2 JUIN 2023

Réponse AFG à la Consultation ACPR sur la DeFi

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

AFG

L'AFG fédère les professionnels de la gestion d'actifs depuis 60 ans, au service des acteurs de l'épargne et de l'économie. Elle est la voix collective de ses membres, les sociétés de gestion de portefeuille, entrepreneuriales ou filiales de groupes bancaires ou d'assurance, français et étrangers. En France, la gestion d'actifs c'est 700 sociétés de gestion, pour 4 600 Mds € d'actifs sous gestion et 85 000 emplois dont 26 000 propres aux SGP.

L'AFG se mobilise pour la gestion d'actifs et sa croissance. Elle définit des positions communes, qu'elle porte et défend auprès des pouvoirs publics, contribue à l'émergence de solutions bénéfiques à tous les acteurs de son écosystème et s'engage dans l'intérêt de tous à favoriser le rayonnement de l'industrie, en France en Europe et au-delà. Elle s'investit pour l'avenir.

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

L'AFG remercie l'ACPR d'associer les professionnels de l'écosystème à ses réflexions sur la DeFi. La qualité pédagogique du document proposé par l'ACPR a permis de mieux comprendre les enjeux de cette consultation et de guider efficacement ses membres dans leurs réponses.

L'AFG soutient notamment l'idée d'une réglementation souple et évolutive fondée sur le principe de l'open source en distinguant les services rendus (par les PSAN par exemple) et les produits technologiques qui en découlent (les *wallet providers* par exemple), ces derniers ne devant pas être soumis aux mêmes obligations.

Celle-ci devra poursuivre les objectifs indispensables que sont : la protection de l'investisseur, l'intégrité et la stabilité des marchés mais également la lutte contre le blanchiment et le financement du terrorisme.

Vous trouverez ci-dessous nos éléments de réponse, mais également nos interrogations concernant le développement de la DeFi.

1- 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 ?

Nous sommes en phase avec la définition de la DEFI. Elle reflète les caractéristiques fondamentales de la DEFI qui combine décentralisation et désintermédiation. Le rapport met bien en évidence l'hypothétique décentralisation pour certaines DAO en raison de la concentration de jetons de gouvernance entre peu de mains. Le choix de déléguer la gestion des clés à un acteur lui-même décentralisé peut être une option et compléter la définition (direct custody vs sub-custody).

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 ?

Les cas d'usage développés en p11,12 et 13 du document ont pour corollaire l'utilité pour l'économie réelle, ce qui nous paraît être une bonne approche. Les cryptoactifs peuvent être perçus par l'industrie financière comme du FOREX, sur lequel reposeront des instruments tirés du cercle 'traditionnel' : c'est typiquement ce que nous montrent les cas d'usages, il n'y a pas à proprement parlé d'innovation à ce niveau. Un point d'attention doit être remonté sur le transfert du risque concernant les activités de 'liquid', à l'instar de la crise de 2008.

Parmi les cas d'usage appelés à se développer dans le futur, il serait souhaitable d'étudier :

- Les stratégies d'investissement encapsulées dans les smart contracts
- Les stratégies ESG/impact qui pourraient être des smart contracts.
- La tokenisation d'actifs réels (RWA)

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

Un équivalent du FOREX pourrait se développer significativement car, pour certains pays et entreprises, cela permettrait de réduire leur dépendance au dollar. A noter que pour le Forex, JarvisNetwork existe déjà.

https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/

Q3 : Que pensez-vous des phénomènes de concentration décrits dans la partie 1-5 du document (Un ecosysteme marqué par une importante concentration à tous les niveaux ?

Le document est très lucide par rapport à ce phénomène de concentration et en reflète bien les enjeux.

Cette concentration à 2 niveaux est très inquiétante ; le proof of stake d'Ethereum augmentera la concentration des détenteurs d'ether (1 er niveau) et déjà 3 applications DEFi représentent 1/3 de la valeur totale. Cela donne l'impression de recréer le phénomène GAFAM du monde Internet.

Derrière ce problème de concentration, il existe des contraintes technologiques et de comportement. En outre, compte tenu du manque de concurrence, cet écosystème génère un risque élevé en termes de conflits d'intérêt et de position dominante.

Le manque de diversité des participants peut être également lié au manque de connaissance du plus grand nombre.

