Conservation et garde d'actifs numériques : questionnaire

Réponse de Woorton, réalisée en concertation avec Gide 255

Définition des services de garde / conservation

En l'état actuel, le projet de loi, dans sa typologie des prestataires de services sur actif numérique, fait mention de « service de conservation pour le compte de tiers d'actifs numériques ou de clés cryptographiques privées, en vue de détenir, stocker et transférer des actifs numériques ». Cette appellation semble néanmoins désigner plusieurs activités distinctes, parmi lesquelles la conservation ou la garde de clés cryptographiques ou encore celle de jetons.

Remarque introductive sur la nature des actifs numériques en lien avec lesquels les services visés par le projet de loi PACTE, dont la conservation, sont rendus :

Le projet de loi PACTE (plan d'action pour la croissance et la transformation des entreprises) définit les prestataires de services sur actifs numériques comme les prestataires fournissant différentes prestations listées dans le projet de loi sur les actifs numériques. Ces actifs sont définis dans le projet de loi et incluent, en substance, la notion de « monnaie virtuelle ». Cette notion est reprise de la directive européenne 2018/843 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme.

Or, cette notion de « monnaie virtuelle » prévue dans la directive européenne 2018/843 est plus large que les crypto-actifs, car elle ne fait pas référence à un quelconque enregistrement sur la blockchain.

Il serait opportun de restreindre les dispositions du projet de loi PACTE, en ce qu'elles concernent le régime d'agrément optionnel pour les prestataires sur actifs numériques, aux seuls prestataires dont les activités sont développées sur des actifs numériques encryptés et enregistrés sur un dispositif d'enregistrement électronique partagé (i.e, les crypto-actifs).

Dans la suite de ce document, les commentaires qui seront faits auront trait uniquement au service de conservation sur crypto-actifs (i.e., actifs numériques encryptés et enregistrés sur un dispositif d'enregistrement électronique partagé).

Par ailleurs, concernant la transposition de la directive européenne 2018/843, le considérant 10 de cette directive distingue de la notion de « monnaie virtuelle » qu'elle introduit de différentes notions, notamment celles mentionnées prévues dans la directive 2015/2366. Cette distinction introduite dans la directive européenne nous semble devoir être introduite dans le projet de loi PACTE.

Il est à noter qu'avec le développement de la technologie blockchain, des nouvelles modalités pour assurer la garde de crypto-actifs dans le but de détenir, stocker et transférer des crypto-actifs sont apparues. En effet les services de garde par un tiers se sont développés du fait de besoins à court terme :

- *des transactions « off-chain » (en dehors de la blockchain et donc notamment sur des plateformes d'échanges centralisées) plus rapides. Du fait des problèmes de passage à l'échelle de la technologie blockchain, les plateformes d'échange ont par le passé principalement été utilisées pour échanger des crypto-actifs.*
- *Besoin de rapidement respecter un cadre réglementaire existant en utilisant un dépositaire ou un service de garde dans certains pays pour garder les clés privées. Cette nécessité réglementaire bien que prévue pour réduire le risque que porte l'investisseur dans le secteur financier traditionnel augmente le risque dans le secteur crypto / blockchain en introduisant une concentration d'actifs chez certains acteurs. Apparait alors potentiellement un risque systémique.*

Actuellement, la blockchain et les smart contracts peuvent être utilisés pour permettre à un acteur de garder ses crypto-actifs selon un dispositif transparent, sécurisé et moins couteux que le cadre actuellement prévu dans la réglementation financière.

Il est donc important, dans le souci d'accompagnement en Europe de l'innovation, de s'interroger sur l'opportunité de faire évoluer à terme les règles européennes sur la conservation et la garde d'actifs pour tenir compte de ces évolutions.

- ***En pratique, quelles différences faites-vous entre ces activités (i.e., la conservation ou la garde de clés cryptographiques ou encore celle de jetons) ?***

Les différences reposent au départ sur les caractéristiques techniques des crypto-actifs et des protocoles blockchain à partir desquels ils sont émis ; et imposent par conséquent de clarifier certaines définitions créées pour les instruments financiers qui ne s'inscrivaient pas, lorsqu'elles ont été écrites, sur le même environnement technologique.

