Mission Smart : Comment sécuriser les smart contracts dans un environnement décentralisé de type blockchain ?

Dossier d'appel à Solutions

Date limite de dépôt de candidature :
06/03/2024 à 23h59 (Heure de Paris)

Lien de la candidature :
innovation.banque-france.fr

Sommaire

Table des matières

1. Présentation générale

Dans le cadre de son plan stratégique, la Banque de France a positionné l'innovation comme un vecteur clé de transformation de l'institution. Elle s'empare ainsi des démarches d'innovation pour construire de nouvelles capacités en s'ouvrant aux acteurs innovants (start-up, fintechs, Académiques…) au travers notamment d'expérimentations menées au sein du Lab, son centre d'Open Innovation (Le Lab). En parallèle, le Campus Cyber est un acteur de référence visant à réunir toutes les parties prenantes de la sécurité numérique au sein d'un lieu totem pour protéger la société et faire rayonner l'excellence française du domaine. L'un des champs d'action du Campus Cyber consiste à travailler sur le développement des synergies entre les acteurs publics et privés pour orienter l'innovation technologique et renforcer son intégration dans le tissu économique.

Dans ce contexte, la Banque de France, déjà membre et résidente du Campus Cyber, lance avec ce dernier un Appel à Solutions afin de travailler sur les smart contracts et sensibiliser l'écosystème sur les questions cyber.

La Banque de France et le Campus Cyber sollicitent l'écosystème sur la question suivante : *comment sécuriser les smart contracts dans un environnement décentralisé de type blockchain ?*

L'objectif de cet Appel à Solutions est à la fois de sensibiliser aux risques cyber associés à un mauvais usage des smart contracts et de renforcer la connaissance et le développement de solution de protection à ces risques.

Cet Appel à Solutions est ouvert à tous candidats établis dans l'Union européenne ou dans un État membre de l'accord sur l'Espace économique européen.
Une seule participation par Candidat est autorisée pendant toute la durée de l'Appel à Solutions. Toute tentative de fraude de la part d'un participant pourra entraîner la nullité de toutes ses participations sur l'ensemble de l'Appel à Solutions.

2. Contexte de l'Appel à Solutions

Avec le développement exponentiel du numérique, la cyber sécurité représente un enjeu stratégique pour tous. L'introduction et l'utilisation de la blockchain représente un des leviers de sécurité car cette dernière répond aux quatre exigences principales de tout dispositif de sécurité :

1. La disponibilité est la propriété d'une information à être accessible et utilisable à la demande par une entité autorisée (ISO/IEC 27001:2018). Par leur décentralisation et distribution au sein d'un réseau, les blockchains ont cette faculté à être hautement disponibles.

2. L'intégrité est la propriété d'une information à être exacte et complète (ISO/IEC 27001:2018). Les blockchains garantissent l'intégrité de l'information qu'elles stockent par des mécanismes cryptographiques.

3. La confidentialité est la propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés (ISO/IEC 27001:2018). Les secrets liés à une Blockchain (clés privées des utilisateurs) sont uniquement stockés par les utilisateurs. La confidentialité est donc garantie par l'utilisateur lui-même.

4. La traçabilité est la capacité à identifier et dater les interactions avec l'information. Cette caractéristique est inhérente aux blockchains.

Paradoxalement, les smart contracts – des programmes autonomes déposés sur la blockchain, sont des cibles de choix pour les hackeurs car tout défaut ou faille dans la conception est difficilement voire non réparable une fois déposé sur la blockchain. Leurs failles peuvent alors être exploitées pour subtiliser des données, des tokens… Un tel scénario peut entraîner des pertes irréversibles.

Cet Appel à Solutions cible plus spécifiquement 4 axes complémentaires de réduction des risques :

- **DETECTER : la détection des vulnérabilités et/ou des menaces lors de la production ou de l'exécution du smart contract**
- **SUPERVISER : monitorer le déclenchement et l'activité des smart contracts**
- **PREVENIR : empêcher l'exécution de transactions malicieuses**
- **REMEDIER : protéger les systèmes et les actifs après la détection d'un incident.**

Avec cet Appel à Solutions, la Banque de France et le Campus Cyber souhaitent mieux comprendre l'écosystème cyber actuel et les solutions aujourd'hui disponibles sur le marché.

3. Catégorisation des dossiers

Cet Appel à Solutions s'adresse aux **Solutions « matures »** : c'est-à-dire aux candidats disposant d'une solution « prête pour la production » directement utilisable par un tiers, après un potentiel « paramétrage ».

Le candidat précisera dans sa candidature le ou les axes (Détecter, Superviser, Prévenir, Remédier) auxquels sa solution répond.

4. Modalités de l'Appel à Solutions

Les règles applicables à cet Appel à Solutions sont détaillées dans le Règlement de l'Appel à Solutions (« le Règlement ») annexé au présent document.

