Paris, 29 septembre 2023

Finance décentralisée : réponse à la consultation de l'AMF 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 et à la réalisation de la transition énergétique.

Le groupe de travail de Paris Europlace sur la finance décentralisée (DeFi), dont la composition figure en annexe de ce document, remercie l'AMF d'avoir lancé une consultation publique sur ce sujet. Cette démarche 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 structurées autour des sept « points de discussion » identifiés par le Papier de l'AMF.

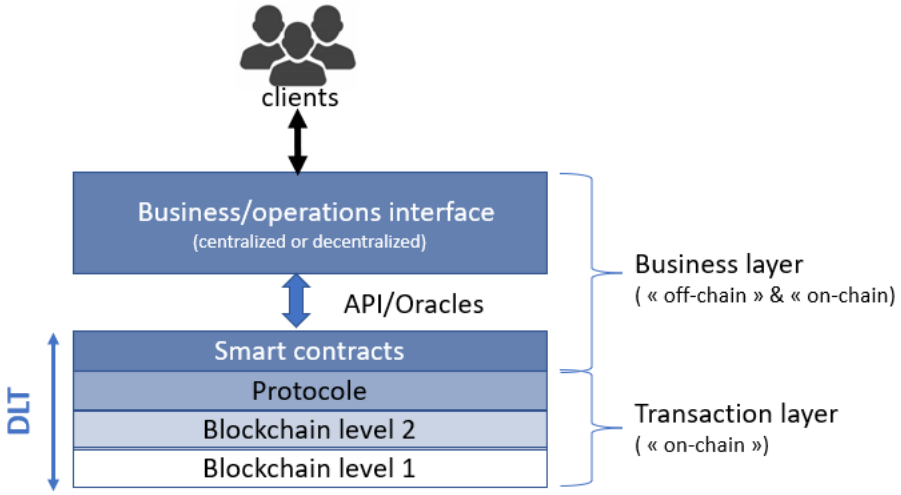
1. Protocoles blockchain permissionnés et non permissionnés

Rappelons tout d'abord que la Blockchain originelle (Bitcoin) est une blockchain publique conçue pour fonctionner de manière totalement autonome, c'est-à-dire sans intervention possible d'un tiers externe. Elle permet à ses utilisateurs d'échanger librement un actif digital natif appelé « crypto-devise », caractérisée notamment par l'absence d'entité émettrice. Les seuls utilisateurs de la blockchain sont de fait des détenteurs de la crypto-devise, et les échanges de crypto-devises sont régis par un protocole informatique très spécifique : d'une part, la responsabilité du transfert de propriété n'est plus centralisée sur une seule entité, mais est « distribuée » sur une partie des détenteurs de crypto-devises, à savoir la communauté des « mineurs » ; d'autre part, les transactions actant du transfert de propriété sont enregistrées de façon simultanée et synchronisée sur chacun des nœuds informatiques associés aux mineurs. Ces mineurs pouvant être des personnes physiques localisées dans diverses parties du monde, ils ne sont de fait pas soumis aux

réglementations existantes basées principalement sur l'encadrement des émetteurs et des intermédiaires financiers.

S'agissant de blockchain, la notion de « permissionnement » est venue plus tard avec un concept presque antinomique de « blockchain privée ». En effet si les modalités techniques d'enregistrement des transactions sur les nœuds restaient en théorie les mêmes entre blockchains privées et blockchains publiques, a contrario la multiplicité et l'indépendance des nœuds, sur lesquels était basée la décentralisation des premières blockchains, n'étaient plus vraiment une « condition » de fonctionnement pour certaines blockchains privées. De fait, la responsabilité du fonctionnement de ces blockchains privées restait plus ou moins centralisée, à l'instar finalement des systèmes traditionnels.

Pour pallier le problème, a été proposé un peu plus tard le concept de « blockchain publique permissionnée », où le permissionnement est appréhendé au travers d'une surcouche applicative au-dessus du protocole de la blockchain publique, ce qui a été rendu possible notamment grâce à la création des smart contracts par Ethereum. Le protocole des blockchains publiques étant censé se limiter à la gestion du consensus et autres relations entre les nœuds, c'est dans cette surcouche applicative qu'est censée se trouver en général l'intelligence applicative de la DeFi, et notamment l'autorisation de participer aux services déployés sur la blockchain sous-jacente. En théorie, cette surcouche applicative peut tout à fait être « off-chain », « on-chain » voire un mix des deux, les « smart contracts » servant alors à encapsuler la partie « on-chain » de cette intelligence applicative. Concernant les éventuelles règles de permissionnement, elle semblent a priori plus faciles à implémenter dans la partie « off-chain » que dans la partie « on-chain » pour les mêmes raisons qu'évoquées précédemment concernant la comparaison entre blockchains privées et publiques. L'existence d'un point d'entrée « off-chain » même réduit pour la DeFi pourrait alors permettre de faciliter la gestion des permissionnements, notamment ceux nécessitant une interaction préalable importante avec l'utilisateur final. Toutefois, si permissionnement il y a à l'entrée, la question peut se poser de savoir s'il s'agit encore véritablement de DeFi.