La concentration trahit la jeunesse de cet écosystème. La DeFi tendra avec le temps vers moins de concentration mais les barrières existent et sont bien mises en avant dans le document. La diversité des protocoles est étroitement liée aux marqueurs différentiant : préférons-nous avoir un protocole industrialisé et efficient ou 100 protocoles de même nature et fragmentés ?

Une réglementation pour encadrer les acteurs de la DeFi devrait contribuer à enrayer ce phénomène de concentration. En outre, même dans le cadre d'une grande concentration des acteurs, si la DAO derrière est bien conçue, cela ne devrait pas altérer le fonctionnement de la Blockchain.

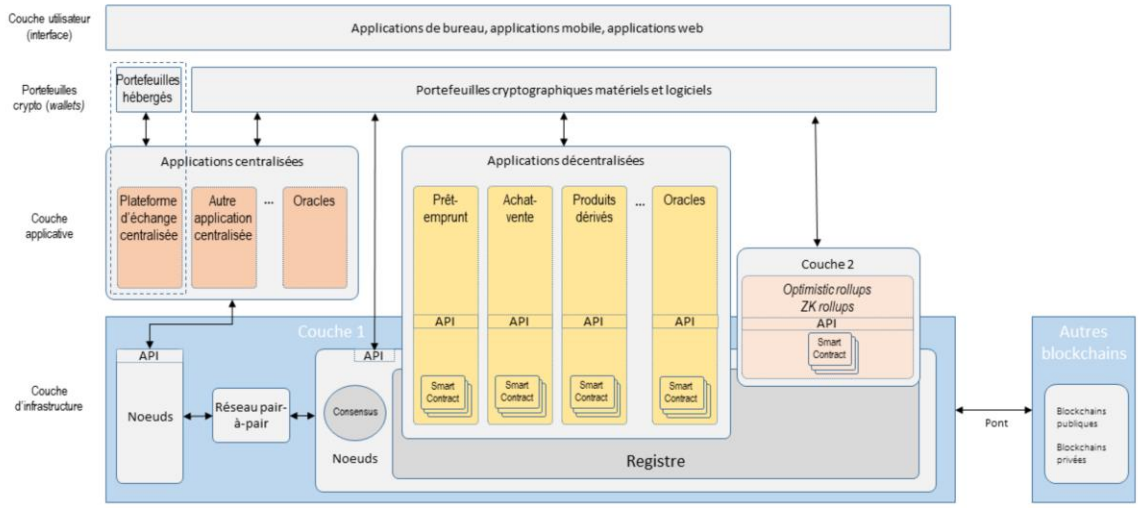
Concernant le minage, même si celui-ci se professionnalise, les mineurs sont de moins en moins nombreux, ce qui met en danger le protocole lui-même.

Enfin, le risque de concentration est un risque important en termes d'AML et de KYC.

Q4 : Avez-vous des commentaires à formuler ou des compléments à apporter sur la présentation schématique de la DeFi figurant en partie 1-6 (voir schéma reproduit ci-dessous)?

La présentation schématique de la DeFi figurant en partie 1-6 nous paraît pédagogique et satisfaisante en l'état de nos connaissances. Toutefois, 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.

Schéma : L'architecture applicative de la *DeFi*



2- 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) ?

Aux risques décrits dans la partie 2-1 du document, nous avons identifié en plus les risques suivants :

- Le risque de mauvaise collatéralisation et au reuse
- Le risque lié à la composabilité
- Le risque d'inefficacité : Une décision décentralisée tente de trouver un compromis entre deux extrêmes, mais cela n'est parfois pas suffisant voir néfaste (voir la théorie de Vitalik Buterin sur les DAOs, utiles lors de situations concaves : https://vitalik.ca/general/2022/09/20/daos.html)

Le risque peut également être le manque de volonté de la communauté, si personne ne vote ou ne propose des évolutions, le protocole n'évoluera pas.

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 ?

Notre vision est que moins il y a de nœuds, moins il y a de sécurité.

Les principaux layers 1 ont toujours été sécurisé. Aujourd'hui 45% des transactions sur l'écosystème ETH passent par ses layers 2 Optimistic et Arbitrum => ce chiffre montre bien que malgré leur jeunesse, ils paraissent incontournables. La zone d'ombre réside dans les informations remontées au layer 1, cela

peut poser problème dans un cadre règlementaire / financier. Typiquement les layers 2 semblent utiles pour une activité de netting comme dans le système traditionnel, la question de la remontée de l'information est clé.

