FORUM FINTECH ACPR-AMF

Synthèse des réponses à la consultation publique du Groupe de Travail ACPR-AMF sur la certification des *Smart Contracts* – Une proposition de certification des *smart contracts* : Vue d'ensemble, considérations techniques et points de discussion réglementaires

1. Introduction

Le 3 février 2025, le groupe de travail sur la certification des *smart contracts*, créé sous l'égide du Forum Fintech ACPR-AMF, a publié un rapport, soumis à consultation publique. Ce rapport présente les réflexions développées par le groupe sur les considérations techniques et les enjeux réglementaires soulevés par la question de la certification des *smart contracts*, dans l'éventualité d'une règlementation à venir de la finance décentralisée (DeFi). À la suite de cette publication, le Groupe de Travail (GT) avait invité les acteurs à faire part de leurs commentaires afin de soutenir la réflexion sur ces travaux exploratoires.

Le rapport visait à étudier les possibilités de certification et les modalités d'audit des *smart contracts* afin d'envisager la façon dont une règlementation pourrait intégrer un mécanisme de certification. Le rapport a ainsi identifié dans un premier temps des principes de sécurité, de gouvernance et de conformité du service fourni, applicables à différents environnements d'exécution des *smart contracts*. Le rapport a ensuite étudié dans un deuxième temps les pratiques et les méthodes d'audit pouvant servir à un processus de certification, en distinguant différents schémas en fonction de la personne délivrant la certification : soit par une autorité publique, sur la base d'un audit effectué par un organisme agréé, soit par l'auditeur lui-même, soit par le fournisseur du *smart contract* via un mécanisme d'auto-certification. Dans un troisième et dernier temps, le rapport a exploré les différentes approches réglementaires possibles, soit l'idée d'une certification optionnelle, d'une certification obligatoire pour tous les *smart contracts*, ou d'une certification intégrant des mesures de proportionnalité.

À la suite de cette publication, un certain nombre de réponses aux questions posées lors de la consultation ont été reçues, permettant de préciser certains des aspects techniques soulevés, et d'approfondir la réflexion. Le présent document propose une présentation synthétique de ces retours de consultation. L'ACPR et l'AMF tiennent à remercier les répondants, et entendent poursuivre la discussion avec eux et les parties prenantes.

> Il est rappelé que le rapport sur la certification des *smart contracts* reflète les travaux et les discussions du groupe de travail, et ne constitue à ce titre ni une proposition d'encadrement règlementaire, ni une position officielle de l'ACPR, de l'AMF, ou d'une autre autorité ayant participé à ce groupe de travail.

Plan du papier de synthèse

Ce document de synthèse, après avoir rapidement précisé le profil des répondants, propose une vue d'ensemble des réponses à la consultation, selon l'ordre des thèmes abordés dans le rapport. Dans un premier temps, il aborde les principes proposés en matière de standards de certification puis les modalités de réalisation des audits de *smart contracts*. Il analyse dans un second temps les réponses apportées aux réflexions réglementaires et les schémas de certification envisagés dans le rapport, avant de conclure sur le contexte règlementaire au niveau européen et international, ainsi que les suites envisagées.

Analyse des réponses : profil des répondants

Le Groupe de travail ACPR-AMF a recueilli 20 réponses au rapport sur la certification des *smart contracts*. Les répondants présentent un profil diversifié, comprenant à la fois des acteurs ayant un lien avec l'univers de la DeFi (porteurs de projets, fondations, ou associations blockchain), des acteurs centralisés du secteur des crypto-actifs, des acteurs de la finance dite « traditionnelle », des cabinets de conseil et d'audit, ou d'autres types d'acteurs, incluant des fournisseurs de technologie, des associations de place sur les activités en crypto-actifs, ou des répondants individuels.