Pour les applicatifs DeFi volontairement conçus sans partie « off-chain », il conviendrait sans doute pour le régulateur de regarder si cette absence est susceptible ou non de favoriser la « reverse sollicitation » et/ou le contournement éventuel des réglementations territoriales en matière de protection des investisseurs. Dans l'hypothèse où la DeFi serait volontairement conçue pour échapper à toute réglementation territoriale, le régulateur ne pourra en tout état de cause que publier comme actuellement des mises en garde aux investisseurs potentiels.

Plus généralement, et indépendamment des modalités techniques d'implémentation (off-chain vs on-chain), pour répondre au 2ème paragraphe du point de discussion de l'AMF, on peut se demander si toute solution reposant sur un permissionnement, donc supposant une entité donnant cette permission, relève bien de la DeFi. Si ce n'est pas le cas, on peut prendre comme hypothèse que ladite entité serait soumise, pour des prestations similaires, aux mêmes règles que la finance centralisée de la part de l'AMF. A l'inverse, en l'absence de tout élément de « centralité », notamment de toute forme de « permission » d'accès, réglementer la DeFi risque fort d'être une gageure.

2. Smart contracts

Les « smart contracts » désignent des lignes de programme informatique exécutant certaines tâches informatiques selon des conditions prédéfinies et le cas échéant sur la base d'informations qui ont été introduites automatiquement ou non dans le champ d'exécution (oracles).

Leur principal intérêt, qui doit être préservé, tient à la prévisibilité (et donc automaticité selon des règles objectives) des mécanismes d'exécution que ces smart contracts emportent. On comprend que son intelligibilité soit réduite, tant au regard du langage de programmation utilisé que dans l'aptitude de déconstruire le programme pour en cerner exactement les tenant et aboutissant.

Fonctionnant dans un environnement réglementé (lorsque les exécutions attendues du smart contract relèvent d'activités réglementées), cela emporte deux principales problématiques :

- Est-il possible d'identifier une personne responsable du « bon » fonctionnement d'un smart contract et est-ce souhaitable en considération de l'approche open source qui favorise le développement et la multiplicité et la composabilité de ceux-ci et leur potentielle interopérabilité, utilisés comme des briques dans des programmes plus vastes (*open source libraries*) ? Eu égard à la difficulté pour tout informaticien de garantir un fonctionnement sans faille d'un programme informatique plus ou moins complexe, peu de développeurs, mais également des promoteurs, seront prêts à assumer une responsabilité ;
- Est-il souhaitable que selon les fonctionnalités proposées par le smart contract, la réglementation impose que soient embarquées dans le code des facultés plus ou

moins discrétionnairement reconnues à certaines personnes (développeur, majorité d'utilisateurs, mais aussi régulateur) de modifier/altérer voire empêcher l'exécution de telle ou telle fonctionnalité ? Si le principe semble justifié, les conditions de ces interventions devraient être précautionneusement déterminées pour éviter toute manipulation ou fraude (par exemple en influençant sur les informations/oracles utilisées pour le déclenchement de telle ou telle mesure d'urgence). Se pose également la question des délais de mise en œuvre de telles mesures pour être efficaces.

Une approche régulatoire des smart contracts pourrait tenir dans l'édiction de recommandations/guidelines non contraignantes, et sur la manière de présenter en langage intelligible les conditions de fonctionnement du smart contract (distinguer les conditions des conséquences), l'existence de tout mécanisme d'intervention, et un certain nombre de déclarations standardisées quant aux éventuelles responsabilités ou non-responsabilité des développeurs, promoteurs ou majorité d'utilisateurs.

3. Utilisation de codes open source

Avant de s'interroger sur les conditions d'usage d'un programme/d'une application libres de tous droits dus à un tiers (développeur ou autre), le phénomène d'open source présente des avantages indéniables en matière d'inventivité/agilité, mais aussi en termes d'aptitude à « tester » la robustesse d'un programme et d'en détecter les failles par les tests libres qui en seraient faits par une communauté de programmeurs ou d'utilisateurs. A ce titre, la robustesse d'un programme peut être mieux éprouvée par l'utilisation très large et répétée de celui-ci, plutôt que par une approche de certification/d'audit confié à une personne, et en l'absence de méthode ou de critères d'audit définis et communément admis. En ce sens, le caractère open source d'un programme peut permettre de mieux discerner les protocoles fiables et efficients de ceux ne présentant pas d'intérêt ou de fiabilité suffisante.