Les solutions de layer 2 reposent sur les layer 1 donc les layer 1 restent à ce jour le socle de sécurité des layer 2, et résolvent le problème de décentralisation et de sécurité du trilemme de la blockchain (décentralisation, sécurité et scalabilité).

Toutefois, il nous paraît compliqué d'avoir une position conclusive sur les rollups car le concept est très nouveau et que nous manquons de recul. Est-ce que le principe du Roll up ne rappellerait pas la titrisation d'instruments financiers comme les subprimes ?

Les rollups ne doivent servir de mesures de contournement à la transparence de la BC (à l'instar des darks pools dans le trading traditionnel). Nous soulignons également la problématique de la MEV (Maximal Extractable Value) qui dans le contexte de la DeFi permet le front-running.

Il est toujours possible de récupérer les informations de chaque transaction même si elles sont envoyées en batch vers le layer 1

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 ? Un rollup exécute les transactions passées sur son réseau, « enroule » ces transactions en une seule opération (d'où son nom), et compresse l'information, en envoyant uniquement les données strictement nécessaires à la vérification des transactions sur la blockchain.

Voir réponse à la question 6

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

Les manipulations des prix de marchés viennent parfois d'un manque de liquidité. L'émergence de layer 2 dans la BC peut fragmenter les pools de liquidité des différents actifs.

Comment éviter la manipulation de données au sein d'un oracle et donc des rémunérations indues aux fournisseurs de données ? Des acteurs peuvent sciemment envoyer des données erronées que l'oracle synthétisera et il calculera une moyenne. Et les fournisseurs de données seront rémunérés pour les données erronées envoyées à l'oracle selon leur proximité à la moyenne.

Nous encourageons les oracles décentralisés comme Chainlink qui pénalisent les informations erronées. Nous aimerions que cette pratique soit généralisée. Les oracles restent un vecteur de risque important pour la Defi, notamment au regard des conséquences qu'ils induisent sur presque tous les protocoles Defi s'ils venaient à être manipulés.

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

Une règlementation sur les Oracles, à l'instar de la réglementation Benchmark, pourrait être envisagée, l'idée étant de pouvoir les référencer et de les garantir en vue d'une utilisation. Dans le même ordre d'idée, les smart contracts doivent être audités et des standards doivent émerger.

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

Le fonctionnement de la DeFi est différent de celui de la finance traditionnelle pour lequel la suspension des cotations est possible : dans la DeFi, les positions sont liquidées automatiquement qu'elles soient gagnantes ou perdantes, quelles que soient les conditions du marché.

La notion de self-custody génère des risques importants d'hacking notamment. Il manque des solutions de protection là-dessus. Nous pourrions nous inspirer des dispositifs de protection existant déjà dans DORA pour les adapter à l'environnement de la DeFi.

En outre, le self custody est à la fois l'ADN de la DeFi mais également un de ces principaux risques. Il existe des solutions de recovery comme Coincover (ou la nouvelle solution proposée par Ledger), qui assure les clés de recovery. Le cadre règlementaire pourrait se tourner vers ce type d'acteur pour assurer un second filet de sécurité ?

La perte de clé, le vol et le risque d'oubli (qui des avoirs-dettes sans maître) sont également des risques à prendre en considération.

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) ?

La combinaison de l'effet de levier élevé et des liquidations automatiques en dessous d'un certain seuil créé un mélange explosif. Concernant les produits dérivés, l'amplification des effets de leviers est liée à la grande volatilité des crypto-monnaies sous-jacentes. La composabilité accentue également fortement la corrélation entre tous les événements dans la Defi, ce qui augmente la volatilité générale, en particulier en cas de crash. Tant que la DEFI se passe entre quelques acteurs, le risque systémique est amoindri. Mais quand la DEFI s'élargira à un nombre important d'acteurs, le risque systémique sera avéré et s'accroîtra avec la présence d'acteurs *'too big to fail'*. Une communication optimale sur les risques associés à ces produits (notamment dérivés) permettrait un investissement éclairé.

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) »)

XOui
☐*Non*
Pour quelles raisons ?

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

Pour éviter le risque systémique. Cela permettra de faire face à un actif encadré dont les flux seront ségrégués et qui sera audité en conséquence. Une homogénéisation de la norme sera de nature à mieux encadrer les risques. Cela ne peut valoir que pour les stablecoins centralisés émis par des émetteurs.

