Paris, 2 juin 2023

Finance décentralisée : réponse à la consultation de l'ACPR proposée par le groupe de travail de Paris Europlace

Paris Europlace fédère et représente la diversité des acteurs, français et internationaux, actifs sur la Place de Paris : émetteurs, investisseurs, intermédiaires financiers et professions auxiliaires. Son action vise à renforcer la compétitivité et l'attractivité de la Place, afin de contribuer au bon financement de l'économie.

Le groupe de travail dont la composition figure en annexe, constitué par Paris Europlace pour répondre aux questions de la consultation publique lancée par l'ACPR sur la finance décentralisée (DeFi)[1], salue cette initiative qui permet d'associer plus étroitement les professionnels de la Place à l'identification des opportunités et des défis que posent de telles innovations technologiques. Les réponses proposées par ce groupe de travail sur la DeFi sont regroupées ci-après en trois blocs : définitions, risques et orientations réglementaires envisageables.

1. La DeFi : définition, cas d'usage et structure schématique

La définition proposée à la question 1 par le document de l'ACPR reflète les caractéristiques fondamentales de la DeFi, qui combine décentralisation et désintermédiation : la gestion d'un dispositif informatique via une organisation reposant sur une base collective et s'exprimant au moyen de votes à travers la recherche d'un consensus.

En revanche, le caractère automatisé de certains aspects de la DeFi, notamment les *smart contracts*, semble moins participer de sa définition même, reflétant plutôt les caractéristiques qu'offre la technologie des dispositifs d'enregistrement électronique partagés.

Cet exercice de définition reste pourtant délicat eu égard (i) à l'hétérogénéité des protocoles utilisés et des règles régissant le fonctionnement de ces dispositifs et (ii) à l'évolution qui fait apparaître de nouveaux modèles et technologies, qui ne peuvent être anticipés et dont on ne

[1] https://acpr.banque-france.fr/finance-decentralisee-ou-desintermediee-quelle-reponse-reglementaire

sait si la définition qui sera retenue les capturera nécessairement. Il n'en reste pas moins que toute définition devra présenter des critères simples et objectifs, permettant de circonscrire précisément le champ d'application de la réglementation qui s'y appliquerait.

En particulier (question 3), on ne peut dire si le phénomène de concentration de l'usage des applications de services de DeFi sur certaines technologies ou dispositifs sera toujours observé, ni s'il s'inversera avec une plus grande maturité du marché. Il n'en reste pas moins que les caractéristiques « d'infrastructure » de certaines technologies peuvent compromettre l'émergence de technologies alternatives si les coûts de développement et d'accès rendent une telle concurrence illusoire. Les modalités de rémunération des validateurs, ou même le coût de l'énergie (ayant une influence sur les règles de consensus notamment), peuvent également avoir une incidence sur le degré de centralisation. Ces aspects ne nous semblent pour autant pas devoir être présumés « contrariants » ou « néfastes » dans la mesure où, à ce jour, les dispositifs les plus partagés semblent, de fait, présenter la plus grande robustesse, de sorte qu'une plus grande décentralisation est *a priori* gage d'une plus grande difficulté à contourner les règles de gouvernance ou de fonctionnement qui auront été établies. On pourra relever enfin qu'un certain niveau de concentration peut être cependant bénéfique pour faire évoluer un protocole rapidement (notamment en cas de découverte d'une erreur de code).

Par ailleurs (question 4), il semble délicat de tenter de réduire la DeFi à des couches d'interfaces ou de fonctionnalités, ou à le faire à partir des interactions plus ou moins directes des utilisateurs, intermédiaires ou finaux, avec telle ou telle couche technologique : en effet, une approche technologiquement neutre de la régulation et de la supervision devrait s'affranchir, dans une grande mesure, de ces particularités ou spécificités. Il reste que la composabilité de ces différents éléments rend plus ardue ne serait-ce que la compréhension des systèmes procurant telle ou telle fonctionnalité, d'autant plus que peuvent se « greffer » des dispositifs plus centralisés. Au total, il convient de mettre en avant la grande évolutivité du secteur, et donc nécessairement de la définition des règles (non pas strictes, mais basées sur des principes directeurs) qui doivent en découler.