Aussi, a priori, le caractère open source d'une application utilisée dans la DeFI ne devrait pas nécessairement appeler un encadrement particulier, notamment réglementaire, à raison de son caractère ouvert et donc en libre utilisation. Cependant, cet usage pourra faire l'objet d'une forme de contrôle s'il y est recouru par une personne rendant un service qui alors sera tenu des obligations qui seront à sa charge réglementairement et/ou contractuellement.

4. Prise en compte des risques des activités DeFi

Il n'est pas contesté que dans la mesure où des activités sont comparables, même si elles sont développées avec des moyens différents, les règles de protection des utilisateurs et des investisseurs devraient être comparables voire identiques (*same activity, same risk, same rule*).

Il convient cependant de s'assurer que les activités menées au sein de la DeFi soient effectivement comparables, tant dans la nature des prestations proposées que des risques engendrés par celles-ci et les modalités de leur offre. Il semble que ce travail devrait être réalisé de manière systématique pour circonscrire exactement celles des activités qui seraient effectivement comparables aux activités développées dans la sphère financière traditionnelle.

A ce titre, la logique de décentralisation intrinsèque aux activités ainsi développées appelle vraisemblablement une approche régulatoire différente de celle traditionnellement appliquée par les régulateurs financiers. Ainsi une approche plus « *principle based* » pourrait être préférée à une approche par agrément ou autorisation préalable, notamment si elle s'accompagne des informations nécessaires pour éclairer les personnes exposées aux risques. De même, la sophistication, l'évolutivité et la grande technicité de certains protocoles ne rendent leur utilisation ou leur accès qu'à des personnes que l'on qualifierait dans la finance centralisée d'investisseur qualifié/averti ou de client professionnel, de sorte que la supervision devrait être de type « *light touch* ». Cela n'empêcherait en revanche pas d'être plus prescriptif dès lors qu'un service est rendu à un tiers par une personne dont on s'assurera alors de la compétence et du professionnalisme.

5. Règles de marché d'un protocole d'échange DeFi

Une fois les risques liés à la DeFi identifiés (cf. point ci-dessus), cerner le rôle que peuvent avoir les smart contracts dans la diffusion, l'amplification ou au contraire la limitation de ces risques est crucial. De l'avis majoritaire du groupe de travail, et bien qu'un smart contract est en lui-même susceptible d'être audité et/ou certifié, aucune méthode d'audit ou de certification ne semble pouvoir garantir que ledit contrat sera parfaitement prévisible dans ses effets ou ses interactions avec les autres éléments on-chain ou off-chain.

Ainsi, la transparence que l'on pourra souhaiter obtenir dans la compréhension des smart contracts ne saurait être comprise comme offrant une forme définitive d'assurance ou de sécurité : face aux utilisations inattendues ou malveillantes des smart contracts, la meilleure riposte semble être la décentralisation des processus de contrôle et leur multiplicité. Une meilleure intelligibilité des smart contracts peut donc être encouragée, mais une certification poserait des questions additionnelles, auxquelles il conviendrait de réfléchir en amont :

i) Quel serait le champ ou la nature des smart contracts soumis à une éventuelle certification, compte tenu du principe de neutralité technologique généralement suivi par les régulateurs ?
ii) Quel sort réserver aux smart contracts non certifiés et à l'historique des transactions qu'ils ont déclenchées ou facilitées ?
iii) Leur certification modifierait-elle les conditions de recevabilité des actions en responsabilité liées à l'utilisation des smart contracts ?

iv) Quelle serait en effet la valeur ou la portée de cette certification, de même que celle-ci induirait-elle une responsabilité des auditeurs ? Le risque pourrait être que certains auditeurs refusent une telle mission ;
v) Cette certification risquerait-elle de brider l'innovation technologique ou de freiner le développement de certaines activités ?

6. Définitions des DEX et des AMM

Par construction, l'attractivité de la DeFi tient notamment à sa constante évolutivité. La rapidité de ses changements fragilise la définition d'un cadre conceptuel simple et stable, puisque l'hétérogénéité, la complexité des protocoles et la question de leur composabilité (avec un risque de course à la liquidité entre protocoles) se sont largement accrues au cours de la période récente. Les dispositions réglementaires devront ainsi demeurer flexibles et adaptables à un grand nombre d'applications possibles.