Le tableau ci-dessous indique la proportion de réponses obtenues par catégorie de répondants :

Type d'acteur	Représentativité par type d'acteur
Acteurs DeFi	**10%**
Acteur Crypto	**5%**
Auditeurs	**15%**
Acteur de finance traditionnelle	**5%**
Associations de place	**35%**
Fournisseur de technologie/outils	**15%**
Autre	**15%**

La démarche du GT ACPR-AMF a été saluée pour avoir établi un point d'ancrage des discussions quant aux potentielles voies permettant un encadrement des *smart contracts* au contexte de la DeFi. Les répondants ont notamment salué l'approche factuelle relayée dans le rapport et l'analyse équilibrée entre risques et opportunités quant aux différents mécanismes de certification envisagés.

Les réponses apportées permettent d'enrichir les réflexions du groupe, à la fois sur les thématiques techniques développées sur les principes de sécurité, de gouvernance et de conformité des *smart contracts* et les méthodes d'audit, ainsi que sur les potentielles pistes réglementaires en lien avec un schéma de certification.

2. Synthèse des réponses sur les aspects techniques (standards, audit)

2.1 Standards

Une majorité des répondants ont exprimé leur accord avec les principes présentés dans le rapport qu'ils indiquent être alignés avec les bonnes pratiques prônées par l'industrie, apportant cependant une certaine nuance sur plusieurs des principes évoqués.

Principes de sécurité, de gouvernance et de conformité

Concernant les **principes de sécurité**, plusieurs répondants ont notamment mis en avant la nécessité de n'adopter que des principes généraux, et technologiquement neutres. En particulier, les réponses ont relevé que les principes développés dans le rapport paraissaient centrés sur une analyse des blockchains de type EVM (*Ethereum Virtual Machine*), se focalisant moins sur d'autres écosystèmes tels que Solana ou Cosmos. Or, il existe des différences de nature technique dans la manière dont les différents standards mis en avant peuvent être appliqués, notamment dans la rédaction du code, et en fonction des environnements d'exécution offerts par ces différentes blockchains. Ces réponses s'accordent avec l'approche hiérarchisée évoquée dans le document : « des principes de haut niveau pouvant s'appliquer à toutes les blockchains et leurs interfaces, puis des recommandations plus précises dépendant de la technologie ou famille technologique employée ».

Certains répondants ont également considéré que le principe de séparation des tâches pour l'exercice de processus métiers distincts (principe n°6) serait contre-productif, eu égard à l'importance des connaissances du rédacteur du *smart contract* pour permettre d'en identifier les failles.

Par ailleurs, les répondants ont également mentionné l'intérêt qu'il peut y avoir à renforcer le principe du moindre privilège, lequel prévoit que chaque entité dispose uniquement des autorisations strictement nécessaires à l'accomplissement de leurs tâches (principe n°5). Ils préconisent dès lors l'ajout de garde-fous et de mécanismes de contrôle des fonctions administratives d'un *smart contract*, comme l'obligation d'utiliser des dispositifs *multisig*[1].

Concernant les **principes de gouvernance**, certains répondants considèrent que la réflexion pourrait davantage souligner les risques liés à la centralisation de la gouvernance, et proposent différentes méthodes pour maîtriser ces risques. En particulier, des mesures de contrôle de la concentration du pouvoir de décision sur l'évolution d'un *smart contract* ou d'un protocole pourraient être ajoutées, notamment au sein d'organisations autonomes décentralisées (DAOs), via des mécanismes permettant de lutter contre les risques de manipulation de vote ou de la gouvernance, tels que le recours au vote quadratique, la mise en place de règles de quorum, ou encore de règles de transparence des délégations de vote.

Une réponse a notamment souligné qu'un mécanisme de certification, en mandatant un audit du modèle de gouvernance, en imposant de mettre en place des mécanismes de protection contre les attaques sur la gouvernance, et des obligations de divulguer la répartition des droits de vote et les changements dans la distribution des jetons de gouvernance, pourrait également permettre d'attester du niveau de décentralisation du protocole. Certains interlocuteurs ont également soulevé l'importance de prendre en compte les étapes de gouvernance ayant lieu *off-chain*[2].