Les stablecoins jouent un rôle essentiel dans les échanges de valeur dans la DeFi. Le depeg (désindexation du stablecoin à sa devise) est un risque réel et peut entraîner l'effondrement en cascade de plusieurs acteurs. Il est donc impératif d'imposer un cadre réglementaire afin d'évaluer les risques de chaque type de stablecoin et éditer des règles claires pour leurs émetteurs. A l'instar des audits de smart contracts, des entreprises privées effectuent également des « Proof of Reserve » qui atteste la disponibilité des fonds détenus par un acteur.

Les stablecoins peuvent apporter de la confiance dans le processus de règlement/livraison.

Attention toutefois au risque d'ultra-traçabilité de la banque centrale, chaque étape de la vie du Stablecoin sera tracée / connue.

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) ?

L'application du règlement TFR en Europe sera un premier pas vers l'adaptation des règles AML/LCBFT. Aujourd'hui des acteurs de la DeFi proposent des solutions de screening de type KyT (Know your Transaction) permettant de blacklister certaines adresses selon par exemple les listes de l'OFAC ou encore selon les politiques de l'acteur. Néanmoins l'utilisation de protocoles comme Tornado Cash ne facilite pas cette tâche.

Le pseudonymat avec les actions concertées de Chainalysis et du FBI ont permis d'arrêter des escrocs et de récupérer des cryptos volés pour environ 1 milliard $. A-t-on mis en place suffisamment de moyens en Europe pour réussir de telles actions de police ?

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

Il faudrait peut-être creuser le risque lié aux opérations de 'liquid' et le risque de transfert de risque. Ce mécanisme permet de continuer des opérations financières tandis que l'actif est en staking. Quid des impacts si l'actif ne vaut plus rien ?

D'autres risques peuvent être également relever : existence de barrières à l'entrée, mauvaise collatéralisation des actifs et réutilisation du collatéral, circulation imparfaite de l'information liée aux roll-ups et dépendance envers le nombre de mineurs ou la mobilisation d'une communauté.

3- Les pistes d'encadrement réglementaire

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) ?

XOui
☐*Non*

Si oui, de quelle façon ? Sinon, pourquoi ?

Il est possible de prendre le contrôle de la structure compte tenu du faible nombre de validateurs (risque des 51%). Limiter la capture de la majorité est une bonne chose. Si on fait de la DEFI, c'est pour justement élargir à un grand nombre de nœuds. La concentration des nœuds n'est donc pas souhaitée. Toutefois, il est compliqué d'envisager un seuil concernant cette concentration

A partir du moment où les applications DeFi sont développées sur des blockchains publiques, une partie de leur solidité et sécurité reposent sur la solidité et la sécurité de la blockchain publique.

Surveiller le degré de concentration des capacités de validation est une bonne piste. Mais nous posons des questions : Comment calculer ce degré ? a-t-on les éléments fiables sur le nombre de validateurs différents à l'instant T et sur une période N ? Cependant cette surveillance reste limitée car rien ne peut empêcher certains validateurs de se regrouper pour jusqu'à atteindre les 51%.

Il serait souhaitable d'ouvrir la réflexion aux nouvelles solutions d'interopérabilité/scalabilité mises en œuvre par les nouvelles blockchains publiques qui se développent aujourd'hui.

Toutefois, si les Blockchains publiques doivent faire l'objet d'un encadrement, celui-ci ne doit pas être figé et doit rester en phase avec les avancées technologiques qui évoluent très vite. Il conviendrait d'envisager davantage des principes directeurs plutôt que des règles strictes et difficiles à faire évoluer.

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 ?

Question préalable : Quelles sont précisément les autorités publiques visées dans l'intitulé de la question ?

X Surveiller la concentration en temps réel :

Il conviendrait pour cela de soumettre les promoteurs d'initiatives DeFi en matière de services financiers à l'obligation de communiquer le nombre de nœuds intervenant dans le fonctionnement de leur

dispositif. Cette mesure serait en lien avec la gouvernance qui doit être contrôlable à tout moment et reposer sur la confiance.

☐*Fixer des plafonds à cette concentration*

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

X Engager d'autres actions (préciser lesquelles)

- Fixer des lignes directrices concernant les plafonds de concentration mais sans seuil « gravé dans le marbre ». S'il y a un plafond, de nouvelles règles de BC publiques pourraient être mises en place pour détourner une telle limite
- Superviser la concentration en tenant compte de la protection des investisseurs/intégrité des marchés
- Idée selon laquelle les BC publiques ne seraient homologuées qu'à condition qu'elles se dotent d'un modérateur
- Les protocoles devraient démontrer la mise en place d'une bonne gouvernance et rendre compte de la manière dont les services sont rendus.

