoi ?

Q18 : Avez-vous d'autres pistes de réglementation à proposer dans le but d'assurer une sécurité minimale de l'infrastructure blockchain ?

☒Oui

☐Non

Si oui, lesquelles ?

L'incitation à un audit et à une certification des protocoles par un service indépendant, avec communication publique des résultats et mise en place d'un stress test régulier pour prévenir les attaques.

Ou aller plus loin en proposant un nouveau standard de reporting, de gouvernance et d'audit qui pèserait sur les blockchain/les protocoles, avec un principe de proportionnalité.

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

Q19 : Un mécanisme de certification constitue-t-il une solution efficace pour définir un périmètre de *smart contracts* « sûrs » (pour un état donné des connaissances) ? Des solutions alternatives permettraient-elles d'aboutir au même résultat ?

A court terme non, car il existe un ensemble d'indicateurs utiles avant certification : âge du code, nombre de contrats l'utilisant, nombre d'audit existant sur ce code. A moyen terme oui : l'utilisation de frameworks de développement (bibliothèques de code sécurisé, outils de vérification automatique, modèles de conception et des normes de codage, entre autres), mise en place de protocoles de gestion des mises à jour et des vulnérabilités, création de registres publics de smart contracts audités et validés. Le nom des auditeurs et validateurs devenant alors public, leur historique permettrait d'apprécier leur niveau de fiabilité. La certification est indispensable pour convaincre les assureurs et autres acteurs réglementés de s'appuyer sur la DeFi pour déployer de nouveaux services / produits

Q20 : Partagez-vous la description qui est faite (partie 3-2-1) des différentes techniques d'audit du code informatique des automates exécuteurs de clauses (*smart contracts)*, y compris de leurs avantages et de leurs inconvénients respectifs ?

Il faut rajouter que l'audit doit être régulier car de nouvelles stratégies d'attaque sont découvertes régulièrement. D'autre part, le mécanisme de preuve formelle doit être uniquement un outil parmi d'autres pour l'auditeur. Un élément d'analyse supplémentaire est de savoir si le langage intègre nativement des mécanismes de protection des transactions (langage orienté ressource, par exemple Cadence par le protocole flow). Il faut être vigilant sur le risque de concentration des ressources d'audit / certification sur un marché de petite taille.

Q21 : Identifiez-vous des exemples de *smart contracts* qui ne devraient pas pouvoir être certifiés du fait de la nature même des services qu'ils rendent ?

☐Oui

☒Non

Si oui, lesquels ?

Q22 : Que pensez-vous des règles proposées dans le document (partie 3-2-2, point a) quant à la manière de certifier les *smart contracts* (certification préalable des composants appelés, cycle de vie de la certification) ?

Q23 : Les *smart contracts* devraient-ils embarquer dans leur code un certain nombre d'exigences réglementaires à l'avenir ?

☐Oui

☐Non

Pourquoi ?

C'est illusoire car la réglementation est évolutive et souvent régionale

Q24 : Qui devrait établir les standards de sécurité des *smart contracts* (cf. partie 3-2-2, point b) et pourquoi ?

Nous considérons que les standards de sécurité et leurs évolutions devraient être définis et établis sur la base de la consultation d'une communauté réunissant les producteurs, les utilisateurs et le régulateur. Ces standards doivent être intégrés ultérieurement dans la communication publique entourant la mise à disposition de chaque produit.

Q25 : L'interaction avec des *smart contracts* non certifiés devrait-elle être découragée ou interdite (cf. partie 3-2-2, point c) ?

☒Découragée

☐Interdite

☐Ni découragée ni interdite

Pourquoi ?

Découragée mais pas interdite. Nous considérons qu'il ne faut pas empêcher des utilisateurs avertis de continuer à utiliser des smart contracts non-certifiés afin de laisser plus de possibilités à l'innovation.

Q26 : Qui devrait supporter le coût de la certification des *smart contracts* (cf. partie 3-2-2, point d) et pourquoi ?

Q27 : Avez-vous des remarques quant à la description des risques inhérents au modèle des oracles décentralisés ? Ces risques peuvent-ils être limités par un système de certification adapté aux spécificités de ces applications (cf. partie 3-2-3) ? Avez-vous des remarques ou des propositions alternatives d'encadrement de l'activité des oracles ?