Enfin, concernant **les principes de conformité**, de nombreuses réponses ont montré leur désaccord avec l'intégration de la notion de « frais de gaz[3] raisonnables », certains considérant qu'un montant « raisonnable » serait trop difficile à définir, d'autres soulignant que les concepteurs de protocole ont peu de moyens pratiques pour encadrer le coût induit qui dépend en particulier de l'infrastructure blockchain sous-jacente. Certains répondants mettent en avant que des recommandations relatives aux questions d'optimisation des frais de gaz sont déjà présentes dans certains rapports d'audits et

[1] Dispositifs de signatures multiples

[2] Environnement technique en dehors de la blockchain (contraire de *on-chain*)

[3] Les frais de gaz sont, sur certaines blockchains, les paiements dus par les initiateurs de transactions afin que ces dernières soient réalisées sur ces blockchains.

que, sauf cas exceptionnel, il est toujours dans l'intérêt des protocoles de voir les frais de gaz diminuer. Un des répondants propose alors de prévoir l'intégration d'une analyse de type coût / performance en ce sens au cours de l'audit.

Certains répondants ont également souligné la difficulté d'intégration d'obligations réglementaires directement au sein des *smart contracts*, considérant que la règlementation a vocation à s'appliquer au niveau de la couche applicative, soit au niveau de l'interface ou de l'intermédiaire permettant l'accès au *smart contract*, plutôt qu'au niveau de la logique programmée (les *smart contracts*). Un répondant ajoute que de telles exigences réglementaires au niveau des *smart contracts* nécessiteraient le maintien du contrôle des développeurs sur le code pour garantir la conformité de ceux-ci au regard de ces exigences (compte tenu que la réglementation financière consiste en des règles établies de manière *off-chain,* qui ne peuvent être traduites automatiquement), ce qui ne serait pas nécessairement souhaitable selon ce répondant.

Cycle de vie des *smart contracts*, bonnes pratiques, et standardisation à l'international

Concernant les réflexions relatives au **cycle de vie des *smart contracts***, les répondants se sont interrogés sur la mise en place pratique du principe prescrivant la sécurisation du *smart contract* tout au long de son cycle de vie, y compris lors de changements subséquents.

Les acteurs ont notamment souligné que le caractère dynamique de la blockchain et des innovations construites sur cette technologie n'est, dans l'ensemble, pas suffisamment pris en compte. Bien que déjà mentionné dans le rapport, certains répondants ont insisté sur l'introduction de mécanismes de *timelock*[4] et de *rollback*[5] en lien avec les mises à jour de code, et ont suggéré que soient précisés les seuils de matérialité relatifs aux « changements subséquents » impactant la mise à jour de la certification.

Un répondant souligne aussi qu'il ne faut pas négliger la question de la fin de vie éventuelle d'un protocole. Selon lui, une politique de mise hors service progressive, assortie d'une notification claire aux utilisateurs et d'un désengagement sécurisé, contribuerait grandement à renforcer la confiance dans les protocoles et à éviter des incidents tardifs.

Enfin, une grande majorité des répondants ont invité dans leurs réponses les autorités de régulation à se rapprocher des acteurs de l'industrie, afin que soient définis des standards et principes alignés avec les bonnes pratiques actuelles, et / ou s'appuyant sur les cadres existants (ISO 27001, NIST, OWASP, EthSecurity, EthAlliance, etc.), soulignant par ailleurs l'importance de l'application coordonnée de tels standards ou principes à l'international. Cette approche est bien reflétée dans le document qui souligne le rôle et la concertation nécessaire des acteurs de l'industrie dans l'établissement des standards.

[4] Un time lock introduit un délai avant l'introduction d'une mise à jour, permettant aux utilisateurs et auditeurs de l'examiner avant qu'elle ne prenne effet.

[5] Un système de rollback permettrait d'annuler une mise à jour en cas de problème, évitant ainsi des incidents catastrophiques.

2.2 Audit

Une majorité de répondants a manifesté son accord avec les pistes étudiées par le groupe de travail dans l'identification des différentes méthodes d'audit et les problématiques et enjeux soulevées par celles-ci.