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 ?

Les promoteurs d'initiatives de BC privées sont pour la plupart des informaticiens : ils ne sont pas régulés et non pas vocation à l'être.

Nous ne sommes pas favorables à ce que des établissements publics opèrent directement une infrastructure BC car cela reviendrait à une nationalisation ou à une ultracentralisation.

Par construction, la BC privée s'inscrit dans le domaine de la liberté et devrait à ce titre être surveillée et contrôlée dans le cadre de la sécurité des utilisateurs.

Toutefois, nous pensons qu'il serait également souhaitable de surveiller l'accès aux compétences pour le développement des BC privées, et parmi elles de réguler le développement des BC privées en vue de rendre des services financiers.

Nous nous interrogeons également sur les règles de territorialité à appliqués en matière de surveillance car les niveaux de protection diffèrent d'une juridiction à l'autre, et entre l'Europe (RGPD, MIF etc…) et les pays tiers.

De là découlent d'autres questions :

Comment définit-on le lieu d'exécution de la prestation ?

A quel pays se réfère-t-on pour la collecte de la TVA (car protocole n'a pas de personnalité morale) ?

☐Oui

X Non sous réserve de la communication publique des utilisateurs des blockchains privées et que l'existence de ceux-ci soient facilement vérifiable. Cette transparence ferait office de réglementation et ne devrait pas limiter le développement des blockchains privées.

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

Pourquoi ? Les acteurs publics doivent jouer un rôle de régulation et ne doivent pas gérer directement les blockchains car ils freineraient les capacités d'innovation de l'écosystème.

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

Si oui, lesquelles ?

- Un plan de secours de la BC en tant qu'infrastructure
- Un plan de migration des services
- Mettre en place des règles encadrant les personnes qui vont développer l'infrastructure dès lors qu'ils fournissent des services à des utilisateurs européens
- S'inspirer du modèle DORA qui prévoit un dispositif de protection pour la fourniture des services financiers
- Interdire la promotion des SM DeFi dès lors qu'ils ne respectent pas les règles de fournitures de services financiers
- Définir des bonnes pratiques concernant les certifications et obliger les organismes certificateurs à les suivre
- Mettre en place un référentiel en précisant ce qu'il couvre et comment on le couvre ?
- Une assurance obligatoire pour couvrir les sinistres causés par des failles de sécurité ou de hack

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

Remarque générale sur les certifications :

Le financement des certifications pose problème : qui finance ces certifications ? L'émetteur ou l'utilisateur ? Et comment elles se financent ?

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

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 ?

Le mécanisme de certification peut constituer une solution efficace à partir du moment où il vise le design des smart contracts mais également leur opérationnalité.

Le programme étant voué à évoluer dans le temps, certaines failles ne sont parfois découvertes qu'après plusieurs mois, voire années, même après des audits de sécurité. Une solution possible serait un audit en continue des smart contracts afin de déterminer l'état de sa sécurité en fonction de l'évolution des technologies.

Un tiers certificateur doit être investi de cette mission et un mécanisme combinant la machine et l'humain nous semble être une bonne idée.

Les certifications pourraient dépendre de la nature du contrat intelligent, c'est-à-dire son utilité économique ou financière. La diversité des ERC disponibles par exemple sur ETH démontre l'hétérogénéité des utilités. Un standard européen semble le bon niveau afin d'éviter les distorsions locales. Un pilote sur certains cas d'usages pourrait permettre à la communauté d'avoir des résultats rapidement.

Toutefois des questions subsistent : quand aura-t-on sur le marché des certificateurs compétents et en nombre suffisant ?

Les certifications existantes (SOC2 pour la plus complète) ne semblent pas permettre de contrôler les smart contracts. Les acteurs spécialisés en cybersécurité pourraient-ils endosser cette compétence ? L'ANNSSI serait-elle en mesure de délivrer une telle certification ?

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 ?

Concernant le code informatique uniquement, nous partageons cette description. Les audits du code des smart contracts sont aujourd'hui la solution de certification la plus largement acceptée. Néanmoins c'est un marché trop jeune qui manque de standards unifiant ces audits. La qualité des audits diffère selon les entreprises qui les délivrent, l'indépendance n'est pas toujours respectée et les rapports sont difficilement accessibles. La transparence de la blockchain donne parfois un faux sentiment de sécurité des utilisateurs. D'un autre côté, les aspects juridiques, de compliance, RGPD ou même encore ESG ne sont pas inclus dans ces audits.