2. Les risques liés à la DeFi

Dans son document, l'ACPR propose une description des risques spécifiques à la finance désintermédiée en distinguant schématiquement les trois grandes strates qui la composent :

- l'infrastructure blockchain : une partie des risques posés par la finance désintermédiée sont étroitement liés aux caractéristiques des technologies qui en font aussi l'intérêt. Ainsi, les solutions recherchées pour améliorer les performances des blockchains – leur « passage à l'échelle » – sont aussi celles qui peuvent fragiliser les mécanismes de consensus (solutions de layer 1) ou créer de nouveaux problèmes de sécurité (solutions de layer 2) ;

- la couche applicative des « services » : à ce niveau, la transparence du code informatique, la composabilité des automates exécuteurs de clauses et leur dépendance aux « oracles », qui sont parmi les bénéfices de la finance désintermédiée, sont aussi des facteurs de vulnérabilité ;
- les dispositifs permettant l'accès des utilisateurs à ces services. Cet accès soulève des questions plus traditionnelles pour un régulateur : la grande volatilité des prix, la complexité des produits et leur accès peu ou pas encadré exposent les utilisateurs à des risques élevés de perte en capital et peuvent menacer la stabilité de l'écosystème, à défaut de représenter – à ce jour – une menace pour la stabilité du système financier dans son ensemble.

C'est pourquoi la réglementation de la finance désintermédiée ne peut se borner à répliquer les dispositifs encadrant actuellement la finance dite « traditionnelle ». Ainsi, si les risques liés à la gouvernance sont les plus faciles à identifier du fait de la connaissance des exigences existantes dans la finance traditionnelle, ils ne sont néanmoins pas simples à résoudre. En effet, la gouvernance mise en place par les protocoles est souvent intrinsèquement liée au fonctionnement dudit protocole et de l'intérêt qu'il peut présenter : ainsi, lorsque la gouvernance est essentielle, elle est alors souvent faussement décentralisée pour tenter de conserver au protocole son caractère de DeFi ; et lorsqu'elle apparaît correctement régulée, elle peut en réalité être illusoire, les décisions essentielles étant prises par d'autres instances. Ainsi, promouvoir des règles de gouvernance claires et transparentes ne saurait empêcher les fraudes, mais pourrait permettre de rendre la finance décentralisée moins opaque, sans que cela la transforme en une finance centralisée.

Par ailleurs, concernant les risques liés aux différentes couches d'applicatifs (question 5), se pose la question de l'interopérabilité ascendante ou par bridge/connexion entre blockchains. Le risque est accru en cas de forks, c'est-à-dire de scissions d'une blockchain en deux blockchains. Or, ces risques se situant notamment au niveau des bridges et swaps, les questions de nature technologique qui y sont sous-jacentes n'entrent pas sans difficultés dans le champ de l'analyse juridique et prudentielle qui est celle du régulateur.

Le recours aux rollups (question 7) n'a pas pour objet d'affecter la transparence de la blockchain mais de diminuer le coût d'enregistrement (gas fee) des transactions et de répondre au problème d'engorgement ou de congestion de la blockchain, augmentant ainsi le nombre de transactions. Il convient cependant de s'assurer que les méthodes alternatives de validation/de calcul utilisées en amont de l'enregistrement sur la blockchain n'affectent pas la conformité et l'exactitude des vérifications en ligne avec le code.

S'agissant des questions liées à la liquidation automatisée de positions (question 10), malgré leur effet procyclique potentiellement déstabilisateur pour l'intégrité d'un marché, les risques de liquidité pourraient être contenus si des règles de transparence, de prévisibilité et d'homogénéité de traitement des ordres étaient établies. Il est néanmoins relevé que la résilience des acteurs à cet effet procyclique reste très incertaine.

Juridiquement, les risques peuvent être divisés en deux grandes catégories :

- les risques purement techniques et/ou technologiques, qui engagent nécessairement les responsables du protocole : en effet, l'article 1218 du Code civil (et ses trois éléments cumulatifs d'application : élément revêtant un caractère d'imprévisibilité, d'irrésistibilité et qui échappe au contrôle des personnes concernées) ne saurait jouer, les risques technologiques ne pouvant jamais être imprévisibles, et restent le plus souvent résistibles ; l'enjeu tient à l'opportunité de responsabiliser un programmeur dont le protocole aura été mis à disposition en open source et utilisable par toute personne (logique du « *take it as it is* ») qui pourrait brider l'innovation.
- les risques liés à des prises de décision ou à des erreurs commises, volontairement ou par négligence, qui posent les questions classiques de la mise en œuvre des conditions de la responsabilité civile, la finance décentralisée ne devant pas s'affranchir par principe de sa sujétion aux principes juridiques applicables en la matière. Il conviendrait de s'interroger si les principes UNIDROIT applicables aux actifs digitaux de janvier 2023, en particulier en matière de conservation et de garde d'actifs, ne pourraient pas procurer des pistes de réflexion, même si l'approche fonctionnelle retenue pour leur élaboration appelle une analyse prudente quant à leur incorporation dans tel ou tel système juridique.