De plus, les crypto-actifs, depuis leur émission sur le marché primaire, jusqu'à leur revente sur le marché secondaire, en passant par leur stockage momentané sur un support technologique sécurisé adapté, nécessitent d'introduire de nouveaux concepts. Notamment, les notions de "garde de crypto-actifs" et de "supports technologiques sécurisés" doivent être distingués très précisément dans leurs fonctionnements respectifs, et en responsabilité juridique, de la notion englobante de "conservation" telle que définie à droit constant.

En pratique, les transactions sur crypto-actifs requièrent une clé privée (afin de signer les transactions) et une clé publique (afin d'identifier le destinataire de la transaction).

Le service de garde, et l'éventuelle obligation de restitution (voir ci-dessous), devrait porter sur les crypto-actifs, même si cette prestation implique, techniquement, que soit générée une clé privée au solde de laquelle seront conservés les crypto-actifs gardés. La restitution des clés privées n'est pas possible et ne correspond pas au fonctionnement des blockchains.

Juridiquement, le propriétaire de crypto-actifs gardés par un prestataire ne perd pas, du fait de l'externalisation de cette garde, son droit de propriété et les prérogatives associées. Cependant, le prestataire du service de garde peut être considéré, du point de vue juridique, comme le détenteur des crypto-actifs.

Le prestataire du service de garde dispose d'un contrôle technique sur les crypto-actifs.

- *Pour que les crypto-actifs gardés par un prestataire puissent faire l'objet d'une quelconque transaction, il sera nécessaire de signer ladite transaction avec la clé privée associée par le prestataire aux crypto-actifs qu'il garde.*
- *En tant que détenteur, le prestataire du service de garde doit reconnaitre qu'il n'est pas propriétaire des crypto-actifs gardés et n'entend pas agir comme tel, comme peut le prouver le contrat qui peut être conclu entre le propriétaire et le gardien.*
- *Le prestataire du service de garde ne doit pouvoir effectuer légitimement d'opérations comme la vente ou le prêt des crypto-actifs que dans la mesure où le propriétaire l'y autorise expressément par voie contractuelle.*

- ***Quels exemples d'acteurs pour chacun de ces services ?***

Différents acteurs peuvent être cités, par exemple :

- *Coinbase, LMAX, Circle, SEBA, Bitgo, Xapo*
- *À côté de ces acteurs traditionnels de garde centralisant les actifs, il convient de pourvoir considérer les smart-contracts et la blockchain comme un service de conservation ou comme une méthode de transfert d'actifs de pair à pair. Exemples :*
    - *Melon : un protocole décentralisé qui permet à un fonds d'être créé, opéré, administré et géré selon des limites de risque prédéfinies par du code inscrit dans des smart-contracts. L'investisseur est propriétaire de ses actifs à tout moment et a le choix de garder lui-même ses clés privées relatives aux crypto-actifs qu'il détient ou de déléguer cette garde à un prestataire. Le smart-contract stocke les actifs du fonds et ne permet qu'au gérant du fonds de « dépenser » les crypto-actifs en conformité avec les règles et le profil de risque du fonds. Aucun vol n'est possible sauf du fait de sévère vulnérabilité du code du smart-contract.*
    - *Ox/Ethfinex/Kyber Network/Uniswap/Airswap: Plateforme d'échanges décentralisée sans garde des crypto-actifs. Les actifs de l'acheteur/vendeur ne sont jamais stockés dans un smart-contract. Il s'agit ici d'un échange de pair à pair sur la blockchain de la même manière qu'un transfert "on chain".*
    - *Oasis Dex/IDEX/Etherdelta/DEXY : Plateforme d'échanges décentralisée avec garde des crypto-actifs. Le transfert de pair à pair entre un acheteur et un vendeur à lieu grâce à un smart contract dans lequel les actifs sont stockés.*

      → Pour les deux types d'acteurs précédents, un service de garde ou de conservation n'est pas requis dans la mesure où les transactions sont sécurisées par l'intégrité de la blockchain et/ou des smart-contracts.

- ***Quelles différences entre la « garde » d'actifs numériques et la conservation d'instruments financiers ?***

Dans la réglementation financière, la notion de « conservation d'instruments financiers » est prévue dans différentes dispositions.