Type d'audit : outils automatiques ou non, et emploi de méthodes formelles

Certains répondants ont souhaité approfondir la réflexion sur les développements techniques du rapport, et ont présenté des avis divergents quant à la réalisation de l'audit en plusieurs étapes. Certains ont estimé que tout cadre de certification devrait encourager l'adoption de plusieurs « couches » d'audit, mettant en œuvre différentes méthodes, considérant qu'il est important de poursuivre l'analyse du *smart contract* après son déploiement et tout au long de son cycle de vie, soulignant l'importance d'une surveillance continue qui pourrait s'appuyer sur des mécanismes d'automatisation permises par la technologie blockchain.

Certains répondants font valoir, en revanche, que la réalisation d'un audit en plusieurs phases, l'une qui porterait sur le code source et l'autre sur le code une fois déployé, introduirait de nouvelles problématiques, notamment la nécessité de prévoir la possibilité de mise à jour (« *upgradability* ») des *smart contracts* déjà déployés pour tenir compte des résultats du second audit, créant ainsi un nouveau vecteur de risque et augmentant le coût et la durée de la certification.

L'usage de la méthode formelle pour réaliser l'audit des *smart contracts* a constitué un point de discussion important. Bien que la valeur de cette méthode ait été reconnue par les répondants, il a été suggéré qu'elle ne soit appliquée qu'aux *smart contracts* considérés comme critiques, car elle implique un usage important de ressources et la mobilisation d'experts spécialisés, dont le nombre est pour l'instant limité ; la détermination du caractère critique d'un *smart contract* faisant par ailleurs écho aux critères de proportionnalité (voir section 3 ci-dessous). Par ailleurs, plusieurs répondants ont indiqué que l'usage combiné de l'audit manuel et d'outils de vérification automatique constituait une bonne pratique déjà en place dans l'industrie.

Enfin l'usage émergent de l'intelligence artificielle (IA) dans l'audit des *smart contracts* est reconnu par des répondants comme un outil pouvant assister dans la délimitation du périmètre du code à auditer plus précisément, mais qui ne peut se substituer aux autres techniques d'audit. Ce point est souligné dans le rapport.

Dans une logique de proportionnalité, certains répondants ont suggéré que des exigences allégées soient appliquées à des *smart contracts* totalement immuables dans la mesure où la gouvernance de ces *smart contracts* et les risques induits par la gouvernance sont en théorie négligeables voire nuls. En effet, d'après ces derniers, l'immuabilité totale des *smart contracts* pourrait résoudre le problème d'une potentielle modification de la logique du protocole contrevenant aux intérêts des utilisateurs, justifiant ainsi que des exigences allégées leurs soient appliquées.

Étendue de l'audit : le *smart contract* et ses dépendances externes

Les répondants ont également débattu de l'étendue de l'audit, afin de savoir si celui-ci devrait se limiter au seul *smart contract* audité, à l'ensemble des *smart contracts* avec lequel le *smart contract* initialement audité interagit, ou à l'ensemble des dépendances de ce *smart contract* (ex : oracles, et autres éléments de dépendance *off-chain*). Des répondants ont défendu une approche extensive intégrant autant que possible ces dépendances externes, ou si cela n'est pas possible, mettant en

évidence pour les utilisateurs que la certification accordée d'un *smart contract* n'intègre pas certaines composantes (comme un oracle par exemple).

Déclenchement de l'audit et durée de la certification

Concernant le déclenchement de l'audit, la question de la proportionnalité reste primordiale pour de nombreux répondants et se rapproche de la notion de criticité des *smart contracts*. En effet, pour une majorité de ceux-ci, il convient d'adopter une approche fondée sur les risques, qui pourrait, comme suggérée dans le rapport, être fonction de la TVL[6], de la criticité du *smart contract*, de son nombre de dépendances externes, ou d'autres facteurs. La définition des critères de proportionnalité est capitale en ce qu'elle permettrait de déterminer quel changement du *smart contract* serait considéré comme significatif ou substantiel, et serait de nature à déclencher un nouvel audit. Cette approche proportionnelle serait également utilisée pour déterminer la durée de validité d'une certification.