En tout état de cause, il est opportun de rappeler que la responsabilité tant civile contractuelle que délictuelle trouverait à s'appliquer en matière de finance décentralisée, et ce dans l'intérêt même des protocoles, en leur assurant une meilleure crédibilité. En effet, des indices de concentration dans le contrôle et/ou de rattachement juridictionnel (par exemple des contrats de travail) pourraient entraîner la requalification en société, rétablissant ainsi un principe de territorialité et de responsabilité. Or, les failles pouvant être potentiellement humaines comme technologiques, il est également crucial à la fois d'éviter la manipulation de données (par exemple en pénalisant la diffusion d'informations erronées) et de veiller à la préservation de bonnes conditions de gouvernance (notamment lorsque les jetons de gouvernance sont concentrés chez quelques acteurs ou lorsque la gestion des clés est déléguée à un acteur lui-même décentralisé).

S'agissant de la gouvernance et des questions qui y sont liées (gestion des conflits d'intérêts ou de position dominante), il est observé que la prise de contrôle d'une structure est d'autant plus aisée que le nombre de validateurs est limité. Afin de contenir ce risque de capture, augmenter le nombre de nœuds et éviter la concentration des nœuds paraissent donc nécessaires. Toutefois, définir un seuil de concentration est complexe, car certains validateurs pourraient se regrouper pour franchir le seuil des 50%.

Enfin, d'autres risques doivent être relevés :

- fraude/vol/perte des accès ;
- existence de barrières à l'entrée ;
- difficulté des blockchains à supporter un nombre élevé de transactions (congestion limitant la scalabilité du fait des coûts de validation) ;
- volatilité des prix, effet de levier (ou pyramide dite de Ponzi) et mécanismes de liquidation automatisée menaçant la stabilité des marchés (sauf existence d'algorithmes d'ajustement des prix) ;
- mauvaise collatéralisation des actifs et/ou réutilisation du collatéral ;
- circulation imparfaite de l'information liée aux *rollups*[2] (non sans analogie avec les travers prêtés aux *subprimes*) ;
- dépendance envers le nombre de mineurs ou la mobilisation d'une communauté (si personne ne vote ou ne propose d'évolutions, le protocole pourrait périmer ou manquer de sécurité).

En ce qui concerne les enjeux de lutte contre le blanchiment et le financement du terrorisme (LCB-FT) (question 12), les risques nous semblent comparables, dans leur manifestation (empilage, pseudonymat, fractionnement, etc.), mais les modalités de remédiation sont en revanche largement tributaires de l'architecture technologique spécifique qui appelle les suggestions suivantes :

- Le caractère automatique de l'exécution des clauses rendrait en principe le dispositif non corruptible. L'audit technique et/ou la preuve de l'expérience devraient démontrer que ces automates exécutent exactement ce qu'ils sont réputés faire (et pas autre chose) de manière absolument étanche (sans porosité avec d'autres sources ou destinations de fonds) ;
- Une vraie décentralisation contribuerait également à rendre le dispositif non corruptible, ou du moins rendrait beaucoup plus difficile son détournement ;
- Le caractère collectif du fonctionnement des *smart contracts* limiterait les circuits fermés (fonctionnement exclusif entre deux acteurs qui se choisissent). Il devrait également diluer l'intérêt de transactions économiquement non justifiées ;
- Une capitalisation importante du jeton de gouvernance d'une DAO devrait limiter de fait la concentration de la gouvernance en la mettant hors de portée d'un individu ou d'une personne morale de droit privé ;
- La surveillance de l'historique des actifs sur blockchain ne devrait pas s'appréhender en nombre de « rebonds » - pratique actuellement généralisée dans la finance centralisée (CeFi) – mais en durée de temps écoulée. Il est très facile d'empiler des rebonds transactionnels pour s'éloigner artificiellement de l'origine des fonds. L'audit

[2] Un rollup exécute les transactions passées sur son réseau, « enroule » ces transactions en une seule opération et compresse l'information, en envoyant uniquement les données strictement nécessaires à la vérification des transactions et la mise à jour de l'état des données sur la blockchain.

sur une durée de temps écoulé serait plus de nature à freiner et à entraver les circuits de blanchiment ;