Tout d'abord, le service de tenue de compte-conservation est un service connexe aux services d'investissement défini à l'article L. 321-2 du code monétaire et financier. Le règlement général[1] précise que cette activité consiste :

- ***à inscrire dans un compte-titres les titres financiers au nom de leur titulaire, c'est-à-dire à reconnaître au titulaire ses droits sur lesdits titres financiers ;***
- ***à conserver les avoirs correspondants ;***
- ***à traiter les événements intervenant dans la vie des titres financiers conservés.***

Le teneur de comptes-conservateur est lié par différentes obligations, dont l'obligation de restituer les titres financiers qui sont inscrits en compte-titres dans ses livres[2].

Ensuite, la notion de conservation est également visée parmi les missions que les dépositaires que les organismes de placement collectifs désignent. Ces derniers assurent notamment la garde des actifs dans lesquels les véhicules investissement[3], ce qui implique, selon la réglementation :

- ***d'assurer la conservation des instruments financiers enregistrés sur un compte d'instruments financiers ouvert dans ses livres et des instruments financiers qui lui sont physiquement livrés ;***
- ***pour les autres actifs, de vérifie qu'ils sont la propriété de l'organisme de placement collectif et en tient le registre.***

A cette obligation de conservation des instruments financiers est attachée par la réglementation une responsabilité en cas de perte par le dépositaire, ou par un tiers auquel la conservation a été déléguée, des instruments financiers conservés[4]. Cette responsabilité peut, selon les textes, être exclue en cas d'événement extérieur échappant à son contrôle raisonnable et dont les conséquences auraient été inévitables malgré tous les efforts raisonnables déployés pour les éviter.

Ces notions sont distinctes du service de garde des crypto-actifs, telle que proposée en pratique par les acteurs. Ce service n'est à ce jour pas défini spécifiquement dans la réglementation[5]. En pratique, ce service vise l'activité de conservation et de surveillance des crypto-actifs pour le compte de leur propriétaire, ainsi que, possiblement, l'obligation de restitution. Il n'inclut pas en général de prestations telles que l'engagement de traiter des évènements intervenant au cours de la vie des crypto-actifs gardés.

La distinction entre la garde de crypto-actifs et la conservation applicable aux instruments financiers, doit tenir compte de la technologie blockchain qui par construction, crée un registre de transactions et d'informations "conservées" de manière immuable dans une "chaîne de blocs". En d'autres termes, l'"inscription"[6] des éléments constitutifs de l'existence d'un instrument (en l'occurrence ici, l'actif numérique), est inhérente à ce type de protocole.

---

[1] Article 322-3 du règlement général de l'AMF
[2] Article 322-7 du règlement général de l'AMF
[3] Articles L. 214-10-5 et L. 214-24-8 du code monétaire et financier
[4] Articles L. 214-11 et L. 214-24-10 du code monétaire et financier
[5] Hormis les cas où l'actif numérique gardé est requalifiable en instrument financier
[6] Au sens de l'article L. 321-2 du code monétaire et financier

- ***La garde porte-t-elle sur les actifs et/ou sur les clés ?***

Il semble que l'objet du service de garde peut être considéré sur les crypto-actifs ou sur les clés privées (qui permettent techniquement de garder des crypto-actifs). Cependant, il est impératif que l'obligation de restitution qui pourrait y être associée ne porte que sur les crypto-actifs - et pas sur les clés privées.

La clé privée est propre à chaque acteur détenant des crypto-actifs afin que ces derniers puissent faire l'objet d'une transaction, que cet acteur détienne ces crypto-actifs en tant que propriétaire ou en tant que prestataire du service de garde. La conservation de clés privées correspond donc à la modalité technique pour conserver des crypto-actifs.

Lorsque le prestataire du service de garde va restituer les crypto-actifs qu'il a gardés pour le compte de leur propriétaire, il les transfère vers un portefeuille auquel est associée une clé privée différente de celle que ce prestataire a générée pour conserver les crypto-actifs de son client. Le prestataire ne peut pas restituer sa clé privée.

Restitution des actifs

Le projet de loi prévoit que ces plateformes doivent, à tout moment, « être en mesure de restituer les actifs numériques ou les clés cryptographiques conservés pour le compte de leurs clients ». Il s'agit d'une contrainte aujourd'hui applicable en matière de conservation d'instruments financiers et qui paraît de bon aloi du point de vue de la protection des investisseurs.