Certains répondants s'opposent cependant à l'idée de mettre en place de tels critères de proportionnalité, dont l'établissement de métriques pertinentes, soulignant l'excessive complexité de leur mise en œuvre.

La question de la durée de validité de l'audit et de la certification qui en découle, a également fait l'objet de réponses divergentes de la part des acteurs. Là où de nombreux répondants ont considéré qu'une durée de validité de 3 ans était appropriée en écho à des standards de diverses industries, d'autres ont proposé des durées et méthodes de renouvellement alternatives. Ainsi, plusieurs acteurs estiment que la durée de 3 ans serait trop longue, et proposent que la certification des *smart contracts* suive le modèle des audits de type SOC II[7], qui fonctionnent sur la base d'un audit complet de re-certification requis tous les deux ans, avec un examen annuel plus léger entre les deux.

Un nombre significatif d'acteurs souhaitent que la durée de validité de l'audit et de la certification qui en résulte ne soit pas fixe mais proportionnelle à la complexité du *smart contract* audité, qui serait par exemple évaluée sur la base du nombre d'interactions ou de dépendances externes, ou du degré de mutabilité.

Enfin certains répondants soulignent qu'un mécanisme de surveillance continu des *smart contracts* serait plus à même de détecter les *smart contracts* ne répondant plus à certaines exigences ayant permis la délivrance de la certification, ce qui permettrait de déclencher proactivement un nouvel audit sans attendre l'échéance planifiée du prochain audit.

Les acteurs de l'audit

Concernant les acteurs de l'audit, les répondants ont invité le groupe de travail à prendre en compte les différentes solutions d'audit décentralisé tels que les *bug bounties*, les audits communautaires, ou les concours d'audit. Ces solutions ont été présentées comme aptes à pouvoir répondre aux exigences mises en avant dans le rapport, tout en permettant aux projets de moins grande envergure d'être audités.

---

[6] *Total Value Locked* : indicateur couramment utilisé DeFi permettant d'évaluer une empreinte des différents protocoles ; il mesure le montant des actifs verrouillés au sein d'un protocole.

[7] SOC 2 est une norme volontaire mise en œuvre par les entreprises de technologie et de *cloud computing* pour garantir la conformité à la confidentialité des données. Le standard est publié par *l'American Institute of Certified Public Accountants* (AICPA).

Dans un contexte de tension, témoigné à ce jour par la majorité des répondants sur la disponibilité des ressources d'auditeurs expérimentés et spécialisés sur les *smart contracts*, ces derniers invitent à l'inclusion d'auditeurs tiers ou individuels dont l'expérience serait démontrée par des certifications ou des formations spécifiques.

Dans ce contexte certains répondants soulignent par ailleurs le besoin d'une démarche organisée de formation des auditeurs en *smart contracts* ou bien d'une certification de ces auditeurs. Un répondant évoque aussi l'idée d'une standardisation du socle de compétences de ces auditeurs afin de permettre le recours à des auditeurs internationaux jugés équivalents et non seulement ceux reconnus par la juridiction de certification des *smart contracts*.

3. Synthèse des réponses pistes règlementaires

Les acteurs de l'industrie ont souligné la pertinence de la distinction entre les différents régimes de certification proposés dans le rapport et ont indiqué leur préférence quant aux différents schémas envisagés. Parmi les répondants qui se sont exprimés sur cette partie du rapport, 85% d'entre eux favorisent l'adoption d'un régime de certification optionnel.

Concernant le **régime optionnel**, les répondants ont considéré qu'il offrirait une plus grande souplesse aux acteurs et préserverait la compétitivité de l'écosystème européen des crypto-actifs, tout en encadrant les risques qui en émergent de manière adéquate. Ce régime favoriserait l'établissement de bonnes pratiques, sans pour autant imposer de contraintes aux acteurs, qui pourraient ainsi décider eux-mêmes d'obtenir la certification une fois la maturité de leur modèle d'affaires atteinte. La certification est, dans ce cas, envisagée comme un avantage compétitif.