- La surveillance de l'historique de circulation des actifs doit être proportionnée à la taille des capitaux, tout en veillant à empiler tous les petits mouvements convergeant vers la même destination. En raison du pseudonymat, des capitaux importants pourraient rester longtemps dispersées entre une multitude d'adresses, mais il faudra bien les regrouper un jour pour les employer dans le monde réel ;
- Les DAO doivent être analysées et évaluées quant à leur caractère réellement décentralisé et supranational. Il faut également tenir compte d'un cycle progressif de décentralisation souvent observé. La réalité n'est pas binaire ;
- Les fonds déposés en CeFi en provenance de la DeFi (blockchains publiques) devraient normalement être justifiés par leur historique de circulation disponible sur les blockchains en remontant soit jusqu'à la création monétaire (récompense de bloc, *yield* ou *airdrop*), soit jusqu'à leur point d'entrée dans la DeFi (origine antérieure des fonds)
- En cas de dispositif d'anonymat renforcé détecté dans l'historique récent, des éléments probants sur l'origine des fonds seraient demandés au déposant. En leur absence, une déclaration de soupçon serait émise par l'acteur centralisé ;
- Les récompenses de bloc (création monétaire) issues du minage ou du *staking* ne posent pas de difficulté du point de vue LCB-FT tant qu'elles sont traçables jusqu'à l'origine sans mélange avec d'autres origines de fonds.

Enfin, les acteurs centralisés auraient besoin de principes d'application sectorielle permettant d'encadrer les interactions avec la DeFi en fonction des différentes configurations pouvant se présenter.

Sur un autre sujet (question 13), les enjeux liés au traitement des données personnelles appelleraient certainement des clarification quant aux conditions d'application de RGPD, même si cela relève d'autres autorités que l'ACPR.

3. Les pistes d'encadrement réglementaire

(Question 14) Il est noté, en premier lieu, que l'autorégulation peut sembler présenter quelque efficacité en matière de DeFi : plusieurs blockchains fonctionnent parce qu'elles sont largement utilisées (et parce que les détenteurs de tokens de gouvernance participent aux votes), donc survivent, tandis que d'autres, devenant obsolescentes dans leurs fonctionnalités et/ou des erreurs de code non corrigées, peuvent être naturellement abandonnées, faute d'évoluer. Il n'en reste pas moins que le degré de décentralisation d'une blockchain amène dans le même temps celle-ci à être moins apte à valider de très nombreuses opérations (scalabilité).

Sans soutenir une approche totalement libertaire, qui laisse chaque utilisateur responsable des décisions qu'il aura prises, le groupe de travail a débattu de l'idée, quoique complexe à mettre en œuvre, d'un scoring de risques, invitant les utilisateurs à exercer un nécessaire et minimum devoir de vigilance. Toutefois, la difficulté réside aussi dans l'explicabilité de ce qui est programmé et de la prévisibilité du résultat qui en découle, car l'utilisateur non expert est souvent contraint de faire confiance à des programmations. Un enjeu pour le régulateur est donc de bien comprendre le cheminement des calculs et de pouvoir vérifier l'exactitude du résultat obtenu par rapport à celui attendu.

A noter également que des acteurs privés peuvent mettre en œuvre des logiques de permissionnement qui, via des *smart contracts*, utilisent in fine des blockchains publiques (tel le modèle CAST de SG Forge[3]).

(Questions 19 et 20) Certes, en principe, un *smart contract* est auditable et certifiable, mais les difficultés résident dans la nature des méthodes de certification, qui permettent de s'assurer que le *smart contract* répond au fonctionnement attendu, mais ne prémunissent pas nécessairement contre des usages non attendus ou détournés. Sur ce point, outre la question de la répartition du coût de la certification, se pose également celle de la composabilité des *smart contracts*, qui ajoute un degré de complexité supplémentaire quant à leur auditabilité. En effet, un processus d'audit ou de certification ne pourra jamais équivaloir à une garantie absolue de pare-feu, certaines erreurs de codage étant par exemple très difficiles à déceler (alors que la transparence de la blockchain donne parfois un faux sentiment de sécurité). Cela renforce l'idée que la décentralisation des blockchain est en principe un gage de sécurité, même si la scalabilité s'en trouve alors réduite.

La certification par un tiers supposerait par ailleurs de déterminer le modèle économique attribuant la charge de cette certification et d'assurer l'indépendance de celle-ci. Par construction, la DeFi repose sur l'autonomie des acteurs et donc sur leur responsabilité individuelle. Se poserait également la question des impacts de l'évolution du code sur une validation préalablement établie (à partir de quel degré ou nature de modification la certification deviendrait obsolète et devrait être réitérée ?). On pourrait toutefois imaginer une solution hybride conduisant à laisser les créateurs de *smart contracts* le soin d'indiquer l'absence de certification ou au contraire l'existence d'une telle certification, la communauté décidant, par l'usage plus ou moins important dudit *smart contract*, si ladite certification apporte effectivement un confort supplémentaire en termes de sécurité et de prédictibilité.