- ***A l'heure actuelle, existe-t-il des garanties de restitutions apportées par certains acteurs ? Cette garantie porte-t-elle sur les clés ou sur les actifs ?***

Nous comprenons qu'actuellement, il n'existe pas de garantie de restitution associée systématiquement aux prestations offertes par les prestataires de service de garde sur crypto-actifs. Cependant, une obligation de restitution des crypto-actifs peut être explicitée dans le contrat conclu avec le client.

Cette obligation de restitution doit être une obligation de moyens, et non pas une obligation de résultat. En effet, une obligation de résultat imposerait un cadre trop contraignant sur les acteurs, risquant de nuire à l'attractivité du régime français et à la compétitivité des acteurs qui y seraient soumis. Elle doit en outre rester exclue en cas de force majeure[7].

- ***Dans quelles conditions ces derniers sont-ils restitués ? (délai, coût éventuel ...)***

Ces conditions varient selon les prestataires et éventuellement les contrats conclus avec leurs clients.

- ***La restitution des actifs numériques et/ou des clés cryptographiques fait-elle l'objet d'un accord/une convention passé(e) préalablement avec le client ?***

Selon les prestataires, un contrat peut en effet être conclu avec le prestataire fournissant le service de garde et son client prévoyant une obligation de restitution.

[7] Article 1929 du code civil

- ***Est-il possible de revendiquer ses actifs numériques en cas de défaut de l'intermédiaire auprès duquel le compte (wallet) a été ouvert ?***

Le propriétaire de crypto-actifs devrait être en mesure de revendiquer des crypto-actifs gardés par un tiers pour son compte dans l'hypothèse où ledit tiers ferait défaut. En effet, le tiers n'étant pas propriétaire des crypto-actifs, il est essentiel que les crypto-actifs gardés ne soient pas inclus dans les procédures collectives (faillite) dont le tiers pourrait faire l'objet.

A cet égard, il semble essentiel de maintenir l'obligation prévue dans le projet de loi PACTE sur la ségrégation entre les crypto-actifs dont le prestataire est propriétaire et ceux qu'il conserve pour le compte de clients.

Enfin, le dispositif prévu en matière de cyber sécurité pourrait faire l'objet d'un cahier des charges et devrait être auditable par les organes de supervision en matière de sécurité des systèmes d'information (ex : ANSSI). Ce dispositif associé aux règles de ségrégation, devrait ainsi permettre le transfert des portefeuilles de clé à un autre prestataire en cas de faillite par exemple.

Au vu de l'évolution de la technologie et de la capacité de celle-ci de permettre à chacun de garder ses actifs de manière plus sécurisée que par le biais de prestataires de garde, il convient de considérer le cas de la « self custody » qui semble être l'avenir logique et attendu de l'écosystème et notamment des développeurs façonnant ces technologies.

Aussi, si un acteur a recours à un smart-contract en tant que conservateur, ce dernier doit être conscient du risque de sécurité et donc du risque financier lié à une sévère vulnérabilité dans le code. Il doit en conséquence y avoir une transparence sur le smart-contract et une documentation facilement disponible sur les précédents et actuels audits du smart-contract.

Si l'utilisateur conserve lui-même ses clés privées il doit être tenu entièrement responsable (cas de Melon ou des plateformes d'échange décentralisée sans garde.

Sur qui porte la responsabilité en cas de perte ou vol des actifs ou des clés confiés à l'intermédiaire en dehors de toute faute du client ?

Le régime de responsabilité est en général précisé dans le contrat conclu avec le client.

Il est essentiel que la réglementation encadrant le service de garde de crypto-actifs prévoie un dispositif clair en termes de responsabilité des prestataires fournissant ce service, afin d'assurer la crédibilité du dispositif.

En cas de perte ou de vol des actifs, et hors cas de force majeure, la réglementation pourrait prévoir la responsabilité du prestataire de service de garde s'il n'a pas fait ses meilleurs efforts pour conserver et restituer les actifs, dans les conditions prévues par le contrat.