Concernant le **régime obligatoire**, plusieurs répondants ont souligné les potentiels risques de centralisation liés à ce type de schéma. Certains estiment qu'il pourrait être en contradiction avec le principe de décentralisation, notamment en créant une barrière à l'entrée de l'écosystème, en particulier pour les développeurs indépendants et les *start-ups*, qui pourraient avoir des difficultés à répondre à ces exigences de conformité. La critique principale insiste sur les coûts et délais qui seraient potentiellement associés à un schéma de certification obligatoire, ce qui pourrait nuire à la compétitivité de l'écosystème européen. Enfin, les répondants soulignent également que, du fait d'un manque de maturité du secteur DeFi, la réglementation interviendrait à un stade de développement prématuré de l'écosystème.

Concernant, le **régime obligatoire avec proportionnalité**, les avis des répondants sont partagés. Bien qu'ils étendent les critiques faites à l'égard du régime obligatoire, plusieurs répondants sont favorables à l'établissement de critères de proportionnalité permettant une prise en compte plus adaptée à chaque *smart contract*.

Le périmètre de certification

Les répondants ont également abordé la question du périmètre de la certification, s'attardant en particulier sur la possibilité ou non de concilier certification d'un protocole et de ses *smart contracts* sous-jacents. Ainsi, certains acteurs considèrent que cette conciliation est possible si elle respecte le caractère modulaire de la DeFi et qu'elle prend en compte l'ensemble des caractéristiques du protocole, en intégrant les interactions des *smart contract*s entre eux ainsi que leurs différents vecteurs de centralisation, caractérisés par l'usage de tout élément constituant des potentiels points de défaillance unique (par exemple : utilisation de *bridges*, d'oracles, ou d'éléments *off-chain*, etc.).

D'autres répondants considèrent en revanche qu'il y a lieu de distinguer entre les *smart contract*s et les protocoles, rejetant le principe de certification du protocole dans son ensemble. D'autres modèles lui sont préférés, par exemple avec pour point de départ un raisonnement fondé sur une base de code partagée (*codebase*[8]), indiquant que la certification d'une première adresse permettrait alors de certifier l'ensemble des adresses ayant la même *codebase*, c'est-à-dire reprenant le même code commun.

Le mécanisme de certification : Publication de la certification

À propos du mécanisme de certification et notamment de son caractère public, les répondants ont apporté leurs réflexions aux méthodes permettant de s'assurer de la publication et de l'affichage de la certification par un acteur. Comme envisagé par le groupe de travail, les solutions présentées préconisent généralement un accès à l'état de certification du *smart contract* (certifié, non certifié, certification révoquée, etc.) directement *on-chain* via des NFTs par exemple, ou par le maintien d'un certificat.

Certains acteurs avancent par ailleurs la distinction entre un modèle de certification statique (soit pour une période donnée) et un modèle de certification dynamique où la surveillance est continue plutôt que périodique. Certains répondants seraient favorables à une certification continue, où certains contrôles automatisés seraient exécutés en permanence à travers des mécanismes *on-chain* ou *off-chain*, les résultats permettant d'indiquer l'état de la certification, qui serait automatiquement publiable sous la forme d'un certificat *on-chain*. Un des répondants mentionne alors la possibilité de construire un protocole de surveillance géré par l'organisme d'accréditation des auditeurs de *smart contracts*, ou par l'autorité de régulation, qui surveillerait directement les mises à niveau ou tout autre changement pertinent apporté à un protocole.