Conscients du faible nombre de solutions opérationnelles sur le marché, la Banque de France et le Campus Cyber souhaitent laisser la liberté aux candidats quant à la responsabilité des éléments qu'ils souhaitent mettre en avant. Au-delà de sa proposition de solution, **le candidat devra donc exposer, tout au long de sa réponse, les éléments de preuve permettant de valider la pertinence de sa démarche et les capacités de sa solution**.

Le dossier sera constitué, dans la mesure du possible, d'un seul livrable (document). Pour faciliter l'analyse des dossiers, il est conseillé aux candidats de proposer une réponse synthétique et concrète : présentation de la solution, ses fonctionnalités, son architecture technique, ses contraintes et limites.

Des questions pourront être adressées aux experts de la Banque de France et du Campus Cyber durant toute la phase de candidature jusqu'au 06/03/2024. Les réponses à ces questions seront partagées à l'ensemble des candidats.

Le Jury sera constitué des représentants Banque de France ainsi que des membres d'un des Groupe de Travail du Campus Cyber.

a. Critères d'éligibilité, de recevabilité et de sélection des candidatures

Sont éligibles les dossiers de candidatures qui remplissent l'ensemble des conditions suivantes, à savoir :

- Répondant explicitement à la question posée par l'Appel à Solutions ;
- Répondant aux exigences formulées dans le cahier des charges et cela tout au long des phases de l'appel à Solutions.
- Dans un format numérique classique, tel que doc, docx, pdf, ppt, odt, (en complément : mp3, mpeg, mov, mp4) sachant qu'aucun exécutable n'est autorisé dans le dossier ;
- Soumis par des candidats établis dans l'Union européenne ou dans un État membre de l'accord sur l'Espace économique européen ;

et, d'une manière générale, conformes aux conditions posées par le Règlement.

Parmi les candidatures éligibles, la sélection sera effectuée sur la base des critères de sélection listés ci-après :

- Pertinence du dossier : adéquation des éléments proposés au regard des attendus de l'Appel à Solutions
- Qualité du dossier : synthèse, mise en avant des éléments clés, analyse bénéfices / risques
- Capacité de la solution : fonctionnalités, maturité de la solution (ancienneté de la solution, nombre de clients à date, périmètres sur lesquels la solution est déployée etc) ;
- Performance de la solution : niveau de sécurité apporté et éléments de preuves associés.

Chaque critère de sélection sera noté de 1 à 5, 5 étant la meilleure note.

b. Finalité

La sélection des dossiers ne permet que de valoriser les meilleurs dossiers.

Les finalistes obtiendront une mise en relation avec des représentants du Campus Cyber afin de leur présenter leur solution, de bénéficier de visibilité et de rencontrer l'écosystème cyber.

c. Nombre de candidatures retenues

La Banque de France et le Campus Cyber sélectionnent parmi les candidatures éligibles un maximum de 5 dossiers. Un candidat ne peut soumettre qu'un seul dossier, mais chaque dossier peut comporter plusieurs propositions, que la Banque de France et le Campus Cyber peuvent sélectionner en tout ou en partie.

À l'issue de cette phase de pré-sélection sur dossiers, les candidats sélectionnés seront appelés à une étape d'approfondissement qui consistera en une présentation orale devant un jury de représentants de la Banque de France et du Campus Cyber. En cas de dossier retenu comportant plusieurs propositions, le candidat sera informé

à cette étape des propositions sélectionnées par la Banque de France et le Campus Cyber.

d. Encadrement de l'Appel à Solutions

1.a.1. Propriété intellectuelle

Les droits et obligations relatifs à la propriété intellectuelle sont précisés dans le Règlement.

1.a.2. Confidentialité

Les obligations de confidentialité applicables à chaque partie sont précisées dans le Règlement.

1.a.3. Droit applicable

Le présent Appel à Solutions est soumis au droit français.

5. Absence de rémunération

La Contribution à l'Appel à Solutions ne donne pas lieu à rémunération. Chaque partie prend à sa charge ses propres coûts liés à la participation et à la constitution du dossier.

6. Lieu d'exécution

L'Appel à Solutions sera exécuté sur la plateforme « innovation.banque-France.fr » et une restitution orale des candidats présélectionnés aura lieu dans les locaux de la Banque de France ou du Campus Cyber à Paris.

Les frais inhérents aux déplacements et aux séjours du candidat pour se rendre en région Ile de France, quelle que soit la localité de départ, sont toujours à sa charge.

En fonction de la localisation du candidat, la restitution orale pour les candidats présélectionnés pourra également être réalisée en visioconférence.

7. Calendrier prévisionnel

Date de publication de l'Appel à Solutions	05/02/24
Date limite de dépôt des candidatures (sous forme numérique)	06/03/24
Date de sélection des finalistes	13/03/24
Soutenances devant le Jury	14/03/24 au 19/03/24
Communication des résultats	à partir du 25/03/24