C'est pourquoi, d'une façon générale, le groupe de travail estime qu'il importe que, par construction, la DeFi fasse l'objet d'une régulation aussi flexible et évolutive que possible. Plutôt que des règles trop figées, donc susceptibles de paraître rapidement obsolètes aux yeux des acteurs concernés et qui brideraient son développement, la DeFi appelle la mise en place de principes directeurs ouverts et souples, adaptés aux enseignements que les cas d'usage de

[3] CAST Framework | Bridging the gap between Capital Markets and Digital Assets (cast-framework.com)

la profession ne manqueront pas de révéler à la communauté des utilisateurs et aux autorités, mais aussi appropriés compte tenu notamment des évolutions observées dans d'autres juridictions.

Pour autant, solliciter très largement la communauté des utilisateurs de la DeFi peut prendre de nombreuses modalités, applicables en particulier pour optimiser le codage d'un *smart contract* ou dans le bon déploiement d'un protocole DAO : promotion d'une multi-signature ou d'un vote (éventuellement renforcé par des règles de quorum), pénalisation de la désinformation (i.e. rétribution en cas d'identification de *fake news*), incitations à la création d'un forum ou d'équipes de *risk assessment*, incitation également à l'analyse et la détection de failles dans le codage contre rétribution (*bug bounty*), obligation d'une publication d'informations (*disclosure*) lorsque existent des jeux de délégations ou des pools de gouvernance (assimilables à une action de concert en droit des sociétés) non aisément détectables, etc.

A cet égard, non seulement le principe de l'open source devrait inspirer tout projet de régulation à venir, mais les autorités, par ailleurs confrontées à l'enjeu de recruter en leur sein des spécialistes, devront savoir précisément distinguer, d'une part, les services réellement essentiels qui recueilleront leur attention (comme dans la régulation des PSAN), et, d'autre part, les produits technologiques qui en dérivent (de type *wallet providers*), qui ne devraient donc pas être soumis aux mêmes obligations.

Ainsi, parmi les objectifs essentiels qui pourrait devoir inspirer la régulation, figurent la protection de l'investisseur non professionnel, l'intégrité et la stabilité des marchés, mais également la lutte contre le blanchiment et le financement du terrorisme (en levant le pseudonymat et/ou en traçant l'origine des capitaux, mais non sans difficultés lorsque des portefeuilles privés ne sont pas intermédiés par un PSAN). De ce fait, les blockchains créées pour proposer des services financiers devraient faire l'objet de standards harmonisés, en raison des problématiques d'extra-territorialité, à un niveau au moins européen (ESMA et EBA) et en s'inspirant de MiCA, de MiFID2 (pour apprécier les compétences financières et l'appétence au risque de l'utilisateur) et de DORA. Si cette inspiration ne doit pas brider l'innovation dans l'approche régulatrice et de supervision, une certaine cohérence et le respect du principe « *same activities, same risks, same rules* » doivent cependant être observés.

Annexe

Composition du groupe de travail

Le groupe de travail, créé au sein de Paris Europlace pour répondre à cette consultation publique en lien avec le comité Finance numérique et cas d'usage, inclut, sous la coordination de Philippe Goutay (Jones Day), les contributeurs suivants[4] :

- Annabelle Bernal (Société Générale Forge)
- Stéphane Blemus (Société Générale Forge)
- Myriam Dana-Thomae (AFG)
- Mia Dassas (Allen & Overy)
- Marianne Demarchi (Swift)
- Hubert de Vauplane (Kramer Levin)
- Jean-Marc Eyssautier (Valparaiso Conseil)
- Muriel Faure (AFG, Tiepolo)
- Delphine Marchand (Allen & Overy)
- Sylvain Prigent (Société Générale Forge)
- Marc Ripault (PwC)
- Olivier Taille (Natixis)
- Olivier Vigna (Paris Europlace)
- Jérémie Vuillquez (La Française)

[4] Les positions exprimées par ces contributeurs ne reflètent pas nécessairement celles de leur institution de rattachement, de la même façon que les réponses du groupe de travail de Paris Europlace ne correspondent pas nécessairement aux vues de l'ensemble des membres de l'association.