Un des répondants a également proposé l'adoption d'un système similaire à celui des certificats SSL/TLS[9] pour les navigateurs web. Il soutient que la mise en œuvre d'un tel système nécessiterait la tenue d'un registre, qui pourrait être un registre ouvert (registre de contrat Ethereum ou une API de base de données *off-chain* que les portefeuilles interrogeraient), indiquant le signalement ou la suppression automatique de certificats expirés. Cela nécessiterait la mise en place d'une infrastructure d'émission de certificats et de surveillance, supervisée par un organisme gouvernemental ou un mécanisme de gouvernance de l'industrie. Idéalement, le répondant soutient que le registre devrait fonctionner de manière décentralisée, ou tel un bien commun maintenu par un consortium, regroupant des experts de la blockchain, de la sécurité et de l'audit ainsi que des régulateurs, afin d'éviter les points de défaillance unique.

Certains répondants penchent également pour un régime de surveillance *ex post* assuré par les autorités de régulation, dans lequel l'ensemble des formes d'audits seraient reconnues (audits décentralisés, *bug bounties*, concours d'audit, etc.). Certains répondants ajoutent qu'un tel schéma supposerait une définition claire des pouvoirs de supervision accordés à ces autorités.

Un des répondants a également mentionné d'autres tentatives de régulation de la DeFi, par exemple grâce à l'exigence pour les protocoles de mettre en place un fonds ou une police d'assurance pour

---

[8] La *codebase* correspond à l'ensemble du code source d'un logiciel, d'un composant ou d'un système.

[9] Les certificats SSL/TLS sont des fichiers numériques utilisés pour sécuriser la communication entre un client (comme un navigateur web) et un serveur (comme un site web) en activant le chiffrement des données échangées. Lorsque quelqu'un accède à un site en HTTPS, le navigateur vérifie le certificat SSL/TLS pour établir une connexion sécurisée.

couvrir certains risques, comme le risque de *hack*, se référant à l'idée d'un « coussin excédentaire » de certains protocoles qui agit comme une police d'assurance couvrant certaines pertes.

4. Conclusion

La consultation menée sur le rapport du Groupe de travail sur la certification des *smart contracts* a permis d'enrichir la réflexion sur les aspects suivants.

Concernant les **standards**, les retours de consultation montrent un accord général avec les principes proposés, jugés globalement alignés avec les bonnes pratiques de l'industrie, tout en appelant à des ajustements. Les répondants recommandent des principes de sécurité plus généraux et neutres technologiquement, soulignent les limites de certains standards trop centrés sur les blockchains EVM, et recommandent d'exploiter au mieux les fonctions décentralisées propices à réduire les risques de sécurité et de gouvernance. Sur la conformité, des réserves sont émises sur la notion de « frais de gaz raisonnables » et l'intégration directe de contraintes réglementaires. Enfin, un appel fort est lancé pour une coordination internationale autour de standards existants.

Les retours sur la partie **audit** du rapport témoignent également d'un accord général avec les pistes évoquées par le groupe, tout en invitant à davantage de nuance. Les répondants soutiennent une approche multicouche combinant audits manuels, outils automatiques et, pour les *smart contracts* critiques, l'utilisation de méthodes formelles. Une logique de proportionnalité est plébiscitée, tant pour déclencher l'audit que pour en définir l'étendue et la durée de validité, bien que certains pointent la complexité de sa mise en œuvre. Les répondants soulignent que l'audit devrait aussi couvrir les dépendances externes. Enfin, les réponses encouragent la reconnaissance d'acteurs variés, incluant audits décentralisés, *bug bounties* et experts tiers certifiés.

Enfin, concernant les **pistes réglementaires,** une large majorité des répondants soutiennent l'instauration d'un régime de certification **optionnel**, jugé plus souple et favorable à l'innovation, tout en permettant d'instaurer de bonnes pratiques sans freiner l'entrée des acteurs. Le **régime obligatoire** est critiqué pour ses risques de centralisation et ses contraintes disproportionnées, notamment pour les petits projets. Le **régime avec proportionnalité** reçoit un accueil plus nuancé. Le **périmètre de certification** suscite débat : certains plaident pour une approche globale par protocole, d'autres préfèrent une certification par base de code (*codebase*). Enfin, les répondants défendent l'idée de **certifications publiques**, dynamiques et vérifiables *on-chain*, potentiellement gérées par un registre décentralisé, un consortium ou par des autorités publiques.