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

Pour tester les protocoles des développeurs par la communauté afin d'identifier les failles, il faudrait préciser s'ils sont en open source, ce qui assurerait une plus grande transparence même quand il n'y a pas de certification. Versus ceux qui ne sont pas en open source : « Acte de foi ».

La mention « open source » est importante pour pouvoir vérifier que ce que font les SM fonctionne vraiment.

A terme, l'ensemble de spécificités sera standardisé, et un programme de vérification formelle sera possible mais à date, il faut encore de l'intelligence humaine.

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 ?

Pour pouvoir répondre à cette question, il faudra maitriser la bibliothèque d'ERC, c'est un travail de fond titanesque, et cela ne concerne qu'ETH, il faut aussi se pencher sur des BC 'finance friendly' comme Avalanche ou Hedera qui ont elles aussi leurs propres équivalents ERC. Il faut également maîtriser totalement les règles de coding car doit être pris en compte tout ce qui est codable et pas seulement l'ERC.

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) ?

Ces règles nous semblent très contraignantes. D'autant qu'une certification ne vaut qu'à un instant T et ne garantit pas la sécurité du code. Si on souhaite modifier le code ou les paramètres, faut-il certifier après chaque modification ? De même, si le compilateur de langage évolue, faut-il certifier toutes les versions du compilateur ? Nous nous inquiétons de la faisabilité de ce dispositif. Ce qui nous conduit à nous interroger sur le périmètre de la certification, sa durée de validité et les modalités concernant ses mises à jour. La DAO devra discloser sur les mises à jour sinon la certification perdra de sa valeur. Raison pour laquelle nous pensons que la définition de standards préalables est un prérequis. S'il faut certifier les composants, il faudra également certifier les oracles, ainsi que les codes en amont et en aval, ainsi que les aspects ESG. Cela nécessitera entre autres une surveillance continue des codes. La transparence du code et de ses paramètres est un élément indispensable pour instaurer la confiance des utilisateurs. Par ailleurs, des outils pédagogiques devront être mis en place pour que les utilisateurs soient à même de lire les certifications et de les comprendre.

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

XOui

☐*Non*

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

Pourquoi ?

Si les smart contracts embarquent dans leur code des exigences règlementaires, cela signifie que les développeurs de smart contrats veulent agir en respectant la règlementation qui doit viser en priorité la protection de l'investisseur non professionnel, l'intégrité des marchés et la lutte anti-blanchiment. Les acteurs qui intégreraient des exigences règlementaires dans le code devraient le faire savoir, ce qui donnerait une information rassurante, comme un label de sécurité, pour les investisseurs.

Cela parait clé pour l'avenir, certains le font déjà notamment en suisse avec par exemple le T-Rex de la plateforme de tokenisation Tokeny. Cet ERC-3643 embarque certains éléments de conformité dans le contrat intelligent.

https://tokeny.com/wp-content/uploads/2019/12/Whitepaper-T-REX-Security-tokens.pdf

Toutefois, ces exigences réglementaires se doivent d'être souples et évolutives pour que le dispositif puisse être efficace.

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

L'ESMA et l'EBA, en concertation avec l'ANSSI, pourraient établir ces standards à l'instar du Comité de Bâle pour les banques. En raison des problématiques d'extra territorialité, ces standards doivent être harmonisés au niveau international afin d'assurer un niveau élevé de sécurité pour les investisseurs. Certains de nos membres considèrent que les standards pourraient être des normes ISO car cela a déjà été fait.

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

X Découragée

☐*Interdite*

☐*Ni découragée ni interdite Pourquoi ?*

S'inspirer de la certification de la conformité des systèmes d'IA dans le cadre du règlement européen est une piste à explorer car elle adresse le même enjeu, à savoir la protection de l'épargnant. Une analogie avec des services qui existent déjà peut être faite telle que la reverse sollicitation : si les utilisateurs veulent utiliser Uniswap par exemple, libre à eux. L'existence ou l'absence de certificat doivent être dans tous les cas mentionnés.