<u>Règles applicables</u>

Les règles actuellement prévues par le projet de loi PACTE pour le service de « conservation » des actifs numériques sont les suivantes :

1° Ils concluent avec leurs clients une convention définissant leurs missions et leurs responsabilités ;
2° Ils établissent une politique de conservation ;

3° Ils s'assurent qu'à tout moment ils sont en mesure de restituer les actifs numériques ou les clés cryptographiques conservés pour le compte de leurs clients ;
4° Ils ségréguent les détentions pour le compte de leurs clients de leurs propres détentions ;
5° Ils s'abstiennent de faire usage des actifs numériques ou des clés cryptographiques conservés pour le compte de leurs clients, sauf consentement exprès et préalable des clients.

- ***Ces règles doivent-elles être adaptées pour tout ou partie des acteurs ?***

Ces dispositions doivent définir un équilibre pour (i) prévoir des contraintes adaptées aux risques générés par la fourniture du service de garde et (ii) ne pas imposer des obligations qui menaceraient l'attractivité du régime.

L'obligation de restitution de la part des prestataires du service de garde est, à ce jour et compte tenu de l'état du marché, une contrainte forte qui ne s'impose pas actuellement aux acteurs fournissant ce service.

Si une telle obligation est prévue, elle doit porter sur les crypto-actifs eux-mêmes et non sur les clés cryptographiques (la restitution de ces dernières étant en pratique impossible). A cet égard, et pour assurer l'effectivité de l'obligation de restitution, un approche fondée sur le principe de proportionnalité pourrait permettre un équilibre entre (i) l'attractivité du régime et (ii) la crédibilité des obligations imposées aux acteurs. Il pourrait être prévu qu'au-delà d'un certain montant de crypto-actifs gardés, des exigences de fonds propres ou d'assurance soient imposées, afin de garantir la capacité des acteurs à restituer les crypto-actifs gardés (lorsque leur responsabilité serait engagée).

En outre, compte tenu de la technologie et du fonctionnement des protocoles blockchain, il est impératif, dans un souci d'attractivité du cadre français, que l'obligation de restitution soit une obligation de moyen et non de résultat. Elle doit également être exclue dans les cas d'évènements échappant au contrôle du prestataire, dont les effets ne peuvent être évités par des mesures appropriées et qui empêchent l'exécution de son obligation. Par exemple, les prestataires ne peuvent être tenus de restituer les actifs en cas de hack de la blockchain sur laquelle sont enregistrés les crypto-actifs.

Pour le secteur financier, comme indiqué ci-dessus, la réglementation européenne a traditionnellement considéré que la garde des actifs de certains acteurs financiers (par exemple les fonds d'investissement) devait être assurée par un tiers agréé (i.e., un dépositaire), dans un souci de protection des investisseurs.

Afin d'encourager l'innovation en Europe et de tenir compte des développements technologiques récents, il semblerait très important d'envisager, à terme, d'adapter ces règles européennes pour certains acteurs du secteur financier. Cette adaptation pourrait notamment permettre de reconnaitre le recours à une technologie de smart-contract ou de blockchain pour tenir le rôle de dépositaire susmentionné tout en gardant le contrôle à l'investisseur.

Ce dispositif permettrait d'assurer la garde d'actifs de façon transparente et moins couteuse que ce que n'impose la réglementation actuelle tout en assurant un même degré de sécurité.

Cette possibilité pourrait être soumise à différentes conditions, dont, par exemple les suivantes (issues des pratiques de marché) :

- *Au moins deux audits de sécurité indépendant doivent être effectués sur le smart-contract et / ou la blockchain avant d'être rendu disponible à tout utilisateur ; et*
- *Des informations claires, notamment sur le régime de responsabilité, pourraient être fournies à l'utilisateur concernant sa responsabilité dans le cas où il souhaite garder lui-même ses accès à la blockchain ou au smart-contract ou faire appel à un service de garde.*

- ***Doivent-elles éventuellement être complétées ? Au niveau de la loi ou via le Règlement général de l'AMF ?***

La proposition pourrait être précisée afin de fournir un confort juridique aux acteurs, dans un souci d'attractivité du cadre, pour préciser la notion de « politique de conservation ».