L'oracle est un élement clé pour la confiance dans l'éco-système. Il y une grande diversité dans la technologie des oracles, au-delà de celle décrite par l'ACPR. Par exemple des projets concurents de Chainlink proposent des solutions d'oracles à étudier, comme Oraichain qui propose un oracle appuyé par une technologie d'intelligence artificielle. Les risques pourraient en effet varier selon la technologie et mode de fonctionnement proposé. Il serait préférable de ne pas imposer de réglementation universelle mais la communication d'indicateurs standardisés sur les oracles (âge de l'organisation, nombre d'utilisateurs, structure de gouvernance...)

Q28 : Avez-vous d'autres pistes de réglementation à proposer en vue de réduire les risques liés à la couche applicative de la *DeFi* ?

☐Oui

☒Non

Si oui, lesquelles ?

Partie 3-3 – L'encadrement de la fourniture et de l'accès aux services

Q29 : Pensez-vous qu'il puisse dans certains cas être nécessaire de « recentraliser » certaines activités sensibles (partie 3-3-1) ?

☐Oui

☐Non

Si oui, lesquelles ? Si non, pourquoi ?

Q30 : Que pensez-vous des propositions formulées quant aux manières d'atteindre cet objectif (obligations de se constituer en société, assujettissement des acteurs exerçant un contrôle effectif, statut juridique pour les DAO) ? Avez-vous des suggestions à faire sur le statut juridique à conférer aux DAO ?

Q31 : Partagez-vous la description des risques liés à la « *CeDeFi* », d'une part, et aux « conglomérats crypto » d'autre part (encadré 6) ?

Q32 : Quelles exigences devraient s'appliquer aux intermédiaires facilitant l'accès à la *DeFi* ?

☐Des obligations d'information

☐Des obligations de conseils et de vigilance

☐Des exigences concernant la publication de livre blanc

☐Des exigences de KYC

☐Un cadre complet inspiré de MiCA

☐Autre

Pourquoi ?

Q33 : Faudrait-il appliquer les mêmes règles à l'ensemble des intermédiaires de la *DeFi* (y compris, le cas échéant, à des interfaces web décentralisées) ?

☐Oui

☐Non

Pourquoi ?

Q34 : L'accès aux produits financiers doit-il être conditionné aux compétences financières des clients et à leur appétence au risque ?

☐Oui

☐Non

Pourquoi ?

Q35 : Avez-vous d'autres pistes de réglementation à proposer concernant l'encadrement de la fourniture et de l'accès aux services ?

☐Oui

☐Non

Si oui, lesquelles ?

Pistes de réglementation – aspects transversaux

Q36 : Comment tenir compte des impératifs de proportionnalité (pour les acteurs de taille modeste) dans les différentes pistes réglementaires avancées par le document (ou proposées par vos soins) ?

La proportionnalité est, à notre avis, complexe à mettre en place au niveau opérationnel : définition difficile d'indicateurs quantitatifs pour établir des seuils, volatilité des volumes pour les nouveaux acteurs, activité nativement internationale.

Q37 : Quelles pistes de réglementation – qu'elles soient ou non proposées dans le document – pourraient permettre de surmonter les problèmes liés à la possible extra-territorialité des acteurs (d'un point de vue national ou européen) ?

Il est nécessaire de traiter le sujet de l'extraterritorialité pour éviter d'en faire un frein au développement de la DeFi. Par exemple en faisant évoluer le mandat des instances internationales pour englober ce sujet ou en remplaçant la dimension territoriale par la mise en responsabilité personnelle des détenteurs de tokens de gouvernance (pas d'anonymisation, mise en garantie du patrimoine des individus). Un principe général à considérer nous semble être la mise en place d'un cadre de gestion du risque des produits DeFi : un service devant respecter un certain nombre de critères : la réplicabilité des opérations, la neutralité des opérations et l'absence d'intervention sur le cours de transaction. La réglementation doit se concentrer sur les aspects de gouvernance et d'administration des services DeFi qui pourraient être dévoyés et en conséquence compromettre ces services.

Q38 : Qui devrait, dans chaque cas, contrôler la mise en œuvre des différentes pistes réglementaires (qu'elles soient avancées dans ce document ou proposées par vos soins) ? Avec quels moyens ?

Les actuaires, pour l'évaluation des risques (engagement, volatilité, gouvernance). Les pouvoirs publics, pour le contrôle des individus détenteurs des token de gouvernance.

Certains risques nous paraissent toutefois impossibles à mesurer et à transférer.