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

Les avantages et inconvénients des solutions de faire payer le développeur ou l'utilisateur sont clairs. Ce sujet pourrait faire l'objet d'une consultation de place qui permettrait de voir où se trouve le

consensus. L'idée d'une taxation est séduisante à condition que sa finalité ne soit pas dévoyée. Nous nous demandons également comment ce sujet est traité par les superviseurs d'autres juridictions. La levée des fonds de certains protocoles qui s'engagent à utiliser une partie des fonds levés pour la certification est une piste intéressante et peut être considérée comme une bonne pratique. Mais qu'en est-il des frais de certification liés à la mise à jour du Code. Dans tous les cas, le coût ne doit pas être supporté par l'investisseur final.

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 ?

Nous sommes en phase avec la solution d'un système de certification des oracles décentralisés et de la mise en place d'un mécanisme de consensus et de coupe circuit. S'inspirer du règlement benchmark nous semble également un modèle dont on peut s'inspirer, dès lors que cela soit techniquement et opérationnellement possible en prenant en compte les spécificités de la DeFi.

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

Si oui, lesquelles ?

Nous pensons que la réglementation devra encadrer les risques de sécurité informatique et couvrir les sujets éthiques, de gouvernance et juridiques.

Exemple de pratique qui s'est développée et qu'il faut encadrer : Les applis non custodial : pour utiliser l'appli, il faut une approbation ; pour na pas avoir à approuver à chaque fois, l'approbation à une durée illimitée pour tous les fonds. Cela revient à signer un « chèque en blanc » et cette pratique s'avère très dangereuse.

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) ?
X Oui
☐*Non*

Si oui, lesquelles ? Si non, pourquoi ?

La recentralisation des activités en lien avec la gouvernance ou la reconnaissance de la centralisation de ces activités doit être faite. « Recentraliser » partiellement peut être nécessaire lorsqu'il y a un devoir de responsabilité et de confiance. A titre d'exemple, la constitution d'une société permet d'identifier

un responsable qui sera tenu de répondre en cas d'action en justice. De même, le KYC est un process réglementaire devant être opéré par un acteur de confiance ou certifié, donc difficilement décentralisable.

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 ?

Les propositions sont intéressantes et semblent logiques. Ces obligations doivent peut-être être imposées en cas de dépassement de certains seuils mesurant la taille de l'application DeFI (volume de transactions gérées, liquidité, nombre d'utilisateurs….) afin de ne pas freiner davantage l'innovation avec des frais juridiques supplémentaires. Le statut juridique des DAO pourrait se comparer à une entreprise classique et ses actionnaires, et devrait différer selon la nature des activités de la DAO.

En outre, nous pensons qu'il est préférable de suivre la démarche du GAFI afin de rester dans une norme internationale connue plutôt que de créer une norme qui ne s'adapterait qu'à des acteurs visant des clients français.

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

Oui, l'erreur humaine a été à la source des principaux épisodes cités. Nous partageons cette description. Ces acteurs devraient être soumis à des règles s'inspirant de la finance classique, et à des audits financiers renforcés et experts dans le domaine.

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

X Des obligations d'information
X Des obligations de conseils et de vigilance
X Des exigences concernant la publication de livre blanc

X Des exigences de KYC
X Un cadre complet inspiré de MiCA

Un MICA 2 à prévoir rapidement devrait intégrer les intermédiaires facilitant l'accès à la DEFI, s'ils ne sont pas déjà concernés. En fournissant une infrastructure facilitant l'accès à la DeFi, ces intermédiaires permettent aux particuliers d'accéder à des services et produits financiers autrefois accessibles uniquement par des professionnels et personnes formées. La technologie BC apporte de la transparence mais les activités de ces intermédiaires sont bien souvent opaques. Il est donc de leur devoir d'être totalement clairs sur leurs opérations, de restreindre l'accès à leurs services en cas de besoin, et de connaître leurs utilisateurs. Cela passe par leur régulation, afin de protéger et avertir les consommateurs.

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

Des obligations d'information et de transparence semble nécessaire. Avec la composabilité, il est compliqué de comprendre à quoi un portefeuille est finalement exposé. Il pourrait être pertinent d'avoir une vue en transparence des cryptoactifs 'natifs' auxquels un portefeuille est exposé.

Il faudrait aussi une explication sur la méthodologie de validation des protocoles et des cryptoactifs proposé par l'intermédiaire pour mieux comprendre les aspects risque également, notamment s'il venait à proposer des protocoles non certifiés (exemple d'Uniswap par exemple).

☐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) ?
X Oui
☐Non

Pourquoi ?

Une distinction est à faire entre les intermédiaires centralisés et les intermédiaires décentralisés.