Face à cette complexité, le groupe de travail entend également relever les avantages et les défis que peuvent préserver les protocoles d'échanges décentralisés reposant sur des carnets d'ordres (DEX) par rapport à ceux utilisant des réserves de liquidité (AMM), mais sans établir de préférence a priori, même si les deux paraissent moins exposés aux attaques (hacks) que les protocoles centralisés :

i) En principe, comme pour les plateformes centralisées traditionnelles, les DEX proposent des achats/ventes dont certains paramètres sont prévisibles, par exemple au meilleur prix disponible (market order) ou à un prix défini (limit order), donc avec des vertus potentiellement stabilisatrices, mais le carnet d'ordre peut être hébergé tantôt on-chain (dans ce cas, chaque ordre peut être vérifié par l'ensemble du réseau), tantôt off-chain (ce tiers pouvant alors être attaqué). L'hébergement on-chain est donc plus transparent, mais les échanges peuvent être plus lents, donc coûteux, puisque chaque ordre passé doit être publié.

ii) A contrario, ces questions d'instantanéité ou de frais se posent moins pour les AMM, mais utiliser ces derniers supposent d'avoir une confiance plus forte dans la fiabilité des smart contracts pour gérer les liquidités mises à disposition, d'autant qu'un risque de volatilité des prix ou d'insuffisance des liquidité demeure.

iii) Au total, pour les autorités de régulation et de supervision, un défi sera donc d'avoir une information en temps réel des transactions afin de réagir lorsque certains risque menaceront de se matérialiser.

7. Niveau de décentralisation et degré de contrôle

La décentralisation étant au cœur de la DeFi, sa mesure est essentielle à la bonne compréhension de ses activités. Certes, l'identification d'adresses IP ou de contrats de travail peut permettre d'éviter aux autorités de se heurter au risque d'extraterritorialité de la régulation ou à celui de l'irresponsabilité de certains acteurs, mais la majorité des situations invite à déceler des cas plus hybrides où les couches d'applications (*layers*) se superposent.

Par ailleurs, même une Blockchain prétendument entièrement décentralisée peut être régie par des acteurs en nombre limité et/ou agissant de concert, avec un risque de capture que l'augmentation du nombre de nœuds ou de jetons de gouvernance peut toutefois contribuer à limiter. En effet, il peut y avoir une concentration des nœuds de validation dans les consensus de proof of stake par voie de *staking.* Se pose alors la question de la titularité ou la propriété de l'actif numérique utilisé pour valider les blocs.

Définir un seuil de concentration au-delà duquel le risque d'action de concert ou de commission de fraudes pourrait être plus élevé est donc extrêmement incertain. La multi-signature, les votes (avec quorum), la sanction infligée en cas de désinformation (ou la gratification des cas d'identification d'erreurs de codage ou de fausses nouvelles) ou l'incitation à créer des forums (pour diffuser les bonnes pratiques ou partager l'analyse des risques identifiés) demeurent néanmoins des outils de nature à promouvoir l'information disponible et donc à protéger les investisseurs non professionnels.

Ces dispositions réglementaires spécifiques devraient toutefois demeurer proportionnelles aux risques identifiés et ne pas excéder, sauf justifications particulières, celles applicables à la finance centralisée.

Annexe

Composition du groupe de travail

Le groupe de travail créé au sein de Paris Europlace inclut, sous la coordination de Philippe Goutay (Jones Day), les contributeurs suivants[1] :

- Annabelle Bernal (Société Générale Forge)
- Stéphane Blemus (Société Générale Forge)
- Victor Charpiat (Kramer Levin)
- Agnès Chatellier (BNP Paribas)
- Yves Chouefaty (Tobam)
- Myriam Dana-Thomae (AFG)
- Mia Dassas (Allen & Overy)
- Marianne Demarchi (Swift)
- Jean-Marc Eyssautier (Valparaiso Conseil)
- Muriel Faure (AFG, Tiepolo)
- Morgane Fournel Reicher (Kramer Levin)
- Mark Kepeneghian (Kriptown)
- Thierry Javois (Lionne Finance)
- Delphine Marchand (Allen & Overy)
- Sébastien Praicheux (Norton Rose Fulbright)
- Sylvain Prigent (Société Générale Forge)
- Thierry Redon (BPCE)
- Diane Richebourg (Jones Day)
- Marc Ripault (PwC)
- Alain Rocher (Société Générale Securities Services)
- Olivier Taille (Natixis)
- Hubert de Vauplane (Kramer Levin)
- Olivier Vigna (Paris Europlace)
- Virginie Vignon-Priam (BNP Paribas)
- Jérémie Vuillquez (La Française)

[1] 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.