En outre, *l'agence nationale de la sécurité des systèmes d'information (ANSSI) pourrait également être saisie pour édicter un cahier des charges techniques* ***assurant un socle minimum de mesures dans la construction du dispositif anti-piratage par exemple ("guidelines", bonnes pratiques ou certificat).***

Autres questions :

Pourriez-vous faire la typologie des différents types de contrôle d'actifs numériques (du type clé privé/publique) ?

N/A

Pourriez-vous faire la typologie des différentes formes d'engagement que la plateforme peut prendre vis-à-vis de ses clients en ce qui concerne le contrôle / la propriété des actifs numériques et/ou des clés?

N/A

Informez-vous vos clients lorsque survient une bifurcation (fork) de blockchain ? Les clients réclament-ils deux actifs à l'issue du fork ? Comment traitez-vous ce type de réclamations ?

Actuellement, il n'existe pas de réponse réglementaire et de traitement uniforme par les acteurs des cas de bifurcations. La diversité des approches constatées à ce jour pourrait justifier l'introduction d'une disposition réglementaire sur cette problématique.

A minima, la réglementation pourrait imposer la définition par les prestataires du service de garde agréés d'une politique de gestion des "forks" et sa publication auprès des clients et clients potentiels. Une telle obligation garantirait la transparence du dispositif mis en place par les prestataires et une mise en concurrence entre eux, tout en évitant un cadre trop contraignant susceptible de nuire à l'attractivité du régime français.

Y a-t-il des obstacles à ce qu'il soit prévu que les conservateurs restituent les actifs aux clients à l'issue des bifurcations ?

La restitution des crypto-actifs générés à l'occasion d'un "fork" au propriétaire des crypto-actifs initiaux ne semble pas être une pratique généralisée sur le marché des crypto-actifs.

Une telle obligation généralisée risquerait de nuire à l'attractivité du régime français et à la compétitivité des acteurs qui y seraient soumis.

Cependant, ce cas pourrait être prévu dans la politique de gestion des "forks" communiquée par le prestataire de service de garde à leurs clients.

A l'heure actuelle, quelle méthode de valorisation de vos actifs numériques employez-vous ?

N/A

Selon vous, quels sont les cas qui amèneraient à rendre la ségrégation des actifs entre clients et prestataire impossible ?

Les supports technologiques utilisés par les prestataires du service de garde peuvent jouer un rôle déterminant dans leur capacité à ségréguer les crypto-actifs gardés.

Dans le cas de la « self custody » (via smart-contract ou accès direct à la blockchain), la ségrégation est par définition extrêmement simple à mettre en place.

Vos clients sont-ils informés de la ségrégation ou non entre leurs actifs numériques et ceux de votre plateforme et ceux des autres clients?

Le dispositif de ségrégation dépend des dispositions contractuelles conclues entre le prestataire et le client.

Dans un système de multi-gouvernance de clé privée, en cas de restitution des actifs numériques, comment procédez-vous ? Quelle procédure est mise en place en cas de demande de restitution émanant d'un seul « propriétaire » de la clé ou de conflit entre les différents propriétaires ?

En général, le contrat conclu entre le prestataire du service de garde et son client prévoit les modalités de fonctionnement du système de multi-gouvernance et les circonstances dans lesquelles le prestataire peut légitimement agir sur les instructions des entités impliquées dans le système de multi-gouvernance.

En général, les dispositions contractuelles conclues entre le prestataire et le client prévoient

N/A

L'obligation de détention de fonds propres pour les plateformes vous paraît-elle possible dans l'état actuel de l'écosystème ?

Une exigence de fonds propres trop élevés risque à nouveau de nuire à l'attractivité du cadre du régime français.

Comme suggéré ci-dessus, une approche proportionnée pourrait permettre un équilibre entre (i) l'attractivité du régime et (ii) la crédibilité des obligations imposées aux acteurs.

Il pourrait être prévu qu'au-delà d'un certain montant de crypto-actifs gardés, des exigences de fonds propres ou d'assurance soient imposées, afin de garantir notamment la capacité des acteurs à restituer les crypto-actifs gardés (lorsque leur responsabilité serait engagée).

Le modèle de réglementation japonais qui prévoit que la propriété et la fiscalité dépendent de l'acteur qui a la clé privée en sa possession, vous paraît-il réalisable en pratique en France ?

N/A

Commentaire :