Un intermédiaire centralisé peut être comparé à un prestataire de finance traditionnelle : les règles à appliquer doivent donc être similaires. L'encadrement doit se faire en fonction de la nature de services de ces acteurs : KYC, règles de bonne conduite, exigences prudentielles.

Toutefois, un principe de proportionnalité pourrait s'appliquer. Pour un acteur petit qui ne dépasse pas certains seuils, dont, au-delà du total des encours (conseillés ou gérés), celui des encours maximums par client, il pourrait y avoir des règles allégées, de manière à permettre à de nouveaux acteurs de tester leur modèle avant de lancer le chantier des demandes d'agréments.

Les intermédiaires décentralisés, eux, ont une nature algorithmique. Si l'audit et la certification du code informatique sont correctement réalisés, les risques de fraude peuvent être éliminés. Un devoir de conseil envers les utilisateurs uniquement peut être imposé à ces intermédiaires, mais leur régulation pourrait être moins restrictive. Comparativement à l'état actuel, elle doit néanmoins être renforcée (KYC, Livre Blanc etc…).

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

Les règles de MIF 2 doivent s'appliquer. Il faudrait peut-être ajouter un socle de compétences technologiques pour comprendre les risques propres et inhérents au cryptoactifs et aux protocoles (principe d'adéquation). Le produit financier, qu'il soit opéré via le circuit traditionnel ou le circuit DeFi, offre des perspectives de rendement sous prise de risque. L'épargnant doit être protégé vis-à-vis de ce couple à hauteur de ses connaissances, c'est typiquement l'ADN de Mifid.
☐Non

FINANCE « DECENTRALISEE » OU « DESINTERMEDIEE » : QUELLE REPONSE REGLEMENTAIRE ?

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 ?

L'accès aux services financiers sur la DeFi pourrait aussi prendre en compte les segment retail / pro / contrepartie éligible à l'instar de Mif 2. Cela va dans le sens de la question 35. Les distributeurs doivent aussi être intégré dans le cadre règlementaire. A l'instar d'Emir, la réglementation pourrait préciser les obligations minimales en termes de reporting.

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) ?

L'enjeu est complexe pour les petits acteurs qui doivent pouvoir continuer à proposer leurs services et pour les régulateurs qui ne doivent pas entraver l'innovation ou engendrer des oligopoles. La piste réglementaire principale ressortant de ce document est la certification des smarts contracts, ou plus globalement de l'application informatique DeFi.
Mais des questions subsistent : quel cout ? et qui paie ?

On pourrait imaginer des plateformes créées, par exemple, par des acteurs comme la CDC ou la BPI où des petits acteurs intégreraient leurs services DEFI. Ces plateformes pourraient permettre aux petits acteurs d'être certifiés à un cout mutualisé, d'utiliser leur KYC …

Peut-être qu'un système de seuil de risque total et par client permettrait de lever certaines obligations (hors KYC et LCBFT) pour opérer temporairement.

Il faut dans tous les cas trouver un mécanisme permettant aux acteurs de taille modeste de se lancer à moindre coût.

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) ?

Deux aspects peuvent être pris en compte : l'intermédiaire (la plateforme) et son activité (les utilisateurs). Pour l'intermédiaire, l'obligation de constituer une entreprise ou d'accorder un statut juridique aux DAO permettrait de renseigner l'origine géographique. Pour l'activité, l'obligation

d'appliquer un KYC semble être une mesure phare, qui permettrait de connaître la nationalité des utilisateurs.

Autres pistes :

- Obliger l'existence d'une résidence (individu) ou d'un siège social (entité) basé en Europe avec mention sur le site internet associé, de sorte qu'à terme, les épargnants comprendront s'ils interagissent avec un acteur respectant la réglementation ou pas en pouvant le vérifier.
- Avoir une base de données Européennes disponible sur le site du régulateur local sur les acteurs agréés ou certifiés MICA 2.

Que proposent les autres pays sur ce sujet ?

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 ?

L'ACPR et AMF selon les services proposés sur DeFi. Les acteurs doivent être sélectionnés par un statut accordé par le régulateur. Les entreprises en charge du contrôle (audit, certification, juridique…) peuvent être des entreprises privées spécialisées dans l'audit de systèmes DeFi.

AFG

Ensemble, s'investir pour demain

41 rue de la Bienfaisance · 75008 Paris · +33 (0)1 44 94 94 00 ■ avenue des Arts 44 · 1000 Bruxelles ■ www.afg.asso.fr